Hewlett Packard Enterprise

Hewlett Packard Enterprise

Hewlett Packard Enterprise OpenSSL 3 Provider
Software version: 3.1.4a

FIPS 140-3 Non-Proprietary Security Policy

Document version: 0.8

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This section describes:

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

This release supplement provides information regarding the Hewlett Packard Enterprise OpenSSL 3 Provider Module software version 3.1.4a FIPS 140-3 Level 1 validation from HPE Aruba Networking. HPE Aruba Networking is a Hewlett Packard Enterprise company. The material in this supplement modifies the general Hewlett Packard Enterprise software 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 OpenSSL 3 Provider Module software version 3.1.4a. 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 OpenSSL 3 Provider Module is referred to as the module, the cryptographic module, and HPE OpenSSL.

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://www.arubanetworks.com/open_source

Legal Notice
The use of HPE Aruba Networking 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, HPE Aruba Networking. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Acronyms and Abbreviations

AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security, a branch of CSE
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSE	Communications Security Establishment
CSP	Critical Security Parameter
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
PCT	Pairwise Consistency Test
PSP	Public Security Parameter
SHA	Secure Hash Algorithm
SSP	Sensitive Security Parameter

1.2 Security Levels

Section	Security Level
1	1
2	1
3	1
4	1
5	1
6	1
7	N/A
8	N/A
9	1
10	1
11	1
12	1

Table 1: Security Levels

1.3 Additional Information

More information is available from the following sources:

- See the Hewlett Packard Enterprise web site for the full line of products from HPE: https://www.hpe.com

- See the HPE Aruba Networking web site for the full line of products from HPE Aruba Networking: https://www.arubanetworks.com

- 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 or HPE Aruba Networking products.

  Select the Certificate Number for the Module Name ‘Hewlett Packard Enterprise OpenSSL 3 Provider Module’.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Hewlett Packard Enterprise OpenSSL 3 Provider Module (also referred to as ‘the module’) is a software type cryptographic module and was validated under FIPS 140-3 Level 1 requirements. The Hewlett Packard Enterprise OpenSSL 3 Provider Module is one of the components within a variety of Hewlett Packard Enterprise and HPE Aruba Networking products, including the Aruba Mobility Conductors, Mobility Controllers/Gateways, and controller-managed HPE Aruba Networking Access Points (APs) running the HPE ANW Wireless Operating System (AOS) operating system running on the HPE Aruba Networking hardware-based equipment or HPE Aruba Networking virtual appliances. The module provides cryptographic services for these products and is installed automatically as part of the product’s software package. For HPE Aruba Networking products, software is installed by HPE Aruba Networking technical support personnel or downloaded from the HPE Aruba Networking Support Portal (ASP) by authenticated licensed customer personnel.

Hewlett Packard Enterprise's development processes are such that future releases under Hewlett Packard Enterprise OpenSSL 3 Provider Module should be FIPS validate-able and meet the claims made in this document. Only the versions that explicitly appear on the certificate, however, are formally validated. Any version of 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. The CMVP makes no claim as to the correct operation of the module or the security strengths of the generated keys when operating under a version that is not listed on the validation certificate.

Module Type: Software

Module Embodiment: Multichip Standalone

Module Characteristics:

Cryptographic Boundary:

The Hewlett Packard Enterprise OpenSSL 3 Provider Module is comprised of a single component, which is a dynamically loadable OpenSSL 3 provider. The boundary of the module is defined as the shared library file, which on Unix/Linux is fips.so.

Tested Operational Environment’s Physical Perimeter (TOEPP):

The physical perimeter is the production grade enclosure of the hardware chassis of the HPE or HPE Aruba Networking hardware device or virtual appliance host.

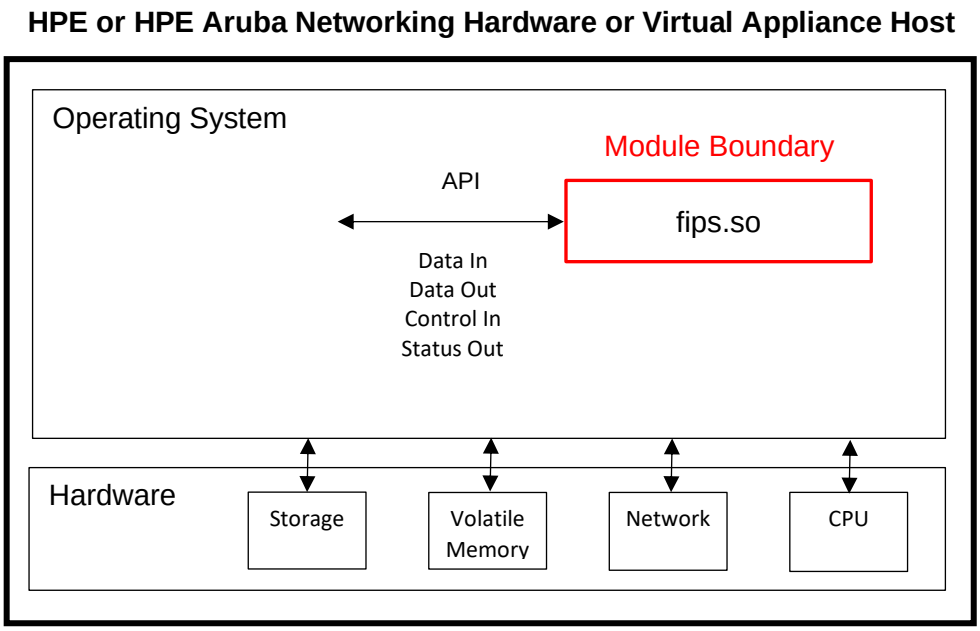

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
N/A	N/A	N/A	N/A	N/A

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Features	Integrity Test
fips.so	3.1.4a	FIPS provider for OpenSSL 3	HMAC-SHA2-256

Table 3: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
N/A	N/A	N/A	N/A	N/A

Table 4: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Ubuntu 22.04	HPE ProLiant ML 110 Gen10	Intel® Xeon® Silver 4110 (Skylake)	Yes	VMWare ESXi 6.7	3.1.4a
Ubuntu 22.04	HPE ProLiant ML 110 Gen10	Intel® Xeon® Silver 4110 (Skylake)	No	VMWare ESXi 6.7	3.1.4a

Table 5: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	6200F
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	6200M
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	6300
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	6300L
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	6400
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	8100
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	8320
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	8325
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	8325P
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	8360
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	8400
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	9300
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	9300S
HPE ANW CX Switch Operating System (AOS-CX) 10.16 or later	10000
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-XS
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-US
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-10104

Operating System	Hardware Platform
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-XS
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-XS (2020)
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-10106
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-10108
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-S
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-S-P
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-M
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-M-P
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-M-P
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-M-H
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-L, EC-L-NM
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-L-P, EC-L-P-NM
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-L-H
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-XL, EC-XL-NM
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-XL-P, EC-XL-P-NM (10G)
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-XL-P, EC-XL-P-NM (25G)
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-XL-H
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later	EC-V
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later running on VMware ESXi/ESX 6.7	EC-V
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later running on VMware ESXi/ESX 7.0	EC-V
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later running on Red Hat KVM 8.x	EC-V
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later running on KVM, QEMU 4.x	EC-V

Operating System	Hardware Platform
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later running on Microsoft Hyper V 10.0	EC-V
HPE ANW EdgeConnect Operating System (AOS-EC) 9.6 or later running on Citrix Xen Server 8.1.0	EC-V
HPE ANW Orchestrator 9.6 or later running on VMware ESXi/ESX 6.7	Orchestrator on-prem
HPE ANW Networking Orchestrator 9.6 or later running on VMware ESXi/ESX 7.0	Orchestrator on-prem
HPE ANW Networking Orchestrator 9.6 or later running on Red Hat KVM 8.x	Orchestrator on-prem
HPE ANW Networking Orchestrator 9.6 or later running on KVM, QEMU 4.x	Orchestrator on-prem
HPE ANW Networking Orchestrator 9.6 or later running on Microsoft Hyper V 10.0	Orchestrator on-prem
HPE ANW Networking Orchestrator 9.6 or later running on Citrix Xen Server 8.1.0	Orchestrator on-prem
HPE ANW Wireless Operating System (AOS) 8.13	AP-51x and AP-57x Wireless Access Points
HPE ANW Wireless Operating System (AOS) 8.13	AP-50x and AP-56x Wireless Access Points
HPE ANW Wireless Operating System (AOS) 8.13	AP-53x, AP-555, AP-58x, and AP-63x Wireless Access Points
HPE ANW Wireless Operating System (AOS) 8.13	AP-515 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 8.13	AP-535 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 8.13	AP-605 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 8.13	AP-610 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 8.13	AP-630 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 8.13	AP-635 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 8.13	AP-650 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 8.13	AP-655 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 8.13	AP-670 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 8.13	AP-730 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 8.13	AP-750 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 8.13	70xx Mobility Controllers

Operating System	Hardware Platform
HPE ANW Wireless Operating System (AOS) 8.13	72xx Mobility Controllers
HPE ANW Wireless Operating System (AOS) 8.13	7220 Mobility Controller
HPE ANW Wireless Operating System (AOS) 8.13	90xx Gateways
HPE ANW Wireless Operating System (AOS) 8.13	92xx Gateways
HPE ANW Wireless Operating System (AOS) 8.13	9012 Gateway
HPE ANW Wireless Operating System (AOS) 8.13	MCR-HW-5K Mobility Conductor Hardware Appliance
HPE ANW Wireless Operating System (AOS) 8.13 running on VMWare ESXi 7.0	MC-VA-50 Mobility Controller Virtual Appliance on HPE ProLiant ML110 Gen10
HPE ANW Wireless Operating System (AOS) 8.13	MCR-HW-xxx Mobility Conductor Hardware Appliances
HPE ANW Wireless Operating System (AOS) 8.13 running on VMWare ESXi 7.0	MC-VA-xxx Mobility Controller Virtual Appliances on HPE ProLiant ML110 Gen10
HPE ANW Wireless Operating System (AOS) 8.13 running on VMWare ESXi 7.0	MCR-VA-xxx Mobility Conductor Virtual Appliances on HPE ProLiant ML110 Gen10
HPE ANW Wireless Operating System (AOS) 8.13 running on VMWare ESXi 7.0	Virtual Appliances on HPE EdgeLine 20
HPE ANW Wireless Operating System (AOS) 8.13 running on VMWare ESXi 7.0	Virtual Appliances on PacStar PS451-1258 Series
HPE ANW Wireless Operating System (AOS) 8.13 running on VMWare ESXi 7.0	Virtual Appliances on device running an equivalent Intel processor (Intel Atom, i5, i7, or Xeon)
HPE ANW Wireless Operating System (AOS) 10.8	AP-51x and AP-57x Wireless Access Points
HPE ANW Wireless Operating System (AOS) 10.8	AP-50x and AP-56x Wireless Access Points
HPE ANW Wireless Operating System (AOS) 10.8	AP-53x, AP-555, AP-58x, and AP-63x Wireless Access Points
HPE ANW Wireless Operating System (AOS) 10.8	AP-515 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 10.8	AP-535 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 10.8	AP-605 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 10.8	AP-610 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 10.8	AP-630 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 10.8	AP-635 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 10.8	AP-650 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 10.8	AP-655 Wireless Access Point

Operating System	Hardware Platform
HPE ANW Wireless Operating System (AOS) 10.8	AP-670 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 10.8	AP-730 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 10.8	AP-750 Wireless Access Point
HPE ANW Wireless Operating System (AOS) 10.8	70xx Mobility Controllers
HPE ANW Wireless Operating System (AOS) 10.8	72xx Mobility Controllers
HPE ANW Wireless Operating System (AOS) 10.8	7220 Mobility Controller
HPE ANW Wireless Operating System (AOS) 10.8	90xx Gateways
HPE ANW Wireless Operating System (AOS) 10.8	92xx Gateways
HPE ANW Wireless Operating System (AOS) 10.8	9012 Gateway
HPE ANW Wireless Operating System (AOS) 10.8	MCR-HW-5K Mobility Conductor Hardware Appliance
HPE ANW Wireless Operating System (AOS) 10.8 running on VMWare ESXi 7.0	MC-VA-50 Mobility Controller Virtual Appliance on HPE ProLiant ML110 Gen10
HPE ANW Wireless Operating System (AOS) 10.8	MCR-HW-xxx Mobility Conductor Hardware Appliances
HPE ANW Wireless Operating System (AOS) 10.8 running on VMWare ESXi 7.0	MC-VA-xxx Mobility Controller Virtual Appliances on HPE ProLiant ML110 Gen10
HPE ANW Wireless Operating System (AOS) 10.8 running on VMWare ESXi 7.0	MCR-VA-xxx Mobility Conductor Virtual Appliances on HPE ProLiant ML110 Gen10
HPE ANW Wireless Operating System (AOS) 10.8 running on VMWare ESXi 7.0	Virtual Appliances on HPE EdgeLine 20
HPE ANW Wireless Operating System (AOS) 10.8 running on VMWare ESXi 7.0	Virtual Appliances on PacStar PS451-1258 Series
HPE ANW Wireless Operating System (AOS) 10.8 running on VMWare ESXi 7.0	Virtual Appliances on device running an equivalent Intel processor (Intel Atom, i5, i7, or Xeon)
HPE ANW Clearpass (CPPM) 6.14 or later	Unicom S1200-R4
HPE ANW Clearpass (CPPM) 6.14 or later	HPE ProLiant DL360
HPE ANW Clearpass (CPPM) 6.14 or later running on VMware ESXi up to 8.0	X86 Architecture
HPE ANW Clearpass (CPPM) 6.14 or later running on Microsoft Hyper-V 2016/2019 R2/2019	X86 Architecture
HPE ANW Clearpass (CPPM) 6.14 or later running on KVM on CentOS 7.7, Ubuntu 18.04, and Ubuntu 20.04	X86 Architecture
HPE ANW Clearpass (CPPM) 6.14 or later running on Amazon AWS (EC2)	X86 Architecture

Operating System	Hardware Platform
HPE ANW Clearpass (CPPM) 6.14 or later running on Amazon AWS (EC2)	X86 Architecture

Table 6: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

Not Applicable – There are no excluded components for the module.

2.4 Modes of Operation

Modes List and Description:

Name	Description	Type	Status Indicator
Approved Mode	When configured per the administrator guidance, the module only supports approved services.	Approved	Successful service completion.

Table 7: Modes List and Description

When configured per section 11.2 Administrator Guidance, the module only supports approved services in an approved manner.

Mode Change Instructions and Status:

Not Applicable – The module only supports a single approved mode of operation.

Degraded Mode Description:

Not Applicable – The module does not support a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size/Key Strength	Use/Function
A4803	AES-CBC	AES	128,192,256 bits	Data Encryption/ Decryption
A4803	AES-CCM	AES	128,192,256 bits	Data Encryption/ Decryption
A4803	AES-CFB128	AES	128,192,256 bits	Data Encryption/ Decryption

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size/Key Strength	Use/Function
A4803	AES-CFB8	AES	128,192,256 bits	Data Encryption/ Decryption
A4803	AES-CMAC	AES	128,192,256 bits	Message Authentication
A4803	AES-CTR	AES	128-256 bits	DRBG
A4803	AES-ECB	AES	128,192,256 bits	Data Encryption/ Decryption
A4803	AES-GCM	AES	128,192,256 bits	Data Encryption/ Decryption
A4803	AES-GMAC	AES	128,192,256 bits	Message Authentication
A4803	AES-KW	AES	128,192,256 bits	Key Transport
A4803	AES-KWP	AES	128,192,256 bits	Key Transport
A4803	AES-OFB	AES	128,192,256 bits	Data Encryption/ Decryption
A4803	AES-XTS Testing Revision 2.0	AES	128,256 bits	Data Encryption/ Decryption
A4803	Counter DRBG	Counter DRBG	128,192,256 bits	Generate random numbers with SP800-90A Rev 1
A4803	ECDSA KeyGen (FIPS186-4)	ECDSA KeyGen (FIPS186	≥ 112 bits	Generate an asymmetric keypair
A4803	ECDSA KeyVer (FIPS186-4)	ECDSA KeyVer (FIPS186	≥ 112 bits	Verify an asymmetric keypair parameters
A4803	ECDSA SigGen (FIPS186-4)	ECDSA SigGen (FIPS186	≥ 112 bits	Generate digital signatures
A4803	ECDSA SigVer (FIPS186-4)	ECDSA SigVer (FIPS186	≥ 112 bits	Verify digital signatures
A4803	HMAC-SHA2-224	HMAC	224 bits	Message Authentication
A4803	HMAC-SHA2-256	HMAC	256 bits	Message Authentication
A4803	HMAC-SHA2-384	HMAC	384 bits	Message Authentication
A4803	HMAC-SHA2-512	HMAC	512 bits	Message Authentication
A4803	HMAC-SHA3-224	HMAC	224 bits	Message Authentication
A4803	HMAC-SHA3-256	HMAC	256 bits	Message Authentication
A4803	HMAC-SHA3-384	HMAC	384 bits	Message Authentication

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size/Key Strength	Use/Function
A4803	HMAC-SHA3-512	HMAC	512 bits	Message Authentication
A4803	KAS-ECC CDH-Component SP800-56Ar3	KAS	112 to 256 bits	Shared Secret Computation
A4803	KAS-ECC-SSC Sp800-56Ar3	KAS	112 to 256 bits	Shared Secret Computation
A4803	KAS-FFC-SSC Sp800-56Ar3	KAS	112 to 200 bits	Shared Secret Computation
A4803	KDA HKDF SP800-56Cr2	KDA HKDF SP800	≥ 112 bits	Key Derivation Function
A4803	KDA OneStep SP800-56Cr2	KDA OneStep SP800	≥ 112 bits	Key Derivation Function
A4803	KDA TwoStep SP800-56Cr2	KDA TwoStep SP800	≥ 112 bits	Key Derivation Function
A4803	KDF KMAC Sp800-108r1	KDF KMAC Sp800	≥ 112 bits	Message Authentication
A4803	KDF SP800-108	KDF SP800	≥ 112 bits	Key Derivation
A4803	KDF SSH	KDF SSH	≥ 112 bits	Key Derivation Function
A4803	KMAC-128	KMAC	128 bits	Message Authentication
A4803	KMAC-256	KMAC	256 bits	Message Authentication
A4803	PBKDF	PBKDF	≥ 112 bits	Perform key derivation
A4803	RSA KeyGen (FIPS186-4)	RSA KeyGen (FIPS186	2048 bits	Generate RSA key pair
A4803	RSA SigGen (FIPS186-4)	RSA SigGen (FIPS186	128-256 bits	Generate RSA digital signatures
A4803	RSA SigVer (FIPS186-4)	RSA SigVer (FIPS186	128-256 bits	Verify RSA digital signatures
A4803	RSA Signature Primitive	RSA Signature Primitive	128-256 bits	Generate RSA digital signatures
A4803	SHA2-224	SHA2	224 bits	Message Digest
A4803	SHA2-256	SHA2	256 bits	Message Digest

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size/Key Strength	Use/Function
A4803	SHA2-384	SHA2	384 bits	Message Digest
A4803	SHA2-512	SHA2	512 bits	Message Digest
A4803	SHA3-224	SHA3	224 bits	Message Digest
A4803	SHA3-256	SHA3	256 bits	Message Digest
A4803	SHA3-384	SHA3	384 bits	Message Digest
A4803	SHA3-512	SHA3	512 bits	Message Digest
A4803	SHAKE-128	SHAKE	128 bits	Message Digest
A4803	SHAKE-256	SHAKE	256 bits	Message Digest
A4803	Safe Primes Key Generation	Safe Primes Key Generation	≥ 112 bits	Safe Primes Key Generation
A4803	Safe Primes Key Verification	Safe Primes Key Verification	≥ 112 bits	Safe Primes Key Verification
A4803	TLS v1.2 KDF RFC7627	TLS v1.2 KDF RFC7627	≥ 112 bits	Key Derivation Function
A4803	TLS v1.3 KDF	TLS v1.3 KDF	≥ 112 bits	Key Derivation Function

Table 8 Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Symmetric keys, seeds for asymmetric keys	-	SP 800-133r2 section 4

Table 9: Vendor-Affirmed Algorithms

The module does not implement any non-approved but allowed algorithms.

The module does not implement any non-approved but allowed algorithms with no security claimed.

The module does not implement any non-approved, not allowed algorithms.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Data Encryption, Decryption	AES	Encrypt or decrypt data	Provides 128 to 256 bits of strength	CBC, CFB128, CFB8, OFB, XTS, ECB, CTR, GCM, CCM, KW, KWP
Key Derivation Function	PBKDF, KBKDF, KDA, CVL	Perform key derivation using a key	Provides ≥ 112 bits	SSH, TLS v1.2 RFC 7627, TLS v1.3, PBKDF, KBKDF, KDA

Name	Type	Description	Properties	Algorithms
		derivation function		
Deterministic Random Bit Generation	DRBG	Generate random numbers with SP800-90A Rev 1	Provides 128 to 256 bits of strength	CTR DRBG
Digital Signature	RSA, ECDSA	Generate or verify RSA or ECDSA digital signatures	Provides 128 to 256 bits of strength	RSA Sig Gen, RSA Sig Ver, ECDSA Sig Gen, ECDSA Sig Ver
Message Authentication	AES, HMAC, KMAC	Generate or verify data integrity	Provides ≥ 112 bits	CMAC Gen, GMAC Gen, HMAC Gen, KMAC Gen
Shared Secret Computation	KAS-SSC-ECC	Perform key agreement primitives on behalf of the calling process (does not establish keys into the module)	Provides 112 to 256 bits of strength	KAS-ECC-SSC, KAS-ECC CDH-Component
Shared Secret Computation	KAS-SSC-FFC	Perform key agreement primitives on behalf of the calling process (does not establish keys into the module)	Provides 112 to 200 bits of strength	KAS-FFC-SSC
Key Generation	RSA, ECDSA, SafePrimes	Generate and verify an asymmetric keypair and DH parameters	Provides ≥ 112 bits	RSA Key Gen, ECDSA Key Gen, ECDSA Key Ver, Safe Prime Gen, Safe Prime Ver
Key Transport	KTS	AES	Provides 128 to 256 bits of strength	GCM, CCM, KW, KWP or AES CBC, CFB128, CFB8, OFB, ECB, CTR with HMAC or CMAC

Name	Type	Description	Properties	Algorithms
Message digest	SHS, SHA-3, SHAKE	Generate a message digest	Provides 112 to 256 bits of strength	SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE-128, SHAKE-256

Table 10: Security Function Implementations

2.7 Algorithm Specific Information

TLS and SSH
No parts of the TLS or SSH protocols, other than the KDF, have been reviewed or tested by the CAVP and CMVP.

AES GCM
The module supports AES-GCM in the context of TLS 1.2 and TLS 1.3. The module's implementation of AES-GCM is used together with an application that runs outside the module's cryptographic boundary. For TLS v1.2, the module's GCM implementation is compatible with RFC 5288 and the ciphersuites from section 3.3.1 of SP 800-52 rev 2. When the counter (nonce_explicit) part of the IV exhausts the maximum number of possible values for session key, the module will return an error, triggering a handshake to establish a new encryption key. For TLS v1.3, the module's GCM implementation is compatible with RFC 8446.

The module also supports randomly generated IVs. The IV is generated using the module's Approved DRBG and the minimum length of the IV is 96 bits.

If power on the host system is lost, the operator must reestablish new keys.

AES XTS
When XTS keys are loaded the module performs a key check per IG C.I to ensure that Key_1 ≠ Key_2.

PBKDF
The module's implementation of PBKDF,

- Uses option 1a from FIPS 140-3 IG D.N, for deriving a data protection key
- Requires passwords between 8 and 128 ASCII characters long. The likelihood of guessing this password at random is 1-in-6.1×10^{15}.
- Uses an iteration count of 1 to 10,000.

2.8 RBG and Entropy

The module receives entropy passively via a callback per IG 9.3.A scenario 2 (b). The caveat 'No assurance of the minimum strength of generated SSPs' applies. The callback must provide a minimum of 112 bits of entropy or return an error if this minimum cannot be met.

2.9 Key Generation

Name	Type	Properties
RSA Key	CKG	Key Type: Asymmetric FIPS 186-4 B.3.6
EC Key	CKG	Key Type: Asymmetric SP 800-56A rev 3 5.6.1.2.2, FIPS 186-4 B.4.2
FFC Key	CKG	Key Type: Asymmetric SP800-56A rev 3 5.6.1.1.4

Table 11: Key Generation

Key generation is provided as a service to the calling application. Generated keys are not used directly by the module.

2.10 Key Establishment

Name	Type	Properties
AEAD	KTS-Wrap	Cipher: AES-GCM, AES-CCM Key sizes: 128, 192, 256
Cipher CMAC	KTS-Wrap	Cipher: AES ECB, CBC, OFB, CFB 8, CFB 128, CTR Authentication: AES-CMAC Key sizes: 128, 192, 256
Cipher HMAC	KTS-Wrap	Cipher: AES ECB, CBC, OFB, CFB 8, CFB 128, CTR Authentication: HMAC with SHA2-224, 256, 384, 512, SHA3-224, 256, 384, 512 Key sizes: 128, 192, 256
KW/KWP	KTS-Wrap	Cipher Modes: KW, KWP Key sizes: 128, 192, 256
ECDH	KAS-ECC-SSC	Domain Parameter Generation Methods: P-224, P-256, P-384, P-521 Scheme: ephemeralUnified KAS Role: initiator, responder
DH	KAS-FFC-SSC	Domain Parameter Generation Methods: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 Scheme: dhEphem KAS Role: initiator, responder

Table 12: Key Establishment

The methods of key transport are approved per FIPS 140-3 IG D.G.

The methods of shared secret computation are approved per FIPS 140-3 IG D.F

Key transport and key agreement are provided as services to the calling application. Established keys are not used directly by the module.

2.11 Industry Protocols

The module implements the KDFs for TLS 1.2, TLS 1.3, and SSH, however does not implement these protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface	Data That Passes
N/A	Data Input	API input parameters for data
N/A	Data Output	API output parameters for data
N/A	Control Input	API function calls
N/A	Status Output	API return codes, status information, error codes

Table 13: Ports and Interfaces

As a software 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.

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.

Notes:

- The module does not implement a control output interface.
- As software, the module does not have a power interface.

3.2 Trusted Channel Specification

Not applicable – The module does not implement a trusted channel.

3.3 Control Interface Not Inhibited

Not applicable – The module does not implement a control interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The Hewlett Packard Enterprise OpenSSL 3 Provider Module does not provide any identification or authentication methods of its own.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	N/A - Authentication not required for Level 1
User	Role	User	N/A - Authentication not required for Level 1

Table 14: Roles

The module supports two distinct operator roles: the Crypto Officer (CO) 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.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	Roles	SSP Access
Initialize Module	The CO loads and initializes the module.	N/A	N/A	Status	None	CO	None
Data Encryption, Decryption	Encrypt or decrypt data	Successful completion	Parameters, plaintext or ciphertext, key	Status, ciphertext or plaintext	CBC, CFB128, CFB8, OFB, XTS, ECB, CTR, GCM, CCM, KW, KWP	User	AES Key: W, E
Key Derivation Function	Perform key derivation using a key derivation function	Successful completion	Parameters, key/password	Status, derived key	SSH, TLS v1.2 RFC 7627, TLS v1.3, PBKDF,	User	KDF Secret: W, E PBKDF Password: W, E

Name	Description	Indicator	Inputs	Outputs	Security Functions	Roles	SSP Access
					KBKDF, KDA		KBKDF Key: W, E Derived Key: G, R PBKDF Derived Key: G, R KBKDF Derived Key: G, R
Deterministic Random Bit Generation	Generate random numbers with SP800-90A Rev 1	Successful completion	N/A	Status, random number	DRBG	User	DRBG Entropy input: W DRBG Seed: G, E DRBG Key: G, E DRBG V: G, E
Digital Signature	Generate or verify RSA or ECDSA digital signatures	Successful completion	Parameters, RSA / ECDSA keys, message	Status, digital signature [1]	RSA, ECDSA	User	RSA Signature Public Key: W, E RSA Signature Private Key: W, E ECDSA Signature Public Key: W, E ECDSA Signature Private Key: W, E
Message Authentication	Generate or verify data integrity	Successful completion	Parameters, message, key	Status, message authentication code[2]	CMAC, GMAC, HMAC, KMAC	User	HMAC Key: W, E KMAC Key: W, E AES Key: W, E
Shared Secret Computation	Perform key agreement primitives on behalf of	Successful completion	Parameters, DH/EC	Status, shared secret	KAS-ECC-SSC,	User	DH Public Key: W, E DH Private Key: W, E

[1] Generate only

[2] Generate only

Name	Description	Indicator	Inputs	Outputs	Security Functions	Roles	SSP Access
	the calling process (does not establish keys into the module)		DH keys		KAS-FFC-SSC		EC DH Public Key: W, E EC DH Private Key: W, E EC DH Shared Secret: G, R DH Shared Secret: G, R
Key Generation	Generate and verify an asymmetric keypair and DH parameters	Successful completion	Parameters	Status, keypair	RSA, ECDSA, Safe Primes	User	DRBG Entropy input: W DRBG Seed: G, E DRBG Key: G, E DRBG V: G, E RSA Signature Public Key: G, R RSA Signature Private Key: G, R ECDSA Signature Public Key: G, R ECDSA Signature Private Key: G, R DH Public Key: G, R DH Private Key: G, R EC DH Public Key: G, R EC DH Private Key: G, R

Name	Description	Indicator	Inputs	Outputs	Security Functions	Roles	SSP Access
Key Wrapping/unwrapping	AES	Successful completion	Parameters, plaintext or ciphertext key, transport key(s)	Status, plaintext or ciphertext key	GCM, CCM, KW, KWP or AES CBC, CFB128, CFB8, OFB, ECB, CTR with HMAC or CMAC	User	Key Wrapping Key: W, E
Message digest	Generate a message digest	Successful completion	Parameters, Message	Status, Digest of the message	SHA-1, SHA2, SHA3	User	N/A
Zeroize	Zeroize all SSPs	N/A	None	Status	None	CO	All SSPs: Z
Show Status	Query the module for status	N/A	None	Status	None	CO	N/A
Show Version	Query the module for name and version information	N/A	None	Status, module version	None	CO	N/A
On demand self-test	Perform FIPS start-up tests on demand through the module's API or by rebooting the host platform.	N/A	None	Status	HMAC-SHA2-256	CO	N/A

Table 15: Approved Services

4.4 Non-Approved Services

Name	Description	Security Functions	Role
N/A	N/A	N/A	N/A

Table 16: Non-Approved Services

Not applicable – The module does not implement any non-approved services.

4.5 External Software/Firmware Loaded

Not applicable – The module does not implement software loading.

4.6 Bypass Actions and Status

Not applicable – The module does not implement bypass.

4.7 Cryptographic Output Actions and Status

Not applicable – The module does not implement self-initiated cryptographic output capability.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs a software integrity test when initialized. The test is performed by calculating the HMAC-SHA2-256 value of the module's shared library file and comparing it with the expected value in the module's configuration file. Prior to performing the integrity test, the module performs a HMAC-SHA2-256 KAT. If the integrity test fails, the module enters an error state where no cryptographic operations are possible.

5.2 Initiate on Demand

The software integrity test can be initiated on demand using the on demand self-test service.

5.3 Open-Source Parameters

The module is distributed in binary form.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

The module's operational environment is Linux, multi-threaded operating system that supports memory protection between processes. The operating control mechanisms protect against unauthorized execution, unauthorized modification, and unauthorized reading of SSPs, control and status data.

6.2 Configuration Settings and Restrictions

No specific configuration settings or restrictions are required.

7 Physical Security

Not applicable – The module is implemented exclusively in software.

8 Non-Invasive Security

Not Applicable – The module does not implement any non-invasive security mitigation techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Volatile Memory	All SSPs are stored in the volatile memory of the Operational Environment.	Dynamic

Table 17: Storage Areas

As specified in the Storage Areas table, the module does not persistently store any SSPs.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
API Entry	Calling application memory	Module memory	Plaintext	Manual	Electronic	N/A
API Output	Module memory	Calling application memory	Plaintext	Manual	Electronic	N/A

Table 18: SSP Input-Output Methods

As specified in the SSP Input-Output table, all SSPs are input and/or output via the module's API within the module's operational environment.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Reboot	All SSPs are zeroized by rebooting the host platform.	SSPs are only stored in volatile memory and so are zeroized by rebooting the host platform.	Rebooting the host platform must be performed under the control of the operator.

Table 19: SSP Zeroization Methods

As specified in the SSP Zeroization Methods table, all SSPs/Keys used in the module are zeroized by rebooting the host platform, indicated implicitly via the successful completion of the reboot. Rebooting the host platform must be performed under the control of the operator.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES Key	Key used for AES operations	128 to 256 bits	AES Key	External	N/A	AES
KDF Secret	Secret used for KDF operations	≥ 112 bits	KDF Secret	External or generated per KAS-SSC	N/A	SSH, TLS v1.2, TLS v1.3, KDA
Derived Key	Key resulting from the module's KDF	≥ 112 bits	Symmetric Key	KDF	N/A	AES
PBKDF Password	Password used for PBKDF operations	8-128	PBKDF Password	External	N/A	PBKDF
PBKDF Derived Key	Key resulting from the module's PBKDF	≥ 112 bits	Symmetric Key	KDF	N/A	AES
KBKDF Key	Key used for key based key derivation	112 to 256 bits	KDF Key	External	N/A	KBKDF
KBKDF Derived Key	Key resulting from the module's KBKDF	≥ 112 bits	Symmetric Key	KDF	N/A	AES
Entropy Input	Externally generated entropy used to seed the DRBG	128 to 256 bits	Entropy	External	N/A	DRBG
DRBG Seed	Internal state for DRBG	256 bits	DRBG Seed	Generated per SP800-90Ar2	N/A	DRBG
DRBG Key	Internal state for DRBG	256 bits	DRBG Internal State	Generated per SP800-90Ar2	N/A	DRBG
DRBG V	Internal state for DRBG	256 bits	DRBG Internal State	Generated per SP800-90Ar2	N/A	DRBG
RSA Signature Public Key	Key used for RSA Signature Verification	≥ 1024 bits Strength: 96 to 256 bits	RSA Signature Keypair	External or generated per FIPS 186-4	N/A	RSA

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RSA Signature Private Key	Key used for RSA Signature Generation	≥ 2048 bits Strength: 112 to 256 bits	RSA Signature Keypair	External or generated per FIPS 186-4	N/A	RSA
ECDSA Signature Public Key	Key used for ECDSA Signature Verification	192 to 521 bits Strength: 96 to 256 bits	ECDSA Signature Keypair	External or generated per FIPS 186-4	N/A	ECDSA
ECDSA Signature Private Key	Key used for ECDSA Signature Generation	224 to 521 bits Strength: 112 to 256 bits	ECDSA Signature Keypair	External or generated per FIPS 186-4	N/A	ECDSA
HMAC Key	Key used for HMAC Operations	≥ 112 bits	HMAC Key	External	N/A	HMAC
KMAC Key	Key used for KMAC Operations	≥ 112 bits	KMAC Key	External	N/A	KMAC
DH Public Key	DH Public Key	2048 – 8192 bits Strength: 112 to 200 bits	DH Keypair	External or generated per SP800-56A rev 3	N/A	KAS-FFC-SSC
DH Private Key	DH Private Key	2048 – 8192 bits Strength: 112 to 200 bits	DH Keypair	External or generated per SP800-56A rev 3	N/A	KAS-FFC-SSC
DH Shared Secret	DH Shared Secret	2048 – 8192 bits Strength: 112 to 200 bits	DH Shared Secret	N/A	Key agreement	SP800-56A rev 3
EC DH Public Key	EC DH Public Key	224 - 521 bits Strength: 112 to 256 bits	EC DH Keypair	External or generated per SP800-56A rev 3	N/A	KAS-ECC-SSC
EC DH Private Key	EC DH Private Key	224 - 521 bits Strength: 112 to 256 bits	EC DH Keypair	External or generated per SP800-56A rev 3	N/A	KAS-ECC-SSC
EC DH Shared Secret	EC DH Shared Secret	112 to 256 bits	EC DH Shared Secret	N/A	Key agreement	SP800-56A rev 3

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Key Wrapping Key	Key Wrapping Key	128 to 256 bits	Key Wrapping Key	External	N/A	KTS

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroisation	Related SSPs
AES Key	Input: Plaintext via API Output: N/A	Plaintext in volatile memory	Until zeroized	Reboot	N/A
KDF Secret	Input: Plaintext via API Output: N/A	Plaintext in volatile memory	Until zeroized	Reboot	Used to derive the Derived Key
Derived Key	Input: N/A Output: Plaintext via API	Plaintext in volatile memory	Until zeroized	Reboot	Derived from KDF Secret
PBKDF Password	Input: Plaintext via API Output: N/A	Plaintext in volatile memory	Until zeroized	Reboot	Used to derive the PBKDF Derived Key
PBKDF Derived Key	Input: N/A Output: Plaintext via API	Plaintext in volatile memory	Until zeroized	Reboot	Derived from PBKDF Password
KBKDF Key	Input: Plaintext via API Output: N/A	Plaintext in volatile memory	Until zeroized	Reboot	Used to derive KBKDF Derived Key
KBKDF Derived Key	Input: N/A Output: Plaintext	Plaintext in volatile memory	Until zeroized	Reboot	Derived from KBKDF Key
Entropy Input	N/A	Plaintext in volatile memory	Until zeroized	Reboot	N/A
DRBG Seed	N/A	Plaintext in volatile memory	Until zeroized	Reboot	Generated from the Entropy Input
DRBG Key	N/A	Plaintext in volatile memory	Until zeroized	Reboot	Generated from the DRBG Seed

Name	Input - Output	Storage	Storage Duration	Zeroisation	Related SSPs
DRBG V	N/A	Plaintext in volatile memory	Until zeroized	Reboot	Generated from the DRBG Seed
RSA Signature Public Key	Plaintext via API	Plaintext in volatile memory	Until zeroized	Reboot	Pair with RSA Signature Private Key
RSA Signature Private Key	Plaintext via API	Plaintext in volatile memory	Until zeroized	Reboot	Pair with RSA Signature Public Key
ECDSA Signature Public Key	Plaintext via API	Plaintext in volatile memory	Until zeroized	Reboot	Pair with ECDSA Signature Private Key
ECDSA Signature Private Key	Input: Plaintext via API Output: N/A	Plaintext in volatile memory	Until zeroized	Reboot	Pair with ECDSA Signature Public Key
HMAC Key	Input: Plaintext via API Output: N/A	Plaintext in volatile memory	Until zeroized	Reboot	N/A
KMAC Key	Input: Plaintext via API Output: N/A	Plaintext in volatile memory	Until zeroized	Reboot	N/A
DH Public Key	Plaintext via API	Plaintext in volatile memory	Until zeroized	Reboot	Pair to DH Private Key
DH Private Key	Plaintext via API	Plaintext in volatile memory	Until zeroized	Reboot	Pair to DH Public Key
DH Shared Secret	Input: N/A Output: Plaintext via API	Plaintext in volatile memory	Until zeroized	Reboot	DH Public Key and Private Key Can be used as the KDF Secret
EC DH Public Key	Plaintext via API	Plaintext in volatile memory	Until zeroized	Reboot	Pair to EC DH Private Key
EC DH Private Key	Plaintext via API	Plaintext in volatile memory	Until zeroized	Reboot	Pair to EC DH Public Key
EC DH Shared Secret	Input: N/A	Plaintext in volatile memory	Until zeroized	Reboot	EC DH Public Key and Private Key

Name	Input - Output	Storage	Storage Duration	Zeroisation	Related SSPs
	Output: Plaintext via API				Can be used as the KDF Secret
Key Wrapping Key	Input: Plaintext via API Output: N/A	Plaintext in volatile memory	Until zeroized	Reboot	N/A

Table 21: SSP Table 2

9.5 Transitions

No algorithm or security strength transitions are forecasted to occur over the lifetime of the validation.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 software Integrity Test	HMAC-SHA2-256 with a 256-bit key	KAT	Software Integrity	Successful initialization of the module	HMAC verification

Table 22: Pre-Operational Self-Tests

The module performs Pre-Operational Self-Tests (POSTs) at initialization. While the module is executing the pre-operational self-tests, services are not available, and so input and output are inhibited.

After the POST and CASTs are successfully concluded, the module automatically transitions to the operational state. If the POST fails, the module enters the Error state.

Self-test results can be obtained using the show status service.

10.2 Conditional Self-Tests

Algorithm	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC	HMAC-SHA2-256	KAT	CAST	Successful initialization of the module	HMAC verification	During module initialization prior to executing the integrity test
SHS		KAT	CAST	Successful initialization of the module	SHA-512	Module Initialization
SHA3		KAT	CAST	Successful initialization of the module	SHA3-256	Module Initialization
AES GCM	AES-GCM-256	KAT	CAST	Successful initialization of the module	Encrypt, Decrypt	Module Initialization

Algorithm	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES ECB	AES-ECB-128	KAT	CAST	Successful initialization of the module	Encrypt, Decrypt	Module Initialization
RSA	2048, SHA-256, PKCS#1-v1.5	KAT	CAST	Successful initialization of the module	Sign, Verify	Module Initialization
ECDSA	P-224	KAT	CAST	Successful initialization of the module	Sign, Verify	Module Initialization
TLS v1.3 KDF		KAT	CAST	Successful initialization of the module	TLS v1.3 KDF	Module Initialization
TLS v1.2 KDF		KAT	CAST	Successful initialization of the module	TLS 1.2 KDFs	Module Initialization
PBKDF2		KAT	CAST	Successful initialization of the module	Derivation of the Master Key	Module Initialization
KBKDF		KAT	CAST	Successful initialization of the module	Counter mode using HMAC-SHA-256	Module Initialization
KDA HKDF		KAT	CAST	Successful initialization of the module	One-Step and Two-Step	Module Initialization
KDA OneStep		KAT	CAST	Successful initialization of the module	One-Step and Two-Step	Module Initialization
DRBG	CTR_DRBG: AES 128-bit with DF	KAT	CAST	Successful initializati	Instantiate, Generate, Reseed	Module Initialization

Algorithm	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				on of the module		
KAS-FFC-SSC	p=2048, q=256	KAT	CAST	Successful initialization of the module	dhEphem	Module Initialization
KAS-ECC-SSC	P-256	KAT	CAST	Successful initialization of the module	Ephemeral Unified	Module Initialization
EC Keypair Generation	Keypair consistency test	PCT	PCT	Success or failure of service	Sign / Verify and SP 800-56Ar3 Assurances per Section 5.6.2	Keypair generation
RSA Keypair Generation	Keypair consistency test	PCT	PCT	Success or failure of service	Sign / Verify using PKCS#1-v1.5	Keypair generation
FFC Keypair Generation	Keypair consistency test	PCT	PCT	Success or failure of service	SP 800-56Ar3 Assurances per Section 5.6.2	Keypair generation
XTS Key Check	Check to confirm Key1 ≠ Key2	Key check	Critical Function	Success or failure of service	Per IG C.I	XTS key entry

Table 23: Conditional Self-Tests

All Cryptographic Algorithm Self-Tests (CASTs) are run at initialization along with the POST. This ensures they are run prior to the first operational use of the cryptographic algorithm.

As with the POST, once the CASTs are successfully concluded the module automatically transitions to the operational state. If a CAST fails, the module enters the Error state.

If a conditional PCT or key check test fails, the service returns an error.

10.3 Periodic Self-Test Information

Not applicable

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	The module's error state.	POST or CAST failure	Reload the module	Status return code

Table 24: Error States

The module has a single error state. While in this state, the module provides no cryptographic functionality and inhibits all data output.

10.5 Operator Initiation of Self-Tests

The module's POST and CASTs can be run anytime using the On-Demand Self-Test service by calling OSSL_PROVIDER_self_test(), or by reloading the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Hewlett Packard Enterprise OpenSSL 3 Provider Module is one of the components within Hewlett Packard Enterprise products. Full details about configuring Hewlett Packard Enterprise products can be found in the product documentation.

The module is initialized by loading the shared library and executing the Initialize Module service.

11.2 Administrator Guidance

Complete Crypto Officer documentation for the Hewlett Packard Enterprise OpenSSL 3 Provider is provided in the module's Administrator guidance documentation.

The module's Show Version service can be invoked by obtaining OSSL_PROV_PARAM_NAME and OSSL_PROV_PARAM_VERSION using OSSL_PROVIDER_get_params(). The module will return the following values:

	Parameter	**Value**
Name	OSSL_PROV_PARAM_NAME	Hewlett Packard Enterprise OpenSSL 3 Provider
Version	OSSL_PROV_PARAM_VERSION	3.1.4a

The module always operates in Approved mode. The Crypto Officer must ensure the following runtime checks, which are enabled by default, are not disabled in the configuration file or using any other method:

- security-checks
- tls1-prf-ems-check
- hpe-hmac-min-key-len

11.3 Non-Administrator Guidance

Complete User documentation for the Hewlett Packard Enterprise OpenSSL 3 Provider is provided in the module's Administrator guidance documentation.

Keys derived from passwords (using PBKDF) shall only be used for storage applications.

11.6 End of Life

Details about end-of-life procedures for Hewlett Packard Enterprise products can be found in the product documentation.

The module itself does not have any special end of life procedures. All SSPs can be zeroized by restarting the host platform.

12 Mitigation of Other Attacks

12.1 Attack List

The module mitigates against timing-based side-channel attacks using constant-time implementations and blinding.

12.2 Mitigation Effectiveness

Constant-time Implementations protect cryptographic implementations in the Module against timing analysis since such attacks exploit differences in execution time depending on the cryptographic operation, and constant-time implementations ensure that the variations in execution time cannot be traced back to the key, CSP or secret data.

Numeric Blinding protects the RSA and ECDSA algorithms from timing attacks. These algorithms are vulnerable to such attacks since attackers can measure the time of signature operations or RSA decryption. To mitigate this the Module generates a random blinding factor which is provided as an input to the decryption/signature operation and is discarded once the operation has completed and resulted in an output. This makes it difficult for attackers to attempt timing attacks on such operations without the knowledge of the blinding factor and therefore the execution time cannot be correlated to the RSA/ ECDSA key.

12.3 Guidance and Constraints

These mitigations are enabled by default.