Palo Alto Networks, Inc.

Palo Alto Networks SD-WAN ION Core Crypto Module

FIPS 140-3 Non-Proprietary Security Policy

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: June 18, 2026
Document Version: 1.1

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

The table below provides the security levels of the various sections of FIPS 140-3 in relation to the Palo Alto Networks SD-WAN ION Core Crypto Module with software version 1.0, hereinafter referred to as the Module.

1.2 Security Levels

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	N/A
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 Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Palo Alto Networks SD-WAN ION Core Crypto Module is utilized in hardware and software ION form factors. These enable the integration of a diverse set of wide area network (WAN) connection types, improve application performance and visibility, enhance security and compliance, and reduce the overall cost and complexity of a WAN.

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

Figure 1 below depicts the cryptographic boundary (yellow area with the blue dashed lines) and the physical perimeter (red dashed line). The cryptographic boundary includes all of the software components of the cryptographic libraries.

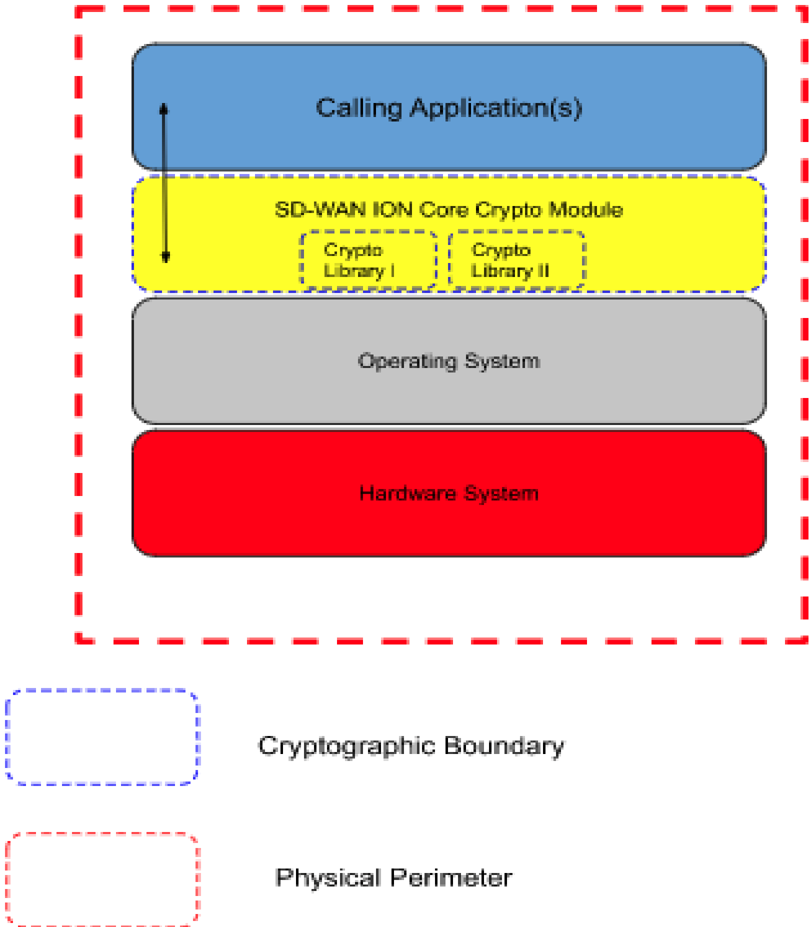

Figure 1– Cryptographic Boundary

Tested Operational Environment's Physical Perimeter (TOEPP):

The TOEPP is defined as the top, bottom, left, right, front, and back of the device on which the module runs detailed in section 2.2 below.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
SD-WAN ION Core Crypto Module	1.0		HMAC-SHA2-256 (Cert. #A3566)

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
ION 6.1	ION 1200	Intel Atom C3436L	Yes		1.0
ION 6.1	ION 1200	Intel Atom C3436L	No		1.0
ION 6.1	ION 1200-C-NA	Intel Atom C3436L	Yes		1.0
ION 6.1	ION 1200-C-NA	Intel Atom C3436L	No		1.0
ION 6.1	ION 1200-C-ROW	Intel Atom C3436L	Yes		1.0
ION 6.1	ION 1200-C-ROW	Intel Atom C3436L	No		1.0
ION 6.1	ION 1200-C-5G-WW	Intel Atom C3436L	Yes		1.0
ION 6.1	ION 1200-C-5G-WW	Intel Atom C3436L	No		1.0
ION 6.1	ION 1200-S	Intel Atom C3436L	Yes		1.0
ION 6.1	ION 1200-S	Intel Atom C3436L	No		1.0
ION 6.1	ION 1200-S-C-NA	Intel Atom C3436L	Yes		1.0
ION 6.1	ION 1200-S-C-NA	Intel Atom C3436L	No		1.0
ION 6.1	ION 1200-S-C-ROW	Intel Atom C3436L	Yes		1.0
ION 6.1	ION 1200-S-C-ROW	Intel Atom C3436L	No		1.0
ION 6.1	ION 1200-S-C-5G-WW	Intel Atom C3436L	Yes		1.0
ION 6.1	ION 1200-S-C-5G-WW	Intel Atom C3436L	No		1.0
ION 6.1	ION 3200	Intel Atom C3558R	Yes		1.0
ION 6.1	ION 3200	Intel Atom C3558R	No		1.0
ION 6.1	ION 5200	Intel Atom C5325	Yes		1.0
ION 6.1	ION 5200	Intel Atom C5325	No		1.0
ION 6.1	ION 9200	Intel Atom P5362	Yes		1.0
ION 6.1	ION 9200	Intel Atom P5362	No		1.0

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

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

Operating System	Hardware Platform
AWS	Dependent on Provider
Azure	Dependent on Provider
Google Cloud	Dependent on Provider
OCI	Dependent on Provider
ION 7108V	GPC
ION 3108V	GPC

Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The module has one approved mode of operation and is always in approved mode after initialization	Approved	Device Mode: "fips" output after following initialization steps in section 11.1

Table 5: Modes List and Description

The module has one approved mode of operation and is always in the approved mode of operation after initial operations are performed (See Section 11). The module does not claim implementation of a degraded mode of operation. Section 4 provides details on the service indicator implemented by the module.

2.5 Algorithms

Approved Algorithms:

Crypto Library - I

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3566	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A3566	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A3566	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-ECB	A3566	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A3566	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256	SP 800-38D
Counter DRBG	A3566	Prediction Resistance - No, Yes Supports Reseed - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - No, Yes Additional Input - Additional Input: 128, Additional Input: 256, Additional Input: 320, Additional Input: 384 Entropy Input - Entropy Input: 128, Entropy Input: 192,	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		Entropy Input: 256, Entropy Input: 320, Entropy Input: 384 Nonce - Nonce: 0, Nonce: 128, Nonce: 64 Personalization String Length - Personalization String Length: 128, Personalization String Length: 256, Personalization String Length: 320, Personalization String Length: 384 Returned Bits - 1152, 448, 768, 832, 896, 960	
ECDSA KeyGen (FIPS186-4)	A3566	Curve - P-256, P-384, P-521 Secret Generation Mode - Extra Bits, Testing Candidates	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3566	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3566	Component - No Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A3566	MAC - MAC: 80-160 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3566	MAC - MAC: 128-256 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3566	MAC - MAC: 192-384 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3566	MAC - MAC: 256-512 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3566	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A3566	Initiator Nonce Length - Initiator Nonce Length: 512 Responder Nonce Length - Responder Nonce Length: 512 Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 2048 Derived Keying Material Length - Derived Keying Material Length: 1056-3072 Increment 8 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF SNMP (CVL)	A3566	Password Length - Password Length: 64, 2048 Engine ID - 00100020003000400050, 12345678901234567890	SP 800-135 Rev. 1
KDF SSH (CVL)	A3566	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-512	SP 800-135 Rev. 1
KDF TLS (CVL)	A3566	TLS Version - v1.2 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A3566	Key Generation Mode - B.3.3 Modulo - 2048, 3072 Primality Tests - Table C.2 Info Generated By Server - No Public Exponent Mode - Random Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A3566	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
RSA SigVer (FIPS186-4)	A3566	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072	FIPS 186-4
SHA-1	A3566	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-256	A3566	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A3566	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-512	A3566	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4

Table 6: Approved Algorithms - Crypto Library - I

Crypto Library - II

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3572	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A3572	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96, 1024 Payload Length - Payload Length: 64-256 Increment 8 AAD Length - AAD Length: 0, 256	SP 800-38D
HMAC DRBG	A3572	Prediction Resistance - Yes Supports Reseed - No Mode - SHA2-512 Entropy Input - Entropy Input: 256 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 256 Additional Input - Additional Input: 256 Returned Bits - 896	SP 800-90A Rev. 1
HMAC-SHA2-256	A3572	MAC - MAC: 128-256 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3572	MAC - MAC: 192-384 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3572	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF TLS (CVL)	A3572	TLS Version - v1.2 Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1
RSA SigVer (FIPS186-4)	A3572	Signature Type - PKCS 1.5 Modulo - 2048	FIPS 186-4
SHA2-256	A3572	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A3572	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4

Table 7: Approved Algorithms - Crypto Library - II

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-512	A3572	MAC - MAC: 256-512 Increment 8 Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
SHA2-512	A3572	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4

Table 8: Approved Algorithms -

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG from CTR DRBG	Key Type:Asymmetric	N/A	SP 800-133r2 Section 4, example 1
CKG from HMAC DRBG	Key Type:Asymmetric	N/A	SP 800-133r2 Section 4, example 1

Table 9: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KAS-ECC-KeyGen (SSHv2)	CKG KAS-KeyGen	KAS-ECC KeyGen used in SSHv2 service	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	CKG from CTR DRBG: () Counter DRBG: (A3566)
KAS-ECC-KeyGen (TLSv1.2)	CKG KAS-KeyGen	KAS-ECC KeyGen used in TLSv1.2 service	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	CKG from CTR DRBG: () CKG from HMAC DRBG: () Counter DRBG: (A3566) HMAC DRBG: (A3572)

Name	Type	Description	Properties	Algorithms
KAS-ECC-KeyGen (IPSec/IKEv2)	CKG KAS-KeyGen	KAS-ECC KeyGen used in IPSec/IKEv2 service	Bit-strength Caveat:Provides between 128 and 192 bits of encryption strength	CKG from CTR DRBG: () Counter DRBG: (A3566)
KAS-ECC (SSHv2)	KAS-Full	KAS-ECC for SSHv2 service	IG:IG D.F Scenario 2, path(2), split Key confirmation:no Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A3566) KDF SSH: (A3566)
KAS-ECC (TLSv1.2)	KAS-Full	KAS-ECC for TLSv1.2 service	IG:IG D.F Scenario 2, path (2), split Key confirmation:no Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A3566, A3572) KDF TLS: (A3566, A3572)
KAS-ECC (IPSec/IKEv2)	KAS-Full	KAS-ECC for IPSec/IKEv2 service	IG:IG D.F Scenario 2, path (2), split Key confirmation:no Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment methodology provides between 128 and 192 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A3566) Domain Parameter Generation Methods: P-256, P-384 KDF IKEv2: (A3566)
KTS (TLSv1.2 with AES and HMAC)	KTS-Unwrap	KTS via TLSv1.2 service by using AES and HMAC	Standard:SP 800-38F IG	AES-CBC: (A3566) Key Length: 128,

Name	Type	Description	Properties	Algorithms
			D.G:"Combination" method - approved symmetric encryption method together with an approved authentication method Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	256 AES-CBC: (A3572) HMAC-SHA2-256: (A3566, A3572) HMAC-SHA2-384: (A3566, A3572) SHA2-256: (A3566, A3572) SHA2-384: (A3566, A3572)
KTS (TLSv1.2 with AES-GCM)	KTS-Unwrap	KTS via TLSv1.2 service by using AES-GCM	Standard:SP 800-38F IG D.G:approved authenticated symmetric encryption mode Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-GCM: (A3566, A3572)
ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for SSHv2 service		ECDSA KeyGen (FIPS186-4): (A3566) Counter DRBG: (A3566) CKG from CTR DRBG: ()
ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for SSHv2 service		ECDSA SigGen (FIPS186-4): (A3566)
ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for SSHv2 service		ECDSA SigVer (FIPS186-4): (A3566)
RSA KeyGen	AsymKeyPair-KeyGen CKG	RSA KeyGen for TLSv1.2 and IPSec/IKEv2 services		RSA KeyGen (FIPS186-4): (A3566) Counter DRBG: (A3566) CKG from CTR DRBG: ()
RSA SigGen	DigSig-SigGen	RSA SigGen for TLSv1.2 and IPSec/IKEv2 services		RSA SigGen (FIPS186-4): (A3566)

Name	Type	Description	Properties	Algorithms
RSA SigVer (TLSv1.2)	DigSig-SigVer	RSA SigVer for TLSv1.2 service		RSA SigVer (FIPS186-4): (A3566, A3572)
RSA SigVer (IPSec/IKEv2)	DigSig-SigVer	RSA SigVer for IPSec/IKEv2 service		RSA SigVer (FIPS186-4): (A3566)
Block Cipher (SSHv2)	BC-UnAuth	Block Cipher for SSHv2 Service		AES-CTR: (A3566)
Block Cipher (TLSv1.2)	BC-Auth BC-UnAuth	Block Cipher for TLSv1.2 Service		AES-CBC: (A3566) Key Length: 128, 256 AES-GCM: (A3566, A3572) AES-ECB: (A3566) AES-CBC: (A3572)
Block Cipher (IPSec/IKEv2)	BC-UnAuth	Block Cipher for IPSec/IKEv2 Service		AES-CBC: (A3566)
Block Cipher (SNMPv3)	BC-UnAuth	Block Cipher for SNMPv3 Service		AES-CFB128: (A3566)
MAC (SSHv2)	MAC	MAC for SSHv2 Service		HMAC-SHA-1: (A3566) HMAC-SHA2-256: (A3566) HMAC-SHA2-512: (A3566) SHA-1: (A3566) SHA2-256: (A3566) SHA2-512: (A3566)
MAC (TLSv1.2)	MAC	MAC for TLSv1.2 Service		HMAC-SHA2-256: (A3566, A3572) HMAC-SHA2-384: (A3566, A3572) SHA2-256: (A3566, A3572) SHA2-384: (A3566, A3572)
MAC (IPSec/IKEv2)	MAC	MAC for IPSec/IKEv2 Service		HMAC-SHA-1: (A3566) HMAC-SHA2-256: (A3566) HMAC-SHA2-384: (A3566) HMAC-SHA2-512: (A3566) SHA-1: (A3566) SHA2-256: (A3566)

Name	Type	Description	Properties	Algorithms
				SHA2-384: (A3566) SHA2-512: (A3566)
MAC (SNMPv3)	MAC	MAC for SNMPv3 Service		HMAC-SHA-1: (A3566) SHA-1: (A3566)
SSHv2 Keying Materials Development	KAS-135KDF	SSHv2 session keying materials, used to derive SSHv2 session keys		KDF SSH: (A3566)
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLSv1.2 session keys		KDF TLS: (A3566, A3572)
IPSec/IKEv2 Keying Materials Development	KAS-135KDF	IPSec/IKEv2 session keying materials, used to derive IPSec/IKEv2 session keys		KDF IKEv2: (A3566)
SNMPv3 Keying Materials Development	KAS-135KDF	SNMPv3 session keying materials, used to derive SNMPv3 session keys		KDF SNMP: (A3566)
DRBG Function	DRBG	Used for DRBG generation		Counter DRBG: (A3566) HMAC DRBG: (A3572) HMAC-SHA2-512: (A3572) SHA2-512: (A3572)

Table 10: Security Function Implementations

2.7 Algorithm Specific Information

As the module can only be operated in the Approved mode of operation, any algorithms not listed above will be rejected by the module while in the approved mode.

AES-GCM

- The module's AES-GCM implementation conforms to FIPS 140-3 IG C.H scenario #1 following RFC 5288 for TLS. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP800-52 Rev1, Section 3.3.1. The operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the module being validated. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. The keys for the client and server negotiated in the TLSv1.2 handshake process (client_write_key and server_write_key) are compared and the module aborts the session if the key values are identical. 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.

FIPS 186-4/186-5

- The module was algorithm tested based on the FIPS 186-4 standard for Digital Signatures prior to Feb 5, 2024. According to IG C.K, this module is 186-5 compliant as all 186-4 CAVP tests performed are mathematically identical to the 186-5 CAVP tests. The Module does not support 186-4 DSA or RSA X9.31 for Signature Generation or Signature Verification.

2.8 RBG and Entropy

Cert Number	Vendor Name
E68	Palo Alto Networks, Inc.
E71	Palo Alto Networks, Inc.

Table 11: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Palo Alto Networks DRNG Entropy Source - Denverton 16 Core Die with FCBGA1310 Package	Physical	Intel Corporation Intel(R) Atom(R) Denverton-16 FCBGA1310 Intel(R) Atom(R) C3958 Processor	128 bits	Full Entropy	A2153 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Snow Ridge 24-Core Die with FCBGA2106 Package	Physical	Intel Corporation Intel(R) Atom(R) Snow Ridge-24 FCBGA2106 Intel(R) Atom(R) P5322 Processor	128 bits	Full Entropy	A2541 (AES-CBC-MAC)

Table 12: Entropy Sources

The operational environment is detailed in the Public Use Document for Entropy Certificate E68 and E71.

The module implements two approved DRBGs based on SP800-90Arev1, including CTR_DRBG with Algo Cert. #A3566, and HMAC_DRBG with Algo Cert. #A3572. Those two DRBGs are used internally by the module (e.g. to generate symmetric keys, seeds for asymmetric key pairs, and random numbers for security functions).

Each DRBG is seeded by the entropy source described in the table above. The module implements CTR_DRBG (AES-128/192/256) both with and without Derivation Function capability. Given that the module's entropy source provides full entropy, CTR_DRBG without a derivation function is compliant with IG D.L. The module also implements HMAC_DRBG (SHA2-512) with Prediction Resistance. Each DRBG is instantiated with a 384-bits long entropy input (corresponding to 384 bits of entropy) and provides at least 256 bits security strength for the cryptographic key generation while in the approved mode.

Note:

- ESV Cert. #E68 is for ION-1200, ION 1200-C-NA, ION 1200-C-ROW, ION 1200-C-5G-WW, ION 1200-S, ION 1200-S-C-NA, ION 1200-S-C-ROW, ION 1200-S-C-5G-WW and ION 3200
- ESV Cert. #E71 is for ION 5200 and ION 9200

2.9 Key Generation

The module generates RSA, ECDSA, and ECDH asymmetric key pairs compliant with FIPS 186-4, using a NIST SP 800-90Ar1 CTR DRBG or HMAC DRBG for random number generation. In accordance with FIPS 140-3 IG D.H, the cryptographic module performs CKG for asymmetric keys as per section 5.1 of NIST SP 800-133rev2 (vendor affirmed) by obtaining a random bit string directly from an approved DRBG. The random bit string supports the required security strength requested by the calling application (without any V, as described in Additional Comments 2 of IG D.H.).

2.10 Key Establishment

The module provides the following key/SSP establishment services in the approved mode of operation:

- KAS-ECC Shared Secret Computation:
    - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength.

2.11 Industry Protocols

The module supports SSHv2, TLS v1.2, SNMPv3 and IPsec/IKEv2 industrial protocols. Please refer to the Security Function Implementations Table for more information. No parts of the SSH, TLS, SNMP and IPSec/IKE protocols, other than the KDFs, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	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

Physical Port	Logical Interface(s)	Data That Passes
N/A	Control Output	N/A
N/A	Status Output	Return values and/or log messages

Table 13: Ports and Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Table 2. The module provides its logical interfaces via Application Programming Interface (API) calls. The logical interfaces provided by the module are mapped onto the FIPS 140-3 interfaces (data input, data output, control input, control output and status output) as above.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The module supports implicit role-based operation, and provides only a Crypto Officer role. The Crypto Officer role has the ability to perform all tasks and administrative actions. The module does not support concurrent operators.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 14: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Self-Test	Initiate and run the pre-operational self-tests	None	Command to trigger self-test	Status of the self-test results	None	Crypto Officer Unauthenticated
Zeroization	Zeroize all unprotected SSPs stored in the module	None	Command to initiate the SSPs zeroization	Status of the SSPs zeroization	None	Crypto Officer - CTR DRBG Entropy Input: Z - CTR DRBG Seed: Z - CTR DRBG Internal State (V, Key): Z - HMAC DRBG Entropy Input: Z - HMAC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DRBG Seed: Z - HMAC DRBG Internal State (V, Key): Z - TLS RSA Private Key: Z - TLS RSA Public Key: Z - TLS ECDHE Private Key: Z - TLS ECDHE Public Key: Z - Peer TLS ECDHE Public Key: Z - TLS ECDHE Shared Secret: Z - TLS Master Secret: Z - TLS Session Encryption Key: Z - TLS Session Authentication Key: Z - IPSec/IKEv2 Pre-Shared Secret: Z - IPSec/IKEv2 RSA Private Key: Z - IPSec/IKEv2 RSA Public Key: Z - IPSec/IKEv2 ECDHE Private Key: Z - IPSec/IKEv2 ECDHE Public Key: Z - Peer IPSec/IKEv2 ECDHE Public Key: Z - IPSec/IKEv2 ECDHE Shared Secret: Z - SKEYSEED: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- IPSec/IKEv2 Session Encryption Key: Z - IPSec/IKEv2 Session Authentication Key: Z - SNMPv3 Authentication Secret: Z - SNMPv3 Session Encryption Key: Z - SNMPv3 Session Authentication Key: Z - SSH ECDHE Private Key: Z - SSH ECDHE Public Key: Z - Peer SSH ECDHE Public Key: Z - SSH ECDHE Shared Secret: Z - SSH ECDSA Private Key: Z - SSH ECDSA Public Key: Z - SSH Session Encryption Key: Z - SSH Session Authentication Key: Z
Show Version	Provides the module's name/ID and versions	None	Command to show version	Module's name/ID and versions	None	Crypto Officer
Show Status	Provides the module's current status and information	None	Command to show status	Module's status information	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Configure Network	Perform the module's network configuration	Global indicator and configuration logs	Commands to configure the module	Status of the completion of network related configuration	None	Crypto Officer
Configure SSHv2 Function	Create a secure SSHv2 channel	Global indicator and SSH connection log message	Commands to configure SSHv2	Status of the completion of SSHv2 configuration	ECDSA KeyGen DRBG Function	Crypto Officer - SSH ECDSA Private Key: G,W - SSH ECDSA Public Key: G,W - CTR DRBG Entropy Input: E - CTR DRBG Seed: E - CTR DRBG Internal State (V, Key): E
Run SSHv2 Function	Negotiation and encrypted data transport via SSH	Global indicator and SSH connection log message	Initiate SSHv2 tunnel establishment request	Status of SSHv2 tunnel establishment	KAS-ECC-KeyGen (SSHv2) KAS-ECC (SSHv2) ECDSA SigGen ECDSA SigVer Block Cipher (SSHv2) MAC (SSHv2) DRBG Function SSHv2 Keying Materials Development	Crypto Officer - SSH ECDHE Private Key: G,W,E - SSH ECDHE Public Key: G,R,W - Peer SSH ECDHE Public Key: W,E - SSH ECDHE Shared Secret: G,W,E - SSH ECDSA Private Key: E - SSH ECDSA Public Key: R - SSH Session Encryption Key: G,W,E - SSH Session Authentication Key: G,W,E - CTR DRBG Entropy Input: E - CTR DRBG Seed: E - CTR DRBG Internal State (V, Key): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Configure TLSv1.2 Function	Create a secure TLSv1.2 channel	Global Indicator and TLS success log message	Commands to configure TLSv1.2	Status of the completion of TLSv1.2 configuration	RSA KeyGen DRBG Function	Crypto Officer - TLS RSA Private Key: G,W - TLS RSA Public Key: G,W - CTR DRBG Entropy Input: E - CTR DRBG Seed: E - CTR DRBG Internal State (V, Key): E
Run TLSv1.2 Function	Negotiation and encrypted data transport via TLS	Global indicator and TLS success log message	Initiate TLSv1.2 tunnel establishment request	Status of TLSv1.2 tunnel establishment	KAS-ECC-KeyGen (TLSv1.2) KAS-ECC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) RSA SigGen RSA SigVer (TLSv1.2) Block Cipher (TLSv1.2) MAC (TLSv1.2) DRBG Function TLSv1.2 Keying Materials Development	Crypto Officer - TLS RSA Private Key: E - TLS RSA Public Key: R - TLS ECDHE Private Key: G,W,E - TLS ECDHE Public Key: G,R,W - Peer TLS ECDHE Public Key: W,E - TLS ECDHE Shared Secret: G,W,E - TLS Master Secret: G,W,E - TLS Session Encryption Key: G,W,E - TLS Session Authentication Key: G,W,E - CTR DRBG Entropy Input: E - CTR DRBG Seed: E - CTR DRBG Internal State (V, Key): E - HMAC DRBG Entropy Input: E - HMAC DRBG Seed:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						E - HMAC DRBG Internal State (V, Key): E
Configure SNMPv3 Function	Create a secure SNMPv3 channel	Global indicator and SNMPv3 success log message	Commands to configure SNMPv3	Status of the completion of SNMPv3 configuration	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM)	Crypto Officer - SNMPv3 Authentication Secret: W
Run SNMPv3 Function	Negotiation and encrypted data transport via SNMPv3	Global indicator and SNMPv3 success log message	Initiate SNMPv3 tunnel establishment request	Status of SNMPv3 tunnel establishment	Block Cipher (SNMPv3) MAC (SNMPv3) SNMPv3 Keying Materials Development	Crypto Officer - SNMPv3 Authentication Secret: E - SNMPv3 Session Encryption Key: G,W,E - SNMPv3 Session Authentication Key: G,W,E
Configure IPSec/IKEv2 Function	Create IPSec/IKEv2 tunnel	Global indicator and IPSec/IKEv2 success log message	Commands to configure IPSec/IKEv2	Status of the completion of IPSec/IKEv2 configuration	KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) RSA KeyGen DRBG Function	Crypto Officer - IPSec/IKEv2 Pre-Shared Secret: W - IPSec/IKEv2 RSA Private Key: G,W - IPSec/IKEv2 RSA Public Key: G,W - CTR DRBG Entropy Input: E - CTR DRBG Seed: E - CTR DRBG Internal State (V, Key): E
Run IPSec/IKEv2 Function	Negotiation and encrypted data transport via IPSec/IKEv2	Global indicator and IPSec/IKEv2 success log message	Initiate IPSec/IKEv2 tunnel establishment request	Status of IPSec/IKEv2 tunnel establishment	KAS-ECC-KeyGen (IPSec/IKEv2) KAS-ECC (IPSec/IKEv2) RSA SigGen RSA SigVer (IPSec/IKEv	Crypto Officer - IPSec/IKEv2 Pre-Shared Secret: E - IPSec/IKEv2 RSA Private Key: E - IPSec/IKEv2 RSA Public Key: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					2) Block Cipher (IPSec/IKEv2) MAC (IPSec/IKEv2) DRBG Function IPSec/IKEv2 Keying Materials Development	- IPSec/IKEv2 ECDHE Private Key: G,W,E - IPSec/IKEv2 ECDHE Public Key: G,R,W - Peer IPSec/IKEv2 ECDHE Public Key: W,E - IPSec/IKEv2 ECDHE Shared Secret: G,W,E - SKEYSEED: G,W,E - IPSec/IKEv2 Session Encryption Key: G,W,E - IPSec/IKEv2 Session Authentication Key: G,W,E - CTR DRBG Entropy Input: E - CTR DRBG Seed: E - CTR DRBG Internal State (V, Key): E

Table 15: Approved Services

G = Generate: The module generates or derives the SSP.
R = Read: The SSP is read from the module (e.g. the SSP is output).
W = Write: The SSP is updated, imported, or written to the module.
E = Execute: The module uses the SSP in performing a cryptographic operation.
Z = Zeroise: The module zeroises the SSP.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

N/A for this module.

4.6 Cryptographic Output Actions and Status

The module implements Self-initiated cryptographic output capability without external operator request. The Crypto Officer shall configure self-initiated cryptographic output capability. Prior to executing the self-initiated cryptographic output capability, the module conducts two independent internal actions to activate the capability to prevent the inadvertent output due to a single error.

4.7 Additional Information

The module supports Unauthenticated service, where the unauthenticated users can run the self-test service by power-cycling the module.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs the Software Integrity test by using HMAC-SHA2-256 (HMAC Cert. #A3566) during the Pre-Operational Self-Test. A Software Integrity Test Key (non-SSP) was preloaded to the module's binary at the factory and used for software integrity test only at the pre-operational self-test. At Module's initialization, the integrity of the runtime executable is verified using an HMAC-SHA2-256 digest which is compared to a value computed at build time. If at the load time the MAC does not match the stored, known MAC value, the module would enter an Error state with all crypto functionality inhibited.

5.2 Initiate on Demand

Integrity test is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on. The operator can power-cycle or reboot the module to initiate the software integrity test on-demand. This automatically performs the integrity test of all software components included within the boundary of the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

7 Physical Security

As the module is a software only module, the physical security requirements are not applicable.

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DRAM within TOEPP	Volatile Memory	Dynamic
HDD within TOEPP	Non-Volatile Memory	Static

Table 16: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Peer Public Key Input	External (Outside of the module's boundary)	HDD within TOEPP	Plaintext	Automated	Electronic	
Module Public Key Output	HDD within TOEPP	External (Outside of the module's boundary)	Plaintext	Automated	Electronic	
Password/Secret Input via TLSv1.2 decrypted by AES and HMAC	External (Outside of the module's boundary)	HDD within TOEPP	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES and HMAC)
Password/Secret Input via TLSv1.2 decrypted by AES-GCM	External (Outside of the module's boundary)	HDD within TOEPP	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES-GCM)

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization Command	CO issues zeroization service	The zeroization command will erase all SSPs stored in the RAM or in the HDD within the TOEPP.	"Disable System" command
Session Termination	Zeroization upon session termination	Session termination will automatically zeroize all session based temporary SSPs	Terminate session

Zeroization Method	Description	Rationale	Operator Initiation
Power Down	Operator powers the module off	Powering off the module will erase all SSPs stored in the RAM within the TOEPP.	"Debug reboot" command or unplugging the module

Table 18: SSP Zeroization Methods

Notes:

1. To initiate zeroization, see Section End of Life / Sanitization in this document for more details.
2. The zeroization operations shall be performed under the control of the CO role.
3. The zeroized SSPs cannot be retrieved or reused. Once the command is initiated, the SSPs are overwritten with 0s.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CTR DRBG Entropy Input	Used to seed the CTR DRBG	256 - 256 bits	Entropy Input - CSP			DRBG Function
CTR DRBG Seed	Used in CTR DRBG Generation	256 - 256 bits	DRBG Seed - CSP			DRBG Function
CTR DRBG Internal State (V, Key)	Used in CTR DRBG Generation	256 - 256 bits	DRBG Internal State - CSP			DRBG Function
HMAC DRBG Entropy Input	Used to seed the HMAC DRBG	256 - 256 bits	Entropy Input - CSP			DRBG Function
HMAC DRBG Seed	Used in HMAC DRBG Generation	256 - 256 bits	DRBG Seed - CSP			DRBG Function
HMAC DRBG Internal State (V, Key)	Used in HMAC DRBG Generation	256 - 256 bits	DRBG Internal State - CSP			DRBG Function
TLS RSA Private Key	Used for TLS peer authenticatio n	2048, 3072 bits - 112, 128 bits	Private Key - CSP	RSA KeyGen		RSA SigGen
TLS RSA Public Key	Used for TLS peer authenticatio n	2048, 3072 bits - 112, 128 bits	Public Key - PSP		RSA KeyGen	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS ECDHE Private Key	Used to derive TLS ECDHE Shared Secret	P-256, P-384, P-521 - 128, 192, 256 bits	Private Key - CSP	KAS-ECC-KeyGen (TLSv1.2)		KAS-ECC (TLSv1.2)
TLS ECDHE Public Key	Used to derive TLS ECDHE Shared Secret	P-256, P-384, P-521 - 128, 192, 256 bits	Public Key - PSP		KAS-ECC-KeyGen (TLSv1.2)	
Peer TLS ECDHE Public Key	Used to derive TLS ECDHE shared secret	P-256, P-384, P-521 - 128, 192, 256 bits	Public Key - PSP			KAS-ECC (TLSv1.2)
TLS ECDHE Shared Secret	Used to derive TLS Master Secret	P-256, P-384, P-521 - 128, 192, 256 bits	Shared Secret - CSP		KAS-ECC (TLSv1.2)	TLSv1.2 Keying Materials Development
TLS Master Secret	Used to derive TLS Encryption Keys, TLS Authentication Keys	384 - 384 bits	Master Secret - CSP		TLSv1.2 Keying Materials Development	TLSv1.2 Keying Materials Development
TLS Session Encryption Key	Used to secure TLS session confidentiality	128 or 256 bits - 128 or 256 bits	Session Key - CSP		TLSv1.2 Keying Materials Development	Block Cipher (TLSv1.2)
TLS Session Authentication Key	Used to secure TLS session integrity	at least 112 bits - at least 112 bits	Session Key - CSP		TLSv1.2 Keying Materials Development	MAC (TLSv1.2)
IPSec/IKEv2 Pre-Shared Secret	Used for IPSec/IKEv2 peer authentication	2048 bits characters - 2048 bits characters	Shared Secret - CSP			
IPSec/IKEv2 RSA Private Key	Used for IPSec/IKEv2 peer authentication	2048, 3072 bits - 112, 128 bits	Private Key - CSP	RSA KeyGen		RSA SigGen
IPSec/IKEv2 RSA Public Key	Used for IPSec/IKEv2 peer authentication	2048, 3072 bits - 112, 128 bits	Public Key - PSP		RSA KeyGen	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
IPSec/IKEv2 ECDHE Private Key	Used to derive IPSec/IKEv2 ECDHE Shared Secret	P-256, P-384 - 128, 192 bits	Private Key - CSP	KAS-ECC-KeyGen (IPSec/IKEv 2)		KAS-ECC (IPSec/IKEv 2)
IPSec/IKEv2 ECDHE Public Key	Used to derive IPSec/IKEv2 ECDHE Shared Secret	P-256, P-384 - 128, 192 bits	Public Key - PSP		KAS-ECC-KeyGen (IPSec/IKEv 2)	
Peer IPSec/IKEv2 ECDHE Public Key	Used to derive IPSec/IKEv2 ECDHE Shared Secrets	P-256, P-384 - 128, 192 bits	Public Key - PSP			KAS-ECC (IPSec/IKEv 2)
IPSec/IKEv2 ECDHE Shared Secret	Used to derive IPSec/IKEv2 Session Encryption Keys, IPSec/IKEv2 Authenticatio n Keys	P-256, P-384 - 128, 192 bits	Shared Secret - CSP		KAS-ECC (IPSec/IKEv 2)	IPSec/IKEv2 Keying Materials Developmen t
SKEYSEED	Keying material used to derive the IPSec/IKEv2 Session Encryption Key and IPSec/IKEv2 Authenticatio n Key	384 - 384 bits	Keying Material - CSP		IPSec/IKEv2 Keying Materials Developmen t	IPSec/IKEv2 Keying Materials Developmen t
IPSec/IKEv2 Session Encryption Key	Used to secure IPSec/IKEv2 session confidentialit y	128, 192 bits - 128, 192 bits	Session Key - CSP		IPSec/IKEv2 Keying Materials Developmen t	Block Cipher (IPSec/IKEv 2)
IPSec/IKEv2 Session Authenticatio n Key	Used to secure IPSec/IKEv2 session integrity	at least 112 bits - at least 112 bits	Session Key - CSP		IPSec/IKEv2 Keying Materials Developmen t	MAC (IPSec/IKEv 2)
SNMPv3 Authenticatio n Secret	Used for SNMPv3 User	8 character s	Authenticatio n Secret - CSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	authentication	minimum - 8 characters minimum				
SNMPv3 Session Encryption Key	Used to secure SNMPv3 session confidentiality	128 bits - 128 bits	Session Key - CSP		SNMPv3 Keying Materials Development	Block Cipher (SNMPv3)
SNMPv3 Session Authentication Key	Used to secure SNMPv3 session integrity	160 bits - at least 112 bits	Session Key - CSP		SNMPv3 Keying Materials Development	MAC (SNMPv3)
SSH ECDHE Private Key	Used to derive the SSH ECDHE Shared Secret	P-256, P-384, P-521 - 128, 192, 256 bits	Private Key - CSP	KAS-ECC-KeyGen (SSHv2)		KAS-ECC (SSHv2)
SSH ECDHE Public Key	Used to derive the SSH ECDHE Shared Secret	P-256, P-384, P-521 - 128, 192, 256 bits	Public Key - PSP		KAS-ECC-KeyGen (SSHv2)	
Peer SSH ECDHE Public Key	Used to derive SSH ECDHE Shared Secret	P-256, P-384, P-521 - N/A	Public Key - PSP			KAS-ECC (SSHv2)
SSH ECDHE Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys	P-256, P-384, P-521 - 128, 192, 256 bits	Shared Secret - CSP		KAS-ECC (SSHv2)	SSHv2 Keying Materials Development
SSH ECDSA Private Key	Used for SSH session authentication	P-256, P-384, P-521 - 128, 192, 256 bits	Private Key - CSP	ECDSA KeyGen		ECDSA SigGen
SSH ECDSA Public Key	Used for SSH Session authentication	P-256, P-384, P-521 - 128, 192, 256	Public Key - PSP		ECDSA KeyGen	
SSH Session	Used for SSH session	128, 192, 256 bits -	Session Key - CSP		SSHv2 Keying Materials	Block Cipher (SSHv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Encryption Key	confidentiality protection	128, 192, 256 bits			Development	
SSH Session Authentication Key	Used for SSH session integrity protection	at least 160 bits - at least 160 bits	Session Key - CSP		SSHv2 Keying Materials Development	MAC (SSHv2)

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
CTR DRBG Entropy Input		DRAM within TOEPP:Plaintext		Zeroization Command Power Down	
CTR DRBG Seed		DRAM within TOEPP:Plaintext		Zeroization Command Power Down	
CTR DRBG Internal State (V, Key)		DRAM within TOEPP:Plaintext		Zeroization Command Power Down	
HMAC DRBG Entropy Input		DRAM within TOEPP:Plaintext		Zeroization Command Power Down	
HMAC DRBG Seed		DRAM within TOEPP:Plaintext		Zeroization Command Power Down	
HMAC DRBG Internal State (V, Key)		DRAM within TOEPP:Plaintext		Zeroization Command Power Down	
TLS RSA Private Key		HDD within TOEPP:Plaintext		Zeroization Command	
TLS RSA Public Key	Module Public Key Output	HDD within TOEPP:Plaintext		Zeroization Command	
TLS ECDHE Private Key		DRAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS ECDHE Public Key	Module Public Key Output	DRAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
Peer TLS ECDHE Public Key	Peer Public Key Input	DRAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS ECDHE Shared Secret		DRAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command	

)

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Power Down Session Termination	
TLS Master Secret		DRAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS Session Encryption Key		DRAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS Session Authentication Key		DRAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKEv2 Pre-Shared Secret	Password/Secret Input via TLSv1.2 decrypted by AES and HMAC Password/Secret Input via TLSv1.2 decrypted by AES-GCM	HDD within TOEPP:Plaintext		Zeroization Command	
IPSec/IKEv2 RSA Private Key		HDD within TOEPP:Plaintext		Zeroization Command	
IPSec/IKEv2 RSA Public Key	Module Public Key Output	HDD within TOEPP:Plaintext		Zeroization Command	
IPSec/IKEv2 ECDHE Private Key		DRAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKEv2 ECDHE Public Key	Module Public Key Output	DRAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
Peer IPSec/IKEv2 ECDHE Public Key	Peer Public Key Input	DRAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKEv2 ECDHE Shared Secret		DRAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SKEYSEED		DRAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKEv2 Session Encryption Key		DRAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKEv2 Session Authentication Key		DRAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
SNMPv3 Authentication Secret	Password/Secret Input via TLSv1.2 decrypted by AES and HMAC Password/Secret Input via TLSv1.2 decrypted by AES-GCM	HDD within TOEPP:Plaintext		Zeroization Command	
SNMPv3 Session Encryption Key		DRAM within TOEPP:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Power Down Session Termination	
SNMPv3 Session Authentication Key		DRAM within TOEPP:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Power Down Session Termination	
SSH ECDHE Private Key		DRAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
SSH ECDHE Public Key	Module Public Key Output	DRAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
Peer SSH ECDHE Public Key	Peer Public Key Input	DRAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
SSH ECDHE Shared Secret		DRAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Session Termination	
SSH ECDSA Private Key		HDD within TOEPP:Plaintext		Zeroization Command	
SSH ECDSA Public Key	Module Public Key Output	HDD within TOEPP:Plaintext		Zeroization Command	
SSH Session Encryption Key		DRAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
SSH Session Authentication Key		DRAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	

Table 20: SSP Table 2

9.5 Transitions

FIPS 186-4/186-5

- As of February 5, 2024, the CMVP does not accept module submissions that implement DSA or RSA X9.31 in the approved mode, other than for signature verification which is approved for legacy use. This module does not implement DSA or RSA X9.31 for signature generation and therefore is unaffected by the current transition from 186-4 to 186-5. As detailed in section 2.7, the CAVP testing performed on the 186-4 algorithms is mathematically similar to the testing performed on the 186-5 algorithms and therefore this module claims compliance with 186-5.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Software Integrity Test	HMAC-SHA2-256	KAT	SW/FW Integrity	Module is in normal state	Hash Comparison

Table 21: Pre-Operational Self-Tests

Prior to the module providing any data output via the data output interface, the module performs and passes the pre-operational self-test listed above. The module performs the cryptographic algorithm self-tests (CASTs) for HMAC-SHA2-256 and SHA2-256 before performing the software integrity test.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt KAT (A3566)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A3566)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
AES-GCM Encrypt KAT (A3566)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-GCM Decrypt KAT (A3566)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
AES-CBC Encrypt KAT (A3572)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A3572)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
AES-GCM Encrypt KAT (A3572)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-GCM Decrypt KAT (A3572)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
Counter DRBG Instantiate KAT (A3566)	AES-256	KAT	CAST	Module is in normal state	Instantiate	Power Up
Counter DRBG Generate KAT (A3566)	AES-256	KAT	CAST	Module is in normal state	Generate	Power Up
Counter DRBG Reseed KAT (A3566)	AES-256	KAT	CAST	Module is in normal state	Reseed	Power Up
ECDSA SigGen KAT (A3566)	P-224 with SHA2-256	KAT	CAST	Module is in normal state	Sign	Power Up
ECDSA SigVer KAT (A3566)	P-224 with SHA2-256	KAT	CAST	Module is in normal state	Verify	Power Up
HMAC DRBG Instantiate KAT (A3572)	HMAC-SHA2-512	KAT	CAST	Module is in normal state	Instantiate KAT	Power Up
HMAC DRBG Reseed KAT (A3572)	HMAC-SHA2-512	KAT	CAST	Module is in normal state	Reseed KAT	Power Up
HMAC DRBG Generate KAT (A3572)	HMAC-SHA2-512	KAT	CAST	Module is in normal state	Generate KAT	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA-1 KAT (A3566)	HMAC-SHA1	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-256 KAT (A3566)	HMAC-SHA2-256	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-384 KAT (A3566)	HMAC-SHA2-384	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-512 KAT (A3566)	HMAC-SHA2-512	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-256 KAT (A3572)	HMAC-SHA2-256	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-384 KAT (A3572)	HMAC-SHA2-384	KAT	CAST	Module is in normal state	N/A	Power Up
KAS-ECC-SSC Sp800-56Ar3 KAT (A3566)	Curve P-256	KAT	CAST	Module is in normal state	Primitive Z KAT	Power Up
KAS-ECC-SSC Sp800-56Ar3 KAT (A3572)	Curve P-256	KAT	CAST	Module is in normal state	Primitive Z KAT	Power Up
KDF IKEv2 KAT (A3566)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SSH KAT (A3566)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF TLS KAT (A3566)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SNMP KAT (A3566)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF TLS KAT (A3572)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
RSA SigGen KAT (A3566)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	Sign	Power Up
RSA SigVer KAT (A3566)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	Verify	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer KAT (A3572)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	Verify	Power Up
SHA-1 KAT (A3566)	SHA-1	KAT	CAST	Module is in normal state	N/A	Power Up
ECDSA KeyGen PCT (A3566)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs on newly generated keypairs before first operational use
RSA KeyGen PCT (A3566)	2048 bit modulus with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs on newly generated keypairs before first operational use
KAS-ECC KeyGen PCT (A3566)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs on newly generated key pairs before first operational use
KAS-ECC KeyGen PCT (A3572)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs on newly generated keypairs before first operational use
Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Power Up
Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Entropy 90B Continuous Repetition Count Test (RPT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Entropy data is generatd from the Entropy Source - Continuous
Entropy 90B Continuous Adaptive Proportions Test (APT)	Adaptive Proportions Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source	Entropy data is generated from the Entropy Source - Continuous

Table 22: Conditional Self-Tests

The Cryptographic Algorithm Self-Tests (CASTs) can be initiated by rebooting the module. All self-tests run without operator intervention.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Software Integrity Test	KAT	SW/FW Integrity	60 Days	Reboot

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt KAT (A3566)	KAT	CAST	60 days	Reboot
AES-CBC Decrypt KAT (A3566)	KAT	CAST	60 Days	Reboot
AES-GCM Encrypt KAT (A3566)	KAT	CAST	60 Days	Reboot
AES-GCM Decrypt KAT (A3566)	KAT	CAST	60 Days	Reboot
AES-CBC Encrypt KAT (A3572)	KAT	CAST	60 Days	Reboot
AES-CBC Decrypt KAT (A3572)	KAT	CAST	60 Days	Reboot
AES-GCM Encrypt KAT (A3572)	KAT	CAST	60 Days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM Decrypt KAT (A3572)	KAT	CAST	60 Days	Reboot
Counter DRBG Instantiate KAT (A3566)	KAT	CAST	60 Days	Reboot
Counter DRBG Generate KAT (A3566)	KAT	CAST	60 Days	Reboot
Counter DRBG Reseed KAT (A3566)	KAT	CAST	60 Days	Reboot
ECDSA SigGen KAT (A3566)	KAT	CAST	60 Days	Reboot
ECDSA SigVer KAT (A3566)	KAT	CAST	60 Days	Reboot
HMAC DRBG Instantiate KAT (A3572)	KAT	CAST	60 Days	Reboot
HMAC DRBG Reseed KAT (A3572)	KAT	CAST	60 Days	Reboot
HMAC DRBG Generate KAT (A3572)	KAT	CAST	60 Days	Reboot
HMAC-SHA-1 KAT (A3566)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-256 KAT (A3566)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-384 KAT (A3566)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-512 KAT (A3566)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-256 KAT (A3572)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-384 KAT (A3572)	KAT	CAST	60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT (A3566)	KAT	CAST	60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT (A3572)	KAT	CAST	60 Days	Reboot
KDF IKEv2 KAT (A3566)	KAT	CAST	60 Days	Reboot
KDF SSH KAT (A3566)	KAT	CAST	60 Days	Reboot
KDF TLS KAT (A3566)	KAT	CAST	60 Days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDF SNMP KAT (A3566)	KAT	CAST	60 Days	Reboot
KDF TLS KAT (A3572)	KAT	CAST	60 Days	Reboot
RSA SigGen KAT (A3566)	KAT	CAST	60 Days	Reboot
RSA SigVer KAT (A3566)	KAT	CAST	60 Days	Reboot
RSA SigVer KAT (A3572)	KAT	CAST	60 Days	Reboot
SHA-1 KAT (A3566)	KAT	CAST	60 Days	Reboot
ECDSA KeyGen PCT (A3566)	PCT	PCT	60 Days	Generate new keypair
RSA KeyGen PCT (A3566)	PCT	PCT	60 Days	Generate new keypair
KAS-ECC KeyGen PCT (A3566)	PCT	PCT	60 Days	Generate new keypair
KAS-ECC KeyGen PCT (A3572)	PCT	PCT	60 Days	Generate new keypair
Entropy 90B Start-up Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
Entropy 90B Start-up Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A
Entropy 90B Continuous Repetition Count Test (RPT)	RCT	CAST	N/A	N/A
Entropy 90B Continuous Adaptive Proportions Test (APT)	APT	CAST	N/A	N/A

Table 24: Conditional Periodic Information

The module performs on-demand self-tests initiated by the operator, by power cycling the module. The full suite of self-tests is then executed. The same procedure may be employed by the operator to perform periodic self-tests.

It is recommended that the Crypto Officer perform periodic testing of the module's on-demand self-tests every 60 days to ensure all components are functioning correctly.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	In the Error State, no cryptographic services are provided and the data output is prohibited	Failed Pre-Operational Software Integrity Test Failed Conditional CAST Failed Conditional PCT Failed SP 800-90B Entropy Source Start-up/Continuous health tests	Reboot the module	System Halt

Table 25: Error States

If any of the above-mentioned self-tests fail, the module reports the cause of the error and enters an error state (there is only one error state). In the Error State, no cryptographic services are provided and data output is prohibited. The only method to recover from the error state is to reboot the module and perform the self-tests, including the pre-operational software integrity test and the conditional CASTs. The module will only enter into the operational state after successfully passing the pre-operational software integrity test and the conditional CASTs.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module is designed to handle the various stages of a module's life-cycle. The sections below highlight the details for each stage.

Secure Delivery Procedures
The module is built into ION 6.1. There is no standalone delivery of the module as a software library. The vendor's internal development process guarantees that the correct version of the module goes with the intended OS.

Secure Operation
The module meets all the Level 1 requirements for FIPS 140-3. Follow the secure operations provided below to place the module in the Approved mode.

The software version is 1.0. The module is initiated into the Approved mode of operation via the following procedure. Note that a Palo Alto ION device running ION 6.1 is needed to access the APIs of the module.

1. Prepare the ION device for use and power-on
2. Using the Controller, navigate to the device that is to be initiated
3. Select "FIPS"
    a. Click "proceed" to begin initialization procedure
4. The module will begin initialization that includes the following:
    a. Zeroization of any sensitive information or data
    b. Power cycle of the device followed by running all self-tests
5. Once initialization is complete, the module provides the following status output:
    a. Device Mode: "fips"
    b. Self-tests: "Power-up self test successful"

Once the module has completed initialization into the Approved mode of operation, any non-Approved configurations/algorithms are rejected automatically by the module and an error message is output.

11.2 Administrator Guidance

Prisma SD-WAN Administrator's Guide from https://docs.paloaltonetworks.com/

11.3 Non-Administrator Guidance

Not Applicable.

11.4 End of Life

End of life dates for the module are announced publicly via Palo Alto Networks' services website. Crypto Officers should follow the procedure below for the secure destruction of their module:

Note: This process will cause the module to no longer function after it has wiped all configurations and keys.

1) Access the module via SSH as Crypto Officer
2) Execute command: "disable system"
    a) Confirm command
3) Module will begin zeroization process and wipe all security parameters and configurations

12 Mitigation of Other Attacks

This module is not designed to mitigate against any other attacks outside of the FIPS 140-3 scope.