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: January 27, 2025
Document Version: 1.0

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 5
2.1 Description 5
2.2 Tested and Vendor Affirmed Module Version and Identification 6
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 8
2.6 Security Function Implementations 11
2.7 Algorithm Specific Information 16
2.8 RBG and Entropy 16
2.9 Key Generation 17
2.10 Key Establishment 17
2.11 Industry Protocols 17
3 Cryptographic Module Interfaces 18
3.1 Ports and Interfaces 18
4 Roles, Services, and Authentication 18
4.1 Authentication Methods 18
4.2 Roles 18
4.3 Approved Services 18
4.4 Non-Approved Services 28
4.5 External Software/Firmware Loaded 28
4.6 Cryptographic Output Actions and Status 28
4.7 Additional Information 29
5 Software/Firmware Security 29
5.1 Integrity Techniques 29
5.2 Initiate on Demand 29
6 Operational Environment 29
6.1 Operational Environment Type and Requirements 29
7 Physical Security 29
8 Non-Invasive Security 29
9 Sensitive Security Parameters Management 29
9.1 Storage Areas 29
9.2 SSP Input-Output Methods 30

9.3 SSP Zeroization Methods 30
9.4 SSPs 31
9.5 Transitions 39
10 Self-Tests 39
10.1 Pre-Operational Self-Tests 39
10.2 Conditional Self-Tests 39
10.3 Periodic Self-Test Information 42
10.4 Error States 45
11 Life-Cycle Assurance 46
11.1 Installation, Initialization, and Startup Procedures 46
11.2 Administrator Guidance 46
11.3 Non-Administrator Guidance 47
11.4 End of Life 47
12 Mitigation of Other Attacks 47

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 6
Table 3: Tested Operational Environments - Software, Firmware, Hybrid 7
Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid 8
Table 5: Modes List and Description 8
Table 6: Approved Algorithms - Crypto Library - I 9
Table 7: Approved Algorithms - Crypto Library - II 10
Table 8: Approved Algorithms - Crypto Library - III 10
Table 9: Approved Algorithms - Crypto Library - IV 11
Table 10: Vendor-Affirmed Algorithms 11
Table 11: Security Function Implementations 15
Table 12: Entropy Certificates 16
Table 13: Entropy Sources 16
Table 14: Ports and Interfaces 18
Table 15: Roles 18
Table 16: Approved Services 28
Table 17: Storage Areas 30
Table 18: SSP Input-Output Methods 30
Table 19: SSP Zeroization Methods 30
Table 20: SSP Table 1 35
Table 21: SSP Table 2 39
Table 22: Pre-Operational Self-Tests 39
Table 23: Conditional Self-Tests 42
Table 24: Pre-Operational Periodic Information 43
Table 25: Conditional Periodic Information 45
Table 26: Error States 45

List of Figures

Figure 1– Cryptographic Boundary 6

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. The physical perimeter is the Tested Operational Environment's Physical Perimeter (TOEPP) on which the module runs.

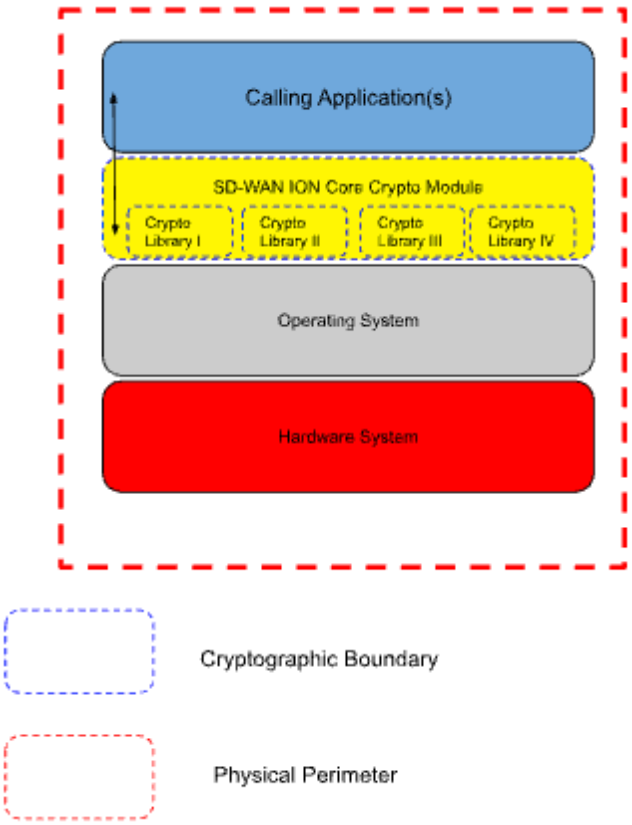

Figure 1– Cryptographic Boundary

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 (HMAC Cert. #A6268)

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 6.4	ION 1200	Intel Atom C3436L	Yes		1.0
ION 6.4	ION 1200	Intel Atom C3436L	No		1.0
ION 6.4	ION 1200-C-NA	Intel Atom C3436L	Yes		1.0
ION 6.4	ION 1200-C-NA	Intel Atom C3436L	No		1.0
ION 6.4	ION 1200-C-ROW	Intel Atom C3436L	Yes		1.0
ION 6.4	ION 1200-C-ROW	Intel Atom C3436L	No		1.0
ION 6.4	ION 1200-C-5G-WW	Intel Atom C3436L	Yes		1.0
ION 6.4	ION 1200-C-5G-WW	Intel Atom C3436L	No		1.0
ION 6.4	ION 1200-S	Intel Atom C3436L	Yes		1.0
ION 6.4	ION 1200-S	Intel Atom C3436L	No		1.0
ION 6.4	ION 1200-S-C-NA	Intel Atom C3436L	Yes		1.0
ION 6.4	ION 1200-S-C-NA	Intel Atom C3436L	No		1.0
ION 6.4	ION 1200-S-C-ROW	Intel Atom C3436L	Yes		1.0
ION 6.4	ION 1200-S-C-ROW	Intel Atom C3436L	No		1.0
ION 6.4	ION 1200-S-C5G-WW	Intel Atom C3436L	Yes		1.0
ION 6.4	ION 1200-S-C5G-WW	Intel Atom C3436L	No		1.0
ION 6.4	ION 3200	Intel Atom C3558R	Yes		1.0
ION 6.4	ION 3200	Intel Atom C3558R	No		1.0
ION 6.4	ION 3200H	Intel Atom C3708	Yes		1.0
ION 6.4	ION 3200H	Intel Atom C3708	No		1.0
ION 6.4	ION 3200H-C5G-WW	Intel Atom C3708	Yes		1.0
ION 6.4	ION 3200H-C5G-WW	Intel Atom C3708	No		1.0
ION 6.4	ION 5200	Intel Atom C5325	Yes		1.0
ION 6.4	ION 5200	Intel Atom C5325	No		1.0
ION 6.4	ION 9200	Intel Atom P5362	Yes		1.0
ION 6.4	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

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

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 via the status output interface upon entering the Approved Mode after initialization

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	A6268	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A6268	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A6268	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A6268	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
Counter DRBG	A6268	Prediction Resistance - No, Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - No, Yes	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
ECDSA KeyGen (FIPS186-5)	A6268	Curve - P-256, P-384, P-521 Secret Generation Mode - extra bits, testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6268	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6268	Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
HMAC-SHA-1	A6268	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6268	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6268	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6268	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6268	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A6268	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)	A6268	Password Length - Password Length: 64, 2048	SP 800-135 Rev. 1
KDF SSH (CVL)	A6268	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-5)	A6268	Key Generation Mode - probable Modulo - 2048, 3072 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
RSA SigGen (FIPS186-5)	A6268	Modulo - 2048, 3072 Signature Type - pkcs1v1.5, pss	FIPS 186-5
RSA SigVer (FIPS186-5)	A6268	Modulo - 2048, 3072 Signature Type - pkcs1v1.5, pss	FIPS 186-5
SHA-1	A6268	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-256	A6268	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A6268	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-512	A6268	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A6268	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1

Table 6: Approved Algorithms - Crypto Library - I

Crypto Library - II

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6269	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A6269	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 256	SP 800-38D
Counter DRBG	A6269	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - No	SP 800-90A Rev. 1
HMAC-SHA2-256	A6269	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6269	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6269	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
RSA SigVer (FIPS186-5)	A6269	Modulo - 2048 Signature Type - pkcs1v1.5	FIPS 186-5
SHA2-256	A6269	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A6269	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A6269	Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1

Table 7: Approved Algorithms - Crypto Library - II

Crypto Library - III

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6270	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
HMAC-SHA2-256	A6270	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6270	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6270	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
SHA2-256	A6270	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A6270	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-512	A6270	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4

Table 8: Approved Algorithms - Crypto Library - III

Crypto Library - IV

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6271	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
HMAC-SHA2-256	A6271	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-384	A6271	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6271	Key Length - Key Length: 256-1120 Increment 8	FIPS 198-1
SHA2-256	A6271	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	A6271	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-512	A6271	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4

Table 9: Approved Algorithms - Crypto Library - IV

Vendor-Affirmed Algorithms:

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

Table 10: 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 (SSH)	CKG KAS-KeyGen	KAS ECC keygen used in SSHv2 service	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	Counter DRBG: (A6268) CKG: ()

Name	Type	Description	Properties	Algorithms
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	Counter DRBG: (A6268, A6269) CKG: ()
KAS-ECC-KeyGen (IPSec/IKE)	CKG KAS-KeyGen	KAS ECC keygen used in IPSec/IKEv2 service	Bit-strength Caveat:Provides between 128 and 192 bits of encryption strength	Counter DRBG: (A6268) CKG: ()
KAS-ECC (SSH)	KAS-Full	Full KAS-ECC Key Agreement used 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: (A6268) KDF SSH: (A6268)
KAS-ECC (TLSv1.2)	KAS-Full	Full KAS-ECC Key Agreement used 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: (A6268, A6269) TLS v1.2 KDF RFC7627: (A6268, A6269)
KAS-ECC (IPSec/IKE)	KAS-Full	Full KAS-ECC Key Agreement used 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	KAS-ECC-SSC Sp800-56Ar3: (A6268) Domain Parameter Generation Methods: P-256, P-384 KDF IKEv2: (A6268)

Name	Type	Description	Properties	Algorithms
			provides between 128 and 192 bits of encryption strength	
KTS (TLSv1.2 with AES and HMAC)	KTS-Unwrap	KTS via TLSv1.2 service by using AES and HMAC	Standard:SP 800-38F IG 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	AES-CBC: (A6269) HMAC-SHA2-256: (A6269) HMAC-SHA2-384: (A6269) SHA2-256: (A6269) SHA2-384: (A6269)
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: (A6269)
SSH ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for SSHv2		ECDSA KeyGen (FIPS186-5): (A6268) Counter DRBG: (A6268) CKG: ()
SSH ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for SSHv2		ECDSA SigGen (FIPS186-5): (A6268)
SSH ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for SSHv2		ECDSA SigVer (FIPS186-5): (A6268)
TLS RSA KeyGen	AsymKeyPair-KeyGen CKG	RSA KeyGen for TLSv1.2		RSA KeyGen (FIPS186-5): (A6268) Counter DRBG:

Name	Type	Description	Properties	Algorithms
				(A6268) CKG: ()
TLS RSA SigGen	DigSig-SigGen	RSA SigGen for TLSv1.2		RSA SigGen (FIPS186-5): (A6268)
TLS RSA SigVer	DigSig-SigVer	RSA SigVer for TLSv1.2		RSA SigVer (FIPS186-5): (A6269, A6268)
IPSec/IKE RSA KeyGen	AsymKeyPair-KeyGen CKG	RSA KeyGen for IPSec/IKEv2		RSA KeyGen (FIPS186-5): (A6268) Counter DRBG: (A6268) CKG: ()
IPSec/IKE RSA SigGen	DigSig-SigGen	RSA SigGen for IPSec/IKEv2		RSA SigGen (FIPS186-5): (A6268)
IPSec/IKE RSA SigVer	DigSig-SigVer	RSA SigVer for IPSec/IKEv2		RSA SigVer (FIPS186-5): (A6268)
Session Encryption/Decryption (SSH)	BC-Auth BC-UnAuth	SSHv2 session protection		AES-CTR: (A6268)
Session Encryption/Decryption (TLSv1.2)	BC-Auth BC-UnAuth	TLSv1.2 session protection		AES-CBC: (A6269, A6268) AES-GCM: (A6269, A6268)
Session Encryption/Decryption (IPSec/IKE)	BC-Auth BC-UnAuth	IPSec/IKE session protection		AES-CBC: (A6268, A6270, A6271)
Session Encryption/Decryption (SNMPv3)	BC-Auth BC-UnAuth	SNMPv3 session protection		AES-CFB128: (A6268)
Session Authentication (SSHv2)	MAC	SSHv2 session authentication		HMAC-SHA-1: (A6268) HMAC-SHA2-256: (A6268) HMAC-SHA2-512: (A6268) SHA-1: (A6268) SHA2-256: (A6268) SHA2-512: (A6268)
Session Authentication (TLSv1.2)	MAC	TLSv1.2 session authentication		HMAC-SHA2-256: (A6269, A6268) HMAC-SHA2-384: (A6269, A6268) SHA2-256: (A6269, A6268)

Name	Type	Description	Properties	Algorithms
				SHA2-384: (A6269, A6268)
Session Authentication (IPSec/IKE)	MAC	IPSec/IKE session authentication		HMAC-SHA-1: (A6268) SHA-1: (A6268) HMAC-SHA2-256: (A6268, A6270, A6271) HMAC-SHA2-384: (A6268, A6270, A6271) HMAC-SHA2-512: (A6268, A6270, A6271) SHA2-256: (A6268, A6270, A6271) SHA2-384: (A6268, A6270, A6271) SHA2-512: (A6268, A6270, A6271)
Session Authentication (SNMPv3)	MAC	SNMPv3 session authentication		HMAC-SHA-1: (A6268) SHA-1: (A6268)
SSHv2 Keying Materials Development	KAS-135KDF	SSHv2 session keying materials, used to derive SSHv2 session keys.		KDF SSH: (A6268)
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLSv1.2 session keys		TLS v1.2 KDF RFC7627: (A6269, A6268)
IPSec/IKE Keying Materials Development	KAS-135KDF	IPSec/IKE session keying materials, used to derive IPSec/IKE session keys		KDF IKEv2: (A6268)
SNMPv3 Keying Materials Development	KAS-135KDF	SNMPv3 session keying materials, used to derive SNMPv3 session keys		KDF SNMP: (A6268)
DRBG Function	DRBG	Used for DRBG generation		Counter DRBG: (A6268, A6269)

Table 11: Security Function Implementations

2.7 Algorithm Specific Information

Notes:

- 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.

- The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. The operations of one of the two parties involved in the IKE key establishment scheme shall be performed entirely within the cryptographic boundary of the module being validated. 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. Two keys established by IKEv2 for one security association (one key for encryption in each direction between the parties) are not identical and abort the session if they are. 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.

- 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.

2.8 RBG and Entropy

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

Table 12: 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 Atom C3436L, Intel Atom C3558R, Intel Atom C3708	128 bits	Full Entropy	A2153 (AES-CBC-MAC)
Palo Alto Networks DRNG Entropy Source - Snow Ridge 24-Core Die with FCBGA2106 Package	Physical	Intel Atom C5325, Intel Atom P5362	128 bits	Full Entropy	A2541 (AES-CBC-MAC)

Table 13: Entropy Sources

The operational environment is detailed in the Public Use Document for the “Palo Alto Networks DRNG Entropy Source” Certificate E68 and E71. The “Palo Alto Networks DRNG Entropy Source” is described as a feedback stabilized metastable latch that provides 128 bits of full entropy per sample. The entropy source is called multiple times in order to seed the DRBGs.

The module implements two approved DRBGs based on SP800-90Arev1, including CTR_DRBG with Algo Cert. #A6268, and CTR_DRBG with Algo Cert. #A6269. Those two DRBGs are used internally by the module (e.g. to generate 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 (Cert. #A6268) with Derivation Function and CTR_DRBG (Cert. #A6269) 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. 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 validated entropy source running on each of 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, ION 3200, ION 3200H, and ION 3200H-C5G-WW tested platforms
- ESV Cert. #E71 is for validated entropy source running on each of ION 5200 and ION 9200 tested platforms

2.9 Key Generation

The module generates RSA, ECDSA, and ECDH asymmetric key pairs compliant with FIPS 186-5, using a NIST SP 800-90Ar1 CTR 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
N/A	Control Output	N/A
N/A	Status Output	Return values and/or log messages

Table 14: Ports and Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Section 2.2. 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 15: 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 - Software Integrity Test Key: E Unauthenticated - Software

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Integrity Test Key: E
Zeroization	Zeroize all unprotected SSPs stored in the module	None	Command to initiate the SSPs zeroization	Status of the SSPs zeroization	None	Crypto Officer - DRBG Entropy Input (A6268): Z - DRBG Seed (A6268): Z - DRBG Internal State V value (A6268): Z - DRBG Key (A6268): Z - DRBG Entropy Input (A6269): Z - DRBG Seed (A6269): Z - DRBG Internal State V value (A6269): Z - DRBG Key (A6269): 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 RSA Pre-Master Secret: Z - TLS Master Secret: Z - TLS Session Encryption

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: Z - TLS Session Authentication Key: Z - IPSec/IKE Pre-Shared Secret: Z - IPSec/IKE RSA Private Key: Z - IPSec/IKE RSA Public Key: Z - IPSec/IKE ECDHE Private Key: Z - IPSec/IKE ECDHE Public Key: Z - Peer IPSec/IKE ECDHE Public Key: Z - IPSec/IKE ECDHE Shared Secret: Z - SKEYSEED: Z - IPSec/IKE Session Encryption Key: Z - IPSec/IKE Session Authentication Key: Z - SNMPv3 Authentication Secret: Z - SNMPv3 Session Encryption Key: Z - SNMPv3 Session Authentication Key: Z - SSH ECDHE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						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
Configure Network	Perform the module's network configuration	Approved Mode Indicator and successful network configuration system log message	Commands to configure the module	Status of the completion of network related configuration	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Configure SSHv2 Function	Create a secure SSHv2 channel	Approved Mode Indicator and successful SSHv2 configuration system log message	Commands to configure SSHv2	Status of the completion of SSHv2 configuration	SSH ECDSA KeyGen DRBG Function	Crypto Officer - SSH ECDSA Private Key: G,W - SSH ECDSA Public Key: G,W - DRBG Entropy Input (A6268): E - DRBG Seed (A6268): E - DRBG Internal State V value (A6268): E - DRBG Key (A6268): E
Configure TLSv1.2 Function	Create a secure TLSv1.2 channel	Approved Mode Indicator and successful TLSv1.2 configuration system log message	Commands to configure TLSv1.2	Status of the completion of TLSv1.2 configuration	TLS RSA KeyGen DRBG Function	Crypto Officer - TLS RSA Private Key: G,W - TLS RSA Public Key: G,W - DRBG Entropy Input (A6268): E - DRBG Seed (A6268): E - DRBG Internal State V value (A6268): E - DRBG Key (A6268): E - DRBG Entropy Input (A6269): E - DRBG Seed (A6269): E - DRBG Internal State V value (A6269): E - DRBG Key (A6269): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Configure SNMPv3 Function	Create a secure SNMPv3 channel	Approved Mode Indicator and successful SNMPv3 configuration system 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 - 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 RSA Pre-Master Secret: W,E - TLS Master Secret: G,W,E - TLS Session Encryption Key: G,W,E - TLS Session Authentication Key: G,W,E - DRBG Entropy Input (A6269): E - DRBG Seed (A6269): E - DRBG Internal State V value (A6269): E - DRBG Key (A6269): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Configure IPSec/IKEv2 Function	Create IPSec/IKEv2 tunnel	Approved Mode Indicator and successful IPSec/IKEv2 configuration system 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) IPSec/IKE RSA KeyGen DRBG Function	Crypto Officer - IPSec/IKE Pre-Shared Secret: W - IPSec/IKE RSA Private Key: G,W - IPSec/IKE RSA Public Key: G,W - 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 RSA Pre-Master Secret: W,E - TLS Master Secret: G,W,E - TLS Session Encryption Key: G,W,E - TLS Session Authentication Key: G,W,E - DRBG Entropy Input (A6268): E - DRBG Seed (A6268): E - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Internal State V value (A6268): E - DRBG Key (A6268): E - DRBG Entropy Input (A6269): E - DRBG Seed (A6269): E - DRBG Internal State V value (A6269): E - DRBG Key (A6269): E
Run SSHv2 Function	Negotiation and encrypted data transport via SSH	Approved Mode Indicator and successful SSHv2 service system log message	Initiate SSHv2 tunnel establishment request	Status of SSHv2 tunnel establishment	KAS-ECC-KeyGen (SSH) KAS-ECC (SSH) SSH ECDSA SigGen SSH ECDSA SigVer Session Encryption/Decryption (SSH) Session Authentication (SSHv2) SSHv2 Keying Materials Development DRBG Function	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 - DRBG Entropy Input (A6268): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Seed (A6268): E - DRBG Internal State V value (A6268): E - DRBG Key (A6268): E
Run TLSv1.2 Function	Negotiation and encrypted data transport via TLS	Approved Mode Indicator and successful TLSv1.2 service system log message	Initiate TLSv.12 tunnel establishment request	Status of SNMPv3 tunnel establishment	KAS-ECC-KeyGen (TLSv1.2) KAS-ECC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) TLS RSA SigGen TLS RSA SigVer Session Encryption/Decryption (TLSv1.2) Session Authentication (TLSv1.2) TLSv1.2 Keying Materials Development DRBG Function	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 RSA Pre-Master Secret: W,E - TLS Master Secret: G,W,E - TLS Session Encryption Key: G,W,E - TLS Session Authentication Key: G,W,E - DRBG Entropy Input (A6268): E - DRBG Seed (A6268): E - DRBG Internal State

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						V value (A6268): E - DRBG Key (A6268): E - DRBG Entropy Input (A6269): E - DRBG Seed (A6269): E - DRBG Internal State V value (A6269): E - DRBG Key (A6269): E
Run SNMPv2 Function	Negotiation and encrypted data transport via SNMPv3	Approved Mode Indicator and successful SNMPv3 service system log message	Initiate SNMPv3 tunnel establishment request	Status of SNMPv3 tunnel establishment	Session Encryption/Decryption (SNMPv3) Session Authentication (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
Run IPSec/IKEv2 Function	Negotiation and encrypted data transport via IPSec	Approved Mode Indicator and successful IPSec/IKEv2 service system log message	Initiate IPSec/IKEv2 tunnel establishment request	Status of IPSec/IKEv2 tunnel establishment	KAS-ECC-KeyGen (IPSec/IKE) KAS-ECC (IPSec/IKE) IPSec/IKE RSA SigGen IPSec/IKE RSA SigVer Session Encryption/Decryption (IPSec/IKE) Session Authentication (IPSec/IKE) IPSec/IKE Keying Materials Development DRBG Function	Crypto Officer - IPSec/IKE Pre-Shared Secret: E - IPSec/IKE RSA Private Key: E - IPSec/IKE RSA Public Key: R - IPSec/IKE ECDHE Private Key: G,W,E - IPSec/IKE ECDHE Public Key: G,R,W - Peer IPSec/IKE ECDHE Public Key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- IPSec/IKE ECDHE Shared Secret: G,W,E - SKEYSEED: G,W,E - IPSec/IKE Session Encryption Key: G,W,E - IPSec/IKE Session Authentication Key: G,W,E - DRBG Entropy Input (A6268): E - DRBG Seed (A6268): E - DRBG Internal State V value (A6268): E - DRBG Key (A6268): E

Table 16: 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

The module does not support the ability to load external software or firmware.

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. #A6268) 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 MAC 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
RAM within TOEPP	Volatile Memory	Dynamic
HDD within TOEPP	Non-Volatile Memory	Static

Table 17: 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 18: 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
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 module

Table 19: 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
DRBG Entropy Input (A6268)	Used to seed the DRBG	256 - 256 bits	DRBG Entropy Input - CSP			DRBG Function
DRBG Seed (A6268)	Used in DRBG Generation	256 - 256 bits	DRBG Seed - CSP			DRBG Function
DRBG Internal State V value (A6268)	Used in DRBG Generation	256 - 256 bits	DRBG Internal State V value - CSP			DRBG Function
DRBG Key (A6268)	Used in DRBG Generation	256 - 256 bits	DRBG Key - CSP			DRBG Function
DRBG Entropy Input (A6269)	Used to seed the DRBG	256 - 256 bits	DRBG Entropy Input - CSP			DRBG Function
DRBG Seed (A6269)	Used in DRBG Generation	256 - 256 bits	DRBG Seed - CSP			DRBG Function
DRBG Internal State V value (A6269)	Used in DRBG Generation	256 - 256 bits	DRBG Internal State V value - CSP			DRBG Function
DRBG Key (A6269)	Used in DRBG Generation	256 - 256 bits	DRBG Key - CSP			DRBG Function
TLS RSA Private Key	Used for TLS peer authentication	2048, 3072 bits - 112, 128 bits	Private Key - CSP	TLS RSA KeyGen		TLS RSA SigGen
TLS RSA Public Key	Used for TLS peer authentication	2048, 3072 bits - 112, 128 bits	Public Key - PSP		TLS 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 RSA Pre-Master Secret	Used to derive TLS Master Secret	384 - 384 bits	Pre-Master Secret - CSP			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	Session Encryption/Decryption (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	Session Authentication (TLSv1.2)
IPSec/IKE Pre-Shared Secret	Used for IPSec/IKE peer authentication	2048 bits characters - 2048 bits characters	Shared Secret - CSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
IPSec/IKE RSA Private Key	Used for IPSec/IKE peer authentication	2048, 3072 bits - 112, 128 bits	Private Key - CSP	IPSec/IKE RSA KeyGen		IPSec/IKE RSA SigGen
IPSec/IKE RSA Public Key	Used for IPSec peer authentication	2048, 3072 bits - 112, 128 bits	Public Key - PSP		IPSec/IKE RSA KeyGen	
IPSec/IKE ECDHE Private Key	Used to derive IPSec/IKE ECDHE Shared Secret	P-256, P-384 - 128, 192 bits	Private Key - CSP	KAS-ECC-KeyGen (IPSec/IKE)		KAS-ECC (IPSec/IKE)
IPSec/IKE ECDHE Public Key	Used to derive IPSec/IKE ECDHE Shared Secret	P-256, P-384 - 128, 192 bits	Public Key - PSP		KAS-ECC-KeyGen (IPSec/IKE)	
Peer IPSec/IKE ECDHE Public Key	Used to derive IPSec/IKE ECDHE Shared Secrets	P-256, P-384 - 128, 192 bits	Public Key - PSP			KAS-ECC (IPSec/IKE)
IPSec/IKE ECDHE Shared Secret	Used to derive IPSec/IKE Session Encryption Keys, IPSec/IKE Authentication Keys	P-256, P-384 - 128, 192 bits	Shared Secret - CSP		KAS-ECC (IPSec/IKE)	IPSec/IKE Keying Materials Development
SKEYSEED	Keying material used to derive the IPSec/IKE Session Encryption Key and IPSec/IKE Authentication Key	384 - 384 bits	Keying Material - CSP		IPSec/IKE Keying Materials Development	IPSec/IKE Keying Materials Development
IPSec/IKE Session Encryption Key	Used to secure IPSec/IKE session	128, 192 bits - 128, 192 bits	Session Key - CSP		IPSec/IKE Keying Materials	Session Encryption/Decryption (IPSec/IKE)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	confidentiality				Development	
IPSec/IKE Session Authentication Key	Used to secure IPSec/IKE session integrity	at least 112 bits - at least 112 bits	Session Key - CSP		IPSec/IKE Keying Materials Development	Session Authentication (IPSec/IKE)
SNMPv3 Authentication Secret	Used for SNMPv3 User authentication	8 characters minimum - 8 characters minimum	Authentication Secret - CSP			
SNMPv3 Session Encryption Key	Used to secure SNMPv3 session confidentiality	128 bits - 128 bits	Session Key - CSP		SNMPv3 Keying Materials Development	Session Encryption/Decryption (SNMPv3)
SNMPv3 Session Authentication Key	Used to secure SNMPv3 session integrity	160 bits - at least 112 bits	Session Key - CSP		SNMPv3 Keying Materials Development	Session Authentication (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 (SSH)		KAS-ECC (SSH)
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 (SSH)	
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 (SSH)
SSH ECDHE Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session	P-256, P-384, P-521 - 128, 192, 256 bits	Shared Secret - CSP		KAS-ECC (SSH)	SSHv2 Keying Materials Development

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Authentication Keys					
SSH ECDSA Private Key	Used for SSH session authentication	P-256, P-384, P-521 - 128, 192, 256 bits	Private Key - CSP	SSH ECDSA KeyGen		SSH ECDSA SigGen
SSH ECDSA Public Key	Used for SSH Session authentication	P-256, P-384, P-521 - 128, 192, 256	Public Key - PSP		SSH ECDSA KeyGen	
SSH Session Encryption Key	Used for SSH session confidentiality protection	128, 192, 256 bits - 128, 192, 256 bits	Session Key - CSP		SSHv2 Keying Materials Development	Session Encryption/Decryption (SSH)
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	Session Authentication (SSHv2)
Software Integrity Test Key	Used for Software Integrity Pre-Operational Self-test. Not an SSP but included for completeness	256 bits - 256 bits	Software Integrity Key - Neither			HMAC-SHA2-256 (A6268)

Table 20: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Entropy Input (A6268)		RAM within TOEPP:Plaintext		Zeroization Command Power Down	
DRBG Seed (A6268)		RAM within TOEPP:Plaintext		Zeroization Command Power Down	
DRBG Internal State V value (A6268)		RAM within TOEPP:Plaintext		Zeroization Command Power Down	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Key (A6268)		RAM within TOEPP:Plaintext		Zeroization Command Power Down	
DRBG Entropy Input (A6269)		RAM within TOEPP:Plaintext		Zeroization Command Power Down	
DRBG Seed (A6269)		RAM within TOEPP:Plaintext		Zeroization Command Power Down	
DRBG Internal State V value (A6269)		RAM within TOEPP:Plaintext		Zeroization Command Power Down	
DRBG Key (A6269)		RAM 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		RAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS ECDHE Public Key	Module Public Key Output	RAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
Peer TLS ECDHE Public Key	Peer Public Key Input	RAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS ECDHE Shared Secret		RAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS RSA Pre-Master Secret	Password/Secret Input via TLSv1.2 decrypted by AES and HMAC Password/Secret Input via TLSv1.2 decrypted by AES-GCM	RAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS Master Secret		RAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Session Termination	
TLS Session Encryption Key		RAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
TLS Session Authentication Key		RAM within TOEPP:Plaintext	While TLS tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKE 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/IKE RSA Private Key		HDD within TOEPP:Plaintext		Zeroization Command	
IPSec/IKE RSA Public Key	Module Public Key Output	HDD within TOEPP:Plaintext		Zeroization Command	
IPSec/IKE ECDHE Private Key		RAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKE ECDHE Public Key	Module Public Key Output	RAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
Peer IPSec/IKE ECDHE Public Key	Peer Public Key Input	RAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKE ECDHE Shared Secret		RAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
SKEYSEED		RAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
IPSec/IKE Session Encryption Key		RAM within TOEPP:Plaintext	While IPSec/IKEv2 tunnel is on	Zeroization Command Power Down Session Termination	
IPSec/IKE Session Authentication Key		RAM 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		RAM within TOEPP:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Power Down Session Termination	
SNMPv3 Session Authentication Key		RAM within TOEPP:Plaintext	While SNMPv3 tunnel is on	Zeroization Command Power Down Session Termination	
SSH ECDHE Private Key		RAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
SSH ECDHE Public Key	Module Public Key Output	RAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
Peer SSH ECDHE Public Key	Peer Public Key Input	RAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
SSH ECDHE Shared Secret		RAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
SSH ECDSA Private Key		HDD within TOEPP:Plaintext		Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH ECDSA Public Key	Module Public Key Output	HDD within TOEPP:Plaintext		Zeroization Command	
SSH Session Encryption Key		RAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
SSH Session Authentication Key		RAM within TOEPP:Plaintext	While SSHv2 tunnel is on	Zeroization Command Power Down Session Termination	
Software Integrity Test Key		HDD within TOEPP:Plaintext		N/A	

Table 21: SSP Table 2

9.5 Transitions

SHA-1
The module implements SHA-1 for use in non-digital-signature applications. This implementation will be non-Approved for all uses starting January 1, 2031. At this time, the user should move to SHA2, which is available in this module.

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 22: Pre-Operational Self-Tests

Note: The module performs conditional algorithm self-test (CAST) 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 (A6268)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A6268)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM Authenticated Encrypt KAT (A6268)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-GCM Authenticated Decrypt KAT (A6268)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
Counter DRBG Instantiate KAT (A6268)	AES-256	KAT	CAST	Module is in normal state	Instantiate KAT	Power Up
Counter DRBG Generate KAT (A6268)	AES-256	KAT	CAST	Module is in normal state	Generate KAT	Power Up
Counter DRBG Reseed KAT (A6268)	AES-256	KAT	CAST	Module is in normal state	Reseed KAT	Power Up
ECDSA SigGen (FIPS186-5) KAT (A6268)	P-224 with SHA2-256	KAT	CAST	Module is in normal state	Sign	Power Up
ECDSA SigVer (FIPS186-5) KAT (A6268)	P-224 with SHA2-256	KAT	CAST	Module is in normal state	Verify	Power Up
SHA-1 KAT (A6268)	Message Length: 8-51200 Increment 8	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA-1 KAT (A6268)	HMAC-SHA-1	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-256 KAT (A6268)	HMAC-SHA2-256	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-384 KAT (A6268)	HMAC-SHA2-384	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-512 KAT (A6268)	HMAC-SHA2-512	KAT	CAST	Module is in normal state	N/A	Power Up
RSA SigGen (FIPS186-5) KAT (A6268)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	Sign	Power Up
RSA SigVer (FIPS186-5) KAT (A6268)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	Verify	Power Up
KAS-ECC-SSC Sp800-56Ar3 KAT (A6268)	Curve P-256	KAT	CAST	Module is in normal state	N/A	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF IKEv2 KAT (A6268)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SNMP KAT (A6268)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SSH KAT (A6268)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
TLS v1.2 KDF RFC7627 KAT (A6268)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
RSA KeyGen (FIPS186-5) PCT (A6268)	2048 bit modulus with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs on newly generated key pairs before first operational use
ECDSA KeyGen (FIPS186-5) PCT (A6268)	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-SSC Sp800-56Ar3 PCT (A6268)	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
AES-CBC Encrypt KAT (A6269)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A6269)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
AES-GCM Authenticated Encrypt KAT (A6269)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-GCM Authenticated Decrypt KAT (A6269)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
Counter DRBG Instantiate KAT (A6269)	AES-256	KAT	CAST	Module is in normal state	Instantiate KAT	Power Up
Counter DRBG Generate KAT (A6269)	AES-256	KAT	CAST	Module is in normal state	Generate KAT	Power Up
Counter DRBG Reseed KAT (A6269)	AES-256	KAT	CAST	Module is in normal state	Reseed KAT	Power Up
RSA SigVer (FIPS186-5) KAT (A6269)	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
HMAC-SHA2-256 KAT (A6269)	HMAC-SHA2-256	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-384 KAT (A6269)	HMAC-SHA2-384	KAT	CAST	Module is in normal state	N/A	Power Up
KAS-ECC-SSC Sp800-56Ar3 KAT (A6269)	Curve P-256	KAT	CAST	Module is in normal state	N/A	Power Up
TLS v1.2 KDF RFC7627 KAT (A6269)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KAS-ECC-SSC Sp800-56Ar3 PCT (A6269)	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
AES-CBC Encrypt KAT (A6270)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A6270)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
HMAC-SHA2-256 KAT (A6270)	HMAC-SHA2-256	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-512 KAT (A6270)	HMAC-SHA2-512	KAT	CAST	Module is in normal state	N/A	Power Up
AES-CBC Encrypt KAT (A6271)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A6271)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
HMAC-SHA2-256 KAT (A6271)	HMAC-SHA2-256	KAT	CAST	Module is in normal state	N/A	Power Up
HMAC-SHA2-512 KAT (A6271)	HMAC-SHA2-512	KAT	CAST	Module is in normal state	N/A	Power Up

Table 23: 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 24: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt KAT (A6268)	KAT	CAST	60 Days	Reboot
AES-CBC Decrypt KAT (A6268)	KAT	CAST	60 Days	Reboot
AES-GCM Authenticated Encrypt KAT (A6268)	KAT	CAST	60 Days	Reboot
AES-GCM Authenticated Decrypt KAT (A6268)	KAT	CAST	60 Days	Reboot
Counter DRBG Instantiate KAT (A6268)	KAT	CAST	60 Days	Reboot
Counter DRBG Generate KAT (A6268)	KAT	CAST	60 Days	Reboot
Counter DRBG Reseed KAT (A6268)	KAT	CAST	60 Days	Reboot
ECDSA SigGen (FIPS186-5) KAT (A6268)	KAT	CAST	60 Days	Reboot
ECDSA SigVer (FIPS186-5) KAT (A6268)	KAT	CAST	60 Days	Reboot
SHA-1 KAT (A6268)	KAT	CAST	60 Days	Reboot
HMAC-SHA-1 KAT (A6268)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-256 KAT (A6268)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-384 KAT (A6268)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-512 KAT (A6268)	KAT	CAST	60 Days	Reboot
RSA SigGen (FIPS186-5) KAT (A6268)	KAT	CAST	60 Days	Reboot
RSA SigVer (FIPS186-5) KAT (A6268)	KAT	CAST	60 Days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-ECC-SSC Sp800-56Ar3 KAT (A6268)	KAT	CAST	60 Days	Reboot
KDF IKEv2 KAT (A6268)	KAT	CAST	60 Days	Reboot
KDF SNMP KAT (A6268)	KAT	CAST	60 Days	Reboot
KDF SSH KAT (A6268)	KAT	CAST	60 Days	Reboot
TLS v1.2 KDF RFC7627 KAT (A6268)	KAT	CAST	60 Days	Reboot
RSA KeyGen (FIPS186-5) PCT (A6268)	PCT	PCT	60 Days	Reboot
ECDSA KeyGen (FIPS186-5) PCT (A6268)	PCT	PCT	60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 PCT (A6268)	PCT	PCT	60 Days	Reboot
AES-CBC Encrypt KAT (A6269)	KAT	CAST	60 Days	Reboot
AES-CBC Decrypt KAT (A6269)	KAT	CAST	60 Days	Reboot
AES-GCM Authenticated Encrypt KAT (A6269)	KAT	CAST	60 Days	Reboot
AES-GCM Authenticated Decrypt KAT (A6269)	KAT	CAST	60 Days	Reboot
Counter DRBG Instantiate KAT (A6269)	KAT	CAST	60 Days	Reboot
Counter DRBG Generate KAT (A6269)	KAT	CAST	60 Days	Reboot
Counter DRBG Reseed KAT (A6269)	KAT	CAST	60 Days	Reboot
RSA SigVer (FIPS186-5) KAT (A6269)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-256 KAT (A6269)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-384 KAT (A6269)	KAT	CAST	60 Days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KAS-ECC-SSC Sp800-56Ar3 KAT (A6269)	KAT	CAST	60 Days	Reboot
TLS v1.2 KDF RFC7627 KAT (A6269)	KAT	CAST	60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 PCT (A6269)	PCT	PCT	60 Days	Reboot
AES-CBC Encrypt KAT (A6270)	KAT	CAST	60 Days	Reboot
AES-CBC Decrypt KAT (A6270)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-256 KAT (A6270)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-512 KAT (A6270)	KAT	CAST	60 Days	Reboot
AES-CBC Encrypt KAT (A6271)	KAT	CAST	60 Days	Reboot
AES-CBC Decrypt KAT (A6271)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-256 KAT (A6271)	KAT	CAST	60 Days	Reboot
HMAC-SHA2-512 KAT (A6271)	KAT	CAST	60 Days	Reboot

Table 25: 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 data output is prohibited.	Self-test failure	Reboot the module	Failed Pre-Operational Software Integrity Test: "Integrity check failed at <location>"; Failed Conditional CAST: "<Crypto Library>: FIPS Self-test failed for <algorithm> Entering error state"; Failed Conditional PCT: "Key verification failed"; Failed SP 800-90B Entropy Source Start-up/Continuous health tests: No random numbers are generated and key generation is halted

Table 26: 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

All ION devices are 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 6.4. When the device is running ION 6.4 , the following command can be used to verify the module's version:

- dump crypto version

This will output the following: *ION Core Crypto Module Version 1.0*

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 6.4 is needed to access the APIs of the module.

1. Prepare 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 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.