# Palo Alto Networks, Inc.

## Palo Alto Networks SD-WAN Virtual Instant-On Network (vION)

# FIPS 140-3 Non-Proprietary Security Policy

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: March 17, 2026
Document Version: 1.0

# 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 Virtual Instant-On Network (vION) with software version 6.4.2 hereinafter referred to as the Module or vION 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 Virtual Instant-On Network (vION) enables the integration of a diverse set of wide area network (WAN) connection types, improves application performance and visibility, enhances security and compliance, and reduces the overall cost and complexity of a WAN. Built with the intent to reduce remote infrastructure, Palo Alto Networks SD-WAN vION enables the cloud-delivered branch.

**Module Type**: Software

**Module Embodiment**: Multi-Chip Standalone

**Cryptographic Boundary:**

Figure 1 below depicts the cryptographic boundary (orange color area) and physical perimeter (light blue color area). The cryptographic boundary includes the vION operating system. The physical perimeter is the Tested Operational Environment's Physical Perimeter (TOEPP) on which the module runs. The Module was tested with and without the Processor's PAA component.

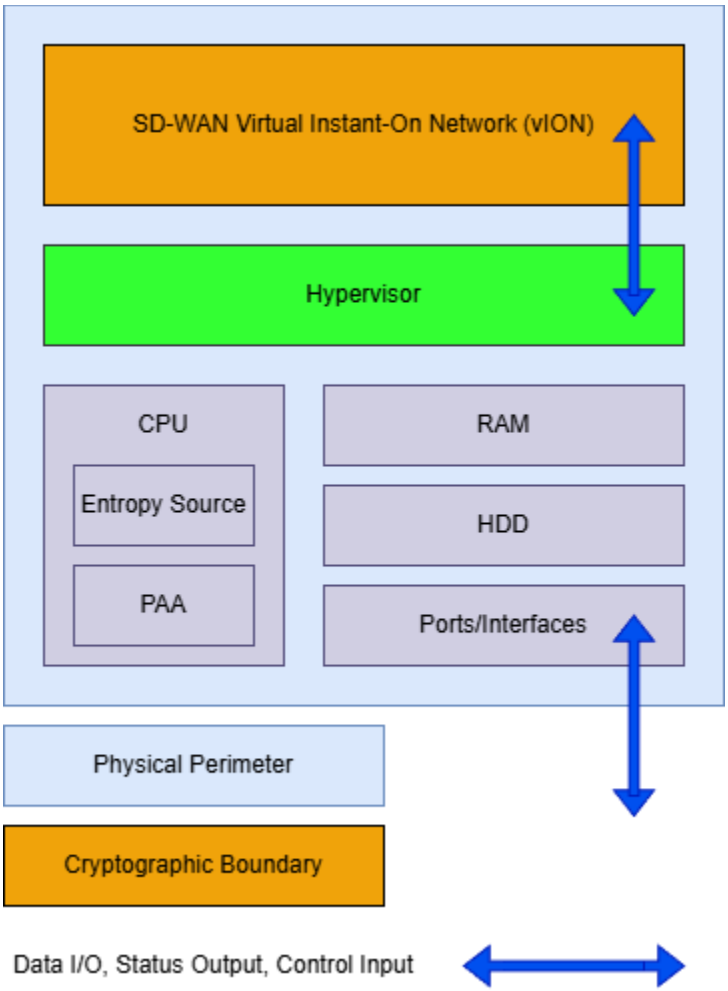


Figure 1– Cryptographic Boundary

## 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 |
|---|---|---|---|
| 3108v-6.4.2-b4-kvm.qcow2 | 6.4.2 | | HMAC-SHA2-256 (HMAC Cert. #A6238) |

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) |
|---|---|---|---|---|---|
| vION | Supermicro SYS-2049-TR | Intel Xeon Gold 6230 | Yes | KVM on Ubuntu 20.04 | 6.4.2 |
| vION | Supermicro SYS-2049-TR | Intel Xeon Gold 6230 | No | KVM on Ubuntu 20.04 | 6.4.2 |

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

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

| Operating System | Hardware Platform |
|---|---|
| vION (3102V/3104V/3108V/7108V) | GPC with ESXi / Hyper-V / KVM |
| vION (7108V) | Dependent on Provider with Azure / AWS / GCP |

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 | A6238 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-CFB128 | A6238 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256 | SP 800-38A |
| AES-CTR | A6238 | Direction - Decrypt, Encrypt<br>Key Length - 128, 192, 256<br>Payload Length - Payload Length: 128<br>Supports Counter larger than maximum value - No<br>Incremental Counter - Yes<br>Counter Tests Performed - Yes | SP 800-38A |
| AES-GCM | A6238 | Direction - Decrypt, Encrypt<br>IV Generation - Internal<br>IV Generation Mode - 8.2.1<br>Key Length - 128, 192, 256<br>Tag Length - 104, 112, 120, 128, 32, 64, 96<br>IV Length - IV Length: 96, 1024<br>Payload Length - Payload Length: 504-1024 Increment 8<br>AAD Length - AAD Length: 0-1024 Increment 8 | SP 800-38D |
| Counter DRBG | A6238 | Prediction Resistance - No, Yes<br>Mode - AES-128, AES-192, AES-256<br>Derivation Function Enabled - Yes | SP 800-90A Rev. 1 |
| ECDSA KeyGen (FIPS186-5) | A6238 | Curve - P-256, P-384, P-521<br>Secret Generation Mode - extra bits, testing candidates | FIPS 186-5 |
| ECDSA SigGen (FIPS186-5) | A6238 | Curve - P-256, P-384, P-521<br>Hash Algorithm - SHA2-256, SHA2-384, SHA2-512<br>Component - No | FIPS 186-5 |
| ECDSA SigVer (FIPS186-5) | A6238 | Curve - P-256, P-384, P-521<br>Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 | FIPS 186-5 |
| HMAC-SHA-1 | A6238 | MAC - MAC: 80-160 Increment 8<br>Key Length - Key Length: 256-1120 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-256 | A6238 | MAC - MAC: 128-256 Increment 8<br>Key Length - Key Length: 256-1120 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-384 | A6238 | MAC - MAC: 192-384 Increment 8<br>Key Length - Key Length: 256-1120 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-512 | A6238 | MAC - MAC: 256-512 Increment 8<br>Key Length - Key Length: 256-1120 Increment 8 | FIPS 198-1 |
| KAS-ECC-SSC Sp800-56Ar3 | A6238 | Domain Parameter Generation Methods - P-256, P-384, P-521<br>Scheme -<br>ephemeralUnified -<br>KAS Role - initiator, responder | SP 800-56A Rev. 3 |
| KDF IKEv2 (CVL) | A6238 | Initiator Nonce Length - Initiator Nonce Length: 512<br>Responder Nonce Length - Responder Nonce | SP 800-135 Rev. 1 |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| | | Length: 512<br>Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 2048<br>Derived Keying Material Length - Derived Keying Material Length: 1056-3072 Increment 8<br>Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512 | |
| KDF SNMP (CVL) | A6238 | Password Length - Password Length: 64, 2048<br>Engine ID - 00100020003000400050, 12345678901234567890 | SP 800-135 Rev. 1 |
| KDF SSH (CVL) | A6238 | Cipher - AES-128, AES-192, AES-256<br>Hash Algorithm - SHA-1, SHA2-256, SHA2-512 | SP 800-135 Rev. 1 |
| RSA KeyGen (FIPS186-5) | A6238 | Key Generation Mode - probable<br>Modulo - 2048, 3072<br>Primality Tests - 2powSecStr<br>Info Generated By Server - No<br>Private Key Format - standard<br>Public Exponent Mode - random | FIPS 186-5 |
| RSA SigGen (FIPS186-5) | A6238 | Modulo - 2048, 3072<br>Signature Type - pkcs1v1.5, pss | FIPS 186-5 |
| RSA SigVer (FIPS186-5) | A6238 | Hash Pair -<br>Hash Algorithm - SHA2-512<br>Modulo - 2048, 3072<br>Signature Type - pkcs1v1.5, pss<br>Mask Function - mgf1<br>Public Exponent Mode - random | FIPS 186-5 |
| SHA-1 | A6238 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |
| SHA2-256 | A6238 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |
| SHA2-384 | A6238 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |
| SHA2-512 | A6238 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |
| TLS v1.2 KDF RFC7627 (CVL) | A6238 | Hash Algorithm - SHA2-256, SHA2-384, SHA2-512<br>Key Block Length - Key Block Length: 1024 | SP 800-135 Rev. 1 |

Table 6: Approved Algorithms - Crypto Library - I

Crypto Library - II

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-CBC | A6239 | Direction - Decrypt, Encrypt<br>Key Length - 128, 256 | SP 800-38A |
| AES-GCM | A6239 | Direction - Decrypt, Encrypt<br>IV Generation - External<br>IV Generation Mode - 8.2.1<br>Key Length - 128, 256<br>Tag Length - 128<br>IV Length - IV Length: 96, 1024<br>Payload Length - Payload Length: 64-256 | SP 800-38D |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| | | Increment 8<br>AAD Length - AAD Length: 0, 256 | |
| Counter DRBG | A6239 | Prediction Resistance - No<br>Supports Reseed - Yes<br>Mode - AES-256<br>Derivation Function Enabled - No<br>Additional Input - Additional Input: 0-384 Increment 16<br>Entropy Input - Entropy Input: 384<br>Nonce - Nonce: 0<br>Personalization String Length - Personalization String Length: 0-384 Increment 16<br>Returned Bits - 2048 | SP 800-90A Rev. 1 |
| HMAC-SHA2-256 | A6239 | MAC - MAC: 128-256 Increment 8<br>Key Length - Key Length: 256-1120 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-384 | A6239 | MAC - MAC: 192-384 Increment 8<br>Key Length - Key Length: 256-1120 Increment 8 | FIPS 198-1 |
| KAS-ECC-SSC Sp800-56Ar3 | A6239 | Domain Parameter Generation Methods - P-256, P-384, P-521<br>Scheme -<br>ephemeralUnified -<br>KAS Role - initiator, responder | SP 800-56A Rev. 3 |
| RSA SigVer (FIPS186-5) | A6239 | Hash Pair -<br>Hash Algorithm - SHA2-224<br>Modulo - 2048<br>Signature Type - pkcs1v1.5<br>Public Exponent Mode - random | FIPS 186-5 |
| SHA2-256 | A6239 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |
| SHA2-384 | A6239 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |
| TLS v1.2 KDF RFC7627 (CVL) | A6239 | Hash Algorithm - SHA2-256, SHA2-384<br>Key Block Length - Key Block Length: 1024 | SP 800-135 Rev. 1 |

Table 7: Approved Algorithms - Crypto Library - II

Crypto Library - III

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-CBC | A6240 | Direction - Decrypt, Encrypt<br>Key Length - 128, 256 | SP 800-38A |
| HMAC-SHA2-256 | A6240 | MAC - MAC: 128-256 Increment 8<br>Key Length - Key Length: 256-1120 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-384 | A6240 | MAC - MAC: 192-384 Increment 8<br>Key Length - Key Length: 256-1120 Increment 8 | FIPS 198-1 |
| HMAC-SHA2-512 | A6240 | MAC - MAC: 256-512 Increment 8<br>Key Length - Key Length: 256-1120 Increment 8 | FIPS 198-1 |
| SHA2-256 | A6240 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |
| SHA2-384 | A6240 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| SHA2-512 | A6240 | Message Length - Message Length: 8-51200 Increment 8 | FIPS 180-4 |

Table 8: Approved Algorithms - Crypto Library - III

**Vendor-Affirmed Algorithms:**

| Name | Properties | Implementation | Reference |
|---|---|---|---|
| CKG | 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 (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: (A6238) CKG: () |
| 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: (A6238, A6239) CKG: () Key Type: Asymmetric |
| 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: (A6238) CKG: () |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| 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: (A6238) KDF SSH: (A6238) |
| 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: (A6239, A6238) TLS v1.2 KDF RFC7627: (A6239, A6238) |
| 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 provides between 128 and 192 bits of encryption strength | KAS-ECC-SSC Sp800-56Ar3: (A6238) Domain Parameter Generation Methods: P-256, P-384 KDF IKEv2: (A6238) |
| 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 | AES-CBC: (A6239) HMAC-SHA2-256: (A6239) HMAC-SHA2-384: (A6239) SHA2-256: (A6239) |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | together with an approved authentication method Caveat:Key establishment methodology provides between 128 and 256 bits of security strength | SHA2-384: (A6239) |
| 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: (A6239) |
| SSH ECDSA KeyGen | AsymKeyPair-KeyGen CKG | ECDSA KeyGen for SSHv2 | | ECDSA KeyGen (FIPS186-5): (A6238) Counter DRBG: (A6238) CKG: () |
| SSH ECDSA SigGen | DigSig-SigGen | ECDSA SigGen for SSHv2 | | ECDSA SigGen (FIPS186-5): (A6238) |
| SSH ECDSA SigVer | DigSig-SigVer | ECDSA SigVer for SSHv2 | | ECDSA SigVer (FIPS186-5): (A6238) |
| TLS RSA KeyGen | AsymKeyPair-KeyGen CKG | RSA KeyGen for TLSv1.2 | | RSA KeyGen (FIPS186-5): (A6238) Counter DRBG: (A6238) CKG: () |
| TLS RSA SigGen | DigSig-SigGen | RSA SigGen for TLSv1.2 | | RSA SigGen (FIPS186-5): (A6238) |
| TLS RSA SigVer | DigSig-SigVer | RSA SigVer for TLSv1.2 | | RSA SigVer (FIPS186-5): (A6239, A6238) |
| IPSec/IKE RSA KeyGen | AsymKeyPair-KeyGen CKG | RSA KeyGen for IPSec/IKEv2 | | RSA KeyGen (FIPS186-5): (A6238) Counter DRBG: |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | (A6238)<br>CKG: () |
| IPSec/IKE RSA SigGen | DigSig-SigGen | RSA SigGen for IPSec/IKEv2 | | RSA SigGen (FIPS186-5): (A6238) |
| IPSec/IKE RSA SigVer | DigSig-SigVer | RSA SigVer for IPSec/IKEv2 | | RSA SigVer (FIPS186-5): (A6238) |
| Session Encryption/Decryption (SSH) | BC-UnAuth | SSHv2 session protection | | AES-CTR: (A6238) |
| Session Encryption/Decryption (TLSv1.2) | BC-Auth<br>BC-UnAuth | TLSv1.2 session protection | | AES-CBC: (A6239, A6238)<br>AES-GCM: (A6239, A6238) |
| Session Encryption/Decryption (IPSec/IKE) | BC-UnAuth | IPSec/IKE session protection | | AES-CBC: (A6238, A6240) |
| Session Encryption/Decryption (SNMPv3) | BC-UnAuth | SNMPv3 session protection | | AES-CFB128: (A6238) |
| Session Authentication (SSHv2) | MAC | SSHv2 session authentication | | HMAC-SHA-1: (A6238)<br>HMAC-SHA2-256: (A6238)<br>HMAC-SHA2-512: (A6238)<br>SHA-1: (A6238)<br>SHA2-256: (A6238)<br>SHA2-512: (A6238) |
| Session Authentication (TLSv1.2) | MAC | TLSv1.2 session authentication | | HMAC-SHA2-256: (A6239, A6238)<br>HMAC-SHA2-384: (A6239, A6238)<br>SHA2-256: (A6239, A6238)<br>SHA2-384: (A6239, A6238) |
| Session Authentication (IPSec/IKE) | MAC | IPSec/IKE session authentication | | HMAC-SHA-1: (A6238)<br>SHA-1: (A6238)<br>HMAC-SHA2-256: (A6238, A6240)<br>HMAC-SHA2-384: (A6238, A6240)<br>HMAC-SHA2- |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | 512: (A6238, A6240)<br>SHA2-256: (A6238, A6240)<br>SHA2-384: (A6238, A6240)<br>SHA2-512: (A6238, A6240) |
| Session Authentication (SMPv3) | MAC | SNMPv3 session authentication | | HMAC-SHA-1: (A6238)<br>SHA-1: (A6238) |
| SSHv2 Keying Materials Development | KAS-135KDF | SSHv2 session keying materials, used to derive SSHv2 session keys. | | KDF SSH: (A6238) |
| TLSv1.2 Keying Materials Development | KAS-135KDF | TLSv1.2 session keying materials, used to derive TLSv1.2 session keys | | TLS v1.2 KDF RFC7627: (A6239, A6238) |
| IPSec/IKE Keying Materials Development | KAS-135KDF | IPSec/IKE session keying materials, used to derive IPSec/IKE session keys | | KDF IKEv2: (A6238) |
| SNMPv3 Keying Materials Development | KAS-135KDF | SNMPv3 session keying materials, used to derive SNMPv3 session keys | | KDF SNMP: (A6238) |
| DRBG Function | DRBG | Used for DRBG generation | | Counter DRBG: (A6238, A6239) |
| Software Load Test | DigSig-SigVer | Signature Verification for software load test | | RSA SigVer (FIPS186-5): (A6238)<br>SHA2-256: (A6238) |

Table 10: Security Function Implementations

## 2.7 Algorithm Specific Information

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.

- 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 |
|---|---|
| E69 | 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 - Skylake 28 Core Die with FCLGA3647 Package | Physical | Intel Xeon Gold 6230 | 128 bits | Full Entropy | A1791 (AES-CBC-MAC) |

Table 12: Entropy Sources

The operational environment is detailed in Entropy Certificate E69 Public Use Document. 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. #A6238, and CTR_DRBG with Algo Cert. #A6239.

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. #A6238) with Derivation Function and CTR_DRBG (Cert.

#A6239) 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.

## 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 13: 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.

## 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<br>- Software Integrity Test Key: E Unauthenticated<br>- Software 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<br>- DRBG Entropy Input (A6238): Z<br>- DRBG Seed (A6238): Z<br>- DRBG Internal State V value (A6238): Z<br>- DRBG Key (A6238): Z<br>- DRBG Entropy Input (A6239): Z<br>- DRBG Seed (A6239): Z<br>- DRBG Internal State V value |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | (A6239): Z<br>- DRBG Key (A6239): Z<br>- TLS RSA Private Key: Z<br>- TLS RSA Public Key: Z<br>- TLS ECDHE Private Key: Z<br>- TLS ECDHE Public Key: Z<br>- Peer TLS ECDHE Public Key: Z<br>- TLS ECDHE Shared Secret: Z<br>- TLS RSA Pre-Master Secret: Z<br>- TLS Master Secret: Z<br>- TLS Session Encryption Key: Z<br>- TLS Session Authentication Key: Z<br>- IPSec/IKE Pre-Shared Secret: Z<br>- IPSec/IKE RSA Private Key: Z<br>- IPSec/IKE RSA Public Key: Z<br>- IPSec/IKE ECDHE Private Key: Z<br>- IPSec/IKE ECDHE Public Key: Z<br>- Peer IPSec/IKE |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | ECDHE Public Key: Z<br>- IPSec/IKE ECDHE Shared Secret: Z<br>- SKEYSEED: Z<br>- IPSec/IKE Session Encryption Key: Z<br>- IPSec/IKE Session Authentication Key: Z<br>- SNMPv3 Authentication Secret: Z<br>- SNMPv3 Session Encryption Key: Z<br>- SNMPv3 Session Authentication Key: Z<br>- SSH ECDHE Private Key: Z<br>- SSH ECDHE Public Key: Z<br>- Peer SSH ECDHE Public Key: Z<br>- SSH ECDHE Shared Secret: Z<br>- SSH ECDSA Private Key: Z<br>- SSH ECDSA Public Key: Z<br>- SSH Session Encryption Key: Z |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - SSH Session Authentication Key: Z |
| Software Update | The module's software is updated to a new version | Approved Mode Indicator and successful Software update completion system log message | Command to upload a new validated software | Status of the updated software installation | Software Load Test | Crypto Officer<br>- Software Load Test Key: E |
| 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 |
| 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<br>DRBG Function | Crypto Officer<br>- SSH ECDSA Private Key: G,W<br>- SSH ECDSA Public Key: G,W<br>- DRBG Entropy Input (A6238): E<br>- DRBG Seed |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | (A6238): E<br>- DRBG Internal State V value<br>(A6238): E<br>- DRBG Key<br>(A6238): E<br>- DRBG Entropy Input<br>(A6239): E<br>- DRBG Seed<br>(A6239): E<br>- DRBG Internal State V value<br>(A6239): E<br>- DRBG Key<br>(A6239): 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<br>KTS (TLSv1.2 with AES and HMAC)<br>KTS (TLSv1.2 with AES-GCM) | Crypto Officer<br>- TLS RSA Private Key: G,W<br>- TLS RSA Public Key: G,W<br>- DRBG Entropy Input<br>(A6238): E<br>- DRBG Seed<br>(A6238): E<br>- DRBG Internal State V value<br>(A6238): E<br>- DRBG Key<br>(A6238): E<br>- DRBG Entropy Input<br>(A6239): E<br>- DRBG Seed<br>(A6239): E<br>- DRBG Internal State V value<br>(A6239): E<br>- DRBG Key<br>(A6239): E |
| Configure SNMPv3 Function | Create a secure SNMPv3 channel | Approved Mode Indicator and | Commands to configure SNMPv3 | Status of the completion of SNMPv3 | KTS (TLSv1.2 with AES and HMAC) | Crypto Officer<br>- SNMPv3 |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | successful SNMPv3 configuration system log message | | configuration | KTS (TLSv1.2 with AES-GCM) | Authentication Secret: W |
| Configure IPSec/IKE v2 Function | Create IPSec/IKE v2 tunnel | Approved Mode Indicator and successful IPSec/IKE v2 configuration system log message | Commands to configure IPSec/IKEv2 | Status of the completion of IPSec/IKEv2 configuration | KTS (TLSv1.2 with AES and HMAC)<br>KTS (TLSv1.2 with AES-GCM)<br>IPSec/IKE RSA KeyGen<br>DRBG Function | Crypto Officer<br>- IPSec/IKE RSA Private Key: G,W<br>- IPSec/IKE RSA Public Key: G,W<br>- IPSec/IKE Pre-Shared Secret: W<br>- DRBG Entropy Input (A6238): E<br>- DRBG Seed (A6238): E<br>- DRBG Internal State V value (A6238): E<br>- DRBG Key (A6238): E<br>- DRBG Entropy Input (A6239): E<br>- DRBG Seed (A6239): E<br>- DRBG Internal State V value (A6239): E<br>- DRBG Key (A6239): 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)<br>KAS-ECC (SSH)<br>SSH ECDSA SigGen<br>SSH ECDSA SigVer<br>Session Encryption/Decryption (SSH)<br>Session Authentication (SSHv2) | Crypto Officer<br>- SSH ECDHE Private Key: G,E,W<br>- SSH ECDHE Public Key: G,W,R<br>- Peer SSH ECDHE Public Key: |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | SSHv2 Keying Materials Development DRBG Function | W,E<br>- SSH ECDHE Shared Secret: G,E<br>- SSH ECDSA Private Key: E<br>- SSH ECDSA Public Key: R<br>- SSH Session Encryption Key: G,E,W<br>- SSH Session Authentication Key: G,E,W<br>- DRBG Entropy Input (A6238): E<br>- DRBG Seed (A6238): E<br>- DRBG Internal State V value (A6238): E<br>- DRBG Key (A6238): E<br>- DRBG Entropy Input (A6239): E<br>- DRBG Seed (A6239): E<br>- DRBG Internal State V value (A6239): E<br>- DRBG Key (A6239): 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)<br>KAS-ECC (TLSv1.2)<br>KTS (TLSv1.2 with AES and HMAC)<br>KTS (TLSv1.2 with AES-GCM)<br>TLS RSA SigGen | Crypto Officer<br>- TLS RSA Private Key: E<br>- TLS RSA Public Key: R<br>- TLS ECDHE Private Key: G,W,E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | TLS RSA SigVer<br>Session Encryption/Decryption (TLSv1.2)<br>Session Authentication (TLSv1.2)<br>TLSv1.2 Keying Materials Development<br>DRBG Function | - TLS ECDHE Public Key: G,W,R<br>- Peer TLS ECDHE Public Key: W,E<br>- TLS ECDHE Shared Secret: G,E,W<br>- TLS RSA Pre-Master Secret: G,E,W<br>- TLS Master Secret: G,W,E<br>- TLS Session Encryption Key: G,W,E<br>- TLS Session Authentication Key: G,W,E<br>- DRBG Entropy Input (A6238): E<br>- DRBG Seed (A6238): E<br>- DRBG Internal State V value (A6238): E<br>- DRBG Key (A6238): E<br>- DRBG Entropy Input (A6239): E<br>- DRBG Seed (A6239): E<br>- DRBG Internal State V value (A6239): E<br>- DRBG Key (A6239): E |
| Run SNMPv2 Function | Negotiation and encrypted | Approved Mode Indicator | Initiate SNMPv3 tunnel | Status of SNMPv3 tunnel | Session Encryption/Decryption (SNMPv3) | Crypto Officer<br>- SNMPv3 |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | data transport via SNMPv3 | and successful SNMPv3 service system log message | establishment request | establishment | Session Authentication (SMPv3)<br>SNMPv3 Keying Materials Development | Authentication Secret: E<br>- SNMPv3 Session Encryption Key: G,W,E<br>- SNMPv3 Session Authentication Key: G,W,E |
| Run IPSec/IKE v2 Function | Negotiation and encrypted data transport via IPSec | Approved Mode Indicator and successful IPSec/IKE v2 service system log message | Initiate IPSec/IKEv2 tunnel establishment request | Status of IPSec/IKEv2 tunnel establishment | KAS-ECC-KeyGen (IPSec/IKE)<br>KAS-ECC (IPSec/IKE)<br>IPSec/IKE RSA SigGen<br>IPSec/IKE RSA SigVer<br>Session Encryption/Decryption (IPSec/IKE)<br>Session Authentication (IPSec/IKE)<br>IPSec/IKE Keying Materials Development<br>DRBG Function | Crypto Officer<br>- IPSec/IKE Pre-Shared Secret: E<br>- IPSec/IKE RSA Private Key: E<br>- IPSec/IKE RSA Public Key: R<br>- IPSec/IKE ECDHE Private Key: G,W,E<br>- IPSec/IKE ECDHE Public Key: G,R<br>- Peer IPSec/IKE ECDHE Public Key: W,E<br>- IPSec/IKE ECDHE Shared Secret: G,W,E<br>- SKEYSEED: G,W,E<br>- IPSec/IKE Session Encryption Key: G,W,E<br>- IPSec/IKE Session Authentication Key: G,W,E<br>- DRBG Entropy Input (A6238): E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - DRBG Seed (A6238): E<br>- DRBG Internal State V value (A6238): E<br>- DRBG Key (A6238): E<br>- DRBG Entropy Input (A6239): E<br>- DRBG Seed (A6239): E<br>- DRBG Internal State V value (A6239): E<br>- DRBG Key (A6239): 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

The module supports the software load test by using RSA 2048 bits with SHA2-256 (RSA Cert. # A6238) for the new validated software to be uploaded into the module. A Software Load Test Key was preloaded to the module's binary at the factory and used for software load test. In order to load new software, the Crypto Officer must authenticate into the module before loading any software. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails. Any firmware/software loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-3 validation.

## 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. #A6238) 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 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 overwrite all SSPs stored in the RAM or in the HDD within the TOEPP with zeros. | "Disable System" command |
| Session Termination | Zeroization upon session termination | Session termination will automatically overwrite all session based temporary SSPs with zeros. | Terminate session |
| Power Down | Operator powers the module off | Powering off the module will overwrite all SSPs stored in the RAM within the TOEPP with zeros. | "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.
4. The Software Load Test Key is only used for Software Load Test Authentication and not subject to the zeroization requirement.

## 9.4 SSPs

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| DRBG Entropy Input (A6238) | Used to seed the DRBG | 256 - 256 bits | Entropy Input - CSP | | | DRBG Function |
| DRBG Seed (A6238) | Used in DRBG Generation | 256 - 256 bits | DRBG Seed - CSP | | | DRBG Function |
| DRBG Internal State V value (A6238) | Used in DRBG Generation | 256 - 256 bits | DRBG Internal State V value - CSP | | | DRBG Function |
| DRBG Key (A6238) | Used in DRBG Generation | 256 - 256 bits | DRBG Key - CSP | | | DRBG Function |
| DRBG Entropy Input (A6239) | Used to seed the DRBG | 256 - 256 bits | Entropy Input - CSP | | | DRBG Function |
| DRBG Seed (A6239) | Used in DRBG Generation | 256 - 256 bits | DRBG Seed - CSP | | | DRBG Function |
| DRBG Internal State V value (A6239) | Used in DRBG Generation | 256 - 256 bits | DRBG Internal State V value - CSP | | | DRBG Function |
| DRBG Key (A6239) | 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 | 2048, 3072 bits | Public Key - PSP | | TLS RSA KeyGen | |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | authentication | - 112, 128 bits | | | | |
| 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 | 2048 bits characters - 2048 bits | Shared Secret - CSP | | | |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| | authentication | characters | | | | |
| 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 |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| IPSec/IKE Session Encryption Key | Used to secure IPSec/IKE session confidentiality | 128, 192 bits - 128, 192 bits | Session Key - CSP | | IPSec/IKE Keying Materials Development | Session Encryption/Decryption (IPSec/IKE) |
| 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 (SMPv3) |
| 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 | Used to derive SSH Session | P-256, P-384, P-521 - | Shared Secret - CSP | | KAS-ECC (SSH) | SSHv2 Keying Materials Development |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| Shared Secret | Encryption Keys, SSH Session Authentication Keys | 128, 192, 256 bits | | | | |
| 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 Load Test Key | Used for Software Load Test | 2048 bits - 112 bits | Public Key - CSP | | | Software Load Test |
| 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 (A6238) |

Table 19: SSP Table 1

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| DRBG Entropy Input (A6238) | | RAM within TOEPP:Plaintext | | Zeroization Command Power Down | |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| DRBG Seed (A6238) | | RAM within TOEPP:Plaintext | | Zeroization Command Power Down | |
| DRBG Internal State V value (A6238) | | RAM within TOEPP:Plaintext | | Zeroization Command Power Down | |
| DRBG Key (A6238) | | RAM within TOEPP:Plaintext | | Zeroization Command Power Down | |
| DRBG Entropy Input (A6239) | | RAM within TOEPP:Plaintext | | Zeroization Command Power Down | |
| DRBG Seed (A6239) | | RAM within TOEPP:Plaintext | | Zeroization Command Power Down | |
| DRBG Internal State V value (A6239) | | RAM within TOEPP:Plaintext | | Zeroization Command Power Down | |
| DRBG Key (A6239) | | 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 | RAM within TOEPP:Plaintext | While TLS tunnel is on | Zeroization Command Power Down Session Termination | |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| | decrypted by AES-GCM | | | | |
| TLS Master Secret | | RAM within TOEPP:Plaintext | While TLS tunnel is on | Zeroization Command Power Down 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 | |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| SKEYSEED | | RAM within TOEPP:Plaintext | While IPSec/IKEv2 tunnel is on | Zeroization Command Power Down Session Termination | |
| 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 | |

| 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 | | 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 Load Test Key | | HDD within TOEPP:Plaintext | | N/A | |
| Software Integrity Test Key | | HDD within TOEPP:Plaintext | | N/A | |

Table 20: 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.

Minimum Key Size
The module implements keys that are 112 bits in strength. This implementation will be non-Approved for all uses starting January 1, 2031. At this time, the user should move to keys of 128 bit strength or greater.

## 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

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 (A6238) | 256 bits | KAT | CAST | Module is in normal state | Encrypt | Power Up |
| AES-CBC Decrypt KAT (A6238) | 256 bits | KAT | CAST | Module is in normal state | Decrypt | Power Up |
| AES-GCM Encrypt KAT (A6238) | 256 bits | KAT | CAST | Module is in normal state | Encrypt | Power Up |
| AES-GCM Decrypt KAT (A6238) | 256 bits | KAT | CAST | Module is in normal state | Decrypt | Power Up |
| Counter DRBG Instantiate KAT (A6238) | AES-256 | KAT | CAST | Module is in normal state | Instantiate KAT | Power Up |
| Counter DRBG Generate KAT (A6238) | AES-256 | KAT | CAST | Module is in normal state | Generate KAT | Power Up |
| Counter DRBG Reseed KAT (A6238) | AES-256 | KAT | CAST | Module is in normal state | Reseed KAT | Power Up |
| ECDSA SigGen (FIPS186-5) KAT (A6238) | P-224 with SHA2-256 | KAT | CAST | Module is in normal state | Sign | Power Up |
| ECDSA SigVer (FIPS186-5) KAT (A6238) | P-224 with SHA2-256 | KAT | CAST | Module is in normal state | Verify | Power Up |
| SHA-1 KAT (A6238) | Message Length: 8-51200 Increment 8 | KAT | CAST | Module is in normal state | N/A | Power Up |
| HMAC-SHA-1 KAT (A6238) | HMAC-SHA-1 | KAT | CAST | Module is in normal state | N/A | Power Up |
| HMAC-SHA2-256 KAT (A6238) | HMAC-SHA2-256 | KAT | CAST | Module is in normal state | N/A | Power Up |
| HMAC-SHA2-384 KAT (A6238) | HMAC-SHA2-384 | KAT | CAST | Module is in normal state | N/A | Power Up |
| HMAC-SHA2-512 KAT (A6238) | HMAC-SHA2-512 | KAT | CAST | Module is in normal state | N/A | Power Up |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| RSA SigGen (FIPS186-5) KAT (A6238) | 2048 bit modulus with SHA2-256 | KAT | CAST | Module is in normal state | Sign | Power Up |
| RSA SigVer (FIPS186-5) KAT (A6238) | 2048 bit modulus with SHA2-256 | KAT | CAST | Module is in normal state | Verify | Power Up |
| KAS-ECC-SSC Sp800-56Ar3 KAT (A6238) | Curve P-256 | KAT | CAST | Module is in normal state | N/A | Power Up |
| KDF IKEv2 KAT (A6238) | N/A | KAT | CAST | Module is in normal state | N/A | Power Up |
| KDF SSH KAT (A6238) | N/A | KAT | CAST | Module is in normal state | N/A | Power Up |
| KDF SNMP KAT (A6238) | N/A | KAT | CAST | Module is in normal state | N/A | Power Up |
| TLS v1.2 KDF RFC7627 KAT (A6238) | N/A | KAT | CAST | Module is in normal state | N/A | Power Up |
| RSA KeyGen (FIPS186-5) PCT (A6238) | 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 (A6238) | 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 (A6238) | 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 (A6239) | 256 bits | KAT | CAST | Module is in normal state | Encrypt | Power Up |
| AES-CBC Decrypt KAT (A6239) | 256 bits | KAT | CAST | Module is in normal state | Decrypt | Power Up |
| AES-GCM Encrypt KAT(A6239) | 256 bits | KAT | CAST | Module is in normal state | Encrypt | Power Up |
| AES-GCM Decrypt KAT (A6239) | 256 bits | KAT | CAST | Module is in normal state | Decrypt | Power Up |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| Counter DRBG Instantiate KAT (A6239) | AES-256 | KAT | CAST | Module is in normal state | Instantiate KAT | Power Up |
| Counter DRBG Generate KAT (A6239) | AES-256 | KAT | CAST | Module is in normal state | Generate KAT | Power Up |
| Counter DRBG Reseed KAT (A6239) | AES-256 | KAT | CAST | Module is in normal state | Reseed KAT | Power Up |
| RSA SigVer (FIPS186-5) KAT (A6239) | 2048 bit modulus with SHA2-256 | KAT | CAST | Module is in normal state | Verify | Power Up |
| HMAC-SHA2-256 KAT (A6239) | HMAC-SHA2-256 | KAT | CAST | Module is in normal state | N/A | Power Up |
| HMAC-SHA2-384 KAT (A6239) | HMAC-SHA2-384 | KAT | CAST | Module is in normal state | N/A | Power Up |
| KAS-ECC-SSC Sp800-56Ar3 KAT (A6239) | Curve P-256 | KAT | CAST | Module is in normal state | N/A | Power Up |
| TLS v1.2 KDF RFC7627 KAT (A6239) | N/A | KAT | CAST | Module is in normal state | N/A | Power Up |
| KAS-ECC-SSC Sp800-56Ar3 PCT (A6239) | 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 (A6240) | 256 bits | KAT | CAST | Module is in normal state | Encrypt | Power Up |
| AES-CBC Decrypt KAT(A6240) | 256 bits | KAT | CAST | Module is in normal state | Decrypt | Power Up |
| HMAC-SHA2-256 KAT (A6240) | HMAC-SHA2-256 | KAT | CAST | Module is in normal state | N/A | Power Up |
| HMAC-SHA2-512 KAT (A6240) | HMAC-SHA2-512 | KAT | CAST | Module is in normal state | N/A | Power Up |
| Software Load Test | RSA 2048 SigVer with SHA2-256 | KAT | SW/FW Load | Module is in normal state | Verify | When software has been uploaded to the module. |

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 (A6238) | KAT | CAST | 60 Days | Reboot |
| AES-CBC Decrypt KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| AES-GCM Encrypt KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| AES-GCM Decrypt KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| Counter DRBG Instantiate KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| Counter DRBG Generate KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| Counter DRBG Reseed KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| ECDSA SigGen (FIPS186-5) KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| ECDSA SigVer (FIPS186-5) KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| SHA-1 KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| HMAC-SHA-1 KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| HMAC-SHA2-256 KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| HMAC-SHA2-384 KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| HMAC-SHA2-512 KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| RSA SigGen (FIPS186-5) KAT (A6238) | KAT | CAST | 60 Days | Reboot |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| RSA SigVer (FIPS186-5) KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| KAS-ECC-SSC Sp800-56Ar3 KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| KDF IKEv2 KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| KDF SSH KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| KDF SNMP KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| TLS v1.2 KDF RFC7627 KAT (A6238) | KAT | CAST | 60 Days | Reboot |
| RSA KeyGen (FIPS186-5) PCT (A6238) | PCT | PCT | 60 Days | Reboot |
| ECDSA KeyGen (FIPS186-5) PCT (A6238) | PCT | PCT | 60 Days | Reboot |
| KAS-ECC-SSC Sp800-56Ar3 PCT (A6238) | PCT | PCT | 60 Days | Reboot |
| AES-CBC Encrypt KAT (A6239) | KAT | CAST | 60 Days | Reboot |
| AES-CBC Decrypt KAT (A6239) | KAT | CAST | 60 Days | Reboot |
| AES-GCM Encrypt KAT(A6239) | KAT | CAST | 60 Days | Reboot |
| AES-GCM Decrypt KAT (A6239) | KAT | CAST | 60 Days | Reboot |
| Counter DRBG Instantiate KAT (A6239) | KAT | CAST | 60 Days | Reboot |
| Counter DRBG Generate KAT (A6239) | KAT | CAST | 60 Days | Reboot |
| Counter DRBG Reseed KAT (A6239) | KAT | CAST | 60 Days | Reboot |
| RSA SigVer (FIPS186-5) KAT (A6239) | KAT | CAST | 60 Days | Reboot |
| HMAC-SHA2-256 KAT (A6239) | KAT | CAST | 60 Days | Reboot |
| HMAC-SHA2-384 KAT (A6239) | KAT | CAST | 60 Days | Reboot |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| KAS-ECC-SSC Sp800-56Ar3 KAT (A6239) | KAT | CAST | 60 Days | Reboot |
| TLS v1.2 KDF RFC7627 KAT (A6239) | KAT | CAST | 60 Days | Reboot |
| KAS-ECC-SSC Sp800-56Ar3 PCT (A6239) | PCT | PCT | 60 Days | Reboot |
| AES-CBC Encrypt KAT (A6240) | KAT | CAST | 60 Days | Reboot |
| AES-CBC Decrypt KAT(A6240) | KAT | CAST | 60 Days | Reboot |
| HMAC-SHA2-256 KAT (A6240) | KAT | CAST | 60 Days | Reboot |
| HMAC-SHA2-512 KAT (A6240) | KAT | CAST | 60 Days | Reboot |
| Software Load Test | KAT | SW/FW Load | 60 Days | Reboot |

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 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 Software Load Test: \"Verification Failure\"; Failed SP 800-90B Entropy Source Start-up/Continuous health tests: No random numbers are generated and key generation is halted |

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

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

Software is available on Palo Alto Networks' support site, which uses TLS 1.2 during the download process. The support site also provides a SHA2-256 checksum that Crypto Officers can use to verify the integrity of the module once it has been transferred/downloaded.

### 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 6.4.2, which is the only allowable software image for this current approved mode of operation. The module is initiated into the Approved mode of operation via the following procedure:

1. Install the vION on the platform
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”
3) Confirm command
4) 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.