Cisco Systems, Inc.

Cisco Adaptive Security Appliance Cryptographic Module (FPR 2100 Series)

FIPS 140-3 Non-Proprietary Security Policy

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This is Cisco Systems, Inc. non-proprietary security policy for the Cisco Adaptive Security Appliance Cryptographic Module (FPR 2100 Series) (hereinafter referred to as ASA or Module), version 9.20. The following details how this module meets the security requirements of FIPS 140-3, SP 800-140 and ISO/IEC 19790 for a Security Level 2 Hardware cryptographic module.

The security requirements cover areas related to the design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operational environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks. The following table indicates the actual security levels for each area of the cryptographic module.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	3
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

This module is a multi-chip standalone hardware cryptographic module deployed under the Next-Generation Firewall (NGFW) with Adaptive Security Appliance (ASA). The module's operational environment is Limited**.**

ASA delivers enterprise-class firewall for businesses, improving security at the Internet edge, high performance and throughput for demanding enterprise data centers. The ASA solution offers the combination of the industry's most deployed stateful firewall with a comprehensive range of next-generation network security services, intrusion prevention system (IPS), content

security and secure unified communications, HTTPS/TLSv1.2, SSHv2, IPsec/IKEv2, SNMPv3 and Cryptographic Cipher Suite B using the ASA Cryptographic Module.

Module Type: Hardware

Module Embodiment: MultiChipStand

Module Characteristics:

Cryptographic Boundary:

The cryptographic boundary is defined as the entire chassis unit's physical perimeter encompassing the "top," "front," "left," "right," "rear" and "bottom" surfaces of the case, and shown in the figures below and in the Physical Security section. The FPR 2110 and FPR 2120 have the same exterior features while FPR 2130 and FPR 2140 have the same exterior features. Where they differ is in Firewall throughput, IPS throughput, IPsec VPN throughput and number of VPN peers allowed.

Figure 1 FPR 2110 and FPR 2120

Figure 2 FPR 2130 and FPR 2140

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
FRP 2110	FPR-2110	9.20	Intel Xeon D-1526 (Broadwell), Octeon III Family Crypto Engine	
FRP 2120	FPR-2120	9.20	Intel Xeon D-1528 (Broadwell), Octeon III Family Crypto Engine	

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
FRP 2130	FPR-2130	9.20	Intel Xeon D-1548 (Broadwell), Octeon III Family Crypto Engine	
FRP 2140	FPR-2140	9.20	Intel Xeon D-1577 (Broadwell), Octeon III Family Crypto Engine	

Table 2: Tested Module Identification – Hardware

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

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

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

N/A for this module.

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 of Operation	The module is always in the approved mode of operation after initial operations are performed.	Approved	Approved mode indicator: "FIPS is currently enabled."

Table 3: 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:

CiscoSSL FOM Cryptographic Implementation

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4446	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A4446	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
Counter DRBG	A4446	Prediction Resistance - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A4446	Curve - P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4446	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4446	Curve - P-256, P-384, P-521	FIPS 186-4
HMAC-SHA-1	A4446	Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-224	A4446	Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4446	Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4446	Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4446	Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4446	Domain Parameter Generation Methods - P-256, P-384, P-521	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A4446	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A4446	Diffie-Hellman Shared Secret Length - Diffie-Hellman Shared Secret Length: 2048 Derived Keying Material Length - Derived Keying Material Length: 3072 Hash Algorithm - SHA-1	SP 800-135 Rev. 1
KDF SNMP (CVL)	A4446	Password Length - Password Length: 256, 64	SP 800-135 Rev. 1
KDF SSH (CVL)	A4446	Cipher - AES-128, AES-192, AES-256	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A4446	Key Generation Mode - B.3.4 Modulo - 2048, 3072 Hash Algorithm - SHA2-256 Private Key Format - Standard	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
RSA SigGen (FIPS186-4)	A4446	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072	FIPS 186-4
RSA SigVer (FIPS186-4)	A4446	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072	FIPS 186-4
Safe Primes Key Generation	A4446	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, modp-2048, modp-3072, modp-4096	SP 800-56A Rev. 3
SHA-1	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-224	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A4446	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4446	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1

Table 4: Approved Algorithms - CiscoSSL FOM Cryptographic Implementation

Octeon III Family Crypyto Engine

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	AES 3301	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	AES 3301	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 192, 256	SP 800-38D
Hash DRBG	DRBG 819	Prediction Resistance - No Mode - SHA2-512	SP 800-90A Rev. 1
HMAC-SHA-1	HMAC 2095	-	FIPS 198-1
HMAC-SHA2-256	HMAC 2095	-	FIPS 198-1
HMAC-SHA2-384	HMAC 2095	-	FIPS 198-1
HMAC-SHA2-512	HMAC 2095	-	FIPS 198-1
SHA-1	SHS 2737	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-256	SHS 2737	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-384	SHS 2737	Message Length - Message Length: 8-102400 Increment 8	FIPS 180-4
SHA2-512	SHS 2737	Message Length - Message Length: 8-102400 Increment 8	FIPS 180-4

Table 5: Approved Algorithms - Octeon III Family Crypyto Engine

Vendor-Affirmed Algorithms:

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

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KAS-ECC-KeyGen (SSHv2)	KAS-KeyGen CKG	KAS ECC keygen used in SSHv2 service	Keysize:128 to 256 bits encryption strength	Counter DRBG: (A4446) Hash DRBG: (DRBG 819) CKG: ()
KAS-FFC-KeyGen (SSHv2)	KAS-KeyGen CKG	KAS FFC keygen used in SSHv2 service	Keysize:112 to 152 bits encryption strength	Counter DRBG: (A4446) Hash DRBG: (DRBG 819) Safe Primes Key Generation: (A4446) Safe Prime Groups: modp-2048, modp-3072, modp-4096 CKG: ()
KAS-ECC-KeyGen (TLSv1.2)	KAS-KeyGen CKG	KAS ECC keygen used in TLSv1.2 service	Keysize:128 to 256 bits encryption strength	Counter DRBG: (A4446) Hash DRBG:

Name	Type	Description	Properties	Algorithms
				(DRBG 819) CKG: ()
KAS-FFC-KeyGen (TLSv1.2)	KAS-KeyGen CKG	KAS FFC keygen used in TLSv1.2 service	Keysize:112 to 152 bits encryption strength	Counter DRBG: (A4446) Hash DRBG: (DRBG 819) Safe Primes Key Generation: (A4446) Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096 CKG: ()
KAS-ECC-KeyGen (IKEv2)	KAS-KeyGen CKG	KAS ECC keygen used in TLSv1.2 service	Keysize:128 to 256 bits encryption strength	Counter DRBG: (A4446) Hash DRBG: (DRBG 819) CKG: ()
KAS-FFC-KeyGen (IKEv2)	KAS-KeyGen CKG	KAS FFC keygen used in IKEv2 service	Keysize:112 to 152 bits encryption strength	Counter DRBG: (A4446) Hash DRBG: (DRBG 819) Safe Primes Key Generation: (A4446) Safe Prime Groups: modp-2048, modp-3072, modp-4096 CKG: ()
KAS-ECC (SSHv2)	KAS-Full	KAS-ECC for SSHv2 service	Security Strength:Provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A4446) KDF SSH: (A4446)
KAS-FFC (SSHv2)	KAS-Full	KAS-FFC SSHv2 service	Security Strength:Provides between 112 to 152 bits of encryption strength	KDF SSH: (A4446) KAS-FFC-SSC Sp800-56Ar3: (A4446) Safe-Prime Groups:: modp-2048, modp-3072, modp-4096

Name	Type	Description	Properties	Algorithms
KAS-ECC (TLSv1.2)	KAS-Full	KAS-ECC for TLSv1.2 service	Security Strength:Provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A4446) TLS v1.2 KDF RFC7627: (A4446)
KAS-FFC (TLSv1.2)	KAS-Full	KAS-FFC for TLSv1.2 service	Security Strength:Provides 112-152 bits of encryption strength	TLS v1.2 KDF RFC7627: (A4446) KAS-FFC-SSC Sp800-56Ar3: (A4446) Safe-Prime Groups: ffdhe2048, ffdhe3082, ffdhe4096
KAS-ECC (IKEv2)	KAS-Full	KAS-ECC for IKEv2 Service	Security Strength:Provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A4446) KDF IKEv2: (A4446)
KAS-FFC (IKEv2)	KAS-Full	KAS-FFC for IKEv2 service	Security Strength:Provides between 112 and 152 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3: (A4446) Safe-Prime Groups: modp-2048, modp-3072, modp-4096 KDF IKEv2: (A4446)
KTS (TLSv1.2 with AES and HMAC)	KTS-Wrap	KTS via TLSv1.2 service by using AES and HMAC	Security Strength:Provides between 128 and 256 bits of encryption strength	AES-CBC: (A4446) Key Length: 128, 256 HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) HMAC-SHA2-384: (A4446) SHA-1: (A4446) SHA2-256: (A4446) SHA2-384: (A4446)

Name	Type	Description	Properties	Algorithms
KTS (TLSv1.2 with AES-GCM)	KTS-Wrap	KTS via TLSv1.2 service by using AES-GCM	Security Strength:Provides between 128 and 256 bits of encryption strength	AES-GCM: (A4446) Key Length: 128, 256
KTS (SSHv2 with AES and HMAC)	KTS-Wrap	KTS via SSHv2 service by using AES and HMAC	Security Strength:Provides between 128 and 256 bits of encryption strength	AES-CBC: (A4446) Key Length: 128, 256 HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) SHA-1: (A4446) SHA2-256: (A4446)
KTS (SSHv2 with AES-GCM)	KTS-Wrap	KTS via SSHv2 service by using AES-GCM	Security Strength:Provides between 128 and 256 bits of encryption strength	AES-GCM: (A4446) Key Length: 128, 256
RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	AsymKeyPair-KeyGen CKG	RSA KeyGen for SSHv2, TLSv1.2, and IKEv2 services		RSA KeyGen (FIPS186-4): (A4446) Counter DRBG: (A4446) Hash DRBG: (DRBG 819) CKG: ()
ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for TLSv1.2 and IKEv2 services		ECDSA KeyGen (FIPS186-4): (A4446) Counter DRBG: (A4446) Hash DRBG: (DRBG 819) CKG: ()
RSA SigGen (SSHv2, TLSv1.2, IKEv2)	DigSig-SigGen	RSA SigGen for SSHv2, TLSv1.2, and IKEv2 services		RSA SigGen (FIPS186-4): (A4446)
ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)	DigSig-SigGen	ECDSA SigGen for TLSv1.2, and IKEv2 services		ECDSA SigGen (FIPS186-4): (A4446)

Name	Type	Description	Properties	Algorithms
RSA SigVer (SSHv2, TLSv1.2, and IKEv2)	DigSig-SigVer	RSA SigVer for SSHv2, TLSv1.2, and IKEv2 services		RSA SigVer (FIPS186-4): (A4446)
ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2)	DigSig-SigVer	ECDSA SigVer for TLSv1.2 and IKEv2 services		ECDSA SigVer (FIPS186-4): (A4446)
Block Cipher (SSHv2)	BC-Auth BC-UnAuth	Block Cipher for SSHv2 service		AES-CBC: (A4446) Key Length: 128, 256 AES-GCM: (A4446) Key Length: 128, 256
Block Cipher (TLSv1.2)	BC-Auth BC-UnAuth	Block Cipher for TLSv1.2 service		AES-GCM: (A4446) Key Length: 128, 256 AES-CBC: (A4446) Key Length: 128, 256
Block Cipher (IPSec/IKE)	BC-Auth BC-UnAuth	Block Cipher for IPSec/IKEv2 service		AES-CBC: (A4446, AES 3301) AES-GCM: (A4446, AES 3301)
Block Cipher (SNMPv3)	BC-UnAuth	Block Cipher for SNMPv3 service		AES-CBC: (A4446) KDF SNMP: (A4446)
MAC (SSHv2)	MAC	MAC for SSHv2 service		HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) SHA-1: (A4446) SHA2-256: (A4446)
MAC (TLSv1.2)	MAC	Message Authentication for TLSv1.2 services		HMAC-SHA-1: (A4446) HMAC-SHA2-256: (A4446) HMAC-SHA2-384: (A4446) SHA-1: (A4446) SHA2-256:

Name	Type	Description	Properties	Algorithms
				(A4446) SHA2-384: (A4446)
MAC (IPSec/IKEv2)	MAC	Message Authentication for IPSec/IKEv2 services		HMAC-SHA2-256: (A4446, HMAC 2095) HMAC-SHA2-384: (A4446, HMAC 2095) HMAC-SHA2-512: (A4446, HMAC 2095) SHA2-256: (A4446, SHS 2737) SHA2-384: (A4446, SHS 2737) SHA2-512: (A4446, SHS 2737) HMAC-SHA-1: (HMAC 2095) SHA-1: (SHS 2737)
MAC (SNMPv3)	MAC	Message Authentication for SNMPv3 service		HMAC-SHA-1: (A4446) SHA-1: (A4446) KDF SNMP: (A4446) HMAC-SHA2-256: (A4446) HMAC-SHA2-384: (A4446) SHA2-256: (A4446) SHA2-384: (A4446) HMAC-SHA2-224: (A4446) SHA2-224: (A4446)
Firmware Load Test	MAC	MAC for firmware load test		HMAC-SHA2-512: (A4446)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

- The module's AES-GCM implementation conforms to Implementation Guidance 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 SP 800-52 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. 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.

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

2.8 RBG and Entropy

Cert Number	Vendor Name
E3	Cisco Systems, Inc.

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Cisco Jitter Entropy Source	Non-Physical	Intel Xeon D-1526 (Broadwell), Intel Xeon D-1528 (Broadwell), Intel Xeon D-1548 (Broadwell), Intel Xeon D-1577(Broadwell)	256 bits	Full Entropy	A2810 (SHA3-256)

Table 9: Entropy Sources

The module implements two approved DRBGs based on SP800-90Arev1, including CRT_DRBG with Algo Cert. #A4446, and HASH_DRBG with DRBG Algo Cert. #819.

Those two DRBGs are used internally by the module (e.g. to generate symmetric keys, seeds for asymmetric key pairs, and random numbers for security functions).

Each DRBG is seeded by the entropy source described in the table above. The CTR_DRBG (AES-128/192/256) enables Derivation Function capability, and the HASH_DRBG (SHA2-512) doesn't support Prediction Resistance. Each DRBG is instantiated with a 384-bits long entropy input (corresponding to 384 bits of entropy) and provides at least 256 bits security strength for the cryptographic keys generation while in the approved mode.

The Cisco JENT entropy source implementation generates an output that is considered to have full entropy. More information can be found in the public use document for ESV cert #E3.

2.9 Key Generation

The module generates RSA, ECDSA, ECDH, and DH asymmetric key pairs compliant with FIPS 186-4, using a NIST SP 800-90Arev1 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-FFC 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-FFC shared secret computation. The shared secret computation provides between 112 and 152 bits of encryption strength.

  - The module supports the use of the safe primes defined in RFC 4419 (SSH), RFC 7919 (TLS) and RFC 3526 (IKE).

    - SSH (RFC 4419):
      MODP-2048 (ID = 14)
      MODP-3072 (ID = 15)
      MODP-4096 (ID = 16)

    - TLS (RFC 7919):
      ffdhe2048 (ID = 256)
      ffdhe3072 (ID = 257)
      ffdhe4096 (ID = 258)

    - IKE (RFC 3526):
      MODP-2048 (ID = 14)
      MODP-3072 (ID = 15)
      MODP-4096 (ID = 16)

- 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 SSPs Table for more information. No parts of IPSec/IKEv2, SNMPv3, SSH and TLS 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
Ethernet Port, SFP (1G) port, SFP+ (10G) port, and Console Port	Data Input	Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data.
Ethernet Port, SFP (1G) port, SFP+ (10G) port and Console Port	Data Output	Data output from the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data.
Ethernet Port, SFP (1G) port, SFP+ (10G) port, Console Port and RESET	Control Input	Control Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and IPsec/IKEv2 service data.
Ethernet Port, SFP (1G) port, SFP+ (10G) port, Console Port and LEDs	Status Output	Status Information output from the module.
N/A	Control Output	N/A
Power	Power	Provide the Power Supply to the module.

Table 10: Ports and Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Table 2. The module provides physical ports which are mapped to logical interfaces provided by the module (data input, data output, control input, control output and status output) as above.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password	The minimum length is eight (8) characters (94 possible characters). The configuration supports at most ten failed attempts to authenticate in a one-minute period.	Password Based	The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8) which is less than 1/1,000,000.	The probability of successfully authenticating to the module within one minute is 10/(94^8), which is less than 1/100,000.
RSA-Based Certificate	The modules support RSA public-key based authentication mechanism using a minimum of RSA 2048 bits, which provides 112 bits of security strength. The probability that a random attempt will succeed is 1/(2^112) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^112), which is less than 1/100,000.	RSA SigVer (FIPS186-4) (A4446)	The probability that a random attempt will succeed is 1/(2^112). Please refer to Description section in this table for more details	the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^112). Please refer to Description section in this table for more details
ECDSA-Based Certificate	The modules support ECDSA public-key based authentication mechanism using a	ECDSA SigVer (FIPS186-4) (A4446)	The probability that a random attempt will succeed is	the probability of successfully authenticating to the module within a one

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	minimum of curve P-256, which provides 128 bits of security strength. The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^128), which is less than 1/100,000.		1/(2^128) which is less than 1/1,000,000. Please refer to Description section in this table for more details	minute period is 17,000 * 60 = 1,020,000/(2^128). Please refer to Description section in this table for more details

Table 11: Authentication Methods

The module implements identity-based authentication. The module supports Crypto Officer role and the User role. The module also allows the concurrent operators.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	Password RSA-Based Certificate ECDSA-Based Certificate
User	Identity	User	Password RSA-Based Certificate ECDSA-Based Certificate

Table 12: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status	Provide Module's current status (return codes and/or syslog messages)	Global Indicator or Syslog Message	Command used to show Module's Status	Module's Operational Status	None	Crypto Officer User
Show Version	Provide Module's name and version information	Console Message	Command to show version	Module's ID and versioning information	None	Crypto Officer User
Perform Self-Tests	Reload the module to perform Self-Tests (Pre-operational self-test and Conditional Self-Tests)	Global Indicator or syslog message	Command to trigger reload or Removal and reconnection of power supply	Status of the self-tests results	None	Crypto Officer User Unauthenticated
Perform Zeroization	Perform Zeroization	Syslog message	Command to zeroize the module	Status of the SSPs zeroization	None	Crypto Officer - DRBG Entropy Input: Z - DRBG Seed: Z - DRBG Internal State (V, Key): Z - DRBG Internal State (V, C): Z - User Password: Z - Crypto Officer Password: Z - RADIUS Secret: Z - TACACS+ Secret: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Firmware Load Test Key: Z - SSH DH Private Key: Z - SSH DH Public Key: Z - SSH Peer DH Public Key: Z - SSH DH Shared Secret: Z - SSH ECDH Private Key: Z - SSH ECDH Public Key: Z - SSH Peer ECDH Public Key: Z - SSH ECDH Shared Secret: Z - SSH RSA Private Key: Z - SSH RSA Public Key: Z - SSH ECDSA Private Key: Z - SSH ECDSA Public Key: Z - SSH Session Encryption Key: Z - SSH Session Authenticatio

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						n Key: Z - TLS DH Private Key: Z - TLS DH Public Key: Z - TLS Peer DH Public Key: Z - TLS DH Shared Secret: Z - TLS ECDH Private Key: Z - TLS ECDH Public Key: Z - TLS Peer ECDH Public Key: Z - TLS ECDH Shared Secret: Z - TLS ECDSA Private Key: Z - TLS ECDSA Public Key: Z - TLS RSA Private Key: Z - TLS RSA Public Key: Z - TLS Master Secret: Z - TLS Session Encryption Key: Z - TLS Session Authenticatio

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						n Key: Z - IPSec/IKE DH Private Key: Z - IPSec/IKE DH Public Key: Z - IPSec/IKE Peer DH Public Key: Z - IPSec/IKE DH Shared Secret: Z - IPSec/IKE ECDH Private Key: Z - IPSec/IKE ECDH Public Key: Z - IPSec/IKE Peer ECDH Public Key: Z - IPSec/IKE ECDH Shared Secret: Z - IPSec/IKE ECDSA Private Key: Z - IPSec/IKE ECDSA Public Key: Z - IPSec/IKE RSA Private Key: Z - IPSec/IKE RSA Public Key: Z - IPSec/IKE Pre-shared Secret: Z - SKEYSEED:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - IPSec/IKE Session Encryption Key: Z - IPSec/IKE Authentication Key: Z - SNMPv3 Shared Secret: Z - SNMPv3 Encryption Key: Z - SNMPv3 Authentication Key: Z
Configure Network	Sets configuration of the systems	None	Commands to configure the network	Status of the completion of network configuration status	None	Crypto Officer
Crypto Officer Authentication	CO Role Authentication	N/A	CO Authentication Request	Status of the CO authentication	None	Crypto Officer - Crypto Officer Password: W,Z
User Authentication	User Role Authentication	N/A	User role authentication request	Status of the User role authentication	None	User - User Password: W,Z
Configure Bypass Capability	Sets the Bypass capability	None	CLI Bypass commands	Status of the completion of Bypass capability configuration	None	Crypto Officer
Configure SSHv2 Function	Configure SSHv2 Function	Global Indicator and SSHv2 configuration success	Commands to configure SSHv2	Status of the completion of the SSHv2 configuration	KAS-ECC-KeyGen (SSHv2) KAS-FFC-KeyGen (SSHv2) KAS-ECC	Crypto Officer - SSH DH Private Key: W,E - SSH DH Public Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		status message			(SSHv2) KAS-FFC (SSHv2) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Block Cipher (SSHv2) MAC (SSHv2)	W,E - SSH Peer DH Public Key: W,E - SSH DH Shared Secret: W,E - SSH ECDH Private Key: W,E - SSH ECDH Public Key: W,E - SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: W,E - SSH RSA Private Key: W,E - SSH RSA Public Key: W,E - SSH ECDSA Private Key: W,E - SSH ECDSA Public Key: W,E - SSH Session Encryption Key: W,E - SSH Session Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						State (V, Key): W,E - DRBG Internal State (V, C): W,E - RADIUS Secret: W - TACACS+ Secret: W
Configure HTTPS over TLSv1.2 Function	Configure HTTPS over TLSv1.2 Function	Global Indicator and HTTPS over TLSv1.2 configuration success status message	Commands to configure TLSv1.2	Status of the completion of TLSv1.2 configuration	KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (TLSv1.2) KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2)	Crypto Officer - TLS DH Private Key: W,E - TLS DH Public Key: W,E - TLS Peer DH Public Key: W,E - TLS DH Shared Secret: W,E - TLS ECDH Private Key: W,E - TLS ECDH Public Key: W,E - TLS Peer ECDH Public Key: W,E - TLS ECDH Shared Secret: W,E - TLS ECDSA Private Key: W,E - TLS ECDSA Public Key: W,E - TLS RSA Private Key: W,E - TLS RSA

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Block Cipher (TLSv1.2) MAC (TLSv1.2)	Public Key: W,E - TLS Master Secret: W,E - TLS Session Encryption Key: W,E - TLS Session Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State (V, Key): W,E - DRBG Internal State (V, C): W,E
Configure IPsec/IKEv2 Function	Configure IPSec/IKEv2 Function	Global Indicator with IPsec/IKEv2 configuration success status message	Commands to configure IPsec/IKEv2	Status of the completion of IPsec/IKEv2 configuration	KAS-ECC-KeyGen (IKEv2) KAS-FFC-KeyGen (IKEv2) KAS-ECC (IKEv2) KAS-FFC (IKEv2) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2,	Crypto Officer - IPSec/IKE DH Private Key: W,E - IPSec/IKE DH Public Key: W,E - IPSec/IKE Peer DH Public Key: W,E - IPSec/IKE DH Shared Secret: W,E - IPSec/IKE ECDH Private Key: W,E - IPSec/IKE ECDH Public Key: W,E - IPSec/IKE

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Block Cipher (IPSec/IKE) MAC (IPSec/IKEv2)	Peer ECDH Public Key: W,E - IPSec/IKE ECDH Shared Secret: W,E - IPSec/IKE ECDSA Private Key: W,E - IPSec/IKE ECDSA Public Key: W,E - IPSec/IKE RSA Private Key: W,E - IPSec/IKE RSA Public Key: W,E - IPSec/IKE Pre-shared Secret: W,E - SKEYSEED: W,E - IPSec/IKE Session Encryption Key: W,E - IPSec/IKE Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State (V, Key): W,E - DRBG Internal State (V, C): W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Run SSHv2 Function	Execute SSHv2 Function	Global Indicator and successful SSHv2 log message	Initiate SSHv2 tunnel establishment	Status of SSHv2 tunnel establishment	KAS-ECC-KeyGen (SSHv2) KAS-FFC-KeyGen (SSHv2) KAS-ECC (SSHv2) KAS-FFC (SSHv2) KTS (SSHv2 with AES and HMAC) KTS (SSHv2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2)	Crypto Officer - SSH DH Public Key: W,E - SSH Peer DH Public Key: W,E - SSH DH Shared Secret: W,E - SSH ECDH Private Key: W,E - SSH ECDH Public Key: W,E - SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: W,E - SSH RSA Private Key: W,E - SSH RSA Public Key: W,E - SSH ECDSA Private Key: W,E - SSH ECDSA Public Key: W,E - SSH Session Encryption Key: W,E - SSH Session Authentication Key: W,E - DRBG Entropy Input: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Block Cipher (SSHv2) MAC (SSHv2)	- DRBG Seed: W,E - DRBG Internal State (V, Key): W,E - DRBG Internal State (V, C): W,E - RADIUS Secret: R,E - TACACS+ Secret: R,E User - SSH DH Private Key: W,E - SSH DH Public Key: W,E - SSH Peer DH Public Key: W,E - SSH DH Shared Secret: W,E - SSH ECDH Private Key: W,E - SSH ECDH Public Key: W,E - SSH Peer ECDH Public Key: W,E - SSH ECDH Shared Secret: W,E - SSH RSA Private Key: W,E - SSH RSA Public Key: W,E - SSH ECDSA Private Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E - SSH ECDSA Public Key: W,E - SSH Session Encryption Key: W,E - SSH Session Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State (V, Key): W,E - DRBG Internal State (V, C): W,E - RADIUS Secret: R,E - TACACS+ Secret: R,E
Run HTTPS over TLSv1.2 Function	Execute HTTPS over TLSv1.2 function	Global Indicator and successful HTTPS over TLSv1.2 log message	Initiate TLSv1.2 tunnel establishment request	Status of TLSv1.2 tunnel establishment	KAS-ECC-KeyGen (TLSv1.2) KAS-FFC-KeyGen (TLSv1.2) KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM)	Crypto Officer - TLS DH Private Key: W,E - TLS DH Public Key: W,E - TLS Peer DH Public Key: W,E - TLS DH Shared Secret: W,E - TLS ECDH Private Key: W,E - TLS ECDH Public Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2, and IKEv2) Block Cipher (TLSv1.2) MAC (TLSv1.2)	W,E - TLS Peer ECDH Public Key: W,E - TLS ECDH Shared Secret: W,E - TLS ECDSA Private Key: W,E - TLS ECDSA Public Key: W,E - TLS RSA Private Key: W,E - TLS RSA Public Key: W,E - TLS Master Secret: W,E - TLS Session Encryption Key: W,E - TLS Session Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State (V, Key): W,E - DRBG Internal State (V, C): W,E User - TLS DH Private Key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS DH Public Key: W,E - TLS Peer DH Public Key: W,E - TLS DH Shared Secret: W,E - TLS ECDH Private Key: W,E - TLS ECDH Public Key: W,E - TLS Peer ECDH Public Key: W,E - TLS ECDH Shared Secret: W,E - TLS ECDSA Private Key: W,E - TLS ECDSA Public Key: W,E - TLS RSA Private Key: W,E - TLS RSA Public Key: W,E - TLS Master Secret: W,E - TLS Session Encryption Key: W,E - TLS Session Authentication Key: W,E - DRBG Entropy Input: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Seed: W,E - DRBG Internal State (V, Key): W,E - DRBG Internal State (V, C): W,E
Run IPSec/IKEv2 Function	Execute IPsec/IKEv2 Function	Global Indicator and succesful IPsec/IKEv2 log message	Initiate IPsec/IKEv2 tunnel establishment request	Status of IPSec/IKEv2 tunnel establishment	KAS-ECC-KeyGen (IKEv2) KAS-FFC-KeyGen (IKEv2) KAS-ECC (IKEv2) KAS-FFC (IKEv2) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (SSHv2, TLSv1.2 and IKEv2) RSA SigVer (SSHv2, TLSv1.2, and IKEv2) ECDSA SigVer (SSHv2, TLSv1.2,	Crypto Officer - IPSec/IKE DH Private Key: W,E - IPSec/IKE DH Public Key: W,E - IPSec/IKE Peer DH Public Key: W,E - IPSec/IKE DH Shared Secret: W,E - IPSec/IKE ECDH Private Key: W,E - IPSec/IKE ECDH Public Key: W,E - IPSec/IKE Peer ECDH Public Key: W,E - IPSec/IKE ECDH Shared Secret: W,E - IPSec/IKE ECDSA Private Key: W,E - IPSec/IKE ECDSA Public Key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					and IKEv2) Block Cipher (IPSec/IKE) MAC (IPSec/IKEv2)	- IPSec/IKE RSA Private Key: W,E - IPSec/IKE RSA Public Key: W,E - IPSec/IKE Pre-shared Secret: W,E - SKEYSEED: W,E - IPSec/IKE Session Encryption Key: W,E - IPSec/IKE Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State (V, Key): W,E - DRBG Internal State (V, C): W,E User - IPSec/IKE DH Private Key: W,E - IPSec/IKE DH Public Key: W,E - IPSec/IKE Peer DH Public Key: W,E - IPSec/IKE DH Shared Secret: W,E - IPSec/IKE ECDH Private Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,E - IPSec/IKE ECDH Public Key: W,E - IPSec/IKE Peer ECDH Public Key: W,E - IPSec/IKE ECDH Shared Secret: W,E - IPSec/IKE ECDSA Private Key: W,E - IPSec/IKE ECDSA Public Key: W,E - IPSec/IKE RSA Private Key: W,E - IPSec/IKE RSA Public Key: W,E - IPSec/IKE Pre-shared Secret: W,E - SKEYSEED: W,E - IPSec/IKE Session Encryption Key: W,E - IPSec/IKE Authentication Key: W,E - DRBG Entropy Input: W,E - DRBG Seed: W,E - DRBG Internal State (V, Key): W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Internal State (V, C): W,E
Configure SNMPv3 Function	Configure SNMPv3 Function	Global Indicator and SNMPv3 configuration success status message	Commands to configure SNMPv3	Status of the completion of SNMPv3 configuration	Block Cipher (SNMPv3) MAC (SNMPv3)	Crypto Officer - SNMPv3 Shared Secret: W,E - SNMPv3 Encryption Key: W,E - SNMPv3 Authentication Key: W,E
Run SNMPv3 Function	Execute SNMPv3 Function	Global Indicator and successful SNMPv3 log message	Initiate SNMPv3 tunnel establishment request	Status of SNMPv3 tunnel establishment	Block Cipher (SNMPv3) MAC (SNMPv3)	Crypto Officer User
Firmware Update	Update the existing Firmware	Global indicator and successful Firmware Loading status message	Commands to load new firmware image	Outcome of the Firmware Update	Firmware Load Test	Crypto Officer - Firmware Load Test Key: R

Table 13: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module supports the firmware load test by using HMAC-SHA2-512 (HMAC Cert. #A4446) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to complete firmware update service, the Crypto Officer must authenticate to the module before loading the firmware. 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.

4.6 Bypass Actions and Status

The module implements alternating Bypass service. Traffic output from the module's data output interface can be cryptographically protected via IPSec/IKE VPN, or passed as plaintext (Bypass state), depending on the VPN tunnel establishment on the dedicated data output interface. The operator shall assume Crypto Officer role so as to configure IPSec/IKE VPN capability. If no IPSec/IKE VPN was configured, after running two independent internal actions, Module would enter the Bypass state.

Before the module executes the Bypass service (sending out plaintext traffic via the data output interface), the module would conduct two independent internal actions to prevent the inadvertent bypass of plaintext data due to a single error. The Crypto Officer can use commands "show access-list" and "show crypto ipsec sa" to verify the module's Bypass status. In Bypass tests fail, the module would enter an error state, and drop the traffic.

4.7 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.

4.8 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 is provided in the form of binary executable code. To ensure firmware security, the module is protected by RSA 2048 bits with SHA2-512 (RSA Cert. #A4446) algorithm. A Firmware Integrity Test Key (non-SSP) was preloaded to the module's binary at the factory and used for firmware integrity test only at the pre-operational self-test. The module uses the RSA 2048 bits modulus public key to verify the digital signature. If the firmware integrity test fails, the module would enter to 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 tested platform to initiate the firmware integrity test on-demand.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper labels (9) with Part number: AIR-AP-FIPSKIT=	Recommend 30 Days	Visible inspection of platform for residual evidence of tampering
Opacity shield (1) with Part number: FPR-2100-FIPS-KIT=	Recommend 30 Days	Visible inspection of platform for evidence of tampering, removal or access

Table 14: Mechanisms and Actions Required

Appling Tamper Evidence Labels

Step 1: Turn off and unplug the module.

Step 2: Clean the chassis of any grease, dirt, oil or any other material other than the surface coating from manufacture before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Step 3: Apply a label to cover the module as shown in the figures below.

The tamper evident labels are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the module will damage the tamper evident labels or the material of the security appliance cover. Because the tamper evident labels have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the security appliance has not been tampered with. Tamper evident labels can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word “FIPS” may appear if the label was peeled back.

7.2 User Placed Tamper Seals

Number: Nine (9)

Placement:

Figure 3 Module front view with opacity shield

Figure 4 FRP 2110/2120 back view

Figure 5 FRP 2130/2140 back view

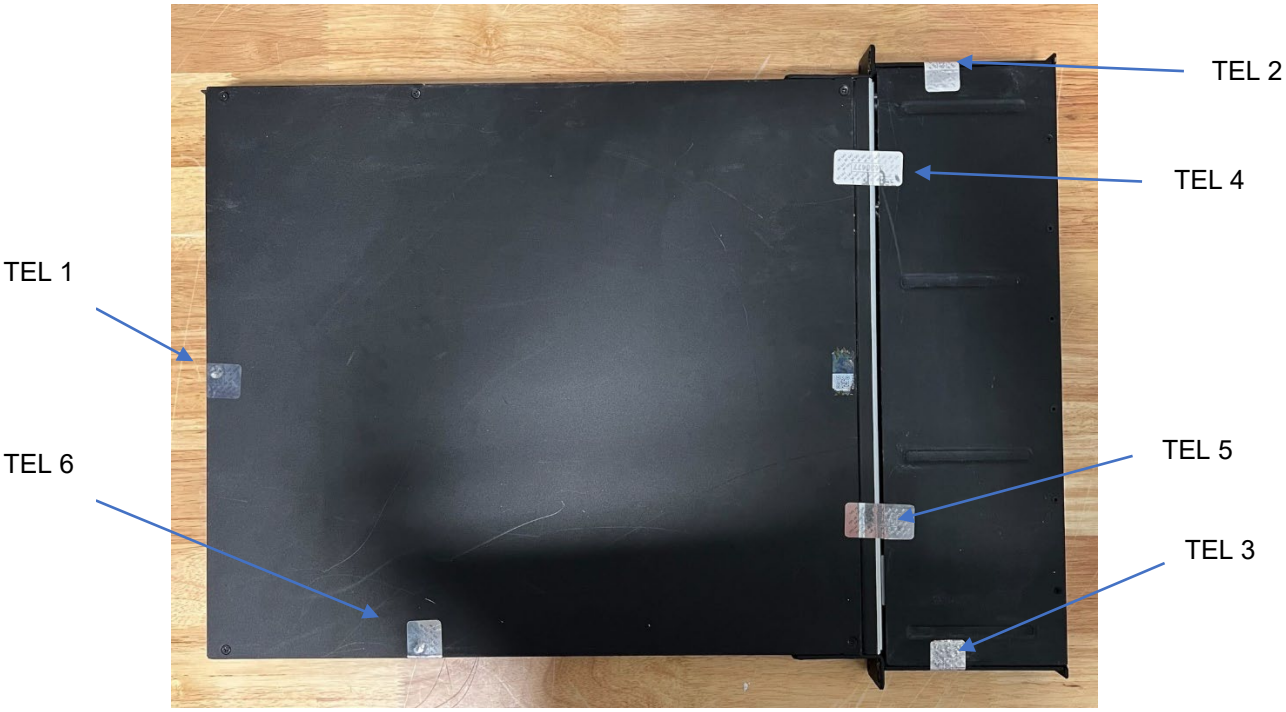


Figure 6 FRP 2110/2120 top view with opacity shield

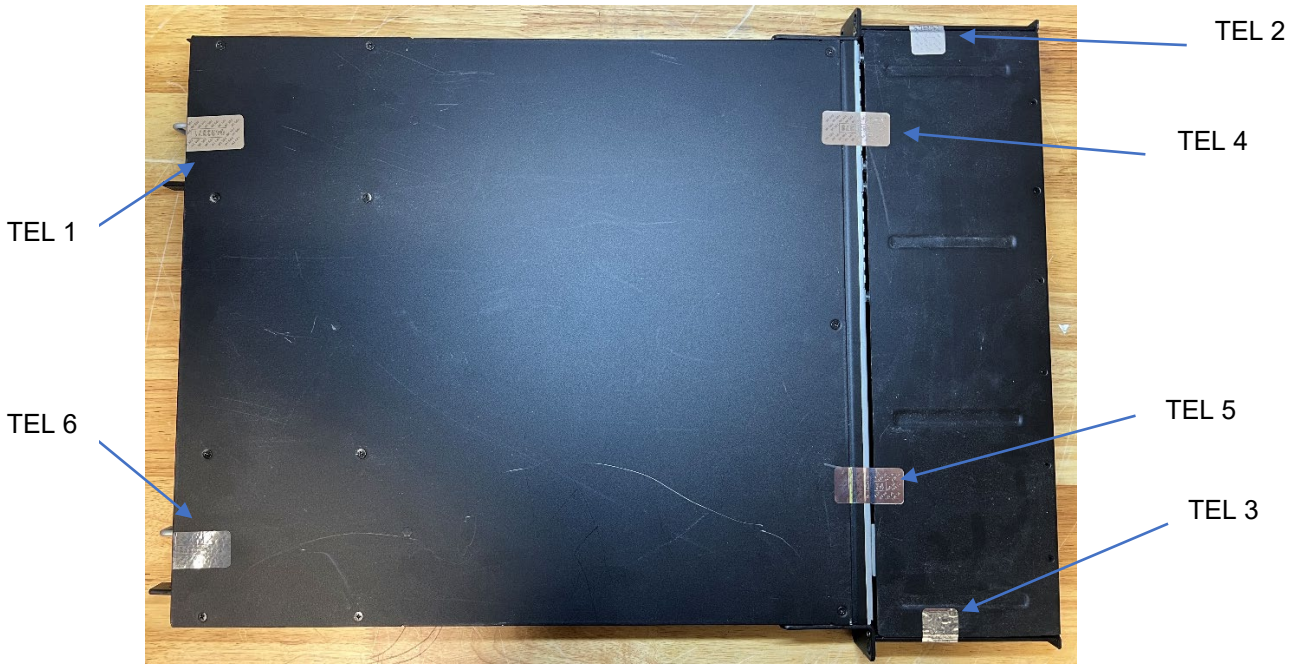


Figure 7 FRP 2130/2140 top view with opacity shield

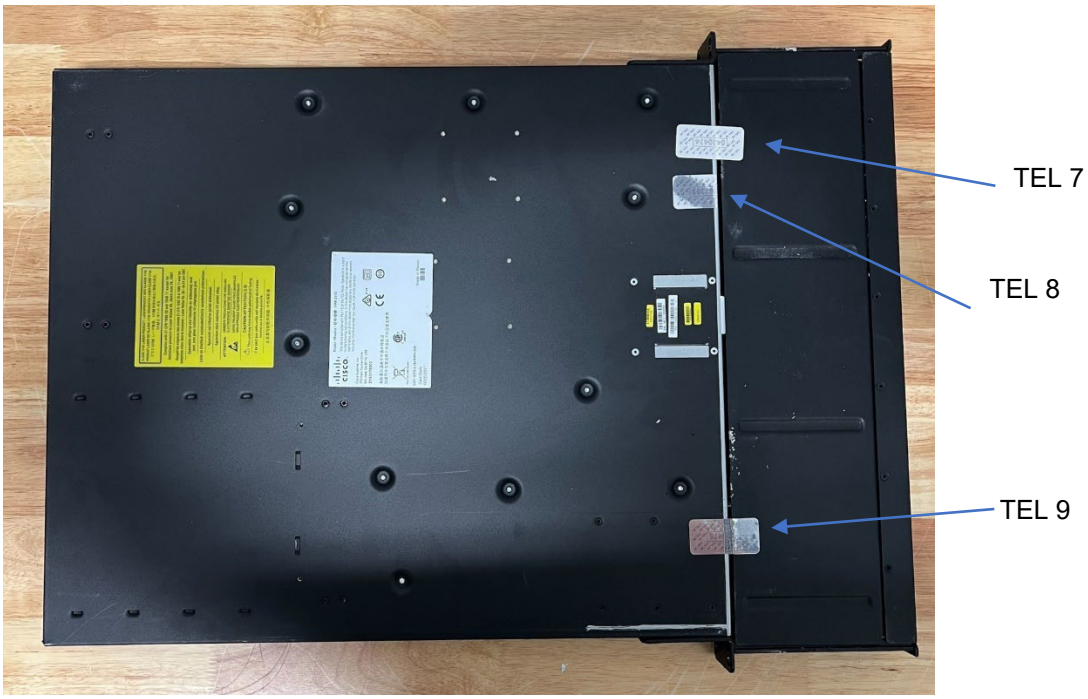


Figure 8 Module's bottom view with opacity shield

Figure 9 Module's left view with opacity shield

Figure 10 Module's right view with opacity shield

Surface Preparation: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Operator Responsible for Securing Unused Seals: It is recommended seals be stored in a secure location under controlled access

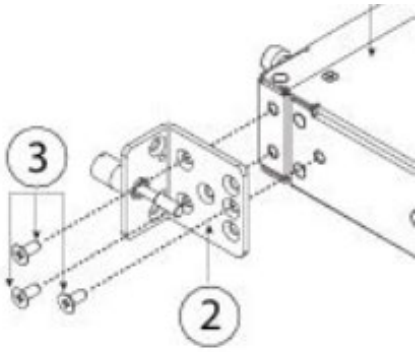
Part Numbers: AIR-AP-FIPSKIT=

7.3 Filler Panels

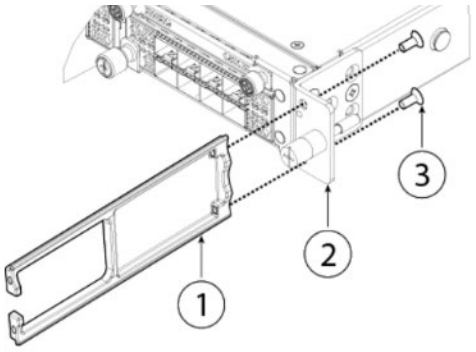
2110, 2120, 2130 and 2140 Opacity Shield

FPR-2100-FIPS-KIT=

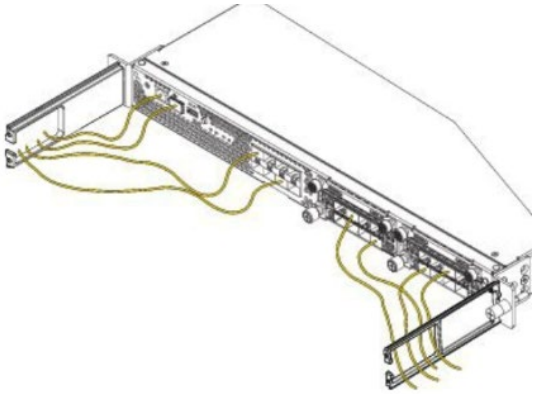
Step 1: Attach the Slide Rail Locking Bracket, #2 in diagram to the Side of the Chassis using the countersink screws #3 in diagram.



Step 2: Attach the Cable Management Bracket (#1) to the Slide Rail Locking Bracket (#2) using the countersink screws (#3)



Step 3: Route the Cables through the Cable Management Brackets



Step 4: Attach the FIPS Opacity Shield (#1) to the Cable Management Brackets (#3) using the countersink screws (#2)

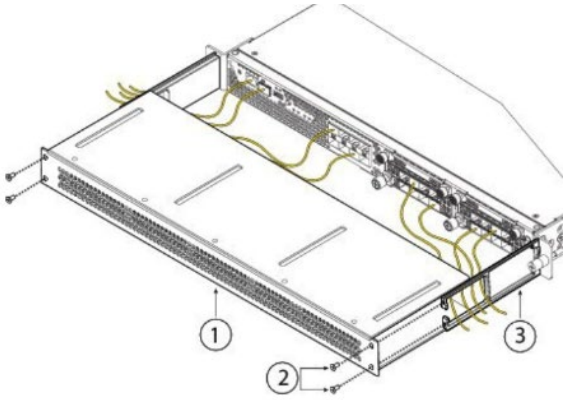


Figure 11 Opacity Shield Brackets

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DRAM	Volatile Memory	Dynamic
Flash	Non-Volatile Memory	Static

Table 15: 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	Module	Plaintext	Automated	Electronic	

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
	Boundary)					
Module Public Key Output	Module	External (Outside of the Module's Boundary)	Plaintext	Automated	Electronic	
Password/Secret Input via SSHv2 encrypted by GCM	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (SSHv2 with AES-GCM)
Password/Secret Input via SSHv2 encrypted by AES and HMAC	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (SSHv2 with AES and HMAC)
Password/Secret Input via TLS encrypted by GCM	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES-GCM)
Password/Secret Input via TLS encrypted by AES and HMAC	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES and HMAC)

Table 16: 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 DRAM or in the Flash of the module.	'configure factory-default'

Table 17: SSP Zeroization Methods

Please note that the Firmware Load Test Key is only used for Firmware 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	Used to seed the DRBG	384 bits - at least 256 bits	Entropy Input - CSP			Counter DRBG (A4446) Hash DRBG (DRBG 819)
DRBG Seed	Used in DRBG Generation	256 bits - 256 bits	DRBG Seed - CSP			Counter DRBG (A4446) Hash DRBG (DRBG 819)
DRBG Internal State (V, Key)	Used in DRBG Generation	256 bits - 256 bits	DRBG Internal State - CSP			Counter DRBG (A4446)
DRBG Internal State (V, C)	Used in DRBG Generation	256 bits - 256 bits	DRBG Internal State - CSP			Hash DRBG (DRBG 819)
User Password	User authentication	8-30 Characters - 8-30 Characters	Authentication Data - CSP			
Crypto Officer Password	Crypto Officer authentication	8-30 Characters - 8-30 Characters	Authentication Data - CSP			
RADIUS Secret	RADIUS Server Authentication	16 Characters - 16 Characters	Authentication Data - CSP			
TACACS+ Secret	TACACS+ Authentication	16 Characters - 16 Characters	Authentication Data - CSP			
Firmware Load Test Key	Used for Firmware Load Test	112 bits - 112 bits	Public Key - CSP			Firmware Load Test

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH DH Private Key	Used to derive the SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Private Key - CSP	KAS-FFC-KeyGen (SSHv2)		KAS-FFC-SSC Sp800-56Ar3 (A4446)
SSH DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Public Key - PSP		Safe Primes Key Generation (A4446)	KAS-FFC-SSC Sp800-56Ar3 (A4446)
SSH Peer DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Public Key - PSP			KAS-FFC-SSC Sp800-56Ar3 (A4446)
SSH DH Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Shared Secret - CSP		KAS-FFC-SSC Sp800-56Ar3 (A4446)	KDF SSH (A4446)
SSH ECDH Private Key	Used to derive the SSH ECDH Shared Secret	Curves: 256, 384, 521 bits - 128 to 256 bits	Private Key - CSP	KAS-ECC-KeyGen (SSHv2)		KAS-ECC-SSC Sp800-56Ar3 (A4446)
SSH ECDH Public Key	Used to derive SSH ECDHE Shared Secret	Curves: 256, 384, 521 bits - 128-256 bits	Public Key - PSP			KAS-ECC-SSC Sp800-56Ar3 (A4446)
SSH Peer ECDH Public Key	Used to derive SSH DH Shared Secret	Curves: 256, 384, 521 bits - 128 to 256 bits	Public Key - PSP			KAS-ECC-SSC Sp800-56Ar3 (A4446)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH ECDH Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys	Curves: 256, 384, 521 bits - 128 to 256 bits	Shared Secret - CSP		KAS-ECC-SSC Sp800-56Ar3 (A4446)	KDF SSH (A4446)
SSH RSA Private Key	Used for SSH session authentication	Modulus 2048 and 3072 bits - 112-128 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		RSA SigGen (FIPS186-4) (A4446)
SSH RSA Public Key	Used for SSH sessions aiuthentication	Modulus 2048 and 3072 bits - 112-128 bits	Public Key - PSP		RSA KeyGen (FIPS186-4) (A4446)	RSA SigVer (FIPS186-4) (A4446)
SSH ECDSA Private Key	Used for SSH session authentication	Curves: 256, 384, 521 bits - 128 to 256 bits	Private Key - CSP	ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		ECDSA SigGen (FIPS186-4) (A4446)
SSH ECDSA Public Key	Used for SSH sessions aiuthentication	Curves: 256, 384, 521 bits - 128 to 256 bits	Public Key - PSP		ECDSA KeyGen (FIPS186-4) (A4446)	ECDSA SigVer (FIPS186-4) (A4446)
SSH Session Encryption Key	Used for SSH Session confidentiality protection	128-256 bits - 128-256 bits	Session Key - CSP		KDF SSH (A4446)	Block Cipher (SSHv2)
SSH Session Authentication Key	Used for SSH Session integrity protection	At least 160 bits - At least 160 bits	Session Key - CSP		KDF SSH (A4446)	MAC (SSHv2)
TLS DH Private Key	Used to Derive TLS DH Shared Secret	ffdhe2048, ffdhe3072, ffdhe4096 - 112-152 bits	Private Key - CSP	KAS-FFC-KeyGen (TLSv1.2)		KAS-FFC-SSC Sp800-56Ar3 (A4446)
TLS DH Public Key	Used to Derive TLS	ffdhe2048,	Public Key - PSP		Safe Primes	KAS-FFC-SSC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	DH Shared Secret	ffdhe3072, ffdhe4096 - 112-152 bits			Key Generation (A4446)	Sp800-56Ar3 (A4446)
TLS Peer DH Public Key	Used to derive TLS DH Shared Secret	ffdhe2048, ffdhe3072, ffdhe4096 - 112-152 bits	Public Key - PSP			KAS-FFC-SSC Sp800-56Ar3 (A4446)
TLS DH Shared Secret	Used to Derive TLS Session Encryption Key and TLS Session Authentication Key	ffdhe2048, ffdhe3072, ffdhe4096 - 112-152 bits	Shared Secret - CSP		KAS-FFC-SSC Sp800-56Ar3 (A4446)	TLS v1.2 KDF RFC7627 (A4446)
TLS ECDH Private Key	Used to Derive TLS ECDH Shared Secret	Curves P-256, P-384, and P-521 - 128-256 bits	Private Key - CSP	KAS-ECC-KeyGen (TLSv1.2)		KAS-ECC-SSC Sp800-56Ar3 (A4446)
TLS ECDH Public Key	Used to Derive TS ECDH Shared Secret	Curves P-256, P-384, and P-521 - 128-256 bits	Public Key - PSP			KAS-ECC-SSC Sp800-56Ar3 (A4446)
TLS Peer ECDH Public Key	Used to derive IKE ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128-256 bits	Public Key - PSP			KAS-ECC-SSC Sp800-56Ar3 (A4446)
TLS ECDH Shared Secret	Used to Derive TLS Session Encryption Key and TLS Session Authentication Key	Curves p-256, P-384, P-521 - 128-256 bits	Shared Secret - CSP		KAS-ECC-SSC Sp800-56Ar3 (A4446)	TLS v1.2 KDF RFC7627 (A4446)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS ECDSA Private Key	Used to support CO and Admin HTTPS interfaces	Curves P-256, P-384, P-521 - 128-256 bits	Private Key - CSP	ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		ECDSA SigGen (FIPS186-4) (A4446)
TLS ECDSA Public Key	Used to support CO and User HTTPS Interfaces	Curves P-256, P-384, P-521 - 128-256 bits	Public Key - PSP		ECDSA KeyGen (FIPS186-4) (A4446)	ECDSA SigVer (FIPS186-4) (A4446)
TLS RSA Private Key	Used to support CO and Admin HTTPS Interfaces	Modulus 2048 and 3072 bits - 112-128 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		RSA SigGen (FIPS186-4) (A4446)
TLS RSA Public Key	Used to support CO and User HTTPS interfaces	Modulus 2048 and 3072 bits - 112-128 bits	Public Key - PSP		RSA KeyGen (FIPS186-4) (A4446)	RSA SigVer (FIPS186-4) (A4446)
TLS Master Secret	Used to protect HTTPS Session. Pre-master secret	At least 112 bits - At least 112 bits	Master Secret - CSP			TLS v1.2 KDF RFC7627 (A4446)
TLS Session Encryption Key	Used to protect HTTPS Session. TLS Master secret	128-256 bits - 128-256 bits	Session Key - CSP		TLS v1.2 KDF RFC7627 (A4446)	Block Cipher (TLSv1.2)
TLS Session Authentication Key	Used to protect HTTPS Session. TLS master secret	at least 112 bits - at least 112 bits	Session Key - CSP		TLS v1.2 KDF RFC7627 (A4446)	MAC (TLSv1.2)
IPSec/IKE DH Private Key	Used to derive IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Private Key - CSP	KAS-FFC-KeyGen (IKEv2)		KAS-FFC-SSC Sp800-56Ar3 (A4446)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
IPSec/IKE DH Public Key	Used to derive IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Public Key - PSP		Safe Primes Key Generation (A4446)	KAS-FFC-SSC Sp800-56Ar3 (A4446)
IPSec/IKE Peer DH Public Key	Used to derive IPSec/IKE DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Public Key - PSP			KAS-FFC-SSC Sp800-56Ar3 (A4446)
IPSec/IKE DH Shared Secret	Used to derive IPSec/IKE Session Encryption Keys, IPSec/IKE Authentication Keys	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Shared Secret - CSP		KAS-FFC-SSC Sp800-56Ar3 (A4446)	KDF IKEv2 (A4446)
IPSec/IKE ECDH Private Key	Used to derive IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128-256 bits	Private Key - CSP	KAS-ECC-KeyGen (IKEv2)		KAS-ECC-SSC Sp800-56Ar3 (A4446)
IPSec/IKE ECDH Public Key	Used to derive IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128-256 bits	Public Key - PSP			KAS-ECC-SSC Sp800-56Ar3 (A4446)
IPSec/IKE Peer ECDH Public Key	Used to derive IPSec/IKE ECDH Shared Secrets	Curves P-256, P-384, P-521 - 128-256 bits	Public Key - PSP			KAS-ECC-SSC Sp800-56Ar3 (A4446)
IPSec/IKE ECDH Shared Secret	Used to derive IPSec/IKE ECDH	Curves P-256, P-384, P-521 -	Shared Secret - CSP		KAS-ECC-SSC Sp800-56Ar3 (A4446)	KDF IKEv2 (A4446)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Shared Secrets	128-256 bits				
IPSec/IKE ECDSA Private Key	Used for IPSec/IKE peer authentication	Curves P-256, P-384, P-521 - 128-256 bits	Private Key - CSP	ECDSA KeyGen (SSHv2, TLSv1.2 and IKEv2)		ECDSA SigGen (FIPS186-4) (A4446)
IPSec/IKE ECDSA Public Key	Used for IPSec/IKE peer authentication	Curves P-256, P-384, P-521 - 128-256 bits	Public Key - PSP		ECDSA KeyGen (FIPS186-4) (A4446)	ECDSA SigVer (FIPS186-4) (A4446)
IPSec/IKE RSA Private Key	Used for IPSec/IKE peer authentication	Modulus 2048 or 3072 - 112 or 128 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		RSA SigGen (FIPS186-4) (A4446)
IPSec/IKE RSA Public Key	Used for IPSec/IKE peer authentication	Modulus 2048 or 3072 - 112 or 128 bits	Public Key - PSP		RSA KeyGen (FIPS186-4) (A4446)	RSA SigVer (FIPS186-4) (A4446)
IPSec/IKE Pre-shared Secret	Used for IPSec/IKE peer authentication	16-32 bytes characters - 16-32 bytes characters	shared secret - CSP			KDF IKEv2 (A4446)
SKEYSEED	Keying material used to derive the IPSec/IKE Session Encryption Key and IPSec/IKE Authentication Key	160 bits - 160 bits	Keying Material - CSP			KDF IKEv2 (A4446)
IPSec/IKE Session Encryption Key	Used to secure IPSec/IKEv2 session confidentiality	128-256 bits - 128-256 bits	Session Key - CSP		KDF IKEv2 (A4446)	Block Cipher (IPSec/IKE)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
IPSec/IKE Authentication Key	Used to secure IPSec/IKEv2 session integrity	at least 160 bits - at least 160 bits	Session Key - CSP		KDF IKEv2 (A4446)	MAC (IPSec/IKEv2)
SNMPv3 Shared Secret	Used for SNMPv3 user authentication	8-32 characters - N/A	Authentication Secret - CSP			
SNMPv3 Encryption Key	Used to protect SNMPv3 traffic confidentiality	128 bits - 128 bits	Encryption Key - CSP		KDF SNMP (A4446)	Block Cipher (SNMPv3)
SNMPv3 Authentication Key	Used to secure SNMPv3 traffic integrity	At least 112 bits - At least 112 bits	Authentication Key - CSP		KDF SNMP (A4446)	MAC (SNMPv3)

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Entropy Input		DRAM:Plaintext	Until Reboot	Zeroization Command	DRBG Seed:Used With DRBG Internal State (V, Key):Used With DRBG Internal State (V, C):Used With
DRBG Seed		DRAM:Plaintext	Until Reboot	Zeroization Command	DRBG Entropy Input:Used With DRBG Internal State (V, Key):Used With DRBG Internal State (V, C):Used With
DRBG Internal State (V, Key)		DRAM:Plaintext	Until Reboot	Zeroization Command	DRBG Entropy Input:Used With DRBG Seed:Used With
DRBG Internal State (V, C)		DRAM:Plaintext	Until Reboot	Zeroization Command	DRBG Entropy Input:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					DRBG Seed:Used With
User Password	Password/Secret Input via TLS encrypted by GCM Password/Secret Input via TLS encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC	Flash:Encrypted		Zeroization Command	
Crypto Officer Password	Password/Secret Input via TLS encrypted by GCM Password/Secret Input via TLS encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC	Flash:Encrypted		Zeroization Command	
RADIUS Secret	Password/Secret Input via TLS encrypted by GCM Password/Secret Input via	Flash:Encrypted		Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	TLS encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC				
TACACS+ Secret	Password/Secret Input via TLS encrypted by GCM Password/Secret Input via TLS encrypted by AES and HMAC Password/Secret Input via SSHv2 encrypted by GCM Password/Secret Input via SSHv2 encrypted by AES and HMAC	Flash:Encrypted		Zeroization Command	
Firmware Load Test Key		Flash:Plaintext		N/A	
SSH DH Private Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH DH Public Key:Paired With SSH Peer DH Public Key:Used With
SSH DH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH DH Private Key:Paired With
SSH Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH DH Private Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH DH Shared Secret		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH DH Private Key:Derived From SSH DH Public Key:Derived From
SSH ECDH Private Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH ECDH Public Key:Paired With SSH Peer ECDH Public Key:Used With
SSH ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH ECDH Private Key:Paired With
SSH Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH ECDH Private Key:Used With
SSH ECDH Shared Secret		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH ECDH Private Key:Derived From SSH ECDH Public Key:Derived From
SSH RSA Private Key		Flash:Plaintext		Zeroization Command	SSH RSA Public Key:Paired With
SSH RSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	SSH RSA Private Key:Paired With
SSH ECDSA Private Key		Flash:Plaintext		Zeroization Command	SSH ECDSA Public Key:Paired With
SSH ECDSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	SSH ECDSA Private Key:Paired With
SSH Session Encryption Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH Session Authentication Key:Used With
SSH Session Authentication Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH Session Encryption Key:Used With
TLS DH Private Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS DH Public Key:Paired With TLS Peer DH Public Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TLS DH Public Key	Module Public Key Output	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS DH Private Key:Paired With
TLS Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	while TLS tunnel is on	Zeroization Command	TLS DH Private Key:Used With
TLS DH Shared Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS ECDH Private Key:Derived From TLS Peer ECDH Public Key:Derived From
TLS ECDH Private Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS ECDH Public Key:Paired With TLS Peer ECDH Public Key:Used With
TLS ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS ECDH Private Key:Paired With
TLS Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	while TLS tunnel is on	Zeroization Command	TLS ECDH Private Key:Used With
TLS ECDH Shared Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS ECDH Private Key:Derived From TLS Peer ECDH Public Key:Derived From
TLS ECDSA Private Key		Flash:Plaintext		Zeroization Command	TLS ECDSA Public Key:Paired With
TLS ECDSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	TLS ECDSA Private Key:Paired With
TLS RSA Private Key		Flash:Plaintext		Zeroization Command	TLS RSA Public Key:Paired With
TLS RSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	TLS RSA Private Key:Paired With
TLS Master Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS ECDH Shared Secret:Derived From
TLS Session		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS Session Authentication Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Encryption Key					
TLS Session Authentication Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS Session Encryption Key:Used With
IPSec/IKE DH Private Key		DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command	IPSec/IKE DH Public Key:Paired With IPSec/IKE Peer DH Public Key:Used With
IPSec/IKE DH Public Key	Module Public Key Output	DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command	IPSec/IKE DH Private Key:Paired With
IPSec/IKE Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	while IPSec/IKE tunnel is on	Zeroization Command	IPsec/IKE DH Private Key:Used With
IPSec/IKE DH Shared Secret		DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command	SKEYSEED:Used With
IPSec/IKE ECDH Private Key		DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command	IPSec/IKE ECDH Public Key:Paired With IPSec/IKE Peer ECDH Public Key:Used With
IPSec/IKE ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command	IPSec/IKE ECDH Private Key:Paired With
IPSec/IKE Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command	IPSec/IKE ECDH Private Key:Used With
IPSec/IKE ECDH Shared Secret		DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command	SKEYSEED:Used With
IPSec/IKE ECDSA Private Key		Flash:Plaintext		Zeroization Command	IPSec/IKE ECDSA Public Key:Paired With
IPSec/IKE ECDSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	IPSec/IKE ECDSA Private Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
IPSec/IKE RSA Private Key		Flash:Plaintext		Zeroization Command	IPSec/IKE RSA Public Key:Paired With
IPSec/IKE RSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	IPSec/IKE RSA Private Key:Paired With
IPSec/IKE Pre-shared Secret		Flash:Encrypted	While IPSec/IKE v2 tunnel is on	Zeroization Command	SKEYSEED:Derived to
SKEYSEED		DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command	IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From IPSec/IKE Pre-shared Secret:Derived From
IPSec/IKE Session Encryption Key		DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command	IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From
IPSec/IKE Authentication Key		DRAM:Plaintext	While IPSec/IKE v2 tunnel is on	Zeroization Command	IPSec/IKE DH Shared Secret:Derived From IPSec/IKE ECDH Shared Secret:Derived From
SNMPv3 Shared Secret	Password/Secret Input via TLS encrypted by GCM Password/Secret Input via TLS encrypted by AES and HMAC Password/Sec	Flash:Encrypted	While SNMPv3 tunnel is on	Zeroization Command	SNMPv3 Encryption Key:Derive To SNMPv3 Authentication Key:Derive To

Name	Input - Output	Storage	Storage Duration	Zeroizatio n	Related SSPs
	ret Input via SSHv2 encrypted by GCM Password/Sec ret Input via SSHv2 encrypted by AES and HMAC				
SNMPv3 Encryption Key		DRAM:Plainte xt	While SNMPv3 tunnel is on	Zeroizatio n Command	SNMPv3 Shared Secret:Derived From
SNMPv3 Authenticati on Key		DRAM:Plainte xt	While SNMPv3 tunnel is on	Zeroizatio n Command	SNMPv3 Shared Secret:Derived From SNMPv3 Encryption Key:Used With

Table 19: SSP Table 2

9.5 Transitions

- SHA-1: The module includes an implementation of SHA-1 for hashing and digital signature verification. 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.

- FIPS 186-4/186-5: As of February 5, 2024, the CMVP does not accept module submissions that implement DSA or RSA X9.31 in the approved mode, other than for signature verification which is approved for legacy use. This module does not implement DSA or RSA X9.31 for signature generation and therefore is unaffected by the current transition from 186-4 to 186-5. As detailed in section 2.7, the CAVP testing performed on the 186-4 algorithms is mathematically similar to the testing performed on the 186-5 algorithms and therefore this module claims compliance with 186-5. This means that no timeline exists in which any of the implemented algorithms will transition from approved to non-approved.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer Firmware Integrity Test	RSA SigVer 2048 bits with SHA2-512	KAT	SW/FW Integrity	Module is in normal state	RSA SigVer
Pre-Operational Bypass Test	N/A	N/A	Bypass	Module is in normal state	N/A

Table 20: Pre-Operational Self-Tests

The module performs the following self-tests, including the pre-operational self-tests and Conditional self-tests. Prior to the module providing any data output via the data output interface, the module performs and passes the pre-operational self-tests. Following the successful pre-operational self-tests, the module executes the Conditional Cryptographic Algorithm Self-tests (CASTs). If anyone of the self-tests fails, the module transitions into an error state and outputs the error message via the module's status output interface. While the module is in the error state, all data through the data output interface and all cryptographic operations are disabled. The error state can only be cleared by reloading the module. All self-tests must be completed successfully before the module transitions to the operational state.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
AES-GCM Authenticated Encrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Authenticated Encrypt	Power Up
AES-GCM Authenticated Decrypt KAT (A4446)	256 bits	KAT	CAST	Module is in normal state	Authenticated Decrypt	Power Up
Counter DRBG Instantiate KAT (A4446)	AES-128	KAT	CAST	Module is in normal state	Instantiate KAT	Power Up
Counter DRBG Generate KAT (A4446)	AES-128	KAT	CAST	Module is in normal state	Generate KAT	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG Reseed KAT (A4446)	AES-128	KAT	CAST	Module is in normal state	Reseed KAT	Power Up
ECDSA SigGen KAT (A4446)	P-256 curve with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigGen KAT	Power Up
ECDSA SigVer KAT (A4446)	P-256 curve with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigVer KAT	Power Up
HMAC-SHA-1 KAT (A4446)	SHA-1	KAT	CAST	Module is in normal state	HMAC-SHA-1	Power Up
HMAC-SHA2-256 KAT (A4446)	SHA2-256	KAT	CAST	Module is in normal state	HMAC-SHA2-256	Power Up
HMAC-SHA2-384 KAT (A4446)	SHA2-384	KAT	CAST	Module is in normal state	HMAC-SHA2-384	Power Up
HMAC-SHA2-512 KAT (A4446)	SHA2-512	KAT	CAST	Module is in normal state	HMAC-SHA2-512	Power Up
KAS-ECC-SSC Sp800-56Ar3 KAT (A4446)	P-256 Curve	KAT	CAST	Module is in normal state	Primitive Z KAT	Power Up
KAS-FFC-SSC Sp800-56Ar3 KAT (A4446)	MODP-2048	KAT	CAST	Module is in normal state	Primitive Z KAT	Power Up
RSA SigGen (FIPS186-4) KAT (A4446)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigGen KAT	Power Up
RSA SigVer (FIPS186-4) KAT (A4446)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigVer KAT	Power Up
KDF IKEv2 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SNMP KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SSH KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
TLS v1.2 KDF RFC7627 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
SHA-1 KAT (A4446)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
AES-CBC Encrypt KAT (AES 3301)	128 bits	KAT	CAST	Module is in normal state	Encrypt KAT	Power Up
AES-CBC Decrypt KAT (AES 3301)	128 bits	KAT	CAST	Module is in normal state	Decrypt KAT	Power Up
AES-GCM Authenticated Encrypt KAT (AES 3301)	128 bits	KAT	CAST	Module is in normal state	Encrypt KAT	Power Up
AES-GCM Authenticated Decrypt KAT (AES 3301)	128 bits	KAT	CAST	Module is in normal state	Decrypt KAT	Power Up
Hash DRBG Instantiate KAT (DRBG 819)	SHA2-512	KAT	CAST	Module is in normal state	Instantiate KAT	Power Up
Hash DRBG Generate KAT (DRBG 819)	SHA2-512	KAT	CAST	Module is in normal state	Generate KAT	Power Up
Hash DRBG Reseed KAT (DRBG 819)	SHA2-512	KAT	CAST	Module is in normal state	Reseed KAT	Power Up
HMAC-SHA-1 KAT (HMAC 2095)	SHA-1	KAT	CAST	Module is in normal state	HMAC-SHA-1	Power Up
HMAC-SHA2-256 KAT (HMAC 2095)	SHA2-256	KAT	CAST	Module is in normal state	HMAC-SHA2-256	Power Up
HMAC-SHA2-384 KAT (HMAC 2095)	SHA2-384	KAT	CAST	Module is in normal state	HMAC-SHA2-384	Power Up
HMAC-SHA2-512 KAT (HMAC 2095)	SHA2-512	KAT	CAST	Module is in normal state	HMAC-SHA2-512	Power Up
ECDSA KeyGen (FIPS186-4) PCT (A4446)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	ECDSA	Performs all required pair-wise consistency tests on the

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						newly generated key pairs before the first operational use.
RSA KeyGen (FIPS186-4) PCT (A4446)	2048 bit Modulus	PCT	PCT	Module is in normal state	RSA	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
KAS-ECC-SSC Sp800-56Ar3 PCT (A4446)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
KAS-FFC-SSC Sp800-56Ar3 PCT (A4446)	MODP-2048	PCT	PCT	Module is in normal state	N/A	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
HMAC-SHA2-512 Firmware Load Test	HMAC-SHA2-512	KAT	SW/FW Load	Module is in normal state	N/A	When firmware has been uploaded to the module

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Conditional Bypass Test	N/A	N/A	Bypass	Module is in normal state	N/A	Performs conditional bypass test before first operational use of bypass service
Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Power Up
Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source	Power Up
Entropy 90B Continuous Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Entropy data is generated from the Entropy Source - Continuous
Entropy 90B Continuous Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some	Entropy data is generated from the Entropy Source - Continuous

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					physical failure or environmental change affecting the noise source	

Table 21: Conditional Self-Tests

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

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer Firmware Integrity Test	KAT	SW/FW Integrity	Recommend 60 Days	Reboot
Pre-Operational Bypass Test	N/A	Bypass	Recommend 60 Days	Reboot

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
AES-CBC Decrypt KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
AES-GCM Authenticated Encrypt KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
AES-GCM Authenticated Decrypt KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
Counter DRBG Instantiate KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
Counter DRBG Generate KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG Reseed KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
ECDSA SigGen KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
ECDSA SigVer KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA-1 KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-256 KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-384 KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-512 KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
KAS-FFC-SSC Sp800-56Ar3 KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
RSA SigGen (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
RSA SigVer (FIPS186-4) KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
KDF IKEv2 KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
KDF SNMP KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
KDF SSH KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
TLS v1.2 KDF RFC7627 KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
SHA-1 KAT (A4446)	KAT	CAST	Recommend 60 Days	Reboot
AES-CBC Encrypt KAT (AES 3301)	KAT	CAST	Recommend 60 Days	Reboot
AES-CBC Decrypt KAT (AES 3301)	KAT	CAST	Recommend 60 Days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM Authenticated Encrypt KAT (AES 3301)	KAT	CAST	Recommend 60 Days	Reboot
AES-GCM Authenticated Decrypt KAT (AES 3301)	KAT	CAST	Recommend 60 Days	Reboot
Hash DRBG Instantiate KAT (DRBG 819)	KAT	CAST	Recommend 60 Days	Reboot
Hash DRBG Generate KAT (DRBG 819)	KAT	CAST	Recommend 60 Days	Reboot
Hash DRBG Reseed KAT (DRBG 819)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA-1 KAT (HMAC 2095)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-256 KAT (HMAC 2095)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-384 KAT (HMAC 2095)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-512 KAT (HMAC 2095)	KAT	CAST	Recommend 60 Days	Reboot
ECDSA KeyGen (FIPS186-4) PCT (A4446)	PCT	PCT	Recommend 60 Days	Reboot
RSA KeyGen (FIPS186-4) PCT (A4446)	PCT	PCT	Recommend 60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 PCT (A4446)	PCT	PCT	Recommend 60 Days	Reboot
KAS-FFC-SSC Sp800-56Ar3 PCT (A4446)	PCT	PCT	Recommend 60 Days	Reboot
HMAC-SHA2-512 Firmware Load Test	KAT	SW/FW Load	N/A	N/A
Conditional Bypass Test	N/A	Bypass	N/A	N/A
Entropy 90B Start-up	RCT	CAST	N/A	N/A

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Repetition Count Test (RCT)				
Entropy 90B Start-up Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A
Entropy 90B Continuous Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
Entropy 90B Continuous Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A

Table 23: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	If self-test tests fail, the module is put into an error state	Self-test failure	Reboot the module	System Halt

Table 24: Error States

If any of the above-mentioned self-tests fail, the module reports the error and enters the 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 firmware integrity test and the conditional CASTs. The module will only enter into the operational state after successfully passing the pre-operational firmware integrity test and the conditional CASTs.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The validated module firmware was installed onto the respective test platforms listed in Table 2 above. 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. The Crypto Officer must configure and enforce the following initialization steps. Operating this module without maintaining the following settings will put the module into a non-compliant state.

Step 1: The Crypto Officer must install opacity shields as described in section Physical Security above.

Step 2: The Crypto Officer must apply tamper evidence labels as described in section Physical Security above.

Step 3: The Crypto Officer must securely store any unused tamper evidence labels.

Note: Each module has a Type A USB 2.0 port, but it is considered to be disabled once the Crypto Officer has applied the TEL #9.

Step 4: Crypto Officer performs the following configurations:

ciscoasa# configure terminal
Note, the Crypto Officer needs to connect the platform to cisco.com to obtain the license for ASA from Cisco.
ciscoasa(config)# license smart register idtoken [token data]
ciscoasa(config)#license smart
ciscoasa(config-smart-lic)# show license all
Smart Licensing Status
==========
Smart Licensing is ENABLED

-OR-

ciscoasa(config-smart-lic)# show license summary
Smart Licensing is ENABLED
Registration:

Step 5. Crypto officer shall perform zeroization operation if the module was previously used before the approved mode configuration.

Step 6: Enable approved mode of operation by using the following command.

ciscoasa(config)# fips enable
Note: Startup operational mode will not take effect until you save configuration and reboot the device
Rebooting the device will force new self-test

Step 7: Crypto Officer can verify the version installed and running the following command.

ciscoasa(config)# show version

Step 8: Crypto Officer will need to issue the following commands to configure module.

ciscoasa> en
ciscoasa# conf t
ciscoasa(config)#

Step 9: Assign users a Privilege Level of 1.

Step 10: Configure IP address for unit and all distant endpoints.

Step 11: Define RADIUS and TACACS+ shared secret keys that are at least 8 characters long and secure traffic between the security module and the RADIUS/TACACS+ server via secure (IPSec, TLS) tunnel.

Note: Perform this step only if RADIUS/TACAS+ is configured, otherwise skip over and proceed to next step.

Step 12: Configure the security module so that any remote connections via Telnet are secured through IPSec connection by using the following commands

crypto map interface
access-list
protocol esp encryption
protocol esp integrity
If IPSec secure connection is not configured, after running two internal independent actions defined in section 4.6 above, the module would enter the Bypass state.

Step 13: Configure the security module so that only approved algorithms are used for all security connections (SSHv2, TLSv1.2, SNMPv3 and IPSec/IKEv2).

Step 14: Configure the security module so that error messages can only be viewed by Crypto Officer.

Step 15: Disable the TFTP server.

Step 16: Disable HTTP for performing system management in approved mode of operation. HTTPS with TLSv1.2 should always be used for Web-based management.

Step 17: Ensure that installed digital certificates are signed using approved algorithms.

Step 18: Save the configuration.

Step 19: Reboot the module.

11.2 Administrator Guidance

No specific Administrator guidance.

11.3 Non-Administrator Guidance

No specific Non-Administrator guidance.

12 Mitigation of Other Attacks

N/A for this module.