Cisco Systems, Inc.

ISO/IEC 19790 and FIPS 140-3 Non-Proprietary

Security Policy

for

Adaptive Security Appliance Virtual Cryptographic Module

Last Updated: June 17, 2024, Version 0.4

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

Table of Content

List of Figures

List of Tables

1 General

This is Cisco Systems, Inc. non-proprietary security policy for the Adaptive Security Appliance Virtual Cryptographic Module (hereinafter referred to as ASAv or the Module), software version 9.16.4. 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 1 Software 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.

ISO/IEC 24759:2017 Section 6	ISO/IEC 24759:2017 and FIPS 140-3 Section Title	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

Table 1 Security Levels

The module has an overall security level of 1.

2 Cryptographic Module Specification

The Module is a multi-chip standalone software module deployed as the virtualized version of the Cisco Firepower Threat Defense which houses ASA, FX-OS and Firepower solutions with underlying operating system identified as Linux 4 (also referred to as **F**irepower e**X**tensible **O**perating **S**ystem or FX-OS throughout this document).

This 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, secure unified communications, TLSv1.2, SSHv2, IPSec/IKEv2 and Cryptographic Cipher Suite B, which delivers enterprise-class security for business-to-enterprise networks in a virtual environment.

The module has been tested on the following Operational Environments.

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	Linux 4 (FX-OS) on VMware ESXi 6.7	UCS C220 M5 SFF Server	INTEL Skylake 6128 (Skylake)	With PAA
2	Linux 4 (FX-OS) on VMware ESXi 6.7	UCS C220 M5 SFF Server	INTEL Skylake 6128 (Skylake)	Without PAA
3	Linux 4 (FX-OS) on VMware ESXi 7.0	UCS C220 M5 SFF Server	INTEL Skylake 6128 (Skylake)	With PAA
4	Linux 4 (FX-OS) on VMware ESXi 7.0	UCS C220 M5 SFF Server	INTEL Skylake 6128 (Skylake)	Without PAA
5	Linux 4 (FX-OS) on NFVIS 4.4	ENCS 5412 Server	Intel Xeon Processor D-1557 (Broadwell)	With PAA
6	Linux 4 (FX-OS) on NFVIS 4.4	ENCS 5412 Server	Intel Xeon Processor D-1557 (Broadwell)	Without PAA

Table 2 Tested Operational Environment

Figure 1 UCS C220 M5 front view with Bezel

Figure 2 UCS C220 M5 front view without Bezel

Figure 3 UCS C220 M5 rear view

Figure 4 ENCS 5412 front view[1]

Figure 5 ENCS 5412 rear view

[1] https://www.cisco.com/c/dam/global/da_dk/assets/training/seminaria-materials/enterprise_network_compute_system_encs_.pdf

#	Operating System	Hardware Platform
1	Linux 4 (FX-OS)	C220 M5 w/KVM/AWS
2	Linux 4 (FX-OS)	C240 M5 w/ESXi/KVM/AWS
3	Linux 4 (FX-OS)	C480 M5 w/ESXi/KVM/AWS
4	Linux 4 (FX-OS)	E160-M3 w/ESXi/KVM/AWS
5	Linux 4 (FX-OS)	E180D-M3 w/ESXi/KVM/AWS
6	Linux 4 (FX-OS)	ENCS 5406
7	Linux 4 (FX-OS)	ENCS 5408

Table 3 Vendor Affirmed Operational Environments

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

Modes of operation

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.

The table below lists all Approved or Vendor-affirmed security functions of the module, including specific key size(s) -in bits unless otherwise noted- employed for approved services, and implemented modes of operation. There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use/Function
A2952 and A3376	AES [FIPS 197; SP800-38A]	CBC	Key Length: 128 and 256 bits	Symmetric encryption and decryption
A2952 and A3376	AES [FIPS 197; SP 800-38D]	GCM	Key Length: 128 and 256 bits	Authenticated symmetric encryption and decryption
A2952 and A3376	KDF SSH [SP 800-135rev1] (CVL)	KDF SSH	N/A	Key derivation function used in SSHv2
A2952 and A3376	TLS v1.2 KDF RFC7627 [RFC7627] (CVL)	TLS v1.2 KDF with RFC7627	N/A	Key derivation function used in TLSv1.2 (RFC7627) with extended master secret
A2952 and A3376	KDF IKEv2 [SP 800-135rev1] (CVL)	KDF IKEv2	N/A	Key derivation function used in IPSec/IKEv2
A2952 and A3376	CTR_DRBG [SP 800-90Arev1]	AES-256 Derivation Function Enabled; Prediction Resistance: Yes	N/A	Deterministic Random Bit Generators (DRBG); uses an algorithm to produce random output

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use/Function
A2952 and A3376	ECDSA [FIPS 186-4]	ECDSA KeyGen	Curves: P-256, P-384, P-521	ECDSA keypair generation
A2952 and A3376	ECDSA [FIPS 186-4]	ECDSA KeyVer	Curves: P-256, P-384, P-521	ECDSA keypair verification
A2952 and A3376	ECDSA [FIPS 186-4]	ECDSA SigGen	Curves: P-256, P-384, P-521	ECDSA signature generation
A2952 and A3376	ECDSA [FIPS 186-4]	ECDSA SigVer	Curves: P-256, P-384, P-521	ECDSA signature verification
A2952 and A3376	HMAC [FIPS 198-1]	HMAC-SHA-1	Key Length: 112 bits or greater	Keyed hash
A2952 and A3376	HMAC [FIPS 198-1]	HMAC-SHA2-256	Key Length: 112 bits or greater	Keyed hash
A2952 and A3376	HMAC [FIPS 198-1]	HMAC-SHA2-384	Key Length: 112 bits or greater	Keyed hash
A2952 and A3376	HMAC [FIPS 198-1]	HMAC-SHA2-512	Key Length: 112 bits or greater	Keyed hash
A2952 and A3376	KAS-SSC [SP 800-56Arev3]	KAS-ECC-SSC: Scheme: ephemeralUnified: KAS Role: initiator, responder	Curves: P-256, P-384, P-521	KAS-ECC shared secret computation
A2952 and A3376	KAS [SP800-56Arev3]	KAS (ECC): Scheme: ephemeralUnified KAS Role: initiator, responder KAS (KAS-SSC Cert. #A2952, TLSv1.2 KDF RFC7627 Cert. A#2952, or KDF IKEv2 Cert. #A2952) KAS (KAS-SSC Cert. #A3376, TLSv1.2 KDF RFC7627 Cert. A#3376, or KDF IKEv2 Cert. #A3376)	Curves: P-256, P-384 and P-521 with TLSv1.2 KDF RFC 7627, or KDF IKEv2 (SP800-135rev1) Key establishment methodology provides between 128 and 256 bits of encryption strength	Key Agreement Scheme per SP800-56Arev3 with key derivation function (SP800-135rev1) Note: The module's KAS (ECC) implementation is FIPS 140-3 IG D.F Scenario 2 (path 2) compliant
A2952 and A3376	KAS-SSC [SP 800-56Arev3]	KAS-FFC-SSC: Scheme: dhEphem: KAS Role: initiator, responder	MODP-2048	KAS-FFC shared secret computation
A2952 and A3376	KAS [SP 800-56Arev3]	KAS (FFC): Scheme: dhEphem KAS Role: initiator, responder KAS (KAS-SSC Cert. #A2952, KDF SSH Cert. #A2952, or KDF IKEv2 Cert. #A2952) KAS (KAS-SSC Cert. #A3376, KDF SSH Cert. #A3376, or KDF IKEv2 Cert. #A3376)	MODP-2048 with KDF SSH or KDF IKEv2 (SP800-135rev1) Key establishment methodology provides 112 bits of encryption strength	Key Agreement Scheme per SP800-56Arev3 with key derivation function (SP800-135rev1) Note: The module's KAS (FFC) implementation is FIPS 140-3 IG D.F Scenario 2 (path 2) compliant
A2952 and A3376	RSA [FIPS 186-4]	RSA KeyGen: - Mode: B.3.4 - 2048/3072 modulus	Modulus: 2048/3072	RSA keypair generation

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use/Function
A2952 and A3376	RSA [FIPS 186-4]	RSA SigGen: - PKCSv1.5 - 2048/3072 modulus with SHA-256/384/512	Modulus: 2048/3072	RSA signature generation
A2952 and A3376	RSA [FIPS 186-4]	RSA SigVer: - PKCSv1.5 - 2048/3072 modulus with SHA-256/384/512	Modulus: 2048/3072	RSA signature verification
A2952 and A3376	Safe Primes Key Generation [SP 800-56Arev3]	KeyGen for KAS-SSC (FFC)	Safe Prime Groups: MODP-2048	KAS-FFC Keypair domain parameters generation
A2952 and A3376	SHS [FIPS 180-4]	SHA-1	N/A	Message digest Note: SHA-1 is not used for digital signature generation
A2952 and A3376	SHS [FIPS 180-4]	SHA2-256	N/A	Message digest
A2952 and A3376	SHS [FIPS 180-4]	SHA2-384	N/A	Message digest
A2952 and A3376	SHS [FIPS 180-4]	SHA2-512	N/A	Message digest
Vendor Affirmed	CKG (SP800-133rev2)	Section 5.1, Section 5.2	Cryptographic Key Generation; SP 800-133rev2 and IG D.H.	Key generation. Note: The cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per section 5 in SP800-133rev2 (vendor affirmed). A seed (i.e., the random value) used in asymmetric key generation is a direct output from SP800-90Arev1 CTR_DRBG.

Table 4 Approved Algorithms

Notes:

- Algorithm Cert. #A2952 was tested for the OE with PAA.
- Algorithm Cert. #A3376 was tested for the OE without PAA.
- 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 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. 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. 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.
- No parts of SSH, TLS and IKE protocols, other than the KDFs, have been tested by the CAVP and CMVP.

As the module can only be operated in the Approved mode of operation, and any algorithms not listed in Table 4 above will be rejected by the module while in the approved mode, the tables defined in SP800-140B for the following categories are missing from this document.

- Non-Approved Algorithms Allowed in Approved Mode of Operation
- Non-Approved Algorithms Allowed in Approved Mode of Operation with No Security Claimed
- Non-Approved Algorithms Not Allowed in Approved Mode of Operation

Cryptographic Boundary

The module is defined as a multi-chip standalone software module (inside red dashed area). The cryptographic boundary includes all of the module's software components, including Guest OS, API and FOM Crypto Library (Cisco FIPS Object Module). The physical perimeter is the Tested Operational Environment's Physical Perimeter (TOEPP) on which the module runs.

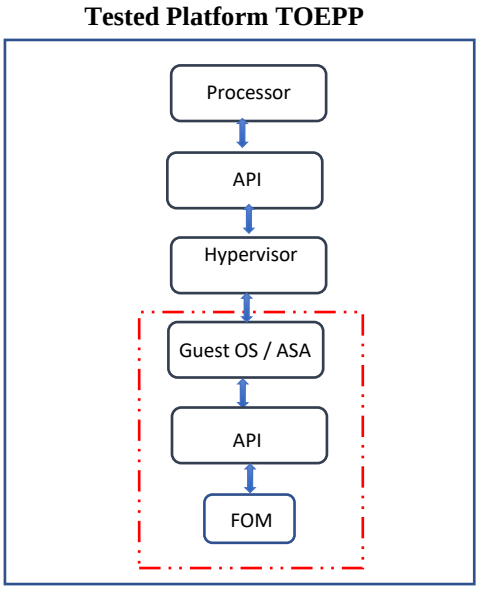

Figure 6 Block Diagram

Note: Block Diagram above is comprised of the following components:

- Processor. Chip handling all processes.
- API = calling between hypervisor and processor

- Hypervisor = VMWare ESXi 6.7, 7.0 or NFVIS 4.4
- Guess OS/ASA = Linux 4 (FX-OS)
- API = calling between the ASA and FOM library
- FOM = Cisco FIPS Object Module (FOM Crypto Library)

3 Cryptographic module interfaces

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

Physical Port	Logical Interface	Data that passes over port/interface
N/A	Data Input Interface	Arguments for an API call that provide the data to be used or processed by the module.
N/A	Data Output Interface	Arguments output from an API call.
N/A	Control Input Interface	Arguments for an API call used to control and configure module operation.
N/A	Control Output Interface	N/A
N/A	Status Output Interface	Return values, and/or log messages.

Table 5 Ports and Interfaces

4 Roles, services, and authentication

The module supports Crypto Officer (CO) role. The cryptographic module does not provide any authentication methods. The module does not allow concurrent operators. The Crypto Officer is implicitly assumed based on the service requested. The module provides the following services to the Crypto Officer role.

Role	Service	Input	Output
Crypto Officer	Show Status	API command to show status	Module's current status
Crypto Officer	Show Version	API commands to show version	Module's name/ID and versioning information
Crypto Officer	Perform Self-Tests	API commands to conduct on-demand Self-Tests	Status of the self-tests results
Crypto Officer	Perform Zeroization	API commands to conduct Zeroization operation or Power down the tested platform	Status of the SSPs zeroization
Crypto Officer	Configure Network	API Commands to configure the module	Status of the completion of network related configuration
Crypto Officer	Configure Bypass capability	API Commands to configure the Bypass capability	Status of the completion of Bypass capability configuration
Crypto Officer	Configure IPsec/IKEv2 Functions	API commands to configure IPsec/IKEv2	Status of completion of IPsec/IKEv2 secure tunnel configuration
Crypto Officer	Configure SSHv2 Function	API commands to configure SSHv2	Status of the completion of SSHv2 configuration
Crypto Officer	Configure HTTPS over TLSv1.2 Function	API commands to configure HTTPS over TLSv1.2	Status of the completion of HTTPS over TLSv1.2 configuration
Crypto Officer	Run SSHv2 Function	API commands to execute SSHv2 service	Status of SSHv2 secure tunnel establishment
Crypto Officer	Run IPsec/IKEv2 Functions	API command to execute IPsec/IKEv2	Status of IPsec/IKEv2 secure tunnel establishment

Crypto Officer	Run Bypass capability	API command to execute Bypass capability	Status of Bypass capability

Table 6 Roles and Services

Table 7 below lists all approved services that can be used in the approved mode of operation. The abbreviations of the access rights to keys and SSPs have the following interpretation:

G = Generate: The module generates or derives the SSP.
R = Read: The SSP is read from the module.
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.
N/A = The service does not access any SSP during its operation.

Services	Description	Approved Security Functions	Keys and /or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Show Status	Provide Module's current status	N/A	N/A	Crypto Officer	N/A	None
Show Version	Provide Module's name/ID and versioning information	N/A	N/A	Crypto Officer	N/A	None
Perform Self-Tests	Perform Self-Tests (Pre-operational self-tests and Conditional Self-Tests)	N/A	Software Integrity Test Key (non-SSP)	Crypto Officer	N/A	None
Perform Zeroization	Perform Zeroization	N/A	All SSPs	Crypto Officer	Z	None
Configure Network	Sets configuration of the systems	N/A	N/A	Crypto Officer	N/A	None
Configure Bypass capability	Sets the Bypass capability	N/A	N/A	Crypto Officer	N/A	None
Configure SSHv2 Function	Configure SSHv2 Function	AES-CBC; CKG; KDF SSH; CTR_DRBG; HMAC-SHA-1; KAS-FFC-SSC; KAS (FFC); RSA KeyGen; RSA SigGen; RSA SigVer; Safe Primes Key Generation; SHA-1	DRBG entropy input; DRBG Seed, Internal State V value, and Key; Diffie-Hellman Private Key; Diffie-Hellman Public Key; Peer Diffie-Hellman Public Key; Diffie-Hellman Shared Secret; RSA Private Key; RSA Public Key; SSH Session Integrity Key;	Crypto Officer	W, E	Global Indicator and SSHv2 configuration success status message

Services	Description	Approved Security Functions	Keys and /or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
			SSH Session Encryption Key			
Configure HTTPS over TLSv1.2 Function	Configure HTTPS over TLSv1.2 Function	AES-CBC; AES-GCM CKG; TLS v1.2 KDF RFC7627; CTR_DRBG ECDSA KeyGen; ECDSA KeyVer; ECDSA SigGen; ECDSA SigVer; HMAC-SHA2-256; HMAC-SHA2-384; HMAC-SHA2-512; KAS-ECC-SSC; KAS (ECC); RSA KeyGen; RSA SigGen; RSA SigVer; SHA2-256; SHA2-384; SHA2-512	DRBG entropy input; DRBG Seed, Internal State V value, and Key; EC Diffie-Hellman Private Key; EC Diffie-Hellman Public Key; Peer EC Diffie-Hellman Public Key; EC Diffie-Hellman Shared Secret; ECDSA Private Key; ECDSA Public Key; RSA Private Key; RSA Public Key; TLS master secret; TLS Session Encryption Key; TLS Session Integrity Key	Crypto Officer	W, E	Global Indicator and HTTPS over TLSv1.2 configuration success status message
Configure IPsec/IKE v2 Function	Configure IPsec/IKEv2 Functions	AES-CBC; AES-GCM; CKG; CTR_DRBG; KDF IKEv2; ECDSA KeyGen; ECDSA KeyVer; ECDSA SigGen; ECDSA SigVer; HMAC-SHA2-256; HMAC-SHA2-384; HMAC-SHA2-512 KAS-ECC-SSC; KAS (ECC); KAS-FFC-SSC; KAS (FFC); RSA KeyGen; RSA SigGen; RSA SigVer; SafePrimes KeyGen; SHA2-256; SHA2-384; SHA2-512	DRBG entropy input; DRBG Seed; Internal State V value; and Key; Diffie-Hellman Private Key; Diffie-Hellman Public Key; Peer Diffie-Hellman Public Key; Diffie-Hellman Shared Secret; EC Diffie-Hellman Private Key; EC Diffie-Hellman Public Key; Peer EC Diffie-Hellman Public Key; EC Diffie-Hellman Shared Secret; ECDSA Private Key; ECDSA Public Key; RSA Private Key; RSA Public Key; IPSec/IKE Pre-Shared Secret; SKEYSEED; IPSec/IKE Session Encryption key;	Crypto Officer	W, E	Global Indicator with IPsec/IKEv2 configuration success status message

Services	Description	Approved Security Functions	Keys and /or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
			IPSec/IKE Session Integrity Key			
Run SSHv2 Function	Execute SSHv2 Function	AES-CBC; CKG; KDF SSH; CTR_DRBG; HMAC-SHA-1; KAS-FFC-SSC; KAS (FFC); RSA KeyGen; RSA SigGen; RSA SigVer; Safe Primes Key Generation; SHA-1	DRBG entropy input; DRBG Seed, Internal State V value, and Key; Diffie-Hellman Private Key; Diffie-Hellman Public Key; Peer Diffie-Hellman Public Key; Diffie-Hellman Shared Secret; RSA Private Key; RSA Public Key; SSH Session Integrity Key; SSH Session Encryption Key	Crypto Officer	W, E	Global Indicator and Successful SSHv2 log message
Run HTTPS over TLSv1.2 Function	Execute HTTPS over TLSv1.2 Function	AES-CBC; AES-GCM; CKG; TLS v1.2 KDF RFC7627; CTR_DRBG; ECDSA KeyGen; ECDSA KeyVer; ECDSA SigGen; ECDSA SigVer; HMAC-SHA2-256; HMAC-SHA2-384; HMAC-SHA2-512; KAS-ECC-SSC; KAS (ECC); RSA KeyGen; RSA SigGen; RSA SigVer; SHA2-256; SHA2-384; SHA2-512	DRBG entropy input; DRBG Seed, Internal State V value, and Key; EC Diffie-Hellman Private Key; EC Diffie-Hellman Public Key; Peer EC Diffie-Hellman Public Key; EC Diffie-Hellman Shared Secret; ECDSA Private Key; ECDSA Public Key; RSA Private Key; RSA Public Key; TLS master secret; TLS Session Encryption Key; TLS Session Integrity Key	Crypto Officer	W, E	Global Indicator and Successful HTTPS over TLSv1.2 log message
Run IPsec/IKE v2 Function	Execute IPsec/IKEv2 Functions	AES-CBC; AES-GCM; CKG; CTR_DRBG; CVL (IKE-KDF); ECDSA KeyGen; ECDSA KeyVer; ECDSA SigGen; ECDSA SigVer; HMAC-SHA2-256; HMAC-SHA2-384; HMAC-SHA2-512	DRBG entropy input; DRBG Seed; Internal State V value; and Key; Diffie-Hellman Private Key; Diffie-Hellman Public Key; Peer Diffie-Hellman Public Key; Diffie-Hellman Shared Secret;	Crypto Officer	W, E	Global Indicator and Successful IPsec/IKEv2 log message

Services	Description	Approved Security Functions	Keys and /or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
		KAS-ECC-SSC; KAS (ECC); KAS-FFC-SSC; KAS (FFC); RSA KeyGen; RSA SigGen; RSA SigVer; SafePrimes KeyGen; SHA2-256; SHA2-384; SHA2-512	EC Diffie-Hellman Private Key; EC Diffie-Hellman Public Key; Peer EC Diffie-Hellman Public Key; EC Diffie-Hellman Shared Secret; ECDSA Private Key; ECDSA Public Key; RSA Private Key; RSA Public Key; IPSec/IKE Pre-Shared Secret; SKEYSEED; IPSec/IKE Session Encryption key; IPSec/IKE Session Integrity Key			
Run Bypass capability	Execute Bypass capability	N/A	N/A	Crypto Officer	N/A	None

Table 7 Approved Services

As the module can only be operated in the Approved mode of operation, and as such any algorithms not listed in Table 4 above will be rejected by the module while in the approved mode, the required table defined in SP800-140B for Non-Approved Services is missing from this document.

5 Software/Firmware security

Integrity techniques

The module is provided in the form of binary executable code. To ensure the software security, the module is protected by RSA 2048 bits with SHA2-512 (RSA and SHA2-512 Cert. #A2952 and #A3376) algorithm. The software integrity test key (non-SSP) was preloaded to the module's binary by/at the factory and used for software integrity test only at the pre-operational self-test. At crypto module library initialization, the signature is recalculated and compared to the hardcoded build-time generated signature value. If at load time the signature does not match, the crypto module library exits with error. If failure occurs during self-test, all crypto functionality is disabled.

Integrity test on-demand

Integrity test is performed as part of the pre-operational self-test. It is automatically executed at power-on. The operator can power cycle or reboot the tested platform to initiate the software integrity test on-demand.

6 Operational environment

The module is a software module, which is operated in a modifiable operational environment per FIPS 140-3 level 1 specifications. The module's software version running on each tested platform is 9.16.4.

The module has control over its own SSPs. The process and memory management functionality of the host device's OS prevent unauthorized access to plaintext private and secret keys, intermediate key generation values and other SSPs by external processes during module execution. The module only allows access to SSPs through its well-defined API. The operational environments provide the capability to separate individual application processes from each other by preventing uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless of whether this data is in the process memory or stored on persistent storage within the operational environment. Processes that are spawned by the module are owned by the module and are not owned by external processes/operators.

7 Physical security

The FIPS 140-3 physical security requirements do not apply to the Module since it is a software module.

8 Non-invasive security

Currently, non-invasive security is not required by FIPS 140-3 (see NIST SP 800-140F). The requirements of this area are not applicable to the module.

9 Sensitive security parameters management

The following table summarizes the keys and Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module.

Key/SSP Name Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
DRBG entropy input (CSP)	384 bits	N/A	Obtained from the Entropy Source within TOEPP (GPS INT Pathways)	Import to the module via Module's API Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when the tested platform is powered down	Random Number Generation
DRBG Seed, Internal State V value, and Key (CSP)	256 bits	CTR_DRBG Certs. #A2952 or #A3376	Internally Derived from entropy input string as defined by SP800-90Arev1	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when the tested platform is powered down	Random Number Generation
Diffie-Hellman Private Key (CSP)	MODP-2048	CKG; CTR_DRBG; KAS (FFC); KAS-FFC-SSC; Safe Primes Key Generation	Internally generated conformant to SP800-133r2 (CKG) using SP800-56A rev3 Diffie-Hellman key generation	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/ SSPs storage.	Automatic zeroization when the tested platform is powered down	Used to derive Diffie-Hellman Shared Secret

Key/SSP Name Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
		Certs. #A2952 or #A3376	method, and the random value used in key generation is generated using SP800-90ARev1 DRBG					
Diffie-Hellman Public Key (PSP)	MODP-2048	KAS (FFC); KAS-FFC-SSC; Safe Primes Key Generation Certs. #A2952 or #A3376	Internally derived per the Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to the SSH Peer application	N/A	N/A: The module does not provide persistent keys/ SSPs storage.	Automatic zeroization when the tested platform is powered down	Used to derive Diffie-Hellman Shared Secret
Peer Diffie-Hellman Public Key (PSP)	MODP-2048	KAS (FFC); KAS-FFC-SSC Certs. #A2952 or #A3376	N/A	Import: to the Module via API Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when the tested platform is powered down	Used to derive Diffie-Hellman Shared Secret
Diffie-Hellman Shared Secret (CSP)	MODP-2048	KAS (FFC); KAS-FFC-SSC Certs. #A2952 or #A3376	Internally generated using SP800-56Arev3 DH shared secret computation	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when the tested platform is powered down	Used to derive SSH session related keys
EC Diffie-Hellman Private Key (CSP)	P-256, P-384 and P-521	CKG; CTR_DRBG; KAS (ECC); KAS-ECC-SSC Certs. #A2952 or #A3376	Internally generated conformant to SP800-133r2 (CKG) using SP800-56A rev3 EC Diffie-Hellman key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/ SSPs storage.	Automatic zeroization when the tested platform is powered down	Used to derive EC Diffie-Hellman Shared Secret
EC Diffie-Hellman Public Key (PSP)	P-256, P-384 and P-521	KAS (ECC); KAS-ECC-SSC Certs. #A2952 or #A3376	Internally derived per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to the TLS Peer application	N/A	N/A: The module does not provide persistent keys/ SSPs storage.	Automatic zeroization when the tested platform is powered down	Used to derive EC Diffie-Hellman Shared Secret

Key/SSP Name Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
Peer EC Diffie-Hellman Public Key (PSP)	P-256, P-384 and P-521	KAS (ECC); KAS-ECC-SSC Certs. #A2952 or #A3376	N/A	Import: to the Module via API Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when the tested platform is powered down	Used to derive EC Diffie-Hellman Shared Secret
EC Diffie-Hellman Shared Secret (CSP)	P-256, P-384 and P-521	KAS (ECC); KAS-ECC-SSC Certs. #A2952 or #A3376	Internally generated using SP800-56Ar3 ECDH shared secret computation	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when the tested platform is powered down	Used to derive TLS session related keys
ECDSA Private Key (CSP)	P-256, P-384 and P-521	CKG; CTR_DRBG ECDSA KeyGen; ECDSA KeyVer; ECDSA SigGen; Certs. #A2952 or #A3376	Internally generated conformant to SP800-133r2 (CKG) using FIPS 186-4 ECDSA key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when the tested platform is powered down	Signature generation and Verification used in TLS or IPSec/IKE
ECDSA Public Key (PSP)	P-256, P-384 and P-521	ECDSA KeyGen; ECDSA KeyVer; ECDSA SigVer; Certs. #A2952 or #A3376	Internally derived per the FIPS 186-4 ECDSA key generation method	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when the tested platform is powered down	Signature generation and Verification used in TLS or IPSec/IKE
RSA Private Key (CSP)	2048 and 3072 bits	CKG; CTR_DRBG; RSA KeyGen; RSA SigGen; Certs. #A2952 or #A3376	Internally generated conformant to SP800-133r2 (CKG) using FIPS 186-4 RSA key generation method, and the random value used in the key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when the tested platform is powered down	Signature generation and Verification used in SSH, TLS or IPSec/IKE
RSA Public Key (PSP)	2048 and	KeyGen; RSA SigVer;	Internally derived per the FIPS 186-4 RSA	Import: No Export: No	N/A	N/A: The module does not	Automatic zeroization when the	Signature generation and Verification

Key/SSP Name Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
	3072 bits	Certs. #A2952 or #A3376	key generation method			provide persistent keys/SSPs storage.	tested platform is powered down	used in SSH, TLS or IPSec/IKE
SSH Session Integrity Key (CSP)	160 bits	KDF SSH; HMAC-SHA-1 Certs. #A2952 or #A3376	Internally Derived per the key derivation function defined in SP800-135 KDF (KDF SSH).	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when SSH session is terminated or when the tested platform is powered down	Used for SSH session integrity protection.
SSH Session Encryption Key (CSP)	128/256 bits	AES-CBC; KDF SSH; Certs. #A2952 or #A3376	Internally Generated via key derivation function defined in SP800-135 KDF (KDF SSH)	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when SSH session is terminated or when the tested platform is powered down	Used for SSH session confidentiality protection
TLS Master Secret (CSP)	48 Bytes	Keying Material	Internally Derived per the key derivation function defined in SP800-135 KDF (KDF-TLS v1.2 RFC7627)	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when TLS session is terminated or when the tested platform is powered down	Keying material used to derive other TLS keys
TLS Session Encryption Key (CSP)	128/256 bits	AES-CBC; AES-GCM; TLS v1.2 KDF RFC7627; Certs. #A2952 or #A3376	Internally Derived per the key derivation function defined in SP800-135 KDF (TLS v1.2 KDF RFC7627)	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when TLS session is terminated or when the tested platform is powered down	Used for TLS session confidentiality protection
TLS Session Integrity Key (CSP)	256-384 bits	HMAC-SHA2-256; HMAC-SHA2-384; TLS v1.2 KDF RFC7627; Certs. #A2952 or #A3376	Internally Derived per the key derivation function defined in SP800-135 KDF (TLS v1.2 KDF RFC7627)	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage.	Automatic zeroization when TLS session is terminated or when the tested platform is powered down	Used for TLS session integrity protection

Key/SSP Name Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
IPSec/IKE Pre-Shared Secret (CSP)	At least 8 characters	N/A	N/A	Import to the Module wrapped with TLS or SSH session keys Export: No	MD/ EE	N/A. The module does not provide persistent keys/ SSPs storage	Zeroized by SSP/CSP/PSP Zeroization Command	Used for IPSec/IKE peer authentication
SKEYSEED (CSP)	160 bits	KDF IKEv2 Certs. #A2952 or #A3376	N/A	Import: No Export: No	N/A	N/A. The module does not provide persistent keys/ SSPs storage	Zeroized when IPSec/IKE session is terminated or when the tested platform is powered down	Used for IPSec/IKE Session Encryption Key and Session Integrity Key derivation
IPSec/IKE Session Encryption Key (CSP)	128/256 bits	AES-CBC; AES-GCM; KDF IKEv2 Certs. #A2952 or #A3376	Internally derived per the key derivation function defined in SP800-135 KDF (KDF IKEv2).	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage	Zeroized when IPSec/IKE session is terminated or when the tested platform is powered down	Used to secure IPSec/IKE session confidentiality
IPSec/IKE Session Integrity Key (CSP)	160-512 bits	HMAC-SHA2-256; HMAC-SHA2-384; HMAC-SHA2-521; KDF IKEv2 Certs. #A2952 or #A3376	Internally derived per the key derivation function defined in SP800-135 KDF (KDF IKEv2).	Import: No Export: No	N/A	N/A: The module does not provide persistent keys/SSPs storage	Zeroized when IPSec/IKE session is terminated or when the tested platform is powered down	Used to secure IPSec/IKE session integrity

Table 8 SSPs

RBG Entropy Source

Entropy sources	Minimum number of bits of entropy	Details
Entropy within the TOEPP was passively load into the Module to seed the 800-90Arev1 DRBG by the Operating System	At least 112 bits	While operating in the Approved Mode, the entropy and seeding material for the SP800-90Arev1 DRBG are provided by the external calling application (and not by the Module) which is outside the Module's Cryptographic boundary but contained within the Module's Tested Operational Environment's Physical Perimeter (TOEPP) boundary. The module receives a LOAD command with entropy obtained from the entropy source (Intel CPU processor with instructions RDRand) inside the TOEPP. The minimum effective strength of the SP 800-90Arev1 DRBG seed is required to be at least 112 bits when used in an approved mode of operation, therefore the minimum

		number of bits of entropy requested when the Module makes a call to the SP 800-90Arev1 DRBG is at least 112 bits. Per the IG 9.3.A Entropy Caveats, the following caveat applies: When operated in approved mode. No assurance of the minimum strength of generated SSPs (e.g., keys).

Table 9 Non-Deterministic Random Number Generation Specification

10 Self-tests

When the module is loaded or instantiated (after being powered off, rebooted, etc.), the module runs pre-operational self-tests. The operating system is responsible for the initialization process and loading of the library. The module is designed with a default entry point (DEP) which ensures that the self-tests are initiated automatically when the module is loaded. 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).

The self-test success or failure results are an output of the return value of the library load API call, which is functioning as the self-test status indicator. If any one 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.

Below are the details of the self-tests conducted by the module.

Pre-Operational Self-Tests:

Pre-operational software integrity test

- RSA 2048 bits with SHA2-512 SigVer KAT
- Software Integrity Test (RSA 2048 bits with SHA2-512)
- Pre-operational Bypass test

Conditional self-test:

- Conditional cryptographic algorithm self-tests (CASTs)
  - AES-CBC 256 bits Encrypt KAT
  - AES-CBC 256 bits Decrypt KAT
  - AES-GCM 256 bits Authenticated Encrypt KAT
  - AES-GCM 256 bits Authenticated Decrypt KAT
  - CTR_DRBG Instantiate KAT
  - CTR_DRBG Generate KAT
  - CTR_DRBG Reseed KAT

  Note: DRBG Health Tests: Generate, Reseed, Instantiate functions per Section 11.3 of SP 800-90Arev1
  - ECDSA P-256 with SHA-256 SigGen KAT
  - ECDSA P-256 with SHA-256 SigVer KAT
  - HMAC-SHA-1 KAT

- HMAC-SHA2-256 KAT
- HMAC-SHA2-384 KAT
- HMAC-SHA2-512 KAT
- KAS-ECC-SSC Primitive Z KAT
- KAS-FFC-SSC Primitive Z KAT
- RSA 2048 bits with SHA2-512 SigGen KAT
- RSA 2048 bits with SHA2-512 SigVer KAT
- SHA-1 KAT
- KDF IKEv2 KAT
- KDF SSH KAT
- TLS v1.2 KDF RFC7627 KAT

- Conditional pair-wise consistency tests (PCTs):
  - RSA PCT
  - ECDSA PCT
  - KAS-ECC PCT
  - KAS-FFC PCT

- Conditional bypass test
  - Conditional bypass test

Periodic/On-Demand 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. In addition, it is recommended for the Crypto Officer to perform the periodic tests a minimum of once every 60 days to ensure all components are functioning correctly.

11 Life-cycle assurance

Secure operations

The module meets all the Level 1 requirements for FIPS 140-3. The validated Module's package asav9-16-4.zip (for VMware ESXi system), or asav9-16-4.qcow2 (for NFVIS system) is the only allowable software image running on the respective tested platform listed in Table 2 above while in the approved mode. The Crypto Officer must configure and enforce the following initialization steps:

Step 1: Install AES licenses to require the module to use AES (for data traffic and SSH).

Step 2: Issue "fips enable" to allow the module to internally enforce approved compliant services.

```
(config)# fips enable
```

Step 3: Disable password recovery.

```
(config)#no service password-recovery
```

Step 4: Set the configuration register to bypass ROMMON prompt at boot.

```
(config)# config-register 0x10011
```

Step 5: Configure the TLS protocol when using HTTPS to protect administrative functions. Due to known issues relating to the use of TLS with certain versions of the Java plugin, we require that you upgrade to JRE 1.5.0_05 or later. The following configuration settings are known to work when launching ASDM in a TLS-only environment with JRE 1.5.0_05:

a. Configure the device to allow only TLSv1.2 packets using the following command:

```
(config)# ssl server-version tlsv2-only
(config)# ssl client-version tlsv2-only
```

b. Check TLS v1.2.0 in both the web browser and JRE security settings.

Step 6: Configure the module to use SSHv2. Note that all operators must still authenticate after remote access is granted.

```
(config)# ssh version 2
```

Step 7: Configure the module such that any remote connections via Telnet are secured through IPSec.

Step 8: Configure the module such that only approved algorithms are used for IPSec tunnels.

Step 9: Configure the IPSec/IKE secure tunnel, including the Access-list (ACL) which classifies the data transferred through the data path to be cryptographic processed or be in Bypass capability.

Step 10: Configure the module such that error messages can only be viewed by a Crypto Officer.

Step 11: Disable the TFTP server.

Step 12: Disable HTTP for performing system management in approved mode of operation. HTTPS with TLS should always be used for Web-based management.

Step 13. Save the configuration.

Step 14: Reboot the Module.

12 Mitigation of other attacks

The requirements under INCITS+ISO+IEC 19790+2012[2014], section 7.12 “Mitigation of other attacks”, are not applicable to the module since the module currently does not support any mitigation of other attacks services.