Cisco Systems, Inc.

Adaptive Security Appliance Virtual Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

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

© 2021-2026
Cisco Systems, Inc.
Cisco Systems logo is registered trademark of Cisco Systems, Inc.

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 5
2.1 Description 5
2.2 Tested and Vendor Affirmed Module Version and Identification 6
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 8
2.6 Security Function Implementations 12
2.7 Algorithm Specific Information 17
2.8 RBG and Entropy 18
2.9 Key Generation 18
2.10 Key Establishment 18
2.11 Industry Protocols 19
3 Cryptographic Module Interfaces 19
3.1 Ports and Interfaces 19
4 Roles, Services, and Authentication 20
4.1 Authentication Methods 20
4.2 Roles 20
4.3 Approved Services 20
4.4 Non-Approved Services 30
4.5 External Software/Firmware Loaded 30
4.6 Bypass Actions and Status 30
4.7 Cryptographic Output Actions and Status 31
4.8 Additional Information 31
5 Software/Firmware Security 31
5.1 Integrity Techniques 31
5.2 Initiate on Demand 31
6 Operational Environment 31
6.1 Operational Environment Type and Requirements 31
7 Physical Security 32
8 Non-Invasive Security 32
9 Sensitive Security Parameters Management 32
9.1 Storage Areas 32

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

9.2 SSP Input-Output Methods 32
9.3 SSP Zeroization Methods 33
9.4 SSPs 33
9.5 Transitions 45
10 Self-Tests 46
10.1 Pre-Operational Self-Tests 46
10.2 Conditional Self-Tests 46
10.3 Periodic Self-Test Information 49
10.4 Error States 51
11 Life-Cycle Assurance 51
11.1 Installation, Initialization, and Startup Procedures 51
11.2 Administrator Guidance 53
11.3 Non-Administrator Guidance 53
12 Mitigation of Other Attacks 53

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 7
Table 3: Tested Module Identification – Hybrid Disjoint Hardware 7
Table 4: Tested Operational Environments - Software, Firmware, Hybrid 7
Table 5: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid 8
Table 6: Modes List and Description 8
Table 7: Approved Algorithms - CiscoSSL FOM - Virtual - PAA 10
Table 8: Approved Algorithms - CiscoSSL FOM - Virtual - Non-PAA 11
Table 9: Vendor-Affirmed Algorithms 12
Table 10: Security Function Implementations 17
Table 11: Ports and Interfaces 19
Table 12: Roles 20
Table 13: Approved Services 30
Table 14: Storage Areas 32
Table 15: SSP Input-Output Methods 33
Table 16: SSP Zeroization Methods 33
Table 17: SSP Table 1 38
Table 18: SSP Table 2 45
Table 19: Pre-Operational Self-Tests 46
Table 20: Conditional Self-Tests 49
Table 21: Pre-Operational Periodic Information 50
Table 22: Conditional Periodic Information 51
Table 23: Error States 51

List of Figures

Figure 1 Block Diagram 6

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

1 General

1.1 Overview

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.

1.2 Security Levels

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

This module is a multi-chip standalone firmware hybrid cryptographic module deployed as the virtualized version of the Cisco Adaptive Security Appliance (ASA) with underlying operating system identified as Linux 4 (also referred to as Firepower eXtensible Operating System or FX-OS throughout this document). The Module’s operational environment is non-modifiable.

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.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Module Characteristics:

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.

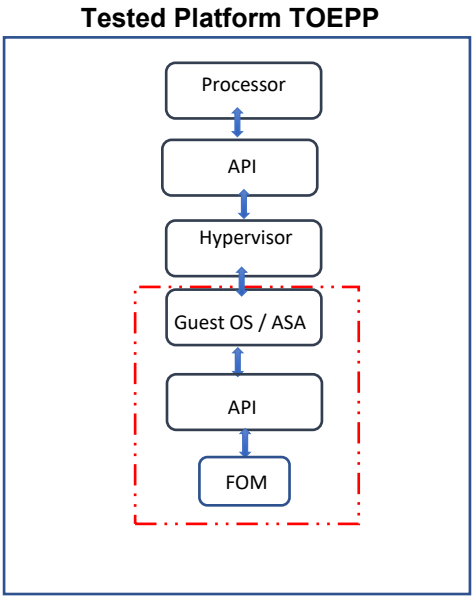

Figure 1 Block Diagram

The Block Diagram above comprises 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)

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Package or File Name	Software/ Firmware Version	Features	Integrity Test
asav9-16-4.zip, asav9-16-4.qcow2	9.16.4		RSA 2048 SigVer with SHA2-512

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

Tested Module Identification – Hybrid Disjoint Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
UCS C220 M5 SFF Server	1.0	VMware ESXi 7.0	Intel Xeon Platinum 8160 (Skylake)	

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Linux 4 (FX-OS) on VMware ESXi 6.7	UCS C220 M5 SFF Server	Intel Xeon Gold 6128 (Skylake)	Yes	VMware ESXi 6.7	9.16.4
Linux 4 (FX-OS) on VMware ESXi 6.7	UCS C220 M5 SFF Server	Intel Xeon Gold 6128 (Skylake)	No	VMware ESXi 6.7	9.16.4
Linux 4 (FX-OS) on VMware ESXi 7.0	UCS C220 M5 SFF Server	Intel Xeon Gold 6128 (Skylake)	Yes	VMware ESXi 7.0	9.16.4
Linux 4 (FX-OS) on VMware ESXi 7.0	UCS C220 M5 SFF Server	Intel Xeon Gold 6128 (Skylake)	No	VMware ESXi 7.0	9.16.4
Linux 4 (FX-OS) on NFVIS 4.4	ENCS 5412 Server	Intel Xeon Processor D-1557 (Broadwell)	Yes	NFVIS 4.4	9.16.4
Linux 4 (FX-OS) on NFVIS 4.4	ENCS 5412 Server	Intel Xeon Processor D-1557 (Broadwell)	No	NFVIS 4.4	9.16.4

Table 4: Tested Operational Environments - Software, Firmware, Hybrid

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

Operating System	Hardware Platform
Linux 4 (FX-OS)	C220 M5 w/KVM/AWS
Linux 4 (FX-OS)	C240 M5 w/ESXi/KVM/AWS
Linux 4 (FX-OS)	C480 M5 w/ESXi/KVM/AWS
Linux 4 (FX-OS)	E160-M3 w/ESXi/KVM/AWS
Linux 4 (FX-OS)	E180D-M3 w/ESXi/KVM/AWS
Linux 4 (FX-OS)	ENCS 5406

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Operating System	Hardware Platform
Linux 4 (FX-OS)	ENCS 5408

Table 5: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved	The module is always in the approved mode of operation after initial operations are performed.	Approved	Approved mode indicator: "FIPS is currently enabled."

Table 6: Modes List and Description

Once the module is configured in the Approved mode of operation by following the steps in section 11 of this document, the module will be ready for approved mode of operation. The module doesn't claim the implementation of a degraded mode operation.

2.5 Algorithms

Approved Algorithms:

CiscoSSL FOM - Virtual - PAA

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A2952	Key Length - 128, 256	SP 800-38A
AES-GCM	A2952	Key Length - 128, 256	SP 800-38D
Counter DRBG	A2952	Prediction Resistance - Yes Supports Reseed - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0-256 Increment 256 Entropy Input - Entropy Input: 128-256 Increment 128, Entropy Input: 256-512 Increment 128 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0-256 Increment 256 Returned Bits - 256	SP 800-90A Rev. 1

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Algorithm	CAVP Cert	Properties	Reference
ECDSA KeyGen (FIPS186-4)	A2952	Curve - P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A2952	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A2952	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A2952	MAC - MAC: 32-160 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-256	A2952	MAC - MAC: 32-256 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-384	A2952	MAC - MAC: 32-384 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-512	A2952	MAC - MAC: 32-512 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A2952	Domain Parameter Generation Methods - P-256, P-384, P-521	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A2952	Domain Parameter Generation Methods - modp-2048	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A2952	Initiator Nonce Length - Initiator Nonce Length: 2048 Responder Nonce Length - Responder Nonce Length: 2048 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 SSH (CVL)	A2952	Cipher - AES-128, AES-192, AES-256, TDES Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A2952	Modulo - 2048, 3072	FIPS 186-4
RSA SigGen (FIPS186-4)	A2952	Signature Type - PKCS 1.5 Modulo - 2048, 3072	FIPS 186-4
RSA SigVer (FIPS186-4)	A2952	Signature Type - PKCS 1.5 Modulo - 2048, 3072	FIPS 186-4
Safe Primes Key Generation	A2952	Safe Prime Groups - modp-2048	SP 800-56A Rev. 3
SHA-1	A2952	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A2952	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A2952	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A2952	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A2952	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1

Table 7: Approved Algorithms - CiscoSSL FOM - Virtual - PAA

CiscoSSL FOM - Virtual - Non-PAA

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3376	Key Length - 128, 256	SP 800-38A
AES-GCM	A3376	Key Length - 128, 256	SP 800-38D
Counter DRBG	A3376	Prediction Resistance - Yes Supports Reseed - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0-256 Increment 256 Entropy Input - Entropy Input: 128-256 Increment 128, Entropy Input: 256-512 Increment 128 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0-256 Increment 256 Returned Bits - 256	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A3376	Curve - P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3376	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3376	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A3376	MAC - MAC: 32-160 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-256	A3376	MAC - MAC: 32-256 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3376	MAC - MAC: 32-384 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-512	A3376	MAC - MAC: 32-512 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A3376	Domain Parameter Generation Methods - P-256, P-384, P-521	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A3376	Domain Parameter Generation Methods - modp-2048	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A3376	Initiator Nonce Length - Initiator Nonce Length: 2048 Responder Nonce Length - Responder Nonce Length: 2048 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 SSH (CVL)	A3376	Cipher - AES-128, AES-192, AES-256, TDES Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A3376	Modulo - 2048, 3072	FIPS 186-4
RSA SigGen (FIPS186-4)	A3376	Modulo - 2048, 3072 Signature Type - PKCS 1.5	FIPS 186-4
RSA SigVer (FIPS186-4)	A3376	Signature Type - PKCS 1.5 Modulo - 2048, 3072	FIPS 186-4
Safe Primes Key Generation	A3376	Safe Prime Groups - modp-2048	SP 800-56A Rev. 3
SHA-1	A3376	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A3376	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A3376	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A3376	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A3376	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1

Table 8: Approved Algorithms - CiscoSSL FOM - Virtual - Non-PAA

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	The cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per sections 4 and 5 in SP800-133rev2 (vendor affirmed) and FIPS

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Properties	Implementation	Reference
			140-3 IG D.H. A seed (i.e., the random value) used in asymmetric key generation is a direct output from SP800-90Arev1 CTR_DRBG (A2952/A3376)

Table 9: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KAS-FFC (SSHv2)	CKG KAS-Full	Full KAS-FFC Key Agreement used for SSHv2 service	Caveat:Key establishment methodology provides 112 bits of security strength IG : IG D.F Path 2, Scenario 2, Split Key Confirmation : No Key Derivation : IG 2.4.B SP 800-135rev1 CVL	KAS-FFC-SSC Sp800-56Ar3: (A2952, A3376) Domain Parameter Generation: MODP-2048 Safe Primes Key Generation: (A2952, A3376) KDF SSH: (A2952, A3376) Counter DRBG: (A2952, A3376) CKG: () Key Type: Asymmetric
KAS-ECC (TLSv1.2)	CKG KAS-Full	Full KAS-ECC Key Agreement used for TLSv1.2 service	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength IG : IG D.F Scenario 2, Path 2, Split Key	KAS-ECC-SSC Sp800-56Ar3: (A2952, A3376) Curves: P-256, P-384, P-521 TLS v1.2 KDF RFC7627: (A2952, A3376) Counter DRBG: (A2952, A3376)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Type	Description	Properties	Algorithms
			Confirmation : No Key Derivation : IG 2.4.B SP 800-135rev1 CVL	CKG: () Key Type: Asymmetric
KAS-FFC (IKEv2)	CKG KAS-Full	Full KAS-FFC Key Agreement used for IKEv2 service	Caveat:Key establishment methodology provides 112 bits of security strength IG : IG D.F Path 2, Scenario 2, Split Key Confirmation : No Key Derivation : IG 2.4.B SP 800-135rev1 CVL	KAS-FFC-SSC Sp800-56Ar3: (A2952, A3376) Domain Parameter Generation: MODP-2048 Safe Primes Key Generation: (A2952, A3376) KDF IKEv2: (A2952, A3376) Counter DRBG: (A2952, A3376) CKG: () Key Type: Asymmetric
KAS-ECC (IKEv2)	CKG KAS-Full	Full KAS-ECC Key Agreement used for IKEv2 service	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength IG : IG D.F Scenario 2, Path 2, Split Key Confirmation : No Key Derivation : IG 2.4.B SP 800-135rev1 CVL	KAS-ECC-SSC Sp800-56Ar3: (A2952, A3376) Curves: P-256, P-384, P-521 KDF IKEv2: (A2952, A3376) Counter DRBG: (A2952, A3376) CKG: () Key Type: Asymmetric
KTS (SSHv2 with AES and HMAC)	KTS-Unwrap KTS-Wrap	KTS via SSHv2 service by using AES and HMAC	Caveat:Key establishment methodology provides 128 or 256 bits of security strength Standard : SP 800-38F IG D.G : "combination" method: use any approved symmetric	AES-CBC: (A2952, A3376) Key Length: 128, 256 bits HMAC-SHA-1: (A2952, A3376) SHA-1: (A2952, A3376)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Type	Description	Properties	Algorithms
			encryption mode together with an approved authentication method	
KTS (TLSv1.2 with AES and HMAC)	KTS-Unwrap KTS-Wrap	KTS via TLSv1.2 service by using AES and HMAC	Caveat:Key establishment methodology provides 128 or 256 bits of security strength Standard : SP 800-38F IG D.G : "combination" method: use any approved symmetric encryption mode together with an approved authentication method	AES-CBC: (A2952, A3376) Key Length: 128, 256 bits HMAC-SHA2-256: (A2952, A3376) HMAC-SHA2-384: (A2952, A3376) HMAC-SHA2-512: (A2952, A3376) SHA2-256: (A2952, A3376) SHA2-384: (A2952, A3376) SHA2-512: (A2952, A3376)
KTS (TLSv1.2 with AES-GCM)	KTS-Unwrap KTS-Wrap	KTS via TLSv1.2 service by using AES-GCM	Caveat:Key establishment methodology provides 128 or 256 bits of security strength Standard : SP 800-38F IG D.G : method: use of any approved authenticated symmetric encryption mode	AES-GCM: (A2952, A3376) Key Length: 128, 256 bits
RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	AsymKeyPair-KeyGen CKG	RSA KeyGen for SSHv2, TLSv1.2, and IKEv2 services		RSA KeyGen (FIPS186-4): (A2952, A3376) Modulus: 2048, 3072 bits Counter DRBG: (A2952, A3376) CKG: () Key Type: Asymmetric

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Type	Description	Properties	Algorithms
ECDSA KeyGen (TLSv1.2, IKEv2)	AsymKeyPair-KeyGen CKG	ECDSA KeyGen for TLSv1.2, and IKEv2 services		ECDSA KeyGen (FIPS186-4): (A2952, A3376) Curves: P-256, P-384, P-521 Counter DRBG: (A2952, A3376) CKG: () Key Type: Asymmetric
RSA SigGen (SSHv2, TLSv1.2, IKEv2)	DigSig-SigGen	RSA SigGen for SSHv2, TLSv1.2, and IKEv2 services		RSA SigGen (FIPS186-4): (A2952, A3376) Modulus: 2048, 3072 bits
ECDSA SigGen (TLSv1.2, IKEv2)	DigSig-SigGen	ECDSA SigGen for TLSv1.2, and IKEv2 services		ECDSA SigGen (FIPS186-4): (A2952, A3376) Curves: P-256, P-384, P-521
RSA SigVer (SSHv2, TLSv1.2, IKEv2)	DigSig-SigVer	RSA SigVer for SSHv2, TLSv1.2, and IKEv2 services		RSA SigVer (FIPS186-4): (A2952, A3376) Modulus: 2048, 3072 bits
ECDSA SigVer (TLSv1.2, IKEv2)	DigSig-SigVer	ECDSA SigVer for TLSv1.2, and IKEv2 services		ECDSA SigVer (FIPS186-4): (A2952, A3376) Curves: P-256, P-384, P-521
SSHv2 Session Encrypt/Decrypt	BC-UnAuth	SSHv2 session protection.	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-CBC: (A2952, A3376) Key Length: 128, 256 bits
SSHv2 Session Authentication	MAC	SSHv2 Session Authentication.		HMAC-SHA-1: (A2952, A3376) SHA-1: (A2952, A3376)
SSHv2 Keying Materials Development	KAS-135KDF	SSHv2 session keying materials, used to derive SSHv2 session keys.		KDF SSH: (A2952, A3376)
TLSv1.2 Session Encrypt/Decrypt	BC-Auth BC-UnAuth	TLSv1.2 session protection	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-CBC: (A2952, A3376) Key Length: 128, 256 bits AES-GCM:

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Type	Description	Properties	Algorithms
				(A2952, A3376) Key Length: 128, 256 bits
TLSv1.2 Session Authentication	MAC	TLSv1.2 session authentication.		HMAC-SHA2-256: (A2952, A3376) HMAC-SHA2-384: (A2952, A3376) HMAC-SHA2-512: (A2952, A3376) SHA2-256: (A2952, A3376) SHA2-384: (A2952, A3376) SHA2-512: (A2952, A3376)
TLSv1.2 Keying Materials Development	KAS-135KDF	TLSv1.2 session keying materials, used to derive TLS session keys.		TLS v1.2 KDF RFC7627: (A2952, A3376)
IPsec/IKEv2 Session Encrypt/Decrypt	BC-Auth BC-UnAuth	IPsec/IKEv2 session protection	Bit-strength Caveat:Provides 128 or 256 bits of encryption strength	AES-CBC: (A2952, A3376) Key Length: 128, 256 bits AES-GCM: (A2952, A3376) Key Length: 128, 256 bits
IPsec/IKEv2 Session Authentication	MAC	IPsec/IKEv2 session authentication.		HMAC-SHA2-256: (A2952, A3376) HMAC-SHA2-384: (A2952, A3376) HMAC-SHA2-512: (A2952, A3376) SHA2-256: (A2952, A3376) SHA2-384: (A2952, A3376) SHA2-512: (A2952, A3376)
IPsec/IKEv2 Keying Materials Development	KAS-135KDF	IPsec/IKEv2 session keying materials, used		KDF IKEv2: (A2952, A3376)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Type	Description	Properties	Algorithms
		to derive IPsec/IKEv2 session keys.		
DRBG Function	DRBG	Used for DRBG generation		Counter DRBG: (A2952, A3376)

Table 10: 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 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. 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. 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. 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.

- In accordance with FIPS 140-3 IG D.H, the cryptographic module performs Cryptographic Key Generation as per section 5 in SP800-133rev2. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90Arev1 DRBG.

- 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.

- Per SP800-131Ar2, the use of SHA-1 is disallowed for digital signature generation, but is permitted for digital signature verification (legacy use) and all non-digital signature applications. This implementation will be non-Approved for all uses starting January 1, 2031. User should move to SHA2, which is available in this module.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

2.8 RBG and Entropy

The module employs a Deterministic Random Bit Generator (DRBG) implementation based on SP800-90Arev1. This DRBG is used internally by the module (e.g. to generate symmetric keys, seeds for asymmetric key pairs, and random numbers for security functions).

The DRBG implemented is an AES-256 Counter DRBG, seeded by the Entropy within the TOEPP which is passively loaded into the Module to seed the SP 800-90Arev1 DRBG by the Operating System. The Counter DRBG utilizes the Derivation Function. It does not employ prediction resistance.

The DRBG is instantiated with a 384-bits long entropy input (corresponding to 384 bits of entropy). Additionally, the DRBG is reseeded with a 256-bits long entropy input (corresponding to 256 bits of entropy).

2.9 Key Generation

The module implements Cryptographic Key Generation (CKG, vendor affirmed), compliant with SP 800- 133r2. When random values are required, they are obtained from the SP 800-90Ar1 approved DRBG, compliant with Section 4 of SP 800-133r2. The following methods are implemented:

- Safe primes key pair generation: compliant with SP 800-133rev2, Section 5.2, which maps to SP 800-56Arev3. The method described in Section 5.6.1.1.4 of SP 800-56Ar3 (“Testing Candidates”) is used.

- RSA key pair generation: compliant with SP 800-133rev2, Section 5.1, which maps to FIPS 186-4. The method described in Appendix B.3 of FIPS 186-4 (“Probable Primes”) is used.

- ECC (ECDH and ECDSA) key pair generation: compliant with SP 800-133r2, Section 5.1, which maps to FIPS 186-4. The method described in Appendix B.4 of FIPS 186-4 (“Testing Candidates”) is used. Note that this generation method is also used to generate ECDH key pairs.

Additionally, the module implements the following key derivation methods:

- SSHv2 KDF, TLS 1.2 KDF, IKEv2 KDF: compliant with SP 800-135r1. These implementations shall only be used to generate secret keys in the context of the SSHv2, TLSv1.2 and IKEv2 KDF protocols, respectively.

Intermediate key generation values are not output from the module and are explicitly zeroized after processing the service

2.10 Key Establishment

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

KAS-FFC Shared Secret Computation:

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

- 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 112 bits of encryption strength.

- The module supports the use of the safe primes defined in RFC 4419 (SSH) and RFC 3526 (IKE). Note that the module only implements domain parameter generation, key pair generation and verification, and shared secret computation.
    - SSH (RFC 4419):
        - MODP-2048 (ID = 14)
    - IKE (RFC 3526):
        - MODP-2048 (ID = 14)

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.

The module also provides the following key transport mechanisms:

- Key wrapping using AES-GCM with a security strength of 128 or 256 bits.

- Key wrapping using AES-CBC with a security strength of 128 or 256 bits with HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512.

2.11 Industry Protocols

The module supports SSHv2, TLSv1.2 and IPsec/IKEv2 industrial protocols. No parts of SSHv2, TLSv1.2 or IPsec/IKEv2 protocols, other than the KDFs, have been tested by the CAVP and CMVP. Please refer to SSPs Table for more information.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

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

Table 11: Ports and Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Table 2. The module provides its logical interfaces via Application Programming Interface (API)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

calls. The logical interfaces provided by the module are mapped onto the FIPS 140-3 interfaces (data input, data output, control input, control output and status output).

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	Crypto Officer	None

Table 12: Roles

The module supports Crypto Officer (CO) role. The module does not allow concurrent operators. The Crypto Officer is implicitly assumed based on the service requested.

4.3 Approved Services

The following tables detail the types of approved services available to each role in approved mode of operation, the types of access for each role and the Keys or SSPs they affect.

- Generate G
- Read Access R
- Write Access W
- Execute Access E
- Zeroize Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status	Provide Module's current status	None	API command to show status.	Module's current status.	None	Crypto Officer
Show Version	Provide Module's name/ID and versioning information.	None	API commands to show version.	Module's name/ID and versioning information	None	Crypto Officer
Perform Self-Tests	Perform Self-Tests (Pre-operational self-tests and Conditiona	None	API commands to conduct on-demand Self-Tests.	Status of the self-tests results.	None	Crypto Officer

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	l Self-Tests)					
Perform Zeroization	Perform Zeroization.	None	API commands to conduct Zeroization operation or Power down the tested platform.	Status of the SSPs zeroization.	None	Crypto Officer - DRBG Entropy Input: Z - DRBG Seed: Z - DRBG Internal State V value: Z - DRBG Key: Z - SSH DH Private Key: Z - SSH DH Public Key: Z - SSH Peer DH Public Key: Z - SSH DH Shared Secret: Z - SSH RSA Private Key: Z - SSH RSA Public Key: Z - SSH Session Encryption Key: Z - SSH Session Authentication Key: Z - TLS ECDH Private Key: Z - TLS ECDH Public Key: Z

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS Peer ECDH Public Key: Z - TLS ECDH Shared Secret: Z - TLS RSA Private Key: Z - TLS RSA Public Key: Z - TLS ECDSA Private Key: Z - TLS ECDSA Public Key: Z - TLS Master Secret: Z - TLS Session Encryption Key: Z - TLS Session Authentication Key: Z - IPsec/IKEv2 DH Private Key: Z - IPsec/IKEv2 DH Public Key: Z - IPsec/IKEv2 Peer DH Public Key: Z - IPsec/IKEv

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						2 DH Shared Secret: Z - IPsec/IKEv2 ECDH Private Key: Z - IPsec/IKEv2 ECDH Public Key: Z - IPsec/IKEv2 Peer ECDH Public Key: Z - IPsec/IKEv2 ECDH Shared Secret: Z - IPsec/IKEv2 RSA Private Key: Z - IPsec/IKEv2 RSA Public Key: Z - IPsec/IKEv2 ECDSA Private Key: Z - IPsec/IKEv2 ECDSA Public Key: Z - IPsec/IKEv2 Pre-Shared Secret: Z

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SKEYSEED: Z - IPsec/IKEv2 Session Encryption Key: Z - IPsec/IKEv2 Authentication Key: Z
Configure Network	Sets configuration of the systems.	None	API commands to configure the module.	Status of the completion of network related configuration.	None	Crypto Officer
Configure Bypass capability	Sets the Bypass capability	None	API commands to configure the Bypass capability.	Status of the completion of Bypass capability configuration.	None	Crypto Officer
Configure SSHv2 Function	Configure SSHv2 Function	Global Indicator and SSHv2 configuration success status message.	API commands to configure SSHv2.	Status of the completion of SSHv2 configuration.	KTS (SSHv2 with AES and HMAC) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) DRBG Function	Crypto Officer - SSH RSA Private Key: G,W,E - SSH RSA Public Key: G,R,W - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Key: G,W,E
Configure HTTPS over TLSv1.2 Function	Configure HTTPS over TLSv1.2 Function.	Global Indicator and HTTPS over TLSv1.2 configuration success status message.	API commands to configure HTTPS over TLSv1.2	Status of the completion of HTTPS over TLSv1.2 configuration.	KTS (SSHv2 with AES and HMAC) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen (TLSv1.2, IKEv2) DRBG Function	Crypto Officer - TLS RSA Private Key: G,W,E - TLS RSA Public Key: G,R,W - TLS ECDSA Private Key: G,W,E - TLS ECDSA Public Key: G,R,W - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E - DRBG Key: G,W,E
Configure IPsec/IKEv2 Functions	Configure IPsec/IKEv2 Functions	Global Indicator with IPsec/IKEv2 configuration success status message.	API commands to configure IPsec/IKEv2.	Status of the completion of IPsec/IKEv2 secure tunnel configuration.	KTS (SSHv2 with AES and HMAC) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) RSA KeyGen (SSHv2, TLSv1.2, IKEv2) ECDSA KeyGen	Crypto Officer - IPsec/IKEv2 RSA Private Key: G,W,E - IPsec/IKEv2 RSA Public Key: G,W,E - IPsec/IKEv2 ECDSA Private Key: G,W,E

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(TLSv1.2, IKEv2) DRBG Function	- IPsec/IKEv2 ECDSA Public Key: G,W,E - IPsec/IKEv2 Pre-Shared Secret: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E - DRBG Key: G,W,E
Run SSHv2 Function	Execute SSHv2 Function	Global Indicator and Successful SSHv2 log message.	API commands to execute SSHv2 service.	Status of SSHv2 secure tunnel establishment.	KAS-FFC (SSHv2) KTS (SSHv2 with AES and HMAC) RSA SigGen (SSHv2, TLSv1.2, IKEv2) RSA SigVer (SSHv2, TLSv1.2, IKEv2) SSHv2 Session Encrypt/Decrypt SSHv2 Session Authentication SSHv2 Keying Materials	Crypto Officer - SSH DH Private Key: G,W,E - SSH DH Public Key: G,R,W - SSH Peer DH Public Key: W,E - SSH DH Shared Secret: G,W,E - SSH RSA Private Key: G,W,E - SSH RSA Public Key: G,R,W - SSH Session Encryption

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Development DRBG Function	Key: G,W,E - SSH Session Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E - DRBG Key: G,W,E
Run HTTPS over TLSv1.2 Function	Execute HTTPS over TLSv1.2 Function.	Global Indicator and Successful HTTPS over TLSv1.2 log message.	API command to execute HTTPS over TLSv1.2 service.	Status of HTTPS over TLSv1.2 establishment.	KAS-ECC (TLSv1.2) KTS (TLSv1.2 with AES and HMAC) KTS (TLSv1.2 with AES-GCM) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (TLSv1.2, IKEv2) RSA SigVer (SSHv2, TLSv1.2, IKEv2) ECDSA SigVer (TLSv1.2, IKEv2) TLSv1.2 Session Encrypt/Decr	Crypto Officer - TLS ECDH Private Key: G,W,E - TLS ECDH Public Key: G,R,W - TLS Peer ECDH Public Key: W,E - TLS ECDH Shared Secret: G,W,E - TLS RSA Private Key: G,W,E - TLS RSA Public Key: G,R,W - TLS ECDSA Private Key: G,W,E

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					ypt TLSv1.2 Session Authentication TLSv1.2 Keying Materials Development DRBG Function	- TLS ECDSA Public Key: G,R,W - TLS Master Secret: G,W,E - TLS Session Encryption Key: G,W,E - TLS Session Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E - DRBG Key: G,W,E
Run IPsec/IKEv2 Functions	Execute IPsec/IKEv2 Functions	Global Indicator and Successful IPsec/IKEv2 log message.	API command to execute IPsec/IKEv2	Status of IPsec/IKEv2 secure tunnel establishment	KAS-FFC (IKEv2) KAS-ECC (IKEv2) RSA SigGen (SSHv2, TLSv1.2, IKEv2) ECDSA SigGen (TLSv1.2, IKEv2) RSA SigVer (SSHv2, TLSv1.2, IKEv2) ECDSA SigVer	Crypto Officer - IPsec/IKEv2 DH Private Key: G,W,E - IPsec/IKEv2 DH Public Key: G,R,W - IPsec/IKEv2 Peer DH Public Key: W,E - IPsec/IKEv

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(TLSv1.2, IKEv2) IPsec/IKEv2 Session Encrypt/Decrypt IPsec/IKEv2 Session Authentication IPsec/IKEv2 Keying Materials Development DRBG Function	2 DH Shared Secret: G,W,E - IPsec/IKEv2 ECDH Private Key: G,W,E - IPsec/IKEv2 ECDH Public Key: G,R,W - IPsec/IKEv2 Peer ECDH Public Key: W,E - IPsec/IKEv2 ECDH Shared Secret: G,W,E - IPsec/IKEv2 RSA Private Key: G,W,E - IPsec/IKEv2 RSA Public Key: G,W,E - IPsec/IKEv2 ECDSA Private Key: G,W,E - IPsec/IKEv2 ECDSA Public Key: G,W,E - IPsec/IKEv2 Pre-

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Shared Secret: G,W,E - SKEYSEED: G,W,E - IPsec/IKEv2 Session Encryption Key: G,W,E - IPsec/IKEv2 Authentication Key: G,W,E - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E - DRBG Key: G,W,E

Table 13: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

N/A for this module.

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

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

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. The unauthenticated operator can trigger 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 software security, the library is protected by RSA 2048 SigVer with SHA2-512 (RSA and SHA2-512 Cert. #A2952 or #A3376) signature calculated at build time. 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.

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 integrity test on-demand.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

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.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

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

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DRAM	Volatile memory provided by the ESXi host for the module temporary.	Dynamic
Flash	Non-Volatile memory provided by the ESXi host for the module to retain memory across power-cycles.	Static

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Peer Public Key Input	External (Outside of the Module's Boundary)	Module	Plaintext	Automated	Electronic	
Module Public Key Output	Module	External (Outside of the Module's Boundary)	Plaintext	Automated	Electronic	
Secret Input via SSHv2	External (Outside of the	Module	Encrypted	Automated	Electronic	KTS (SSHv2

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
encrypted by AES and HMAC	Module's Boundary)					with AES and HMAC)
Secret Input via TLS encrypted by GCM	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	KTS (TLSv1.2 with AES-GCM)
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 15: 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 of the module.	`configure factory-default`
Session Termination	Zeroization upon session termination	Session termination will automatically zeroize all session based temporary SSPs	Terminate session
Reboot	Zeroization upon rebooting the module	Reboot to zeroize all temporary SSPs stored in volatile memory	Reboot

Table 16: SSP Zeroization Methods

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			DRBG Function
DRBG Seed	Used in DRBG Generation	256 bits - 256 bits	DRBG Seed - CSP			DRBG Function
DRBG Internal State V value	Used in DRBG Generation	256 bits - 256 bits	DRBG Internal State V value - CSP			DRBG Function

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Key	Used in DRBG Generation	256 bits - 256 bits	DRBG Key - CSP			DRBG Function
SSH DH Private Key	Used to derive the SSH DH Shared Secret	MODP-2048 - 112 bits	Private Key - CSP	KAS-FFC (SSHv2)		KAS-FFC (SSHv2)
SSH DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048 - 112 bits	Public Key - PSP		KAS-FFC (SSHv2)	
SSH Peer DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048 - 112 bits	Public Key - PSP			KAS-FFC (SSHv2)
SSH DH Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys	MODP-2048 - 112 bits	Shared Secret - CSP		KAS-FFC (SSHv2)	SSHv2 Keying Materials Development
SSH RSA Private Key	Used for SSH session authentication	Modulus 2048 and 3072 bits - 112 or 128 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		RSA SigGen (SSHv2, TLSv1.2, IKEv2)
SSH RSA Public Key	Used for SSH session authentication	Modulus 2048 and 3072 bits - 112 or 128 bits	Public Key - PSP		RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	
SSH Session Encryption Key	Used for SSH session confidentiality protection	128, 256 bits - 128 or 256 bits	Symmetric Key - CSP		SSHv2 Keying Materials Development	SSHv2 Session Encrypt/Decrypt
SSH Session	Used for SSH Session	At least 160 bits	Session Key - CSP		SSHv2 Keying Materials	SSHv2 Session

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Authentication Key	integrity protection	- At least 160 bits			Development	Authentication
TLS ECDH Private Key	Used to Derive TLS ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Private Key - CSP	KAS-ECC (TLSv1.2)		KAS-ECC (TLSv1.2)
TLS ECDH Public Key	Used to Derive TLS ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		KAS-ECC (TLSv1.2)	
TLS Peer ECDH Public Key	Used to derive TLS ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP			KAS-ECC (TLSv1.2)
TLS ECDH Shared Secret	Used to Derive TLS Session Encryption Key and TLS Session Authentication Key	Curves: P-256, P-384, P-521 - 128 to 256 bits	Shared Secret - CSP		KAS-ECC (TLSv1.2)	TLSv1.2 Keying Materials Development
TLS RSA Private Key	Used to support CO HTTPS interfaces	Modulus 2048 and 3072 bits - 112 or 128 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		RSA SigGen (SSHv2, TLSv1.2, IKEv2)
TLS RSA Public Key	Used to support CO HTTPS interfaces	Modulus 2048 and 3072 bits - 112 or 128 bits	Public Key - PSP		RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	
TLS ECDSA Private Key	Used to support CO HTTPS interfaces	Curves: P-256, P-384, P-521 -	Private Key - CSP	ECDSA KeyGen (TLSv1.2, IKEv2)		ECDSA SigGen (TLSv1.2, IKEv2)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128 to 256 bits				
TLS ECDSA Public Key	Used to support CO HTTPS interfaces	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		ECDSA KeyGen (TLSv1.2, IKEv2)	
TLS Master Secret	Used to protect HTTPS Session	384 bits - 384 bits	Master Secret - CSP		TLSv1.2 Keying Materials Development	TLSv1.2 Session Encrypt/Decrypt TLSv1.2 Session Authentication
TLS Session Encryption Key	Used to protect HTTPS Session	128, 256 bits - 128 or 256 bits	Symmetric Key - CSP		TLSv1.2 Keying Materials Development	TLSv1.2 Session Encrypt/Decrypt
TLS Session Authentication Key	Used to authenticate HTTPS Session	160, 256, 384 bits - 160, 256 or 384 bits	Message Authentication Key - CSP		TLSv1.2 Keying Materials Development	TLSv1.2 Session Authentication
IPsec/IKEv2 DH Private Key	Used to derive IPsec/IKEv2 DH Shared Secret	MODP-2048 - 112 bits	Private Key - CSP	KAS-FFC (IKEv2)		KAS-FFC (IKEv2)
IPsec/IKEv2 DH Public Key	Used to derive IPsec/IKEv2 DH Shared Secret	MODP-2048 - 112 bits	Public Key - PSP		KAS-FFC (IKEv2)	
IPsec/IKEv2 Peer DH Public Key	Used to derive IPsec/IKEv2 DH Shared Secret	MODP-2048 - 112 bits	Public Key - PSP			KAS-FFC (IKEv2)

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
IPsec/IKEv2 DH Shared Secret	Used to derive IPsec/IKEv2 Session Shared Secret	MODP-2048 - 112 bits	Shared Secret - CSP		KAS-FFC (IKEv2)	IPsec/IKEv2 Keying Materials Development
IPsec/IKEv2 ECDH Private Key	Used to derive IPsec/IKEv2 ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Private key - CSP	KAS-ECC (IKEv2)		KAS-ECC (IKEv2)
IPsec/IKEv2 ECDH Public Key	Used to derive IPsec/IKEv2 ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		KAS-ECC (IKEv2)	
IPsec/IKEv2 Peer ECDH Public Key	Used to derive IPsec/IKEv2 ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP			KAS-ECC (IKEv2)
IPsec/IKEv2 ECDH Shared Secret	Used to derive IPsec/IKEv2 ECDH Shared Secret	Curves: P-256, P-384, P-521 - 128 to 256 bits	Shared Secret - CSP		KAS-ECC (IKEv2)	IPsec/IKEv2 Keying Materials Development
IPsec/IKEv2 RSA Private Key	Used for IPsec/IKEv2 authentication	Modulus 2048 and 3072 bits - 112 or 128 bits	Private Key - CSP	RSA KeyGen (SSHv2, TLSv1.2, IKEv2)		RSA SigGen (SSHv2, TLSv1.2, IKEv2)
IPsec/IKEv2 RSA Public Key	Used for IPsec/IKEv2 authentication	Modulus 2048 and 3072 bits - 112 or 128 bits	Public Key - PSP		RSA KeyGen (SSHv2, TLSv1.2, IKEv2)	
IPsec/IKEv2 ECDSA Private Key	Used for IPsec/IKEv2	Curves: P-256, P-384,	Private Key - CSP	ECDSA KeyGen		ECDSA SigGen

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	authentication	P-521 - 128 to 256 bits		(TLSv1.2, IKEv2)		(TLSv1.2, IKEv2)
IPsec/IKEv2 ECDSA Public Key	Used for IPsec/IKEv2 authentication	Curves: P-256, P-384, P-521 - 128 to 256 bits	Public Key - PSP		ECDSA KeyGen (TLSv1.2, IKEv2)	
IPsec/IKEv2 Pre-Shared Secret	Used for IPsec/IKEv2 authentication	1-128 characters - 1-128 characters	Shared Secret - CSP			
SKEYSEED	Keying material used to derive the IPSec/IKE Session Encryption Key and IPSec/IKE Authentication Key	160 bits - 160 bits	Keying Material - CSP		IPsec/IKEv2 Keying Materials Development	IPsec/IKEv2 Session Encrypt/Decrypt IPsec/IKEv2 Session Authentication
IPsec/IKEv2 Session Encryption Key	Used to secure IPsec/IKEv2 session confidentiality	128, 256 bits - 128 or 256 bits	Symmetric Key - CSP		IPsec/IKEv2 Keying Materials Development	IPsec/IKEv2 Session Encrypt/Decrypt
IPsec/IKEv2 Authentication Key	Used to secure IPsec/IKEv2 session authentication	at least 160 bits - at least 160 bits	Message Authentication Key - CSP		IPsec/IKEv2 Keying Materials Development	IPsec/IKEv2 Session Authentication

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Entropy Input		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	DRBG Seed:Used With DRBG Internal State V value:Used With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					DRBG Key:Used With
DRBG Seed		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	DRBG Entropy Input:Used With DRBG Internal State V value:Used With DRBG Key:Used With
DRBG Internal State V value		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Key:Used With
DRBG Key		DRAM:Plaintext	Until Reboot	Zeroization Command Reboot	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Internal State V value:Used With
SSH DH Private Key		DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	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 session is active	Zeroization Command Session Termination Reboot	SSH DH Private Key:Paired With
SSH Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH DH Private Key:Used With
SSH DH Shared Secret		DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH DH Private Key:Derived From SSH Peer DH Public Key:Derived From
SSH RSA Private Key		Flash:Plaintext		Zeroization Command	SSH RSA Public Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH RSA Public Key	Module Public Key Output Secret Input via SSHv2 encrypted by AES and HMAC Secret Input via TLS encrypted by GCM Secret Input via TLS encrypted by AES and HMAC	Flash:Plaintext		Zeroization Command	SSH RSA Private Key:Paired With
SSH Session Encryption Key		DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH Session Authentication Key:Used With
SSH Session Authentication Key		DRAM:Plaintext	While SSH session is active	Zeroization Command Session Termination Reboot	SSH Session Encryption Key:Used With
TLS ECDH Private Key		DRAM:Plaintext	While TLS session is active	Zeroization Command Session Termination Reboot	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 session is active	Zeroization Command Session Termination Reboot	TLS ECDH Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TLS Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While TLS session is active	Zeroization Command Session Termination Reboot	TLS ECDH Private Key:Used With
TLS ECDH Shared Secret		DRAM:Plaintext	While TLS session is active	Zeroization Command Session Termination Reboot	TLS ECDH Private Key:Derived From TLS Peer ECDH Public Key:Derived From
TLS RSA Private Key		Flash:Plaintext		Zeroization Command	TLS RSA Public Key:Paired With
TLS RSA Public Key	Module Public Key Output Secret Input via SSHv2 encrypted by AES and HMAC Secret Input via TLS encrypted by GCM Secret Input via TLS encrypted by AES and HMAC	Flash:Plaintext		Zeroization Command	TLS RSA Private Key:Paired With
TLS ECDSA Private Key		Flash:Plaintext		Zeroization Command	TLS ECDSA Public Key:Paired With
TLS ECDSA Public Key	Module Public Key Output Secret Input via SSHv2 encrypte	Flash:Plaintext		Zeroization Command	TLS ECDSA Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	d by AES and HMAC Secret Input via TLS encrypted by GCM Secret Input via TLS encrypted by AES and HMAC				
TLS Master Secret		DRAM:Plaintext	While TLS session is active	Zeroization Command Session Termination Reboot	TLS ECDH Shared Secret:Derived From
TLS Session Encryption Key		DRAM:Plaintext	While TLS session is active	Zeroization Command Session Termination Reboot	TLS Session Authentication Key:Used With TLS Master Secret:Derived From
TLS Session Authentication Key		DRAM:Plaintext	While TLS session is active	Zeroization Command Session Termination Reboot	TLS Session Encryption Key:Used With TLS Master Secret:Derived From
IPsec/IKEv2 DH Private Key		DRAM:Plaintext	While IPsec/IKEv2 tunnel is active	Zeroization Command Session Termination Reboot	IPsec/IKEv2 DH Public Key:Paired With IPsec/IKEv2 Peer DH Public Key:Used With
IPsec/IKEv2 DH Public Key	Module Public Key Output	DRAM:Plaintext	While IPsec/IKEv2 tunnel is active	Zeroization Command Session Termination Reboot	IPsec/IKEv2 DH Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
IPsec/IKEv2 Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	While IPsec/IKEv2 tunnel is active	Zeroization Command Session Termination Reboot	IPsec/IKEv2 DH Private Key:Used With
IPsec/IKEv2 DH Shared Secret		DRAM:Plaintext	While IPsec/IKEv2 tunnel is active	Zeroization Command Session Termination Reboot	SKEYSEED:Used With
IPsec/IKEv2 ECDH Private Key		DRAM:Plaintext	While IPsec/IKEv2 tunnel is active	Zeroization Command Session Termination Reboot	IPsec/IKEv2 ECDH Public Key:Paired With IPsec/IKEv2 Peer ECDH Public Key:Used With
IPsec/IKEv2 ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While IPsec/IKEv2 tunnel is active	Zeroization Command Session Termination Reboot	IPsec/IKEv2 ECDH Private Key:Paired With
IPsec/IKEv2 Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While IPsec/IKEv2 tunnel is active	Zeroization Command Session Termination Reboot	IPsec/IKEv2 ECDH Private Key:Used With
IPsec/IKEv2 ECDH Shared Secret		DRAM:Plaintext	While IPsec/IKEv2 tunnel is active	Zeroization Command Session Termination Reboot	IPsec/IKEv2 ECDH Private Key:Derived From IPsec/IKEv2 Peer ECDH Public Key:Derived From SKEYSEED:Used With
IPsec/IKEv2 RSA Private Key		Flash:Plaintext		Zeroization Command	IPsec/IKEv2 RSA Public Key:Paired With
IPsec/IKEv2 RSA Public Key	Module Public Key Output Secret Input via SSHv2	Flash:Plaintext		Zeroization Command	IPsec/IKEv2 RSA Private Key:Paired With

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Input - Output	Storage	Storage Duration	Zeroizatio n	Related SSPs
	encrypte d by AES and HMAC Secret Input via TLS encrypte d by GCM Secret Input via TLS encrypte d by AES and HMAC				
IPsec/IKEv2 ECDSA Private Key		Flash:Plaintext		Zeroization Command	IPsec/IKEv2 ECDSA Public Key:Paired With
IPsec/IKEv2 ECDSA Public Key	Module Public Key Output Secret Input via SSHv2 encrypte d by AES and HMAC Secret Input via TLS encrypte d by GCM Secret Input via TLS encrypte d by AES and HMAC	Flash:Plaintext		Zeroization Command	IPsec/IKEv2 ECDSA Private Key:Paired With
IPsec/IKEv2 Pre-Shared Secret	Secret Input via SSHv2 encrypte	Flash:Plaintext		Zeroization Command	SKEYSEED:Derive d to

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Name	Input - Output	Storage	Storage Duration	Zeroizatio n	Related SSPs
	d by AES and HMAC Secret Input via TLS encrypte d by GCM Secret Input via TLS encrypte d by AES and HMAC				
SKEYSEED		DRAM:Plaintex t	While IPsec/IKEv 2 tunnel is active	Zeroization Command Session Terminatio n Reboot	IPsec/IKEv2 DH Shared Secret:Derived From IPsec/IKEv2 ECDH Shared Secret:Derived From IPsec/IKEv2 Pre-Shared Secret:Derived From
IPsec/IKEv2 Session Encryption Key		DRAM:Plaintex t	While IPsec/IKEv 2 tunnel is active	Zeroization Command Session Terminatio n Reboot	SKEYSEED:Derive d From
IPsec/IKEv2 Authenticatio n Key		DRAM:Plaintex t	While IPsec/IKEv 2 tunnel is active	Zeroization Command Session Terminatio n Reboot	SKEYSEED:Derive d From

Table 18: SSP Table 2

9.5 Transitions

FIPS 186-4/186-5
As of February 5, 2024, the CMVP does not accept module submissions that implement DSA or RSA X9.31 in the approved mode, other than for signature verification which is approved for

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

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 (FIPS186-4) (A2952/A3376)	RSA 2048 SigVer 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 19: Pre-Operational Self-Tests

The module performs the following self-tests, including Pre-operational 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). 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 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 (A2952/A3376)	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power up
AES-CBC decrypt KAT (A2952/A3376)	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power up
AES-GCM authenticated encrypt KAT (A2952/A3376)	256 bits	KAT	CAST	Module is in normal state	Authenticated Encrypt	Power up

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM authenticated decrypt KAT (A2952/A3376)	256 bits	KAT	CAST	Module is in normal state	Authenticated Decrypt	Power up
Counter DRBG Instantiate/Generate/Reseed KAT (A2952/A3376)	AES-128	KAT	CAST	Module is in normal state	Instantiate, Generate, and Reseed KATs	Power up
ECDSA SigGen (FIPS186-4) KAT (A2952/A3376)	Curve P-256 with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigGen KAT	Power up
ECDSA SigVer (FIPS186-4) KAT (A2952/A3376)	Curve P-256 with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigVer KAT	Power up
HMAC-SHA-1 KAT (A2952/A3376)	SHA-1	KAT	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-256 KAT (A2952/A3376)	SHA2-256	KAT	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-384 KAT (A2952/A3376)	SHA2-384	KAT	CAST	Module is in normal state	N/A	Power up
HMAC-SHA2-512 KAT (A2952/A3376)	SHA2-512	KAT	CAST	Module is in normal state	N/A	Power up
KAS-ECC-SSC Sp800-56Ar3 KAT (A2952/A3376)	Curve P-256	KAT	CAST	Module is in normal state	Primitive Z KAT	Power up
KAS-FFC-SSC Sp800-56Ar3 KAT (A2952/A3376)	MODP-2048	KAT	CAST	Module is in normal state	Primitive Z KAT	Power up
KDF IKEv2 KAT (A2952/A3376)	N/A	KAT	CAST	Module is in normal state	N/A	Power up
KDF SSH KAT (A2952/A3376)	N/A	KAT	CAST	Module is in	N/A	Power up

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				normal state		
RSA SigGen (FIPS186-4) KAT (A2952/A3376)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigGen KAT	Power up
RSA SigVer (FIPS186-4) KAT (A2952/A3376)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigVer KAT	Power up
SHA-1 KAT (A2952/A3376)	N/A	KAT	CAST	Module is in normal state	N/A	Power up
TLS v1.2 KDF RFC7627 KAT (A2952/A3376)	N/A	KAT	CAST	Module is in normal state	N/A	Power up
ECDSA KeyGen (FIPS186-4) PCT (A2952/A3376)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	ECDSA	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
KAS-ECC-SSC Sp800-56Ar3 PCT (A2952/A3376)	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

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						operational use.
KAS-FFC-SSC Sp800-56Ar3 PCT (A2952/A3376)	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.
RSA KeyGen (FIPS186-4) PCT (A2952/A3376)	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.
Conditional Bypass	N/A	N/A	Bypass	Module is in normal state	N/A	Performs conditional bypass test before first operational use of bypass service

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A2952/A3376)	KAT	SW/FW Integrity	Recommend 60 Days	Reboot
Pre-Operational Bypass Test	N/A	Bypass	Recommend 60 Days	Reboot

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC encrypt KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
AES-CBC decrypt KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
AES-GCM authenticated encrypt KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
AES-GCM authenticated decrypt KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
Counter DRBG Instantiate/Generate/Reseed KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
ECDSA SigGen (FIPS186-4) KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
ECDSA SigVer (FIPS186-4) KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA-1 KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-256 KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-384 KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-512 KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
KAS-FFC-SSC Sp800-56Ar3 KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
KDF IKEv2 KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
KDF SSH KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
RSA SigGen (FIPS186-4) KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
RSA SigVer (FIPS186-4) KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
SHA-1 KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
TLS v1.2 KDF RFC7627 KAT (A2952/A3376)	KAT	CAST	Recommend 60 Days	Reboot
ECDSA KeyGen (FIPS186-4) PCT (A2952/A3376)	PCT	PCT	Recommend 60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 PCT (A2952/A3376)	PCT	PCT	Recommend 60 Days	Reboot
KAS-FFC-SSC Sp800-56Ar3 PCT (A2952/A3376)	PCT	PCT	Recommend 60 Days	Reboot
RSA KeyGen (FIPS186-4) PCT (A2952/A3376)	PCT	PCT	Recommend 60 Days	Reboot
Conditional Bypass	N/A	Bypass	Recommend 60 Days	Reboot

Table 22: Conditional Periodic Information

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.

10.4 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 23: 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 integrity test and the conditional CASTs. The module will only enter into the operational state after successfully passing the pre-operational integrity test and the conditional CASTs.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

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. Operating this module without maintaining the following settings would put module operated in a non-compliance state.

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

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Step 2: Crypto officer shall perform zeroization operation if the module was previously used before the approved mode configuration.

Step 3: Issue “fips enable” to allow the module to internally enforce approved compliant services.

(config)# **fips enable**

Step 4: Disable password recovery.

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

Step 5: Set the configuration register to bypass ROMMON prompt at boot.

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

Step 6: 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 7: Configure the module to use SSHv2. Note that all operators must still authenticate after remote access is granted.

(config)# **ssh version 2**

Step 8: Configure the module such that any remote connections via Telnet are secured through IPSec.

Step 9: Configure the module such that only approved algorithms are used for IPSec tunnels.

Step 10: 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.

Note: 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 11: Configure the module such that error messages can only be viewed by a Crypto Officer.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice

Step 12: Disable the TFTP server.

Step 13: Disable HTTP for performing system management in approved mode of operation. HTTPS with TLS should always be used for Web-based management.

Step 14: Save the configuration.

Step 15: 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

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.

© 2021-2026 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice