Cisco Systems, Inc.

IOS Common Cryptographic Module (IC2M)

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is Cisco's non-proprietary security policy for the IOS Common Cryptographic Module (IC2M) with firmware version Rel5b (herein referred to as "IC2Mrel5b" or the "module"). The following details how this module meets the security requirements of FIPS 140-3, NIST SP 800-140, and ISO/IEC 19790 for a Security Level 1 Firmware cryptographic module.

The security requirements cover areas related to the design and implementation of a 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	1
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:

IC2Mrel5b is a single binary object file (sub_crypto_ic2m_k9.o) and is classified as a multi-chip standalone firmware module.

IC2Mrel5b is a cryptographic library that supports cryptographic operations executed by a calling application. The calling application leverages the module's well-defined API to initialize the module and call cryptographic algorithms for encryption/decryption, key generation, signature generation/verification, and hashing. The cryptographic library does not implement any protocols, but does provide the cryptographic primitives for IPsec/IKEv2, SNMPv3, SRTP, SSHv2, and TLSv1.2/v1.3. No SSPs are stored within the cryptographic boundary of the module.

The module is intended for use on any Cisco device that runs the IOS-XE OS, so the physical perimeter of the module is the testing platform. The module's operational environment is non-modifiable.

Module Type: Firmware

Module Embodiment: Multi-Chip Standalone

Module Characteristics:

Cryptographic Boundary:

Figure 1 below depicts the Module's cryptographic boundary (red dashed line).

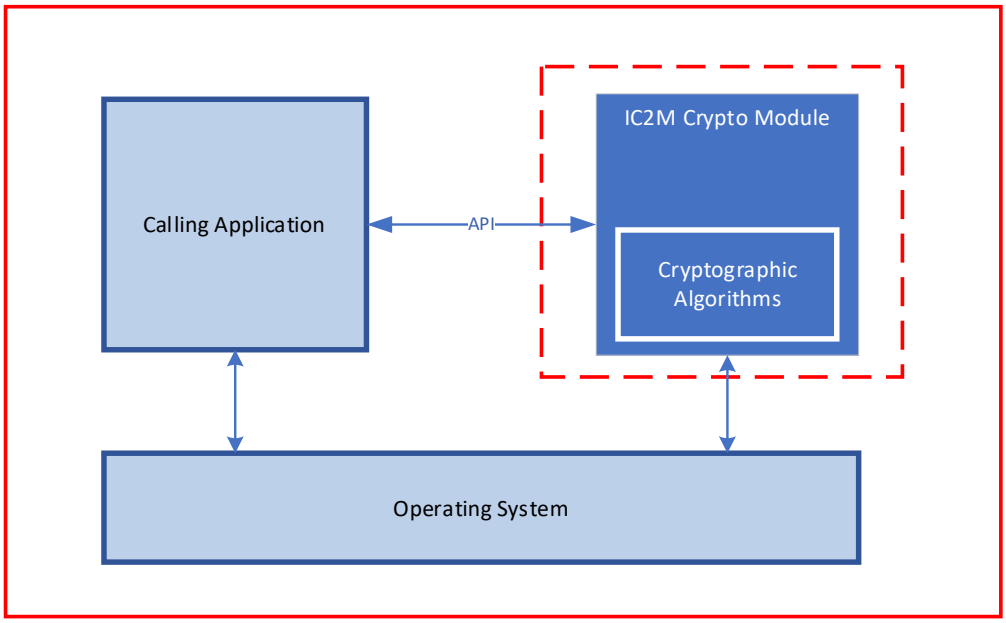

Figure 1: Block Diagram

Tested Operational Environment's Physical Perimeter (TOEPP):

In Figure 1 above, the TOEPP is represented by the solid red line. The physical perimeter is the Tested Operational Environment's Physical Perimeter (TOEPP) on which the module runs.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
sub_crypto_ic2m_k9.o	Rel5b		HMAC-SHA2-256

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

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
IOS-XE 17.12	Cisco Aggregated Services Router (ASR) 1001-HX	Intel Xeon E3-1125C v2	No		Rel5b

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

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

Operating System	Hardware Platform
IOS-XE 17.12	Catalyst 9200 Series Switches
IOS-XE 17.12	Catalyst 9300 Series Switches
IOS-XE 17.12	Catalyst 9400 Series Switches
IOS-XE 17.12	Catalyst 9500 Series Switches
IOS-XE 17.12	Catalyst 9600 Series Switches
IOS-XE 17.12	Cisco Embedded Services 3300 Series Switch
IOS-XE 17.12	Cisco Embedded Services 9300 Series Switch
IOS-XE 17.12	Cisco Catalyst Industrial Ethernet 3000 Series Switch
IOS-XE 17.12	Cisco Catalyst Industrial Ethernet 9300 Series Switch
IOS-XE 17.12	Cisco C8500, C8500L Series Edge Platforms
IOS-XE 17.12	Cisco C8200, C8200L, C8300 Series Edge Platforms
IOS-XE 17.12	Cisco Aggregation Services Router (ASR) 1000 series
IOS-XE 17.12	Cisco Integrated Services Router (ISR) 4000 series
IOS-XE 17.12	Cisco Integrated Services Router (ISR) 1000 series
IOS-XE 17.12	Cisco C8000V Edge Software Router
IOS-XE 17.12	Cisco IR 1100, 1800, 8100, 8300 Series Industrial Routers
IOS-XE 17.12	Cisco 8100 Series Secure Routers
IOS-XE 17.12	Cisco 8400 Series Secure Routers

Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

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

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	Automatically entered whenever an approved service is requested.	Approved	Equivalent to the indicator of the requested service.
Non-Approved Mode	Automatically entered whenever a non-approved service is requested.	Non-Approved	Equivalent to the indicator of the requested service.

Table 5: Modes List and Description

The module supports both approved and non-approved mode of operation. The module will be in approved mode when all pre-operational self-tests have completed successfully and only approved algorithms/services are invoked. See Section 4.3 below for a list of non-approved algorithms/non-approved services.

Mode Change Instructions and Status:

The non-approved mode is entered when a non-approved algorithm/non-approved service is invoked. See Section 4.4 below for a list of non-approved algorithms/non-approved services. The Approved mode of operation can only be transitioned into the non-Approved mode by calling one of the non-Approved services listed in Section 4.4.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4354	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CFB128	A4354	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A4354	Direction - Generation, Verification Key Length - 128, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 32-4096 Increment 8	SP 800-38B
AES-ECB	A4354	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A4354	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 16, 128, 136, 256, 264 AAD Length - AAD Length: 0, 128, 136, 256	
AES-GMAC	A4354	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128 Tag Length - 128 IV Length - IV Length: 96 AAD Length - AAD Length: 0, 128, 136, 256	SP 800-38D
AES-KW	A4354	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 128	SP 800-38F
Counter DRBG	A4354	Prediction Resistance - No Supports Reseed - Yes Mode - AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0-256 Increment 256 Entropy Input - 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)	A4354	Curve - P-256, P-384 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4354	Curve - P-256, P-384 Hash Algorithm - SHA2-256, SHA2-384	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A4354	Curve - P-256, P-384 Hash Algorithm - SHA2-256, SHA2-384	FIPS 186-4
HMAC-SHA-1	A4354	MAC - MAC: 32-160 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4354	MAC - MAC: 32-256 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4354	MAC - MAC: 32-384 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-512	A4354	MAC - MAC: 32-512 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4354	Domain Parameter Generation Methods - P-256, P-384, P-521 Hash Function Z - SHA2-512 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A4354	Domain Parameter Generation Methods - modp-2048, modp-3072, modp-4096 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF IKEv2 (CVL)	A4354	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 SNMP (CVL)	A4354	Password Length - Password Length: 128, 64 Engine ID - 000002b87766554433221100, 800002B805123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456	SP 800-135 Rev. 1
KDF SRTP (CVL)	A4354	AES Key Length - 128, 192, 256 Supports Empty KDR - No KDR Exponents - 1, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 2, 20, 21, 22, 23, 24, 3, 4, 5, 6, 7, 8, 9 Supports 48 bit SRTCP Index - No	SP 800-135 Rev. 1
KDF SSH (CVL)	A4354	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-4)	A4354	Key Generation Mode - B.3.4 Modulo - 2048, 3072, 4096 Hash Algorithm - SHA2-256 Info Generated By Server - Yes Public Exponent Mode - Fixed Fixed Public Exponent - 010001 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A4354	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA2-256	FIPS 186-4
RSA SigVer (FIPS186-4)	A4354	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA2-256	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
		Public Exponent Mode - Fixed Fixed Public Exponent - 010001	
Safe Primes Key Generation	A4354	Safe Prime Groups - modp-2048, modp-3072, modp-4096	SP 800-56A Rev. 3
SHA-1	A4354	Message Length - Message Length: 0-4096 Increment 8	FIPS 180-4
SHA2-256	A4354	Message Length - Message Length: 0-4096 Increment 8	FIPS 180-4
SHA2-384	A4354	Message Length - Message Length: 0-4096 Increment 8	FIPS 180-4
SHA2-512	A4354	Message Length - Message Length: 0-4096 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4354	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A4354	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

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

Table 7: 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:

Name	Use and Function
MD5	Message Digest
RSA	Key Encapsulation
Triple-DES	Encryption/Decryption

Table 8: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KAS-ECC-KeyGen	CKG KAS-KeyGen	KAS-ECC KeyGen using the direct output of the DRBG per SP 800-133r2 section 5.2	Bit-strength Caveat:Provides between 128 and 256 bits of encryption strength	Counter DRBG: (A4354) CKG: ()
KAS-FFC-KeyGen	CKG KAS-KeyGen	KAS-FFC KeyGen using the direct output of the DRBG per SP 800-133r2 section 5.2	Bit-strength Caveat:Provides between 112 and 152 bit of encryption strength	Counter DRBG: (A4354) Safe Primes Key Generation: (A4354) CKG: ()
KAS-ECC-SSC	KAS-SSC	KAS-ECC Shared Secret Computation	IG:IG D.F Scenario 2, path (1) Key confirmation:no Key derivation:no Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A4354)
KAS-FFC-SSC	KAS-SSC	KAS-FFC Shared Secret Computation	IG:IG D.F Scenario 2, path (1) Key confirmation:no Key derivation:no Caveat:Key	KAS-FFC-SSC Sp800-56Ar3: (A4354)

Name	Type	Description	Properties	Algorithms
			establishment methodology provides between 112 and 152 bits of security strength	
Symmetric Key Generation	CKG	Symmetric Key Generation for AES and HMAC using the direct output of the DRBG per SP 800-133r2 section 6.1		Counter DRBG: (A4354) CKG: ()
AES Encryption/Decryption	BC-Auth BC-UnAuth	Encryption/Decryption Security Function		AES-CBC: (A4354) AES-CFB128: (A4354) AES-ECB: (A4354) AES-CMAC: (A4354) AES-GMAC: (A4354) AES-GCM: (A4354)
RSA KeyGen	AsymKeyPair-KeyGen CKG	RSA Key Generation Security Function using the direct output of the DRBG per SP 800-133r2 section 5.1		RSA KeyGen (FIPS186-4): (A4354) Counter DRBG: (A4354) CKG: ()
RSA SigGen	DigSig-SigGen	RSA Signature Generation Security Function		RSA SigGen (FIPS186-4): (A4354)
RSA SigVer	DigSig-SigVer	RSA Signature Verification Security Function		RSA SigVer (FIPS186-4): (A4354)
ECDSA KeyGen	AsymKeyPair-KeyGen CKG	ECDSA Key Generation Security Function using the direct output of the		ECDSA KeyGen (FIPS186-4): (A4354)

Name	Type	Description	Properties	Algorithms
		DRBG per SP800-133r2 section 5.1		Counter DRBG: (A4354) CKG: ()
ECDSA SigGen	DigSig-SigGen	ECDSA Signature Generation Security Function		ECDSA SigGen (FIPS186-4): (A4354)
ECDSA SigVer	DigSig-SigVer	ECDSA Signature Verification Security Function		ECDSA SigVer (FIPS186-4): (A4354)
AES Key Wrapping (KW)	BC-Auth	Key Wrapping Security Function		AES-KW: (A4354)
IKEv2 Key Derivation	KAS-135KDF	IKEv2 KDF Security Function		KDF IKEv2: (A4354)
SNMPv3 Key Derivation	KAS-135KDF	SNMPv3 KDF Security Fucntion		KDF SNMP: (A4354)
SRTP Key Derivation	KAS-135KDF	SRTP KDF Security Function		KDF SRTP: (A4354)
SSHv2 Key Derivation	KAS-135KDF	SSHv2 KDF Security Function		KDF SSH: (A4354)
TLSv1.2 Key Derivation	KAS-135KDF	TLSv1.2 KDF Security Function		TLS v1.2 KDF RFC7627: (A4354)
TLSv1.3 Key Derivation	KAS-135KDF	TLSv1.3 KDF Security Function		TLS v1.3 KDF: (A4354)
HMAC	MAC	Message Authentication Code Generation		HMAC-SHA-1: (A4354) HMAC-SHA2-256: (A4354) HMAC-SHA2-384: (A4354) HMAC-SHA2-512: (A4354)
SHA	SHA	Secure Hashing Security Function		SHA-1: (A4354) SHA2-256: (A4354)

Name	Type	Description	Properties	Algorithms
				SHA2-384: (A4354) SHA2-512: (A4354)
Counter DRBG	DRBG	Random Number Generator		Counter DRBG: (A4354)

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

AES-GCM IV:

- The AES-GCM IV is constructed in compliance with IG C.H, scenario 1 (TLS v1.2), scenario 2 (IPsec-v3), and scenario 5 (TLS v1.3). Users should consult IG C.H specific scenarios for all the requirements using AES-GCM mode. The TLS and IPsec/IKE protocols have not been reviewed or tested by the CAVP and CMVP.

- The AES-GCM IV generation follows RFC 5288 and shall only be used for the TLS protocol v1.2. The counter portion of the IV is set by the module within its cryptographic boundary. The module does not implement the TLS protocol. The module's implementation of AES-GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the TLS protocol implicitly ensures that the nonce_explicit, or counter portion of the IV will not exhaust all of its possible values.

- The AES-GCM IV generation follows RFC 4106 and shall only be used for the IPsec-v3 protocol version 3. The counter portion of the IV is set by the module within its cryptographic boundary. The module does not implement the IPsec protocol. The module's implementation of AES-GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the IPsec protocol implicitly ensures that the nonce_explicit, or counter portion of the IV will not exhaust all of its possible values.

- The AES-GCM IV generation follows RFC 8446 and shall only be used for the TLS protocol v1.3. The counter portion of the IV is set by the module within its cryptographic boundary. The module does not implement the TLS protocol. The module's implementation of AES-GCM is used together with an application that runs outside the module's cryptographic boundary. The design of the TLS protocol implicitly ensures that the nonce_explicit, or counter portion of the IV will not exhaust all of its possible values.

- In these protocols if the module's power is lost and then restored, the key used for the AES GCM encryption/decryption shall be re-distributed. This condition is not enforced by the module; however, it is met implicitly. The module does not retain any state when power is lost. The AES-GCM key/IVs are not persistently stored during power off: therefore, there is no re-connection possible when the power is restored with re-generation of the key used for AES-GCM. After restoration of the power, the user of the

module (e.g., TLS, IKE) along with User application that implements the protocol, must perform a complete new key establishment operation using new random numbers (Entropy input string, DRBG seed, DRBG internal state V and Key, shared secret values that are not retained during power cycle) and subsequent KDF operations to establish a new AES-GCM key/IV pair on either side of the network communication channel.

FIPS186-4/186-5 Equivalence:

- The module was algorithm tested based on the FIPS 186-4 standard for Digital Signatures prior to Feb 5, 2024. 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.

KAS-FFC-SSC/KAS-ECC-SSC

- The module does not establish SSPs using an approved key agreement scheme (KAS). However, it does offer some or all of the underlying KAS cryptographic functionality to be used by an external operator/application as part of an approved KAS.

2.8 RBG and Entropy

The OS passively loads entropy within the TOEPP into the module to seed the NIST SP 800-90Arev1 DRBG.

While in the approved mode of operation, the entropy and seeding material for the NIST SP 800-90Arev1 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 physical perimeter. The module receives a LOAD command with entropy obtained from the entropy source inside the TOEPP. The minimum effective strength of the NIST 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 NIST SP 800-90Arev1 DRBG is at least 112-bits.

Per the IG 9.3.A Entropy Caveats, the following caveat applies: No assurance of the minimum strength of generated SSPs (e.g., keys).

The Approved DRBG for random number generation is a NIST SP 800-90Arev1 CTR_DRBG using AES-256 with derivation function and without prediction resistance. The numbers used for key generation are all generated by the CTR_DRBG within the module. Per NIST SP 800-90Arev1, section 10.2.1.1, the internal state is the values of *V* and *Key*.

2.9 Key Generation

The module generates RSA, ECDSA, ECDH, and DH asymmetric key pairs compliant with FIPS 186-4, using a NIST SP 800-90Arev1 CTR DRBG for random number generation. In accordance with FIPS 140-3 IG D.H, the cryptographic module performs CKG for asymmetric keys as per section 5.1 of NIST SP 800-133rev2 (vendor affirmed) by obtaining a random bit string directly from an approved DRBG. The random bit string supports the required security strength requested by the calling application (without any V, as described in Additional Comments 2 of IG D.H.).

The module generates AES symmetric keys compliant with FIPS PUB 197 and HMAC key compliant with FIPS PUB 198. All symmetric key generation is performed using a NIST SP 800-90Arev1 CRT_DRBG for random number generation. In accordance with FIPS 140-3 IG D.H, the cryptographic module performs CKG for symmetric keys as per section 6.1 of NIST SP 800-133rev2.

2.10 Key Establishment

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

- KAS-FFC Shared Secret Computation:
  - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (1) with KAS-FFC shared secret computation. The shared secret computation provides between 112 and 152 bits of encryption strength.

  - The module supports the use of the safe primes defined in RFC 4419 (SSH) and RFC 3526 (IKE) with the following Domain Parameters:

    - MODP-2048 (ID = 14)
    - MODP-3072 (ID = 15)
    - MODP-4096 (ID = 16)

- KAS-ECC Shared Secret Computation:

  - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (1) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength. The module supports Curves: P-256, P-384 and P-521

2.11 Industry Protocols

No parts of IPSec/IKEv2, SNMPv3, SSH, SRTP and TLS protocols, other than the KDFs, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	API input parameters - plaintext and/or ciphertext data
N/A	Data Output	API output parameters - plaintext and/or ciphertext data

Physical Port	Logical Interface(s)	Data That Passes
N/A	Control Input	API input parameters - function calls, or input arguments that specify commands and control data used to control the operation of the module
N/A	Control Output	Not Applicable
N/A	Status Output	API return codes- function return codes, error codes, or output arguments that receive status information used to indicate the status of the module
N/A	Power	Not applicable

Table 10: Ports and Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in section 2 above. No data passes in or out of these physical ports. The module provides logical interfaces via well-defined APIs.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The module does not provide any authentication methods.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 11: Roles

The module supports the CO role. The module does not allow concurrent operators. The CO role is implicitly assumed when an API call is made to initiate a service.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Initialize Module	Initialization occurs when the module is loaded	N/A	None	Module Loaded	None	Crypto Officer Unauthenticated
Show Status	Display running status of the module	N/A	API Command	Module's current status	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Perform Self-Test	Perform Self-tests (Pre-operational self-tests and Conditional CASTs)	N/A	API Command	Output display on each algorithm running self-test and pass/fail indicator	None	Crypto Officer Unauthenticated
Show Version	Provide module's name and version information	N/A	API Command	Displays the module's name/ID and versioning information	None	Crypto Officer
Symmetric Cipher Operation	Perform encryption/decryption of data	API return value for success	API commands, key, and plaintext/ciphertext data	Plaintext or ciphertext	AES Encryption/Decryption Symmetric Key Generation	Crypto Officer - AES EDK: G,R,W,E
Asymmetric Cipher Operation	Perform signature generation/verification and key generation	API return value for success	API commands, keys, and ciphertext/plaintext	Signature and plaintext/ciphertext	RSA KeyGen RSA SigGen RSA SigVer ECDSA KeyGen ECDSA SigGen ECDSA SigVer Counter DRBG	Crypto Officer - RSA SGK: G,R,W,E - RSA SVK: G,R,W,E - ECDSA SGK: G,R,W,E - ECDSA SVK: G,R,W,E,Z - DRBG Entropy Input: G,R,W,E - DRBG Seed: G,R,W,E - DRBG Internal State (V,

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key): G,R,W,E
Key Exchange/Agreement Component	Perform key agreement primitives on behalf of the calling application (does not establish keys into the module)	API return value for success	Api commands, asymmetric keys	Asymmetric keypair or key agreement component	KAS-ECC-KeyGen KAS-FFC-KeyGen KAS-ECC-SSC KAS-FFC-SSC Counter DRBG	Crypto Officer - DH Private Key: G,R,W,E - DH Public Key: G,R,W,E - DH Shared Secret: G,R - ECDH Private Key: G,R,W,E - ECDH Public Key: G,R,W,E - ECDH Shared Secret: G,R - DRBG Entropy Input: G,R,W,E - DRBG Seed: G,R,W,E - DRBG Internal State (V, Key): G,R,W,E
Key Wrapping (KW)	Encrypt a key value on behalf of the calling application	API return value for success	API commands, wrapping key, key	Wrapped key	AES Key Wrapping (KW) Symmetric Key Generation	Crypto Officer - AES KWK: G,R,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
KDF IKEv2 Function	Derive keys for IKEv2 protocol	API return value for success	IKEv2 (existing application specific): IKEv2 parameters	IKEv2 Keying Materials	IKEv2 Key Derivation	Crypto Officer - DH Shared Secret: W,E - ECDH Shared Secret: W,E - IKEv2 Keying Materials: G,R
KDF SNMPv3 Function	Derive keys for SNMPv3 protocol	API return value for success	SNMPv3 (existing application specific): SNMPv3 parameters	SNMPv3 Keying Materials	SNMPv3 Key Derivation	Crypto Officer - DH Shared Secret: W,E - ECDH Shared Secret: W,E - SNMPv3 Keying Materials: G,R
KDF SRTP Function	Derive keys for SRTP protocol	API return value for success	SRTP (existing application specific): SRTP parameters	SRTP Keying Materials	SRTP Key Derivation	Crypto Officer - DH Shared Secret: W,E - ECDH Shared Secret: W,E - SRTP Keying Materials: G,R
KDF SSHv2 Function	Derive keys for SSHv2 protocol	API return value for	SSHv2 (existing application specific):	SSHv2 Keying Materials	SSHv2 Key Derivation	Crypto Officer - DH Shared Secret:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		success	SSHv2 parameters			W,E - ECDH Shared Secret: W,E - SSHv2 Keying Materials: G,R
KDF TLSv1.2 Function	Derive keys for TLSv1.2 protocol	API return value for success	TLSv1.2 (existing application specific): TLSv1.2 parameters	TLSv1.2 Keying Materials	TLSv1.2 Key Derivation	Crypto Officer - DH Shared Secret: W,E - ECDH Shared Secret: W,E - TLSv1.2 Keying Materials: G,R
KDF TLSv1.3 Function	Derive keys for TLSv1.3 protocol	API return value for success	TLSv1.3 (existing application specific): TLSv1.3 parameters	TLSv1.3 Keying Materials	TLSv1.3 Key Derivation	Crypto Officer - DH Shared Secret: W,E - ECDH Shared Secret: W,E - TLSv1.3 Keying Materials: G,R
Keyed Hash Function	Generate keyed hash	API return value for success	API commands, HMAC key, plaintext	MAC value	HMAC Symmetric Key Generation	Crypto Officer - HMAC Key: G,R,W,E
Message Digest	Generate message digest (secure	API return value for	API commands, plaintext	Hash value	SHA	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	hashing function)	success				
Random number generation	Provide random data for key generation	API return value for success	API commands	Random bits	Counter DRBG	Crypto Officer - DRBG Entropy Input: G,R,W,E - DRBG Seed: G,R,W,E - DRBG Internal State (V, Key): G,R,W,E
Zeroization	Zeroize all SSPs stored in allocated mempory. Cleanup is the responsibility of the calling application.	N/A	API commands	None	None	Crypto Officer - AES EDK: Z - AES KWK: Z - RSA SGK: Z - RSA SVK: Z - ECDSA SGK: Z - ECDSA SVK: Z - DH Private Key: Z - DH Public Key: Z - DH Shared Secret: Z - ECDH Private Key: Z - ECDH Public Key: Z - ECDH Shared Secret: Z - HMAC

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: Z - DRBG Entropy Input: Z - DRBG Seed: Z - DRBG Internal State (V, Key): Z - IKEv2 Keying Materials: Z - SSHv2 Keying Materials: Z - SNMPv3 Keying Materials: Z - SRTP Keying Materials: Z - TLSv1.2 Keying Materials: Z - TLSv1.3 Keying Materials: Z

Table 12: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Message digest using MD5	Generate message digest using MD5	MD5	CO
Non-SP 800-56Br2-compliant Key Transport scheme using RSA	Perform RSA key encapsulation/un-encapsulation using RSA 2048 bits (not approved, not allowed per IG D.G)	RSA	CO

Name	Description	Algorithms	Role
Symmetric operation using Triple-DES	Perform symmetric operation using Triple-DES	Triple-DES	CO

Table 13: Non-Approved Services

4.5 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 IC2Mrel5b cryptographic module is a binary file (sub_crypto_ic2m_k9.o) statically linked within the IOS-XE OS. To ensure firmware security, the module is protected by an HMAC-SHA2-256 (HMAC Cert. #A4354) algorithm. The firmware integrity test key (non-SSP) was preloaded to the module's binary at the factory and used only for the pre-operational firmware integrity self-test. During initialization of the module, the integrity of the runtime executable is verified using an HMAC-SHA2-256 which is compared to a value computed at build time. If at load time the MAC does not match the stored, known MAC value, the module enters a critical error state where all crypto functionality inhibited. The module must be reloaded to attempt the integrity test again.

5.2 Initiate on Demand

The 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: Non-Modifiable

How Requirements are Satisfied:

The module is operated in a non-modifiable operational environment per ISO/IEC 19790, section 7.6, level 1 specifications. The module is delivered as part of the IOS-XE OS. The OS is restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded). The application that makes calls to the module is the single user of the module. The module's firmware version running on each tested platform is Rel5b.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Production-grade components with standard passivation	N/A	N/A

Table 14: Mechanisms and Actions Required

Per ISO/IEC 19790, section 7.7, the module is defined as a multi-chip standalone firmware cryptographic module. The module runs on a host appliance made of production-grade components with standard passivation techniques.

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM of the TOEPP	The module stores SSPs in RAM provided by the operational environment. They are received for use or generated by the module only at the command of the calling application. The operating system protects all SSPs through the memory separation and protection mechanisms. No process other than the module itself can access the SSPs in its process' memory.	Dynamic

Table 15: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
API Input	Calling application (Within TOEPP)	Module	Plaintext	Manual	Electronic	
API Output	Module	Calling application (Within TOEPP)	Plaintext	Manual	Electronic	

Table 16: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Remove power from the module	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed.	Removing power from the module

Table 17: SSP Zeroization Methods

The module does not possess persistent storage of SSPs. The SSP value only exists in volatile memory of the host appliance and that value vanishes when the module is powered off. The procedure for secure sanitization of the module at the end of life is simply to power off the tested platform.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES EDK	AES Encryption/Decryption Key	128-256 bits - 128-256 bits	Symmetric Key - CSP	Symmetric Key Generation		AES Encryption/Decryption
AES KWK	AES Key Wrapping Key	128-256 bits - 128-256 bits	Symmetric Key - CSP	Symmetric Key Generation		AES Key Wrapping (KW)
RSA SGK	RSA Signature Generation Key	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Private Asymmetric Key - CSP	RSA KeyGen		RSA SigGen
RSA SVK	RSA Signature Verification Key	MODP-2048, MODP-3072, MODP-4096 - 112-	Public Asymmetric Key - PSP		RSA KeyGen	RSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		152 bits				
ECDSA SGK	ECDSA Signature Generation Key	P-256, P-384, P-521 - 128-256 bits	Private Asymmetric Key - CSP	ECDSA KeyGen		ECDSA SigGen
ECDSA SVK	ECDSA Signature Verification Key	P-256, P-384, P-521 - 128-256 bits	Public Asymmetric Key - PSP		ECDSA KeyGen	ECDSA SigVer
DH Private Key	Used to derive the DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Private Asymmetric Key - CSP	KAS-FFC-KeyGen		KAS-FFC-SSC
DH Public Key	Used by peer to derive the DH Shared Secret	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Public Asymmetric Key - PSP		KAS-FFC-KeyGen	
DH Shared Secret	Used in a KDF to derive Encryption and Authentication Keys	MODP-2048, MODP-3072, MODP-4096 - 112-152 bits	Shared Secret - CSP		KAS-FFC-SSC	IKEv2 Key Derivation SNMPv3 Key Derivation SRTP Key Derivation SSHv2 Key Derivation TLSv1.2 Key Derivation TLSv1.3 Key Derivation
ECDH Private Key	Used to derive the ECDH Shared Secret	P-256, P-384, P-521 -	Private Asymmetri	KAS-ECC-KeyGen		KAS-ECC-SSC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128-256 bits	c Key - CSP			
ECDH Public Key	Used by peer to derive the ECDH Shared Secret	P-256, P-384, P-521 - 128-256 bits	Public Asymmetric Key - PSP		KAS-ECC-KeyGen	
ECDH Shared Secret	Used in a KDF to derive Encryption and Authentication Keys	P-256, P-384, P-521 - 128-256 bits	Shared Secret - CSP		KAS-ECC-SSC	IKEv2 Key Derivation SNMPv3 Key Derivation SRTP Key Derivation SSHv2 Key Derivation TLSv1.2 Key Derivation TLSv1.3 Key Derivation
HMAC Key	HMAC Generation Key	160 bits or greater - 112 bits or greater	Authentication Key - CSP	Symmetric Key Generation		HMAC
DRBG Entropy Input	Used to seed the DRBG	at least 112 bits - at least 112 bits	Entropy Input - CSP			Counter DRBG
DRBG Seed	Used in DRBG Generation	384 bits - 384 bits	DRBG Seed - CSP			Counter DRBG
DRBG Internal State (V, Key)	Used in DRBG Generation	384 bits - 384 bits	DRBG Internal State - CSP			Counter DRBG
IKEv2 Keying Materials	Output of KDF used to derive IKEv2 Keys	at least 128 bits - 112	Keying Materials - CSP		IKEv2 Key Derivation	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		bits or greater				
SNMPv3 Keying Materials	Output of KDF used to derive SNMPv3 Keys	at least 128 bits - 112 bits or greater	Keying Materials - CSP		SNMPv3 Key Derivation	
SRTP Keying Materials	Output of KDF used to derive SRTP Keys	at least 128 bits - 112 bits or greater	Keying Materials - CSP		SRTP Key Derivation	
SSHv2 Keying Materials	Output of KDF used to derive SSHv2 Keys	at least 128 bits - 112 bits or greater	Keying Materials - CSP		SSHv2 Key Derivation	
TLSv1.2 Keying Materials	Output of KDF used to derive TLSv1.2 Keys	at least 128 bits - 112 bits or greater	Keying Materials - CSP		TLSv1.2 Key Derivation	
TLSv1.3 Keying Materials	Output of KDF used to derive TLSv1.3 Keys	at least 128 bits - 112 bits or greater	Keying Materials - CSP		TLSv1.3 Key Derivation	

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES EDK	API Input API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
AES KWK	API Input API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
RSA SGK	API Input	RAM of the TOEPP:Plaintext		Remove power from the module	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	API Output				
RSA SVK	API Input API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
ECDSA SGK	API Input API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
ECDSA SVK	API Input API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
DH Private Key	API Input API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
DH Public Key	API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
DH Shared Secret	API Input API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
ECDH Private Key	API Input API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
ECDH Public Key	API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
ECDH Shared Secret	API Input API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
HMAC Key	API Input API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
DRBG Entropy Input		RAM of the TOEPP:Plaintext		Remove power from the module	
DRBG Seed		RAM of the TOEPP:Plaintext		Remove power from the module	
DRBG Internal State (V, Key)		RAM of the TOEPP:Plaintext		Remove power from the module	
IKEv2 Keying Materials	API Output	RAM of the TOEPP:Plaintext		Remove power from the module	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SNMPv3 Keying Materials	API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
SRTP Keying Materials	API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
SSHv2 Keying Materials	API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
TLSv1.2 Keying Materials	API Output	RAM of the TOEPP:Plaintext		Remove power from the module	
TLSv1.3 Keying Materials	API Output	RAM of the TOEPP:Plaintext		Remove power from the module	

Table 19: SSP Table 2

9.5 Transitions

SHA-1
The module includes an implementation of SHA-1 for hashing and digital signature verification. This implementation will be non-Approved for all uses starting January 1, 2031. At this time, the user should move to SHA2, which is available in this module.

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

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware Integrity Test	HMAC-SHA2-256	KAT	SW/FW Integrity	Module is in normal state	Firmware Integrity Test

Table 20: Pre-Operational Self-Tests

The module performs Pre-Operational Self-Tests and CASTs before entering an approved mode of operation. The module is single threaded and will not return to the calling application until all self-tests are complete.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB Encrypt KAT	128 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-ECB Decrypt KAT	128 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
AES-GCM Encrypt KAT	256 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-GCM Decrypt KAT	256 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
Counter DRBG Instantiate KAT	AES-128	KAT	CAST	Module is in normal state	Instantiate KAT	Power Up
Counter DRBG Generate KAT	AES-128	KAT	CAST	Module is in normal state	Generate KAT	Power Up
Counter DRBG Reseed KAT	AES-128	KAT	CAST	Module is in normal state	Reseed KAT	Power Up
HMAC-SHA2-256 KAT	SHA2-256	KAT	CAST	Module is in normal state	HMAC-SHA2-256	Power Up
SHA-1 KAT	SHA-1	KAT	CAST	Module is in normal state	SHA-1	Power Up
SHA2-256 KAT	SHA2-256	KAT	CAST	Module is in normal state	SHA2-256	Power Up
SHA2-512 KAT	SHA2-512	KAT	CAST	Module is in normal state	SHA2-512	Power Up
ECDSA SigGen KAT	P-256 with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigGen KAT	Power Up
ECDSA SigVer KAT	P-256 with SHA2-256	KAT	CAST	Module is in normal state	ECDSA SigVer KAT	Power Up
RSA SigGen KAT	2048-bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigGen KAT	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer KAT	2048-bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigVer KAT	Power Up
KAS-FFC-SSC Sp800-56Ar3 KAT	MODP-2048	KAT	CAST	Module is in normal state	Primitive Z KAT	Power Up
KAS-ECC-SSC Sp800-56Ar3 KAT	P-256	KAT	CAST	Module is in normal state	Primitive Z KAT	Power Up
KDF IKEv2 KAT	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SNMP KAT	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SRTP KAT	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
KDF SSH KAT	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
TLSv1.2 KSF with RFC7627 KAT	N/A	KAT	CAST	Module is in normal state	With RFC7627	Power Up
TLSv1.3 KDF KAT	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
ECDSA KeyGen PCT	P-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
RSA KeyGen PCT	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

Table 21: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware Integrity Test	KAT	SW/FW Integrity	Recommend 60 days	Reboot

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB Encrypt KAT	KAT	CAST	Recommend 60 days	Reboot
AES-ECB Decrypt KAT	KAT	CAST	Recommend 60 days	Reboot
AES-GCM Encrypt KAT	KAT	CAST	Recommend 60 days	Reboot
AES-GCM Decrypt KAT	KAT	CAST	Recommend 60 days	Reboot
Counter DRBG Instantiate KAT	KAT	CAST	Recommend 60 days	Reboot
Counter DRBG Generate KAT	KAT	CAST	Recommend 60 days	Reboot
Counter DRBG Reseed KAT	KAT	CAST	Recommend 60 days	Reboot
HMAC-SHA2-256 KAT	KAT	CAST	Recommend 60 days	Reboot
SHA-1 KAT	KAT	CAST	Recommend 60 days	Reboot
SHA2-256 KAT	KAT	CAST	Recommend 60 days	Reboot
SHA2-512 KAT	KAT	CAST	Recommend 60 days	Reboot
ECDSA SigGen KAT	KAT	CAST	Recommend 60 days	Reboot
ECDSA SigVer KAT	KAT	CAST	Recommend 60 days	Reboot
RSA SigGen KAT	KAT	CAST	Recommend 60 days	Reboot
RSA SigVer KAT	KAT	CAST	Recommend 60 days	Reboot
KAS-FFC-SSC Sp800-56Ar3 KAT	KAT	CAST	Recommend 60 days	Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT	KAT	CAST	Recommend 60 days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDF IKEv2 KAT	KAT	CAST	Recommend 60 days	Reboot
KDF SNMP KAT	KAT	CAST	Recommend 60 days	Reboot
KDF SRTP KAT	KAT	CAST	Recommend 60 days	Reboot
KDF SSH KAT	KAT	CAST	Recommend 60 days	Reboot
TLSv1.2 KSF with RFC7627 KAT	KAT	CAST	Recommend 60 days	Reboot
TLSv1.3 KDF KAT	KAT	CAST	Recommend 60 days	Reboot
ECDSA KeyGen PCT	PCT	PCT	Recommend 60 days	Reboot
RSA KeyGen PCT	PCT	PCT	Recommend 60 days	Reboot

Table 23: Conditional Periodic Information

In addition to the automatic execution of self-tests at cryptographic module initialization, the CO can manually initiate self-tests on demand by executing the “test crypto self-test” command through the console of the host appliance. This command calls the “crypto_engine_nist_run_self_tests() function”. Self-tests can be executed on demand by power-cycling the module.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Critical Error State	If any of the pre-operational or conditional CASTS fail, the module is put into an error state	Self-test failure	Reboot the module	System Halt

Table 24: Error States

The module supports two Error states, critical error state and soft error state. If any of the pre-operational self-tests or conditional cryptographic algorithm self-tests fail, the module enters a critical error state and sends an error to the OS. Following is an example of the error message displayed on the console of the host appliance in a critical error state:

%CRYPTO-0-SELF_TEST_FAILURE: Encryption self-test failed (<failing test description>)

In a critical error state, no cryptographic operations are performed and data output is prohibited. The CO can clear the error state by restarting the module.

If a PCT fails, the module enters a soft error state, deletes the key, logs an error, and returns to the approved mode of operation. In the approved mode of operation the service may be retried

or a new service may be performed. Following is an example of the error message displayed on the console of the host appliance in a soft error state:

%CRYPTO-3-RSA_SELFTEST_FAILED: Generated RSA key failed self test

If the module fails to retrieve enough entropy, the module enters a soft error state. The module deletes the DRBG value, then reseeds and reinitializes the DRBG.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module meets all the Level 1 requirements for FIPS 140-3. The module is completely and permanently embedded into Host Device IOS-XE OS. There are no installation considerations besides the loading of the IOS-XE OS. The module cannot be modified, replaced, or upgraded except by loading a new Host Device IOS-XE version in its entirety.

During system start-up, the IOS-XE OS will call module's ic2m_init() function. The ic2m_init() function is the default entry point for the module. The ic2m_init() function initiates all self-tests and does not return to the IOS-XE OS until all self-tests are completed successfully and the module is in an approved mode of operation. No other tasks are executed while the self-tests are performed so no data is passed and all cryptographic operations are prohibited. If a self-test fails, the module enters a critical error state and must be reloaded to clear the error state and retry the self-tests.

11.2 Administrator Guidance

An additional guidance document, if required, can be obtained by contacting Cisco Systems, Inc. using the information posted on the validation certificate.

11.3 Non-Administrator Guidance

Not Applicable.

12 Mitigation of Other Attacks

N/A for this module.