Cisco ISR 1000 Series Routers without MACSEC

Firmware version:

Cisco IOS-XE 16.12

Hardware versions:

ISR 1101, ISR 1111

FIPS-140 Non-Proprietary Security Policy - Security Level 1

Cisco Systems, Inc.

Version 1.3

Table of Contents

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for Cisco ISR 1K network router modules. This security policy describes how modules meet the security requirements of FIPS 140-2 and how to run the modules in a FIPS 140-2 mode of operation.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.1 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Cisco Systems website (http://www.cisco.com) contains information on the full line of products from Cisco Systems.
- The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the module.

1.2 FIPS 140-2 Submission Package

The security policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the submission package includes:

- Vendor Evidence
- Finite State Machine
- Other supporting documentation as additional references

With the exception of this non-proprietary security policy, the FIPS 140-2 validation documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems, Inc. See “Obtaining Technical Assistance” section for more information.

2 Module Description

2.1 Cisco ISR (1101 and 1111)

The Cisco 1100 Series Integrated Services Routers (ISRs) with Cisco IOS-XE 16.12 Software combine Internet access, comprehensive security, and wireless services (LTE Advanced 3.0 wireless WAN and 802.11ac wireless LAN) in a single, high-performance device. The routers are easy to deploy and manage, with cutting-edge, scalable, multicore separate data and control plane capabilities.

The Cisco 1100 Series ISRs are well suited for deployment as Customer Premises Equipment (CPE) in enterprise branch offices, in service provider managed environments as well as smaller form factor and M2M use cases.

Figure 1: ISR 1101

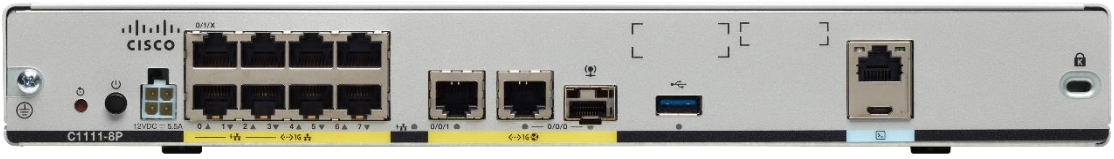

Figure 2: ISR 1111

2.2 Validated and Vendor Equivalent Hardware

The validated hardware (running Cisco IOS-XE 16.12) consists of:

- ISR 1101
- ISR 1111

2.3 FIPS and non-FIPS modes of operation

The ISR 1000 Series Routers supports a FIPS and non-FIPS mode of operation. The non-FIPS mode of operation is not a recommended operational mode but because the module allows for non-approved algorithms and non-approved key sizes, a non-approved mode of operation exists. The following services are available in a FIPS Approved mode of operation:

- SSH
- IPSec
- SNMPv3

The following services are available in a non-FIPS-Approved mode of operation:

- SSH
- TLS
- IPSec
- SNMPv3

When the services are used in non-FIPS mode they are considered to be non-compliant. If the device is in the non-FIPS mode of operation, the Cryptographic Officer must follow the instructions in section 9.1 of this security policy to transfer into a FIPS approved mode of operation. The FIPS Approved mode supports the approved and allowed algorithms, functions and protocols identified in Section 7 of this document. The FIPS Approved mode of operation is entered when the module is configured for FIPS mode (detailed in Section 9) and successfully passes all the power on self-tests (POST).

2.4 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
Overall	**Overall module validation level**	**1**

Table 1: Module Validation Level

3 Cryptographic Boundary

The cryptographic boundary for the Cisco ISR 1101 and ISR 1111 are defined as encompassing the “top,” “bottom,” “front,” “back,” “left” and “right” surfaces of the case.

4 Cryptographic Module Ports and Interfaces

Each module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following tables:

Physical Interfaces	FIPS 140-2 Logical Interfaces
Ethernet Ports (5) Console Port (1)	Data Input Interface
Ethernet Ports (5) Console Port (1)	Data Output Interface
Ethernet Ports (5) Console Port (1) USB Ports (1) Power Button (1) Reset Button (1)	Control Input Interface
Ethernet Ports (5) Console Port (1) USB Ports (1) LEDs	Status Output Interface
Power connector	Power interface

Table 2: ISR 1101

Physical Interfaces	FIPS 140-2 Logical Interfaces
Ethernet Ports (11) Console Port (2)	Data Input Interface
Ethernet Ports (11) Console Port (2)	Data Output Interface
Ethernet Ports (11) Console Port (2) USB Ports (1) Power Button (1) Reset Button (1)	Control Input Interface
Ethernet Ports (11)	Status Output Interface

Physical Interfaces	FIPS 140-2 Logical Interfaces
Console Port (2) USB Ports (1) LEDs	
Power connector	Power interface

Table 3: ISR 1111

5 Roles, Services, and Authentication

Authentication is identity-based. Each user is authenticated upon initial access to the module. There are two main roles in the router that operators may assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. The module supports RADIUS and TACACS+ for authentication. A complete description of all the management and configuration capabilities of the modules can be found in the Cisco ISR 1000 Series Integrated Services Routers Software Configuration Guide Manual[1] and in the online help for the modules.

The User and Crypto Officer passwords and all shared secrets must each be at a minimum of eight (8) characters long, and must include at least six (6) integers, at least one alphabetic character and at least one special character (enforced procedurally). See the Secure Operation section for more information. If a minimum 8 character password is used with six (6) integers, one (1) alphabetic character and one (1) special character without repetition for an eight (8) character password, the probability of randomly guessing the correct sequence is one (1) in 14,089,420,800. This calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. With this information the calculation should be $1/(10x9x8x7x6x5x32x52)x56^{2}$ = 1/(251,596,800)x56 = 1/14,089,420,800. Therefore, the associated probability of a successful random attempt is approximately 1 in 14,089,420,800, which is less than the 1 in 1,000,000 required by FIPS 140-2.

The module has a delayed timed entry mechanism that enforces a 3 second delay between each password input attempt. With the assumption that it takes approximately zero (0) seconds to process each failed password entry attempt, the absolute maximum number of attempts in a one-minute period is 20. With this assumption the probability of success with multiple consecutive attempts in a one-minute period is 20/14,089,420,800=704,471,040. Therefore, the associated probability of a successful

[1] Link located in Section 10.

[2] 8!/(6!1!1!) = 8x7 = 56

random attempt in a one-minute period is approximately 1 in 704,471,040, which is less than the 1 in 100,000 required by FIPS 140-2.

Additionally, when using RSA-based authentication, RSA key pair has a modulus size of either 2048 or 3072 bits, thus providing at least 112 bits of strength. Assuming the low end of that range (2048 bits), an attacker would have a 1 in 2^{112} chance of randomly obtaining the key, which is much stronger than the one-in-a-million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 8.6×10^{31} ($5.2 \times 10^{33} / 60 = 8.6 \times 10^{31}$) attempts per second, which far exceeds the operational capabilities of the modules to support.

It should be noted that the same services are available to both Users and Cryptographic officers, regardless of whether or not they are in a non-FIPS approved mode of operation or a FIPS approved mode of operation.

5.1 User Services

A User enters the system by accessing the console/auxiliary port with a terminal program or SSH v2 session to a LAN port or the 10/100 management Ethernet port. The module prompts the User for their username/password combination. If the username/password combination is correct, the User is allowed entry to the module management functionality. The services available to the User role consist of the following:

- Status Functions - View state of interfaces and protocols, firmware version
- Terminal Functions - Adjust the terminal session (e.g., lock the terminal, adjust flow control)
- Directory Services - Display directory of files kept in memory
- Perform Self-Tests – Perform the FIPS 140 start-up tests on demand
- Perform Cryptography – Use the cryptography provided by the module:
    - SSH
    - IPSec
    - SNMPv3

5.2 Cryptographic Officer Services

A Crypto Officer enters the system by accessing the console/auxiliary port with a terminal program or SSH v2 session to a LAN port or the 10/100 management Ethernet port. The Crypto Officer authenticates in the same manner as a User. The Crypto Officer is identified by accounts that have a privilege level 15 (versus the privilege level 1 for users). A Crypto Officer may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration and maintenance of the router. The Crypto Officer services consist of the following:

- Configure the module - Define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.

- Define Rules and Filters - Create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.

- Status Functions - View the module configuration, routing tables, active sessions, use get commands to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.

- Manage the module - Log off users, shutdown or reload the router, manually back up router configurations, view complete configurations, manage user rights, initiate power-on self-tests on demand and restore router configurations.

- Set Encryption- Set up the configuration tables for IP tunneling. Set keys and algorithms to be used for each IP range.

- Perform Self-Tests – Perform the FIPS 140 start-up tests on demand.

- Perform Cryptography – Use the cryptography provided by the module:
    - SSH
    - IPSec
    - SNMPv3

- Zeroization – Erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data.

5.3 Unauthenticated User Services

The services for someone without an authorized role are to view the status output from the module's LED pins and cycle power.

6 Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are protected by the password-protection of the Crypto Officer role login and can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are exchanged and entered electronically or via Internet Key Exchange (IKE) or SSH.

The module supports the following keys and critical security parameters (CSPs):

Key/CSP Name	Key/CSP Type	Description	Storage	Generation/Input	Output	Zeroization
General Keys/CSPs						
DRBG entropy input (CSP)	SP800-90A CTR_DRBG 256-bit	HW based entropy source output used to construct the seed.	DRAM (plaintext)	Internally generated	Never output from the module	Power cycle the device
DRBG Seed (IOS XE) (CSP)	SP800-90A CTR_DRBG 384-bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from hardware-based entropy source.	DRAM (plaintext)	Internally generated	Never output from the module	Automatically every 400 bytes or turn off the router.
DRBG V (CSP)	SP800-90A CTR_DRBG 256-bit	Internal V value used as part of SP 800-90A CTR_DRBG	DRAM (plaintext)	Internally generated	Never output from the module	Power cycle the device
DRBG Key (CSP)	SP800-90A CTR_DRBG 256-bit	Internal Key value used as part of SP 800-90A CTR_DRBG	DRAM (plaintext)	Internally generated	Never output from the module	Power cycle the device

Key/CSP Name	Key/CSP Type	Description	Storage	Generation/Input	Output	Zeroization
Diffie-Hellman Shared Secret (CSP)	DH 2048 – 4096 bits	The shared exponent established using Diffie-Hellman key agreement.	DRAM (plaintext)	Established via Diffie-Hellman key agreement scheme.	Never output from the module	Power cycle the device.
Diffie Hellman private key (CSP)	DH 224-379 bits	The private key used in Diffie-Hellman key agreement scheme.	DRAM (plaintext)	Generated internally by calling approved DRBG.	Never output from the module	Power cycle the device.
Diffie Hellman public key	DH 2048 – 4096 bits	The public key used in Diffie-Hellman key agreement scheme.	DRAM (plaintext)	Derived internally in compliance with Diffie-Hellman key agreement scheme.	Per the Diffie-Hellman key agreement scheme	Power cycle the device
EC Diffie-Hellman private key (CSP)	ECDH (Curves: P-256, P-384)	The private key used in EC Diffie-Hellman key agreement scheme.	DRAM (plaintext)	Generated internally by calling approved DRBG.	Never output from the module	Power cycle the device
EC Diffie-Hellman public key	ECDH (Curves: P-256, P-384)	The public key used in EC Diffie-Hellman key agreement scheme.	DRAM (plaintext)	Derived internally in compliance with EC Diffie-Hellman key agreement scheme.	Per the EC Diffie-Hellman key agreement scheme	Power cycle the device
EC Diffie-Hellman shared secret (CSP)	ECDH (Curves: P-256, P-384)	The shared exponent established using EC Diffie-Hellman key agreement.	DRAM (plaintext)	Established via EC Diffie-Hellman key agreement scheme.	Never output from the module	Power cycle the device
Operator password (CSP)	Password, at least eight characters	The password of the operator.	NVRAM (plaintext)	Externally generated and entered by the User and/or CO when logging in.	Never output from the module	Overwrite with new password

Key/CSP Name	Key/CSP Type	Description	Storage	Generation/Input	Output	Zeroization
Enable password (CSP)	Password, at least eight characters	The plaintext password of the CO role.	NVRAM (plaintext)	Externally generated and entered by the CO.	Never output from the module	Overwrite with new password
Enable secret (CSP)	Password, at least eight characters	The obfuscated password of the CO role. However, the algorithm used to obfuscate this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password. The Cryptographic Operator optionally configures the module to obfuscate the Enable password.	NVRAM (plaintext)	Externally generated and entered by the CO.	Never output from the module	Overwrite with new password
RADIUS secret (CSP)	Shared Secret, 16 characters	The RADIUS shared secret.	NVRAM (plaintext), DRAM (plaintext)	Externally generated and entered by the CO.	Never output from the module	By running, '# no radius-server key' command
RADIUSOverIPSecEncryptionKey (CSP)	AES-CBC, AES-GCM	Encryption/decryption key, used in IPSec tunnel between module and RADIUS to encrypt/decrypt EAP keys.	NVRAM (plaintext), DRAM (plaintext)	This key is derived in accordance with the IKE Protocol	Never output from the module	Power Cycle
RADIUSOverIPSecIntegrityKey (CSP)	HMAC	Integrity/ Authenticity key, used in IPSec tunnel between module and RADIUS	NVRAM (plaintext), DRAM (plaintext)	This key is derived in accordance with the IKE Protocol	Never output from the module	Power Cycle

Key/CSP Name	Key/CSP Type	Description	Storage	Generation/Input	Output	Zeroization
TACACS+ secret (CSP)	Shared Secret, 16 characters	The TACACS+ shared secret.	NVRAM (plaintext), DRAM (plaintext)	Externally generated and entered by the CO.	Never output from the module	By running, '# no tacacs-server key' command
IKE/IPSec						
Skeyid (CSP)	HMAC SHA-1 160-bits	A string derived from secret material known only to the active players in the IKE exchange.	DRAM (plaintext)	Internally generated	Never output from the module	Automatically after IKE session terminated.
skeyid_a (CSP)	HMAC SHA-1 160-bits	The keying material used by ISAKMP SA to authenticate its messages.	DRAM (plaintext)	Internally generated	Never output from the module	Automatically after IKE session terminated.
skeyid_d (CSP)	HMAC SHA-1 160-bits	The keying material used to derive keys for non ISAKMP security associations.	DRAM (plaintext)	Internally generated	Never output from the module	Automatically after IKE session terminated.
skeyid_e (CSP)	HMAC SHA-1 160-bits	The keying material used by the ISAKMP SA to protect the confidentiality of its messages.	DRAM (plaintext)	Internally generated	Never output from the module	Automatically after IKE session terminated.
IKE session encrypt key (CSP)	AES 128-, 192-, or 256- bits	The IKE session encrypt key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Internally generated	Never output from the module	Automatically after IKE session terminated.
IKE session authentication key (CSP)	HMAC SHA-1 160-bits	The IKE session authentication key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Internally generated	Never output from the module	Automatically after IKE session terminated.

Key/CSP Name	Key/CSP Type	Description	Storage	Generation/Input	Output	Zeroization
ISAKMP pre-shared key (CSP)	Shared Secret, at least eight characters	Used to generate IKE skeyid during preshared-key authentication. This key can have two forms based on whether the key is related to the hostname or the IP address.	NVRAM (plaintext)	Externally generated and entered by the CO.	Never output from the module	By running, '# no crypto isakmp key' command
IKE RSA Private Key (CSP)	RSA (Private Key) 2048, 3072 bits	The private key used in IKE authentication.	NVRAM (plaintext)	Generated internally by calling approved DRBG	Never output from the module	By running, '# crypto key zeroize rsa' command
IKE RSA Public Key	RSA (Public Key) 2048, 3072 bits	The public key used in IKE authentication.	NVRAM (plaintext)	Internally generated	Output from the module per IKE protocol	By running, '# crypto key zeroize rsa' command
IPsec encryption key (CSP)	AES 128-, 192-, or 256- bits	The IPsec encryption key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Internally generated	Never output from the module	Automatically when IPsec session terminated.
IPsec authentication key (CSP)	SHA-1 HMAC 160-bits	The IPsec authentication key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Internally generated	Never output from the module	Automatically when IPsec session terminated.
SSH						

Key/CSP Name	Key/CSP Type	Description	Storage	Generation/Input	Output	Zeroization
SSH Private Key (CSP)	RSA (Private Key) 2048, 3072 bits	The SSH private key for the module.	NVRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	SSH private key is zeroized by either deletion (via **# crypto key zeroize rsa**) or by overwriting with a new value of the key
SSH Public Key	RSA (Public Key) 2048, 3072 bits	The SSH public key for the module.	NVRAM (plaintext)	Internally generated	Output from the module per SSH protocol	Zeroized upon deletion.
SSH Session Key (CSP)	AES 128-, 192-, or 256- bits	The SSH session key. This key is created through SSH key establishment.	DRAM (plaintext)	Internally generated	Never output from the module	Automatically when the SSH session is terminated.
SSH Integrity Key (CSP)	SHA-1 HMAC 160-bits	Used for SSH connections integrity to assure the traffic integrity.	DRAM (plaintext)	Internally generated	Never output from the module	Automatically when the SSH session is terminated.
SNMPv3						
SNMPv3 Password (CSP)	Shared Secret, at least eight characters	Used to derive HMAC-SHA1 key for SNMPv3 Authentication	DRAM	Externally generated and entered by the CO.	Never output from the module	Power cycle

Key/CSP Name	Key/CSP Type	Description	Storage	Generation/Input	Output	Zeroization
snmpEngineID (CSP)	Shared secret 32-bits	Unique string to identify the SNMP engine	NVRAM	Externally generated and entered by the CO.	Never output from the module	By running, '# no snmp-server engineID local engineid-string' or overwriting with new engine ID
SNMP session key (CSP)	AES 128-bit	Encrypts SNMP traffic	DRAM	Derived via key derivation function defined in SP800-135 KDF	Never output from the module	Power cycle

Table 4: Cryptographic Keys and CSPs

6.1 User Services and CSP Access

The services accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below.

Services & Access	Description	Keys & CSPs
View Status Functions	View state of interfaces and protocols, firmware version.	Operator password – r
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	Operator password – r
Directory Services	Display directory of files kept in memory.	Operator password – r
Self-Tests	Execute the FIPS 140 start-up tests on demand	N/A
Random Number Generation	Key generation and seeds for asymmetric key generation	DRBG entropy input, DRBG seed, DRBG V, DRBG Key – r, w, d
Key Exchange	Key exchange over Diffie-Hellman and EC Diffie-Hellman	Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, EC Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman shared secret – w, d
TACACS+	User & CO authentication to the module using TACACS+.	TACACS+ secret - r
RADIUS Key Wrap	Establishment and subsequent receive 802.11 PMK from the RADIUS server.	RADIUSOverIPSecEncryptionKey, RADIUSOverIPSecIntegrityKey, RADIUS Server Shared Secret – w, d
SSH Functions	Negotiation and encrypted data transport via SSH	Operator password, SSH private key, SSH public key, SSH integrity key, SSH Session Key – r

Module Read-only Configuration	Viewing of configuration settings	Operator password – r

Table 5: User Services

6.2 Crypto Officer Services and CSP Access

Services & Access	Description	Keys & CSPs
View Status Functions	View the switch configuration, routing tables, active sessions, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	Operator password, Enable password – r, w, d
Define Rules and Filters	Create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.	Operator password, Enable password – r, w, d
Self-Tests	Execute the FIPS 140 start-up tests on demand	N/A
Random Number Generation	Key generation and seeds for asymmetric key generation	DRBG entropy input, DRBG seed, DRBG V, DRBG Key – r, w, d
Key Exchange	Key exchange over Diffie-Hellman and EC Diffie-Hellman	Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, EC Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman shared secret – r, w, d
TACACS+	User & CO authentication to the module using TACACS+.	TACACS+ secret– r, w, d
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in Table 4, Zeroization column.	All Keys and CSPs will be destroyed
Module Configuration	Selection of non-cryptographic configuration settings	N/A

SNMPv3	Non-security related monitoring by the CO using SNMPv3	snmpEngineID, SNMPv3 Password, SNMP session key – r, w, d
SSH	Establishment and subsequent data transfer of an SSH session for use between the module and the CO.	Operator password, SSH private key, SSH public key, SSH integrity key, SSH Session Key – r, w, d
IPsec	Configure IPsec VPN parameters, provide entry and output of CSPs.	skeyid, skeyid_a, skeyid_d, skeyid_e, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE RSA private Key, IKE RSA public key, IPsec encryption key, IPsec authentication key, DRBG entropy input, DRBG V, DRBG Key – r, w, d
RADIUS Key Wrap	Establishment and subsequent receipt of 802.11 PMK from the RADIUS server.	RADIUSOverIPSecEncryptionKey, RADIUSOverIPSecIntegrityKey, RADIUS Server Shared Secret – r, w, d

Table 6: CO Services

7 Cryptographic Algorithms

7.1 Approved Cryptographic Algorithms

The Cisco ISR 1000 supports many different cryptographic algorithms. However, only FIPS approved algorithms may be used while in the FIPS mode of operation. The following table identifies the approved algorithms for use in the FIPS mode of operation.

Algorithm[3]	Supported Mode	Cert. #
IC2M		
AES (SP 800-38 A/B/D/F)	ECB (128, 192, 256); CBC (128, 192, 256); CMAC (128, 256); GMAC (128, 192, 256); CFB128 (128, 192, 256), GCM (128, 256); KW (128, 256)	A1462
SHS (FIPS 180-4)	SHA-1, -256, -384, and -512 (Byte Oriented)	A1462
HMAC (FIPS 198-1)	SHA-1, -256, -384, and -512	A1462
DRBG (SP 800-90A)	CTR (using AES-256)	A1462
RSA (FIPS 186-2/4)	Key Generation (2048-3072 bits); PKCS#1 v.1.5, 1024-4096 bit key SigGen, SigVer • 1024-bit keys allowed for signature verification only.	A1462
CVL (SP800-135)	IKEv2 KDF, SSH KDF, SNMP KDF Note: The IKEv2, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.	A1462
KAS-ECC-SSC (NIST SP 800-56Arev3)	KAS-ECC-SSC: - Curves: o P-256 o P-384	A1462
KAS-FFC-SSC (SP 800-56Arev3)	KAS-FFC-SSC: - modp-2048 - modp-3072 - modp-4096	A1462
CKG (SP800-133)		Vendor affirmed

Table 7: Algorithm Certificates

[3] Not all algorithms/modes tested on the CAVP validation certificates are implemented in the module.

- There are some algorithm modes that were tested but not implemented by the modules. Only the algorithms, modes, and key sizes that are implemented by the modules are shown in this table.

- In accordance with FIPS 140-2 IG D.12, the cryptographic modules perform Cryptographic Key Generation as per scenario 1 of section 5 in SP800-133. The resulting seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 7296 for IPSec/IKEv2. The module provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. 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. During operational testing, the module was tested against an independently developed instance of IPsec-v3 with IKEv2 and was found to act correctly.

- KTS (AES Cert. #A1462; key establishment methodology provides 128 or 256 bits of encryption strength)

- KTS (AES Cert. #A1462 and HMAC Cert. #A1462; key establishment methodology provides between 128 and 256 bits of encryption strength)

- KAS (KAS-SSC Cert. #A1462, CVL Cert. #A1462; key establishment methodology provides between 128 and 192 bits of encryption strength)

- KAS (KAS-SSC Cert. #A1462, CVL Cert. #A1462; key establishment methodology provides between 112 and 152 bits of encryption strength)

  The KAS FFC and KAS ECC strengths are as follows:
  KAS-ECC-SSC: 128 and 192 bits of encryption strength
  KAS-FFC-SSC: 112 and 152 bits of encryption strength

7.2 Non-Approved Algorithms allowed for use in FIPS-mode

The ISR 1000 cryptographic module implements the following non-Approved algorithms that are allowed for use in FIPS-mode:

- Non-approved RNG for seeding the DRBG.

7.3 Non-Approved Algorithms

The ISR 1000 cryptographic module implements the following non-approved algorithms that are not permitted for use in FIPS 140-2 mode of operations:

Service	Non-Approved Algorithm
SSH (non-compliant)	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES, Triple-DES Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman
TLS (non-compliant)	Hashing: MD5, SHA MACing: HMAC MD5, HMAC SHA Symmetric: AES, DES, RC4, Triple-DES Asymmetric: ECDSA, RSA, DH, ECDH KDF: TLS KDF
IPsec (non-compliant)	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES, RC4, Triple-DES Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman
SNMP (non-compliant)	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman
Initialization**	SHA-1 (non-compliant)
RSA Key Wrapping	RSA Key Wrapping (Key establishment providing 112 or 128 bits of security strength

Table 8: Non-Approved Algorithms

Note: Services marked with a double asterisk (**) make use of a non-compliant hash algorithm at various points during initialization. This algorithm is does not provide any cryptographic protection.

7.4 Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. The modules implement the following power-on self-tests:

- Known Answer Tests:
    - AES (Encrypt and Decrypt) KATs,
    - AES-GCM KAT,
    - SHA-1 KAT,
    - SHA-256 KAT,
    - SHA-384 KAT,
    - SHA-512 KAT,
    - HMAC SHA-1 KAT,
    - HMAC SHA-256 KAT,
    - HMAC SHA-384 KAT,
    - HMAC SHA-512 KAT,
    - DRBG KAT,
    - KAS ECC Primitive "Z" KAT(NIST SP 800-56Arev3),
    - KAS FFC Primitive "Z" KAT (NIST SP 800-56Arev3),
    - IKEv2 KDF KAT,
    - SNMP KDF KAT,
    - SRTP KDF KAT,
    - SSH KDF KAT,
    - RSA (Sign and Verify) KAT
  - Firmware Integrity Test (RSA 2048 w/ SHA-256)

The modules perform all power-on self-tests automatically at boot. All power-on self-tests must be passed before any operator can perform cryptographic services. The power-on self-tests are performed after the cryptographic systems are initialized but prior any other operations; this prevents the module from passing any data during a power-on self-test failure. In addition, the modules also provide the following conditional self-tests:

- Continuous Random Number Generator test for the approved DRBG
- RCT for the non-approved RNG
- Pair-Wise Consistency Test for RSA signature keys
- Pair-Wise Consistency Test for RSA keys used in key establishment
- Firmware Load Test

8 Physical Security

The modules physical embodiment is that of a multi-chip standalone device that meets Level 1 Physical Security requirements. The module is entirely contained within a metal production-grade enclosure.

9 Secure Operation

The module meets all of the overall Security Level 1 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the module is shipped in Cisco boxes with Cisco adhesive, so if tampered with the recipient will notice. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this module without maintaining the following settings will remove the module from the FIPS approved mode of operation. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Upon initial boot from the factory, the ISR is in a non-FIPS mode of operation. To transition from a non-FIPS mode of operation to a FIPS mode of operation, the Cryptographic Officer must follow all steps detailed in section 9.1 of this security policy

9.1 System Initialization and Configuration

Step1 - The value of the boot field must be 0x2102. This setting disables break from the console to the ROM monitor and automatically boots. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

config-register 0x2102

Step 2 - The Crypto Officer must create the “enable” password for the Crypto Officer role. Procedurally, the password must be at least 8 characters, including at least one letter and at least one number without repetition and is entered when the Crypto Officer first engages the “enable” command. The Crypto Officer enters the following syntax at the “#” prompt:

enable secret [PASSWORD]

Step 3 - The Crypto Officer must set up the operators of the module. The Crypto Officer enters the following syntax at the “#” prompt:

Username [USERNAME]

Password [PASSWORD]

Step 4 – For the created operators, the Crypto Officer must always assign passwords (of at least 8 characters, including at least six (6) integers, one (1) special character and one (1) alphabet are used without repetition) to users. Identification and authentication on the console port is required for Users. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

line con 0

password [PASSWORD]

login local

Step 5 - The Crypto Officer may configure the module to use RADIUS or TACACS+ for authentication. Configuring the module to use RADIUS or TACACS+ for authentication is optional. If the module is configured to use RADIUS or TACACS+, the Crypto-Officer must define RADIUS or TACACS+ shared secret keys that are at least 16 characters long, including at least one letter and at least one number.

Step 6 - Dual IOS mode is not allowed. ROMMON variable IOSXE_DUAL_IOS must be set to 0.

Step 7 - In service software upgrade (ISSU) is not allowed. The operator should not perform in service software upgrade of an ISR1000 FIPS validated firmware image

Step 8 - Use of the debug.conf file is not allowed. The operator should not create the bootflash:/debug.conf file and use it for setting environment variables values.

Step 9 – Execute the “platform ipsec fips-mode” command.

Step 10 – After executing reload/ reboot command. The device will enter the FIPS mode.

NOTE: The keys and CSPs generated in the cryptographic module during FIPS mode of operation cannot be used when the module transitions to non-FIPS mode and vice versa. While the module transitions from FIPS to non-FIPS mode or from non-FIPS to FIPS mode, all the keys and CSPs are to be zeroized by the Crypto Officer.

9.2 IPsec Requirements and Cryptographic Algorithms

Step 1 - The only type of key management that is allowed in FIPS mode is Internet Key Exchange (IKE).

Step 2 - Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms shall be used in a FIPS 140-2 configuration:

- ah-sha-hmac
- ah-sha256-hmac
- ah-sha384-hmac
- ah-sha512-hmac
- esp-sha-hmac
- esp-sha256-hmac
- esp-sha384-hmac
- esp-sha512-hmac
- esp-aes
- esp-gcm

Step 3 - The following algorithms shall not be used:

- MD-5 for signing
- MD-5 HMAC
- DES

9.3 Protocols

Secure DNS and GDOI are not permitted in FIPS mode of operation and shall not be configured.

9.4 Remote Access

SSH access to the module is allowed in FIPS approved mode of operation, using SSH v2 and a FIPS approved algorithm.

SNMPv3 communications with the module are allowed in FIPS approved mode.

9.5 Key Strength

Key sizes with security strength of less than 112-bits shall not be used in FIPS mode.

10 Related Documentation

This document deals only with operations and capabilities of the security appliances in the technical terms of a FIPS 140-2 cryptographic device security policy. More information is available on the security appliances from the sources listed in this section and from the following source:

- The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the security appliances.
- Software Configuration Guide (https://www.cisco.com/c/en/us/td/docs/routers/access/1100/software/configuration/xe-16-12/cisco_1100_series_swcfg_xe_16_12_x.html)
- For LED related information please read the following document (https://www.cisco.com/c/en/us/td/docs/routers/access/1100/hardware/installation/guide/b-cisco-1100-series-hig/isr1k-hig-overview.html)

11 Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

11.1 Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

11.2 Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

11.3 Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

12 Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

13 Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://tools.cisco.com/security/center/rss.x?i=44

13.1 Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*. Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

14 Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

14.1 Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output.

Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

14.2 Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

14.3 Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1) – Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2) – Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3) – Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4) – You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

15 Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

http://www.cisco.com/packet

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

http://www.cisco.com/en/US/learning/index.html

16 Definitions List

ACL	Access Control List
AES	Advanced Encryption Standard
ISR	Integrated Services Router
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment (Canada)
CSP	Critical Security Parameter
DRAM	Dynamic RAM
DRBG	Deterministic random bit generator
EDC	Error Detection Code
ESP	Embedded Services Processor
FIPS	Federal Information Processing Standard
Gbps	Gigabits per second
GigE	Gigabit Ethernet
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
ISAKMP	Internet Security Association and Key Management Protocol
ISSU	In service software upgrade
KAT	Known Answer Test
KDF	Key Derivation Function
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
MPLS	Multiprotocol Label Switching
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random Access Memory
PIN	Personal Identification Number
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory

RNG	Random Number Generator
RP	Route Processor
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
VPN	Virtual Private Network