Cisco ASR 1000 Series Routers with MACsec

Firmware version:

Cisco IOS-XE 16.9

Hardware versions:

ASR1001-HX, ASR1002-HX, ASR1006-X, and ASR1009-X

Embedded Services Processor (ESP) Hardware versions:

ASR1000-ESP40, ASR1000-ESP100 and ASR1000-ESP200;

Route Processor (RP) Hardware versions:

ASR-1000-RP2, and ASR-1000-RP3

Modular Interface Processor Hardware versions:

ASR1000-MIP100

Line Card Hardware versions:

EPA-10X10GE, and EPA-1X40GE QSFP+

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

Cisco Systems, Inc.

Version 1.1

Table of Contents

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for Cisco ASR 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 ASR (1001-HX, 1002-HX, 1006-X, and 1009-X)

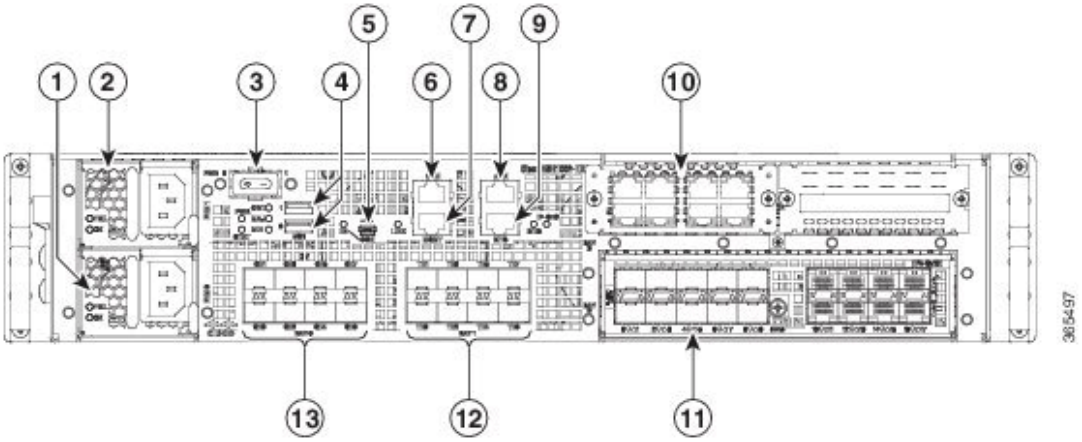
The Cisco ASR 1000 Series Routers (1001-HX, 1002-HX, 1006-X, and 1009-X) are highly scalable WAN and Internet Edge router platforms that deliver embedded hardware acceleration for multiple Cisco IOS Software services without the need for separate service blades. In addition, the Cisco ASR 1000 Series Router is designed for business-class resiliency, featuring redundant Route and Embedded Services Processors, as well as software-based redundancy.

With routing performance and IPsec Virtual Private Network (VPN) acceleration around ten-fold that of previous midrange aggregation routers with services enabled, the Cisco ASR 1000 Series Routers provides a cost-effective approach to meet the latest services aggregation requirement. This is accomplished while still leveraging existing network designs and operational best practices.

Figure 1: ASR 1001-HX

Figure 2: ASR 1002-HX

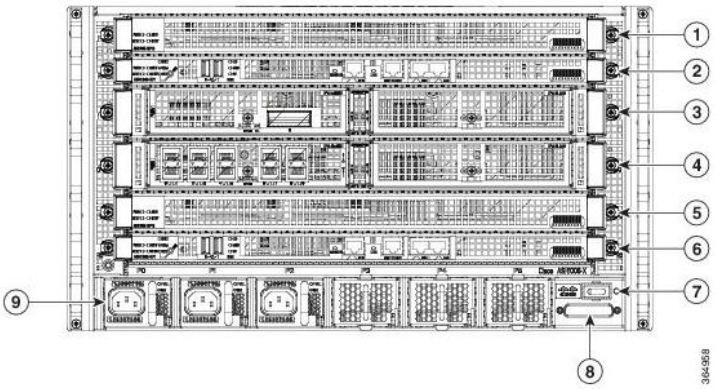
The EPA-18X1GE was not part of the tested configuration.



1	Power supply (PEM 0)	8	AUX–RJ-45/RS-232 compatible auxiliary port
2	Power supply (PEM 1)	9	BITS–RJ-48 Building Integrated Timing Supply port **Note** The BITS port is not supported in this software release.
3	Power (PWR) switch	10	Bay 3–NIM slot
4	USB ports 0 and 1	11	Bay 2–EPA slot
5	CON–Mini USB console port	12	Bay 1–10GE SFP+ ports
6	CON–RJ-45/RS-232 compatible console port	13	Bay 0–1GE SFP ports
7	MGMT–RJ-45 10/100/1000 management Ethernet port		

Figure 3: ASR 1002-HX Overall Chassis View

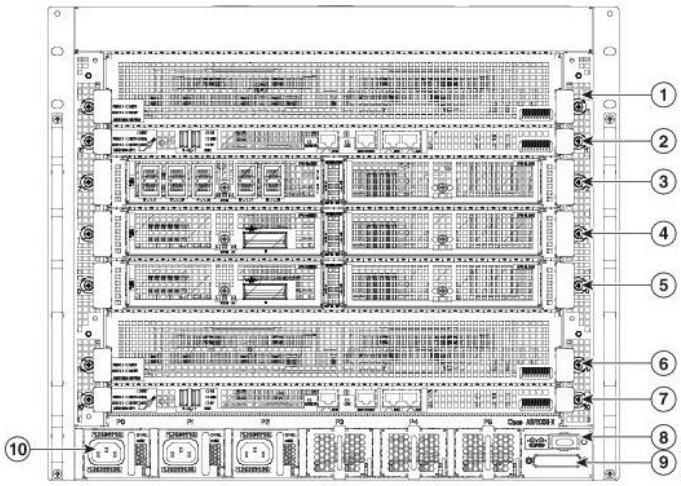
Figure 4: ASR 1006-X



1	Slot F1	6	Slot R0
2	Slot R1	7	Standby/ON switch
3	Slot 1	8	DB-25 Alarm Connector
4	Slot 0	9	Power shelf that has power supplies from P0 to P5
5	Slot F0		

Figure 5: ASR 1006-X Overall Chassis View

Figure 6: ASR 1009-X



1	Slot F1	6	Slot F0
2	Slot R1	7	Slot R0
3	Slot 2	8	Standby/ON switch
4	Slot 1	9	DB-25 Alarm connector
5	Slot 0	10	Power shelf that has power supplies from P0 to P5

Figure 7: ASR 1009-X Overall Chassis View

2.2 Embedded Services Processor (40, 100 and 200 Gbps)

The Cisco ASR 1000 Series Embedded Service Processors (ESPs) are based on the innovative, industry-leading Cisco QuantumFlow Processor for next-generation forwarding and queuing in silicon. These components use the first generation of the hardware and software architecture known as Cisco QuantumFlow Processor.

The 40-, 100-, and 200-Gbps Cisco ASR 1000 Series ESPs provide centralized forwarding-engine options for the Cisco ASR 1000 Series Aggregation Services Routers.

ESP40	

ESP100	
ESP200	

Figure 8: ESPs

The Cisco ASR 1000 Series ESPs are responsible for the data-plane processing tasks, and all network traffic flows through them. The modules perform all baseline packet routing operations, including MAC classification, Layer 2 and Layer 3 forwarding, quality-of-service (QoS) classification, policing and shaping, security access control lists (ACLs), VPN, load balancing, and NetFlow.

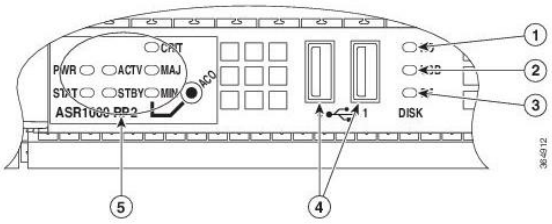
*It should be noted that the ASR1001-HX and ASR1002-HX uses an integrated ESP. They do not have a distinct part number but is referred to as the, ESP2.5.

2.3 Router Processor (RP2, RP3)

The Cisco ASR 1000 Series Route Processors running IOS-XE 16.9 address the route-processing requirements of carrier-grade IP and Multiprotocol Label Switching (MPLS) packet infrastructures. Not only do they provide advanced routing capabilities, but they also monitor and manage the other components in the Cisco ASR 1000 Series Aggregation Services Router.

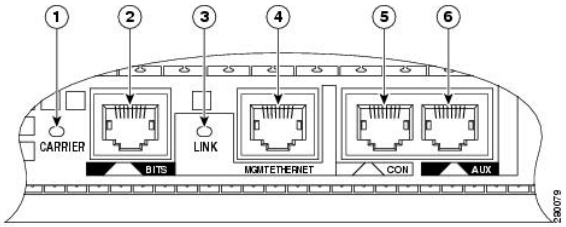
*It should be noted that ASR1001-HX and ASR1002-HX employs an integrated RP.

Figure 9: (a) RP2 and (b) RP3



1	Internal hard drive LED	4	USB 0, USB 1 connector
2	External USB Flash LED	5	ASR1000-RP2 LEDs
3	Internal USB bootflash LED	–	–

Figure 10: RP LEDs and USBs



1	CARRIER LED	4	MGMT Ethernet connector
2	BITS connector	5	CON connector
3	LINK LED	6	AUX connector

Figure 11: RP Connections

2.4 ASR 1000 Series Modular Interface Processor (ASR1000-MIP100)

The Cisco ASR 1000 Series Modular Interface Processor (ASR1000-MIP100) (Figure 7) is a full-duplex 100-Gbps modular Ethernet line card that is capable of hosting up to two Cisco ASR 1000 Series Ethernet Port Adapters (EPAs) (Figures 8 and 9). The EPAs are new interface cards that introduce 40 Gigabit Ethernet and 100 Gigabit Ethernet connectivity to the Cisco ASR 1000 Series.

Figure 12: ASR1000-MIP100

Figure 13: EPA-10X10GE

Figure 14: EPA-1X40GE QSFP+

2.5 Validated and Vendor Affirmed Hardware

The validated configurations are comprised of the following components:

Chassis:

1. ASR1001-HX
2. ASR1002-HX
3. ASR1006-X
4. ASR1009-X

Route Processors (RP):

Embedded Service Processors (ESP):

1. ASR1000-ESP40
2. ASR1000-ESP100
3. ASR1000-ESP200

Line Cards (LC):

1. ASR-1000-RP2
2. ASR-1000-RP3

1. EPA-10X10GE
2. EPA-1X40GE QSFP+

Chassis	Hardware Configurations		
	Route Processor	Embedded Service Provider	Line Card
ASR 1001-HX	Fixed configuration		Not Applicable
ASR 1002-HX	Fixed configuration		Not Applicable
ASR 1006-X	Dual RP2	Dual ESP40	EPA-10X10GE, EPA-1X40GE QSFP+
		Dual ESP100	
	Dual RP3	Dual ESP40	
		Dual ESP100	
ASR 1009-X	Dual RP2	Dual ESP40	EPA-10X10GE, EPA-1X40GE QSFP+
		Dual ESP100	
		Dual ESP200	
	Dual RP3	Dual ESP40	
		Dual ESP100	
		Dual ESP200	

Table 1: Module Hardware Configurations running IOS-XE 16.9

Chassis	Vendor Affirmed Hardware Configurations		
	Route Processor	Embedded Service Provider	Line Card
ASR 1001-X	Fixed configuration		Not Applicable
ASR 1013	Dual RP2	Dual ESP40	EPA-18X1GE, EPA-1X100GE, EPA-CPAK-2X40GE, EPA-1X100GE QSFP+, EPA-2X40GE QSFP+
		Dual ESP100	
		Dual ESP200	
	Dual RP3	Dual ESP40	
		Dual ESP100	
		Dual ESP200	

Table 2: Vendor Affirmed Models[1]

2.6 FIPS and non-FIPS modes of operation

The ASR 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 both a FIPS and a non-FIPS mode of operation:

- SSH

[1] Vendor affirmed devices use the same firmware image (IOS-XE 16.9) as the modules tested. No claim to conformance can be made as these models were not tested by a CSTL or reviewed by CMVP.

- TLS
- IPSec
- SNMPv3
- MACsec

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.

2.7 Module Validation Level

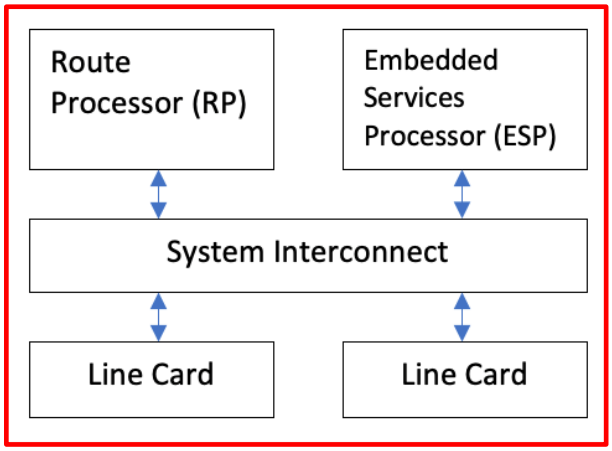
The following table lists the level of validation for each area in the FIPS PUB 140-2.

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 3: Module Validation Level

3 Cryptographic Boundary

The cryptographic boundary for the Cisco ASR 1001-HX, ASR 1002-HX, ASR 1006-X, and ASR 1009-X are defined as encompassing the “top,” “bottom,” “front,” “back,” “left” and “right” surfaces of the case; all portions of the "backplane" 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 (16) Console Port (1) Auxiliary Port (1) 10/100 Management Ethernet Port (1) Backplane (1)	Data Input Interface
Ethernet Ports (16) Console Port (1) Auxiliary Port (1) 10/100 Management Ethernet Port (1) Backplane (1)	Data Output Interface
Ethernet Ports (16) Console Port (1) USB Ports (2) Auxiliary Port (1) 10/100 BITS RJ-48 Port (2) 10/100 Management Ethernet Port (1)	Control Input Interface

Physical Interfaces	FIPS 140-2 Logical Interfaces
Power Switch (1) Backplane (1)	
Ethernet Ports (16) LEDs USB Ports (2) Console Port (1) Auxiliary Port (1) 10/100 Management Ethernet Port (1) Backplane (1)	Status Output Interface
Power Plug(s)	Power interface

Table 4: ASR 1001-HX

Physical Interfaces	FIPS 140-2 Logical Interfaces
Port Adapter Interface (2) Console Port (1) Auxiliary Port (1) 10/100 Management Ethernet Port (1) GigE port (16) Backplane (1)	Data Input Interface
Port Adapter Interface (2) Console Port (1) Auxiliary Port (1) 10/100 Management Ethernet Port (1) GigE port (16) Backplane (1)	Data Output Interface
Port Adapter Interface (2) Console Port (1) Auxiliary Port (1) 10/100 BITS Ethernet Port (1) 10/100 Management Ethernet Port (1) USB Ports (2) GigE port (16) Power Switch (1) Backplane (1)	Control Input Interface
Port Adapter Interface (2) Console Port (1) Auxiliary Port (1) 10/100 Management Ethernet Port (1) LEDs (2) USB Ports (2) GigE port (16) Backplane (1)	Status Output Interface
Power Plug(s)	Power interface

Table 5: ASR 1002-HX

Physical Interfaces	FIPS 140-2 Logical Interfaces
Port Adapter Interface (6) Console Port (1) Auxiliary Port (1 per RP) 10/100 Management Ethernet Port (1 per RP) GigE port (10) Backplane (1)	Data Input Interface
Port Adapter Interface (6) Console Port (1) Auxiliary Port (1 per RP) 10/100 Management Ethernet Port (1 per RP) GigE port (10) Backplane (1)	Data Output Interface
Port Adapter Interface (6) Console Port (1) USB Ports (2 per RP) Auxiliary Port (1 per RP) 10/100 BITS Ethernet Port (1 per RP) 10/100 Management Ethernet Port (1 per RP) Backplane (1) Power Switch	Control Input Interface
Port Adapter Interface (6) LEDs USB Ports (2 per RP) Console Port (1) Auxiliary Port (1 per RP) Backplane (1) 10/100 Management Ethernet Port (1 per RP)	Status Output Interface
Power Plug(s)	Power interface

Table 6: ASR 1006-X with dual RP 2 or RP 3 and dual ESP40 or ESP100

Physical Interfaces	FIPS 140-2 Logical Interfaces
Port Adapter Interface (7) Console Port (1 per RP) Auxiliary Port (1 per RP) 10/100 Management Ethernet Port (1 per RP) GigE port (10) QSFP+ (1)	Data Input Interface
Port Adapter Interface (7) Console Port (1 per RP) Auxiliary Port (1 per RP) 10/100 Management Ethernet Port (1 per RP) GigE port (10) QSFP+ (1)	Data Output Interface
Port Adapter Interface (7) Console Port (1 per RP) USB Ports (2 per RP) Auxiliary Port (1 per RP) 10/100 BITS Ethernet Port (1 per RP) 10/100 Management Ethernet Port (1 per RP) Power Switch	Control Input Interface
Port Adapter Interface (7) LEDs USB Ports (2 per RP) Console Port (1 per RP) Auxiliary Port (1 per RP) 10/100 Management Ethernet Port (1 per RP)	Status Output Interface
Power Plug(s)	Power interface

Table 7: ASR 1009-X with dual RP 2 or RP 3 and dual ESP40 or ESP 100 or ESP 200

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 ASR 1000 Series Aggregation Services Routers Software Configuration Guide Manual[2] and in the online help for the modules.

The User and Crypto Officer passwords and all shared secrets must each be at least eight (8) characters long, including at least one letter and at least one number character, in length (enforced procedurally). See the Secure Operation section for more information. If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 251,596,800 (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. Since it is claimed to be for 8 characters with no repetition, then the calculation should be, 10x9x8x7x6x5x32x52. In order to successfully guess the sequence in one minute would require the ability to make over 4,193,280 guesses per second, which far exceeds the operational capabilities of the module.

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

[2] Link located in Section 10.

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
    - TLS
    - IPSec
    - SNMPv3
    - MACsec

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 or allow plaintext packets to be set from specified IP address.

- Perform Self-Tests – Perform the FIPS 140 start-up tests on demand.
- 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), TLS or SSH.

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

Key/CSP Name	Key Type	Description	Storage	Generation /Input	Output	Zeroization
General Keys/CSPs						
DRBG entropy input	CTR (using AES-256) 256-bit	This is the entropy for SP 800-90 RNG.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Power cycle the device
DRBG Seed (IOS XE)	CTR (using AES-256) 384-bits	This DRBG seed is collected from the onboard Cavium cryptographic processor.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Automatically every 400 bytes or turn off the router.
DRBG V	CTR (using AES-256) 256-bit	Internal V value used as part of SP 800-90 CTR_DRBG	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Power cycle the device
DRBG Key	CTR (using AES-256) 256-bit	Internal Key value used as part of SP 800-90 CTR_DRBG	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Power cycle the device
Diffie-Hellman Shared Secret	DH 2048 – 4096 bits	The shared exponent used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman protocol.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Zeroized upon deletion.

Key/CSP Name	Key Type	Description	Storage	Generation /Input	Output	Zeroization
Diffie Hellman private key	DH 224-379 bits	The private exponent used in Diffie-Hellman (DH) exchange. This CSP is created using the SP 800-90 CTR_DRBG.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Zeroized upon deletion.
Diffie Hellman public key	DH 2048 – 4096 bits	The p used in Diffie-Hellman (DH) exchange. This CSP is created using the SP 800-90 CTR_DRBG.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Zeroized upon deletion.
EC Diffie-Hellman private key	ECDH (Curves: P-256, P-384)	Used for key agreement	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Power cycle the device
EC Diffie-Hellman public key	ECDH (Curves: P-256, P-384)	Used for key agreement	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Power cycle the device
EC Diffie-Hellman shared secret	ECDH (Curves: P-256, P-384)	Used for key agreement	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Power cycle the device
Operator password	Password, at least eight characters	The password of the operator. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	Externally generated and entered by the User and/or CO when logging in	Never output from the module	Overwrite with new password
Enable password	Password, at least eight characters	The plaintext password of the CO role. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	Externally generated and entered by the CO.	Never output from the module	Overwrite with new password

Key/CSP Name	Key Type	Description	Storage	Generation /Input	Output	Zeroization
Enable secret	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. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	Externally generated and entered by the CO.	Never output from the module	Overwrite with new password
RADIUS secret	Shared Secret, 16 characters	The RADIUS shared secret. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext), DRAM (plaintext)	Externally generated and entered by the CO.	Never output from the module	# no radius-server key
RADIUSOverIPSecEncryptionKey	AES-CBC, AES-GCM	AES-128/AES-256 encryption/decryption key, used in IPSec tunnel between module and RADIUS to encrypt/decrypt EAP keys.	NVRAM (plaintext), DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Power Cycle

Key/CSP Name	Key Type	Description	Storage	Generation /Input	Output	Zeroization
RADIUSOverIP SecIntegrityKey	HMAC	Integrity/authentication key, used in IPSec tunnel between module and RADIUS	NVRAM (plaintext), DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Power Cycle
TACACS+ secret	Shared Secret, 16 characters	The TACACS+ shared secret. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext), DRAM (plaintext)	Externally generated and entered by the CO.	Never output from the module	# no tacacs-server key
IKE/IPSec						
skeyid	HMAC SHA-1 160-bits	Value derived per the IKE protocol based on the peer authentication SSH method chosen.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Automatically after IKE session terminated.
skeyid_a	HMAC SHA-1 160-bits	The IKE key derivation key for non ISAKMP security associations.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Automatically after IKE session terminated.
skeyid_d	HMAC SHA-1 160-bits	The IKE key derivation key for non ISAKMP security associations.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Automatically after IKE session terminated.
skeyid_e	HMAC SHA-1 160-bits	The IKE key derivation key for non ISAKMP security associations.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Automatically after IKE session terminated.
IKE session encrypt key	Triple-DES -168 bits	The IKE session encrypt key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Automatically after IKE session terminated.
	AES -128, 192, or 256 bits				Never output from the module	

Key/CSP Name	Key Type	Description	Storage	Generation /Input	Output	Zeroization
IKE session authentication key	HMAC SHA-1 160-bits	The IKE session authentication key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Automatically after IKE session terminated.
ISAKMP preshared	Secret At least eight characters	The key used to generate IKE skeyid during preshared-key authentication. # **no crypto isakmp key** command zeroizes it. This key can have two forms based on whether the key is related to the hostname or the IP address. This CSP is entered by the Cryptographic Officer.	NVRAM (plaintext)	Externally generated and entered by the CO.	Never output from the module	# no crypto isakmp key
IKE RSA Private Key	RSA (Private Key) 2048 – 3072 bits	The key used in IKE authentication. # **crypto key zeroize rsa** command zeroizes it.	NVRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	# crypto key zeroize rsa
IKE RSA Public Key	RSA (Public Key) 2048 – 3072 bits	The key used in IKE authentication. # **crypto key zeroize rsa** command zeroizes it.	NVRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	# crypto key zeroize rsa
IPsec encryption key	Triple-DES -168 bits	The IPsec encryption key. This key is	DRAM (plaintext)	Generated internally via	Never output from the module	Automatically when IPsec

Key/CSP Name	Key Type	Description	Storage	Generation /Input	Output	Zeroization
	AES -128, 192, or 256 bits	created per the Internet Key Exchange Key Establishment protocol.		a call to the DRBG.	Never output from the module	session terminated.
IPsec authentication key	HMAC SHA-1 160-bits	The IPsec authentication key. This key is created per the Internet Key Exchange Key Establishment protocol.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Automatically when IPsec session terminated.
SSH						
SSH Private Key	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
	EC Diffie-Hellman P-256, P-384					
	AES 128-, 192-, or 256-bits					
SSH Public Key	RSA (Public Key) 2048 – 3072 bits	The SSH public key for the module.	NVRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Zeroized upon deletion.
	EC Diffie-Hellman P-256, P-384					
	AES 128-, 192-, or 256- bits					
SSH Session Key	Triple-DES 168-bits	The SSH session key. This key is created through SSH key establishment.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Automatically when the SSH session is terminated.
	AES 128-, 192-, or 256- bits					

Key/CSP Name	Key Type	Description	Storage	Generation /Input	Output	Zeroization
SSH Integrity Key	SHA-1 HMAC 160-bits	Used for SSH connections integrity to assure the traffic integrity.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Automatically when the SSH session is terminated.
TLS						
TLS RSA private key	RSA (Private Key) 2048 – 3072 bits	Identity certificates for module itself and also used in TLS negotiations. Generated using the "crypto key generate rsa"	NVRAM plaintext	Generated internally via a call to the DRBG.	Never output from the module	TLS Server RSA private key is zeroized by either deletion (via **# crypto key zeroize rsa**) or by overwriting with a new value of the key.
TLS RSA public key	RSA (Public Key) 2048 – 3072 bits	Identity certificates for module itself and also used in TLS negotiations. Generated using the "crypto key generate rsa"	NVRAM plaintext	Generated internally via a call to the DRBG.	Never output from the module	Zeroized upon deletion.
TLS pre-master secret	Shared Secret, 384-bits	Shared secret created using asymmetric cryptography from which new TLS session keys can be created. Created as part of TLS session establishment	DRAM (plaintext)	Generated internally via pseudo-random function	Never output from the module	Automatically when TLS session terminated.
TLS master secret	Keying material	Keying material used to derive other TLS keys. This key was derived from TLS pre-master secret during the TLS session establishment.	DRAM (plaintext)	Generated internally via pseudo-random function	Never output from the module	Automatically when TLS session is terminated
TLS Encryption Keys	Triple-DES 168-bits	This is the TLS session key.	DRAM (plaintext)	Generated internally via		Automatically when TLS

Key/CSP Name	Key Type	Description	Storage	Generation /Input	Output	Zeroization
	AES 128-,192-,256-bits	Generated using the TLS protocol.		a call to the DRBG.	Never output from the module	session terminated.
TLS Integrity Key	SHA-1 HMAC 160-bits	Used for TLS integrity to assure the traffic integrity.	DRAM (plaintext)	Generated internally via a call to the DRBG.	Never output from the module	Automatically when TLS session terminated.
	AES 128-,192-,256-bits				Never output from the module	
	HMAC SHA-1 160-bits				Never output from the module	
SNMPv3						
SNMPv3 Password	Secret 256 bits	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication	DRAM	Externally generated and entered by the CO.	Never output from the module	Powercycle
snmpEngineID	Shared secret 32-bits	Unique string to identify the SNMP engine	NVRAM	Externally generated and entered by the CO.	Never output from the module	# no snmp-server engineID local engineid-string, overwritten with new engine ID
SNMP session key	AES 128-bit	Encrypts SNMP traffic	DRAM	Internally generated via SNMP KDF	Never output from the module	Power cycle
MACSec						

Key/CSP Name	Key Type	Description	Storage	Generation /Input	Output	Zeroization
MACsec Security Association Key (SAK)	AES-GCM 128/256 bits	Used for creating Security Associations (SA) for encrypting/decrypting the MACSec traffic in the MACSec hardware.	MACsec PHY (plaintext)	Derived from the CAK using the SP800-108 KDF.	Output from the module to other members of a MACsec connectivity association when encrypted by the KEK	Automatically when session expires
MACsec Connectivity Association Key (CAK)	AES-GCM 128/256 bits	A secret key possessed by members of a MACSec connectivity association.	MACsec PHY (plaintext)	Externally generated and entered by the CO.	Never output from the module	Automatically when session expires
MACsec KEK	AES-GCM 128/256 bits	Used to transmit SAKs to other members of a MACSec connectivity association	MACsec PHY (plaintext)	Derived from the CAK using the SP800-108 KDF.	Never output from the module	Automatically when session expires
MACsec ICK	Secret	Used to verify the integrity and authenticity.	MACsec PHY (plaintext)	Derived from the CAK using the SP800-108 KDF.	Never output from the module	Automatically when session expires

Table 8: Key and CSP Management

6.1 User Services and CSP Access

The services accessing the CSPs, the type of access – read (R), write (W), 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
TLS	Establishment and subsequent data transfer of a TLS session for use between the module and the user.	TLS pre-master secret, TLS encryption key, TLS integrity key – w, d
SSH Functions	Negotiation and encrypted data transport via SSH	Operator password, SSH private key, SSH public key, SSH encryption key, SSH integrity key, SSH Session Key – r
Module Read-only Configuration	Viewing of configuration settings	Operator password – r

Table 9: User Services and CSPs

6.2 Crypto Officer Services and CSP Access

Services & Access	Description	Keys & CSPs[3]
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

[3] r = CSP is read by module, w = CSP is generated, derived and/or used by module =, d = CSP is zeroized by module.

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 – w, d
Zeroization	Zeroize CSPs and cryptographic keys by cycling power to zeroize all cryptographic keys stored in SDRAM. The CSPs (password, secret, engineID) stored in Flash can be zeroized by overwriting with a new value.	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 – 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 encryption key, SSH integrity key, Session Key – w, d
TLS	Establishment and subsequent data transfer of a TLS session for use between the module and the CO.	TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption key and TLS integrity key – 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 – w, d
RADIUS Key Wrap	Establishment and subsequent receipt of 802.11 PMK from the RADIUS server.	RADIUSOverIPSecEncryptionKey, RADIUSOverIPSecIntegrityKey, RADIUS Server Shared Secret – w, d
MACSec Functions	Establishment and subsequent data transfer of an MACSec session for use between the module and the CO	MACsec Security Association Key, MACsec Connectivity Association Key, MACsec KEK, MACsec ICK – w, d

Table 10: Crypto Officer Services and CSPs

7 Cryptographic Algorithms

7.1 Approved Cryptographic Algorithms

The Cisco ASR 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 included in the ASR 1000 for use in the FIPS mode of operation.

Algorithm[4]	Supported Mode	Cert. #
IOS (Route Processor 2 and Route Processor 3)		
AES	ECB (128 , 192 , 256); CBC (128 , 192 , 256); CMAC (128 , 192 , 256); GMAC (128 , 192 , 256); CFB128 (128 , 192 , 256), CTR (128 , 192 , 256), GCM (128 , 192 , 256); KW (128, 256)	4583
		C 462
SHS	SHA-1, -256, -384, and -512 (Byte Oriented)	3760
		C 462
HMAC	SHA-1, -256, -384, and -512	3034
		C 462
DRBG	CTR (using AES-256)	1529
		C 462
ECDSA	KeyGen, KeyVer, SigGen, SigVer (P-256, P-384)	1241
		C 462
RSA	Key Generation (2048-3072 bits); PKCS#1 v.1.5, 1024-4096 bit key SigGen, SigVer • 1024-bit keys allowed for signature verification only.	2500
		C 462
Triple-DES	TCBC (KO 1)	2436
		C 462
CVL	TLS KDF, IKEv1/IKEv2 KDF, SSH KDF, SNMP KDF, SRTP KDF Note: The TLS, IKEv1/IKEv2, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.	1258
		C 462
KAS-ECC Component (CVL)	Curves: P-256 and P-384	1257
		C 462

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

Algorithm[4]	Supported Mode	Cert. #
KAS-FFC Component (CVL)	SHA-256	1257
		C 462
KBKDF (SP800-108)[5]	HMAC-SHA1	139
		C 462
CKG		Vendor affirmed
Cavium Nitrox CN2460 (Embedded Services Processor 40)		
AES	CBC (128, 192, 256)	333
SHS (SHA-1)	Byte Oriented	408
HMAC SHA-1	Byte Oriented	137
Triple-DES	KO 1, CBC	397
Cavium Octeon II CN6870 (Embedded Services Processor 100)		
AES	ECB, CBC (128, 192, 256)	2346
SHS (SHA-1)	Byte Oriented	2023
HMAC SHA-1	Byte Oriented	1455
Triple-DES	KO 1, CBC	1469
Cavium Octeon II CN6880 (Embedded Services Processor 200)		
AES	ECB, CBC (128, 192, 256)	2346
SHS (SHA-1)	Byte Oriented	2023
HMAC SHA-1	Byte Oriented	1455
Triple-DES	KO 1 - CBC	1469
S12411PRI (AKA X120) Macom / APM (EPA-1X40GE)		
AES	GCM (128, 256)	3160
Microsemi / Vitesse VSC8490 (EPA-10X10GE)		
AES	GCM (128, 256)	3505

Table 11: FIPS Approved Algorithms

- In accordance with CMVP IG A.13, when operating in a FIPS approved mode of operation, the same Triple-DES key shall not be used to encrypt more than 2^{20} 64-bit data blocks. Each of TLS, SSH and IPSec protocols governs the generation of the respective Triple- DES keys. Refer to RFC 5246 (TLS), RFC 4253 (SSH) and RFC 6071 (IPSec) for details relevant to the generation of the individual Triple-DES encryption keys. The user is responsible for ensuring the module limits the number of encryptions with the same key to 2^20.

- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS and RFC 7296 for IPSec/IKEv2. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52

[5] KBKDF tested in counter mode

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. The module uses RFC 7296 compliant IKEv2 to establish the shared secret from which the AES GCM encryption keys are derived. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

- When supporting the MACsec protocol in the FIPS approved modes of operation the implementation (see CAVP cert # AES 4583) conforms to IG A.5, scenario #3, when operating in a FIPS approved mode of operation. AES GCM, IVs are generated both internally and deterministically and are a minimum of 96-bits in length as specified in SP 800-38D, Section 8.2.1.

- KTS (AES Certs. #4583 and #C462; key wrapping; key establishment methodology provides between 128 and 256 bits of encryption strength)

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

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

- Diffie-Hellman – (key agreement; key establishment provides between 112 and 150-bits of encryption strength.) Diffie-Hellman with less than 112-bit of security strength is non-compliant and may not be used.

- EC Diffie-Hellman – (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength.) EC Diffie-Hellman with less than 128-bit of security strength is non-compliant and may not be used.

- RSA Key Wrapping – (key wrapping; key establishment methodology provides 112 or 128-bits of encryption strength.) RSA with less than 112-bit of security strength is non-compliant and may not be used.

- NDRNG to seed FIPS approved DRBG (256 bits)

7.3 Non-Approved Algorithms

The ASR 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 Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman
TLS (non-compliant)	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 1024-bit RSA, 1024-bit Diffie-Hellman
IPsec (non-compliant)	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES, RC4 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

Table 12: Non-Approved Algorithms

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:

- Route Processor (Integrated, RP2 and RP3)
    - Known Answer Tests:
        - AES KAT,
        - 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,
        - Triple-DES KAT,
        - DRBG KAT,
        - ECDSA KAT,
        - KAS ECC Primitive "Z" KAT
        - KAS FFC Primitive "Z" KAT
        - RSA KAT.
    - Firmware Integrity Test (RSA 2048 w/ SHA-256)
- Embedded Services Processor (Integrated, ESP40, ESP100, and ESP200)
    - Known Answer Tests:
        - AES KAT,
        - SHS KAT,
        - HMAC KAT,
        - Triple-DES KAT,

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:

- Route Processor (Integrated, RP2, and RP3)
    - Continuous Random Number Generator test for the FIPS-approved DRBG
    - Continuous Random Number Generator test 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 are production grade multi-chip standalone cryptographic modules that meet level 1 physical security requirements.

9 Secure Operation

The module meets all the 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.

Upon initial boot from the factory, the ASR 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, 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 one letter and at least one number) to users. Identification and authentication on the console/auxiliary 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 ASR1000 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 are allowed 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-3des
- 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 is not allowed 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.

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

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/asr1000/configuration/guide/chassis/asr1000-software-config-guide.html)

- For LED related information please read the following document (https://www.cisco.com/c/en/us/td/docs/routers/asr1000/install/guide/modular_linecard/asr1_mlc_hig/mlc_asr1_overview.html)

11 Definitions List

ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header
ASR	Aggregation 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	Encapsulating Security Payload
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
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
USB	Universal Serial Bus
VPN	Virtual Private Network