Juniper Networks ACX5448-M Router

Firmware: Junos OS 20.3R1

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Document Version: 1.4

Date: December 17, 2021

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Contents

List of Tables

List of Figures

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Juniper Networks ACX5448-M Universal Metro Router. The ACX5448-M series provides dedicated high-performance processing for flows and sessions and integrates advanced security capabilities that protect the network infrastructure as well as user data.

This FIPS 140-2 validation includes the ACX5448-M router. The FIPS validated version of firmware is Junos OS 20.3R1. The name of the image file is:

- junos-vmhost-install-acx-x86-64-20.3R1.8.tgz

The cryptographic boundary for the ACX5448-M is defined as the outer edge of the router. The cryptographic module provides for an encrypted connection, using SSH, between the management station and the module. The cryptographic modules also provide for an encrypted connection, using MACsec, between devices. All other data input to or output from the modules are considered plaintext for this FIPS 140-2 validation.

The cryptographic modules are defined as a multiple-chip standalone module that executes Junos OS 20.3R1 firmware on the Juniper Networks ACX5448-M Universal Metro Router as listed in Table 1 below.

Table 1 – Cryptographic Module Hardware Configurations

Model	Hardware Versions	Chassis differences	Network Ports
ACX5448-M	ACX5448-M-AC-AFO ACX5448-M-DC-AFO ACX5448-M-AC-AFI ACX5448-M-DC-AFI	AC Unit Air flow out DC Unit Air flow out AC Unit Air flow in DC Unit Air flow in	44 SFP+/SFP ports (MACsec) + 6 QSFP28 ports

The module is designed to meet FIPS 140-2 Level 1 overall:

Table 2 – Security Level of Security Requirements

Area	Description	Level
1	Module Specification	1
2	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	Key Management	1
8	EMI/EMC	1
9	Self-test	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
	Overall	1

The module has a non-modifiable operational environment as per the FIPS 140-2 definitions. It includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into the modules are out of the scope of this validation and require a separate FIPS 140-2 validation.

The module does not implement any mitigations of other attacks as defined by FIPS 140-2.

Juniper's development processes are such that future releases of Junos should be FIPS validate-able when run on the same hardware platform and meet the claims made in this document. Only the versions that explicitly appear on the certificate, however, are formally validated. The CMVP makes no claim as to the correct operation of the module or the security strengths of the generated keys when operating under a version that is not listed on the validation certificate.

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the module is depicted in Figure 1 below. The cryptographic boundary is defined as the outer edge of the chassis. The module does not rely on external devices for input and output of critical security parameters (CSPs).

Figure 1 – Physical Cryptographic Boundary ACX5448-M

Table 3 – Ports and Interfaces

Port	Device (# of ports)	Description	Logical Interface Type
Ethernet	Management port (1), 44 SFP+/SFP ports (MACsec) + 6 QSFP28 ports	LAN Communications/Remote management	Control in, Data in, Data out, Status out
Serial	1	Console serial port	Control in, Data in, Data out Status out
USB	1	USB port - load Junos image	Control in, Data in
Power	1	Power connector	Power
LEDs	6	Status indicator lighting	Status out
Reset Button	1	Reset	Control in
Clocking ports (1PPS and 10 MHz GPS)	2	connect the module to external clock signal sources	Control in

1.2 Modes of Operation

The module supports a FIPS Approved mode of operation and a non-Approved mode of operation. The module must always be zeroized when switching between FIPS Approved mode of operation and the non-Approved mode of operation and vice versa.

1.2.1 FIPS Approved Mode

The module with Junos OS 20.3R1 installed, contains a FIPS-Approved mode of operation and a non-Approved mode of operation. The Crypto-Officer places the module in an Approved mode of operation by following the instructions in Crypto-Officer guidance (section 6.1).

The Crypto-Officer can verify that the cryptographic module is in an Approved mode by observing the console prompt and running the "show version" command. When operating in FIPS mode, the prompt will read "<user>@<device name>:fips>" (e.g. crypto-officer@ACX5448-M:fips>). The "show version" command will allow the Crypto-Officer to verify that the validated firmware version is running on the module. The Crypto-Officer can also use the "show system fips chassis level" command to determine if the module is operating in FIPS mode.

The Approved mode supports the approved and allowed algorithms, functions and protocols identified in Table 4 – 11. The services available in this mode are described in Tables 14 and 16.

1.2.2 Non-Approved Mode

The cryptographic module supports a non-Approved mode of operation. When operated in the non-Approved mode of operation, the module supports the algorithms identified in Section 2.2 as well as the algorithms supported in the Approved mode of operation.

The Crypto-Officer can place the module into a non-approved mode of operation by following the instructions in the Crypto-Officer guidance (section 6.1).

1.3 Zeroization

The cryptographic module provides a non-Approved mode of operation in which non-Approved cryptographic algorithms are supported. When transitioning between the non-Approved mode of operation and the FIPS-Approved mode of operation, or vice-versa, the Crypto-Officer shall zeroize all keys and CSPs.

Zeroization completely erases all configuration information on the device, including all cryptographic keys and CSPs and returning the module to its factory default state. The Crypto-Officer initiates the zeroization process by entering the "*request vmhost zeroize no-forwarding"* operational command from the CLI after enabling FIPS mode. Use of this command is restricted to the Crypto-Officer.

The Crypto-Officer shall perform zeroization in the following situations:

1. Before FIPS Operation: To prepare the device for operation as a FIPS cryptographic module by erasing all CSPs and other user-created data on a device before its operation as a FIPS cryptographic module.
2. Before non-FIPS Operation: To conduct erasure of all CSPs and other user-created data on a device in preparation for repurposing the device for non-FIPS operation.

CAUTION: Perform system zeroization with care. After the zeroization process is complete, no data is left on the Routing Engine. The device is returned to the factory default state, equivalent to a fresh installation of the firmware, without any configured users or configuration files.

To zeroize the device:

1. From the CLI, enter

   Crypto-officer@device> **request vmhost zeroize no-forwarding**
   warning: System will be rebooted and may not boot without configuration
   Erase all data, including configuration and log files? [yes, no] (no)

2. To initiate the zeroization process, type yes at the prompt:

   Erase all data, including configuration and log files? [yes, no] (no)
yes

3. When the system finishes rebooting the system will be in a factory default state.

Note: The Crypto-Officer must retain control of the module while zeroization is in process.

2 Cryptographic Functionality

The module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in Tables 4, 5, 6, 7, 8, 9 and 10 below. Table 11 summarizes the high-level protocol algorithm support. There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this/these table(s).

2.1 Approved Algorithms

Table 4 – Kernel Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
A869	DRBG	SP800-90A	HMAC	SHA-256	Random Bit Generation
A869	HMAC	FIPS 198	SHA-1	Key size: 160 bits, λ = 96	Message Authentication, DRBG Primitive
			SHA-256	Key size: 256 bits, λ = 128, 256	
A869	SHS	FIPS 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation

Table 5 – LibMD Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
A873	HMAC	FIPS 198	SHA-1	Key size: 160 bits, λ = 96	Message Authentication
			SHA-256	Key size: 256 bits, λ = 128, 256	
A873	SHS	FIPS 180-4	SHA-1 SHA-256 SHA-512		Message Digest Generation

Table 6 – OpenSSL Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
A871	AES	FIPS 197 SP800-38A	CBC, CTR, ECB	Key Sizes: 128, 192, 256	Encrypt, Decrypt
N/A[1]	CKG	SP 800 133	Section 6.1		Asymmetric key generation using unmodified DRBG output

[1] Vendor Affirmed

N/A[2]	KAS-SSC	SP 800-56Arev3	ECC DH	P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	Key Agreement Scheme
A871	CVL	SP 800-135	SSH	SHA 1, 256, 384, 512	Key Derivation
A871	DRBG	SP 800-90A	HMAC	SHA-256	Random Number Generation
A871	ECDSA	FIPS 186-4	B.4.2 Testing Candidates	P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	SigGen, KeyGen, SigVer, PKV
A871	HMAC	FIPS 198	SHA-1	Key size: 160 bits, λ = 160	Message Authentication
			SHA-224	Key size: 224 bits, λ = 192	
			SHA-512	Key size: 512 bits, λ = 512	
			SHA-256	Key size: 256, bits, λ = 256	Message Authentication, DRBG Primitive
N/A	KTS		AES CBC Cert. # A871 and HMAC Cert. # A871		key establishment methodology provides between 128 and 256 bits of encryption strength
			Triple-DES CBC Cert. # A871 and HMAC Cert. # A871		key establishment methodology provides 112 bits of encryption strength
A871	RSA	FIPS 186-4		n=2048 (SHA 256, 512) n=3072 (SHA 256, 512) n=4096 (SHA 256, 512)	KeyGen, SigGen, SigVer
A871	SHS	FIPS 180-4	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation, KDF Primitive
			SHA-224		Message Digest Generation
A871	Triple-DES	SP 800-67	TCBC	Key Size: 192	Encrypt, Decrypt

[2] Vendor Affirmed as per IG D.1-rev3

Table 7 – QuickSec Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
A872	HMAC	FIPS 198	SHA-1 SHA-256 SHA-384	Key size: 256, bits, λ = 256	
A872	SHS	SP800- 180-4	SHA1 SHA-256 SHA-384		Message Digest Generation, KDF Primitive
A872	DRBG	SP800-90A	HMAC	SHA-256	Random Bit Generation

Table 8 – MACsec Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
A870	AES	SP800- 197-38A	ECB, CBC	Key Sizes: 128, 256	AES CMAC
		SP800-38D	CMAC	Key Sizes: 128,256	Key Derivation SP 800-108: Used to generate MACsec keys
		SP800-38F	KW	Key Size: 128	Key Wrapping for MACsec keys
A870	KBKDF	SP 800-108	Counter	CMAC AES128 CMAC AES256	KDF for MACsec keys
N/A	KTS		AES KW # A870		Key Wrapping (key establishment methodology provides 128 bits of encryption strength)

Table 9 – Microsemi VSC8258 Chip

CAVP Cert.	Algorithm	Standard	Mode	Description	Functions
AES 3969	AES	SP800-38D, 802.11AE	GCM, XPN	Key Sizes: 128, 256	Encrypt, Decrypt

2.2 Allowed Algorithms

Table 10 – Allowed Cryptographic Functions

Algorithm	Caveat	Use
NDRNG IG 7.14 Scenario 1a	The module generates a minimum of 256 bits of entropy for key generation.	Seeding the DRBG

2.3 Protocols

Table 11 – Protocols using approved algorithms in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
MACsec MKA	MACsec Key Agreement	Shared secret	AES GCM 128/256 AES XPN 128/256	HMAC-SHA-256
SSHv2[3]	EC Diffie-Hellman P-256, P-384, P-521	ECDSA P-256 ECDSA P-384 ECDSA P-521 RSA 2048 RSA 3072 RSA 4096	Triple-DES CBC AES CBC 128/192/256 AES CTR 128/192/256	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-512

No part of these protocols, other than the KDF, have been tested by the CAVP and CMVP. The MACsec and SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In Table 11 above, each column of options for a given protocol is independent and may be used in any viable combination.

The modules can take on the role of Peer or Authenticator in reference to the MACsec protocol. The AES GCM IV construction is performed in compliance with IEEE 802.1AE and its amendments.

2.4 Disallowed Algorithms

These algorithms and protocols are non-Approved algorithms that are disabled when the module is operated in an Approved mode of operation. The algorithms are available as part of the SSH connect service when the module is operated in the non-Approved mode.

Algorithms

- RSA with key size less than 2048
- ECDSA with ed25519 curve
- ECDH with ed25519 curve
- ARCFOUR
- Blowfish
- CAST
- DSA (SigGen, SigVer; non-compliant)
- HMAC-MD5
- HMAC-RIPEMD160
- UMAC
- Diffie-Hellman
- Chacha20
- Poly
- OpenSSL AES-GCM

[3] RFC 4253 governs the generation of the Triple-DES encryption key for use with the SSHv2 protocol

2.5 Critical Security Parameters

All CSPs and public keys used by the module are described in this section.

Table 12 – Critical Security Parameters (CSPs)

Name	Description and usage
DRBG_Seed	Seed material used to seed or reseed the HMAC DRBG
DRBG_State	Values V and Key which comprise the HMAC_DRBG state
Entropy Input	256 bits entropy (min) input used to instantiate the HMAC DRBG
ECDH Shared Secret	The Diffie-Hellman shared secret used in EC Diffie-Hellman (ECDH) exchange. Created per the EC Diffie-Hellman protocol. Provides between 128-256 bits of security.
SSH PHK	SSH Private host key. 1st time SSH is configured, the keys are generated. ECDSA P-256. RSA 2048
SSH ECDH	Ephemeral EC Diffie-Hellman private key used in SSH. ECDH P-256, P-384, or P-521
SSH-SEKs	SSH Session Keys: SSH Session Encryption Key: 3-Key Triple-DES or AES (128,192,256); SSH Session Integrity Key: HMAC (SHA-1, SHA-256, SHA2-512).
MACsec CAK	Externally generated pre-shared key entered when MACsec static connectivity association key (CAK) security mode is enabled (32 characters for 128-bit AES keys or 64 characters for 256-bit AES keys). Entered by the CO when configuring the module via SSH or the serial interface[4].
MACsec CKN	Externally generated pre-shared key used to identify the CAK (64 characters). Entered by the CO when configuring the module via SSH or the serial interface[5].
MACsec SAK	Security Association Key used to encrypt/decrypt traffic for a given session. Derived from CAK using KDF SP 800-108. (128-bit AES).
MACsec KEK	Key Encryption Key used to transmit SAK to other members of a MACsec connectivity association. Derived from CAK using KDF SP 800-108. (128-bit AES).
MACsec ICK	Integrity Check Key used to verify the integrity and authenticity of MPDUs. Derived from CAK using KDF SP 800-108. (128/256-bit CMAC).
HMAC Key	The LibMD HMAC keys: message digest for hashing password and critical function test.
User Password	Passwords used to authenticate Users to the module.
CO Password	Passwords used to authenticate COs to the module.

[4] When entered via the serial interface, the CO must use a non-network GPC.
[5] When entered via the serial interface, the CO must use a non-network GPC.

Table 13 – Public Keys

Name	Description and usage
SSH-PUB	SSH Public Host Key used to identify the host. ECDSA P-256. RSA 2048, 4096.
SSH-ECDH-PUB	Ephemeral EC Diffie-Hellman public key used in SSH key establishment. ECDH P-256, P-384, or P-521
Auth-User Pub	User Authentication Public Keys. Used to authenticate users to the module. ECDSA P-256, P-384, or P-521; RSA 2048, 4096
Auth-CO Pub	CO Authentication Public Keys. Used to authenticate CO to the module. ECDSA P-256, P-384, or P-521; RSA 2048, 4096
Root CA	ECDSA P-256 X.509 Certificate; Used to verify the validity of the Juniper Package CA at software load and also at runtime for integrity.
Package CA	ECDSA P-256 X.509 Certificate; Used to verify the validity the Juniper Image at software load and also at runtime for integrity.

3 Roles, Authentication and Services

3.1 Roles and Authentication of Operators to Roles

The module supports two roles: Crypto-Officer (CO) and User. The module supports concurrent operators but does not support a maintenance role and/or bypass capability. The module enforces the separation of roles using identity-based operator authentication.

The Crypto-Officer role configures and monitors the module via a console or SSH connection. As root or super-user, the Crypto-Officer has permission to view and edit secrets within the module.

The User role monitors the router via the console or SSH. The User role cannot change the configuration.

3.2 Authentication Methods

The module implements two forms of Identity-Based authentication, Username and password over the Console and SSH as well as Username and ECDSA or RSA public key over SSH.

Password authentication: The module enforces 10-character passwords (at minimum) chosen from the 96 human readable ASCII characters. The maximum password length is 20-characters. Thus, the probability of a successful random attempt is $1/96^{10}$, which is less than 1/1 million.

The module enforces a timed access mechanism as follows: For the first two failed attempts (assuming 0 time to process), no timed access is enforced. Upon the third attempt, the module enforces a 5-second delay. Each failed attempt thereafter results in an additional 5-second delay above the previous (e.g. 4th failed attempt = 10-second delay, 5th failed attempt = 15-second delay, 6th failed attempt = 20-second delay, 7th failed attempt = 25-second delay).

This leads to a maximum of 7 possible attempts in a one-minute period for each getty. The best approach for the attacker would be to disconnect after 4 failed attempts and wait for a new getty to be spawned. This would allow the attacker to perform roughly 9.6 attempts per minute (576 attempts per hour/60 mins); this would be rounded down to 9 per minute, because there is no such thing as 0.6 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is $9/(96^{10})$, which is less than 1/100,000.

ECDSA signature verification: SSH public-key authentication. The module supports ECDSA (P-256, P-384, and P-521), which has a minimum equivalent computational resistance to attack of either 2^{128}, 2^{192} or 2^{256} depending on the curve. Thus, the probability of a successful random attempt is $1/ (2^{128})$, which is less than 1/1,000,000. Configurable SSH connection establishment rate limits the number of connection attempts, and thus failed authentication attempts in a one-minute period to a maximum of 15,000 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is $15,000/(2^{128})$, which is less than 1/100,000.

RSA signature verification: SSH public-key authentication. The module supports RSA (2048, 4096), which has a minimum equivalent computational resistance to attack of 2^{112} (2048). Thus, the probability of a successful random attempt is $1/ (2^{112})$, which is less than 1/1,000,000. Configurable SSH connection establishment rate limits the number of connection attempts, and thus failed authentication attempts in a one-minute period to a maximum of 15,000 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is 15,000/ (2^{112}), which is less than 1/100,000.

3.3 Approved Services

All services implemented by the module are listed in the tables below. Table 18 lists the access to CSPs by each service.

Table 14 – Authenticated Services

Service	Description	CO	User
Configure security	Security relevant configuration	x	
Configure	Non-security relevant configuration	x	
Secure Traffic	MACsec encrypted transfer of data	x	
Status	Show status	x	x
Zeroize	Destroy all CSPs	x	
SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	x	x
MACsec connect	Initiate MACsec connection	x	
Console access	Console monitoring and control (CLI)	x	x
Remote reset	Software initiated reset, performs self-tests on demand.	x	
Load Image	Verification and loading of a validated firmware image into the	x	

Table 15 – Unauthenticated Services

Service	Description
Local reset	Hardware reset or power cycle
Traffic	Traffic requiring no cryptographic services (e.g. OSPF, BGP)
LED Status	Basic

Table 16 – CSP Access Rights within Services

Service	CSPs														
	DRBG_Seed	DRBG_State	Entropy Input String	ECDH Shared Secret	SSH PHK	SSH ECDH	SSH-SEK	MACsec SAK	MACsec CAK	MACsec CKN	MACsec KEK	MACsec ICK	HMAC Key	CO-PW	User-PW
Configure security	--	E	--	GWR	G W R	--	--	GW R	W R	W R	G W	G W	G	W	W
Configure	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Secure traffic	--	--	--	--	--	--	--	E	--	--	E	--	--	--	--
Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
SSH connect	--	E	--	E	E	GE	GE	--	--	--	--	--	--	E	E
MACsec connect	--	E	--	--	--	--	--	GE	--	--	GE	GE	--	--	--
Console access	--	--	--	--	--	--	--	--	--	--	--	--	--	E	E
Remote reset	G EZ	GZ	GZ	Z	--	Z	Z	Z	--	--	--	Z	--	--	--
Load Image	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Local reset	G EZ	GZ	GZ	Z	--	Z	Z	Z	--	--	--	Z	--	--	--
Traffic	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

G = Generate: The module generates the CSP
R = Read: The CSP is read from the module (e.g. the CSP is output)
E = Execute: The module executes using the CSP
W = Write: The CSP is updated or written to the module (persistent storage) Z = Zeroize: The module zeroizes the CSP.

3.4 Non-Approved Services

The following services are available in the non-Approved mode of operation. The security functions provided by the non-Approved services are identical to the Approved counterparts with the exception of SSH Connect (non-compliant). SSH Connect (non-compliant) supports the security functions identified in Section 2.2 and the SSHv2 row of Table 11.

Table 17 – Non-Approved Authenticated Services

Service	Description	CO	User
Configure security (non-compliant)	Security relevant configuration	x	
Configure (non-compliant)	Non-security relevant configuration	x	
Secure Traffic (non-compliant)	MACsec encrypted transfer of data	x	
Status (non-compliant)	Show status	x	x
Zeroize (non-compliant)	Destroy all CSPs	x	
SSH connect (non-compliant)	Initiate SSH connection for SSH monitoring and control (CLI)	x	x
MACsec connect (non-compliant)	Initiate MACsec connection	x	
Console access (non-compliant)	Console monitoring and control (CLI)	x	x
Remote reset (non-compliant)	Software initiated reset, performs self-tests on demand	x	
Load Image (non-compliant)	Verification and loading of a validated firmware image into the switch.	x	

Table 18 – Non-Approved Unauthenticated Services

Service	Description
Local reset	Hardware reset or power cycle
Traffic	Traffic requiring no cryptographic services (e.g. OSPF, BGP)
LED Status	Basic

4 Self-tests

Each time the module is powered up it tests that the cryptographic algorithms still operate correctly, and that sensitive data have not been damaged. Power-up self–tests are available on demand by power cycling the module (Remote reset service).

On power up or reset, the module performs the self-tests described below. All KATs must be completed successfully prior to any other use of cryptography by the module in the FIPS Mode of operation. If any one of the fails, the module enters the Error state.

- **Firmware Integrity check**: using ECDSA P-256 with SHA-256
- **Kernel KATs**
  - SP 800-90A HMAC DRBG KAT
    - Health-tests initialize, re-seed, and generate
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
  - SHA-384 KAT
  - SHA-512 KAT
- **OpenSSL KATs**
  - AES-CBC (128/192/256) Encrypt KAT
  - AES-CBC (128/192/256) Decrypt KAT
  - SP 800-90A HMAC DRBG KAT
    - Health-tests initialize, re-seed, and generate
  - ECDSA P-256 Sign/Verify PCT
  - ECDH P-256 KAT
    - Derivation of the expected shared secret.
  - HMAC-SHA-1 KAT
  - HMAC-SHA-224 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-512 KAT
  - KAS -ECC KAT
  - KDF-SSH KAT
  - RSA 2048 w/ SHA-256 Sign KAT
  - RSA 2048 w/ SHA-256 Verify KAT
  - Triple-DES-CBC Encrypt KAT
  - Triple-DES-CBC Decrypt KAT
- **LibMD KATs**
  - HMAC-SHA-1
  - HMAC-SHA-256
  - SHA-512
- **QuickSec KATs**
  - SP 800-90A HMAC DRBG KAT
    - Health-tests initialize, re-seed, and generate
  - HMAC-SHA-1 KAT
  - HMAC-SHA-256 KAT
- **MacSec KATs**

  - AES128-CMAC KAT
  - AES256-CMAC KAT
  - AES-ECB (128/256) Encrypt KAT
  - AES-ECB (128/256) Decrypt KAT
  - AES-KEYWRAP wrapping/unwrapping with AES GCM (128, 192, 256) KAT
  - SP 800-108 KBKDF KAT
- **VSC8258**
  - AES GCM Encrypt/Decrypt with AES 256 KAT

The module also performs the following conditional self-tests:

- Continuous RNG Test on the SP 800-90A HMAC-DRBGs in the OpenSSL and Quicksec libraries.
- Continuous RNG test on the NDRNG.
- SP 800-56A assurances as per SP 800-56Arev3 Sections 5.5.2,5.6.2, and/or 5.6.3, in accordance to IG 9.6.
- Pairwise consistency test when generating ECDSA, and RSA key pairs.
- Firmware Load Test (ECDSA signature verification).

5 Physical Security Policy

The modules physical embodiment is that of a multi-chip standalone device that meets Level 1 Physical Security requirements. The module is completely enclosed in a rectangular nickel or clear zinc coated, cold rolled steel, plated steel and brushed aluminum enclosure. There are no ventilation holes, gaps, slits, cracks, slots, or crevices that would allow for any sort of observation of any component contained within the cryptographic boundary.

6 Security Rules and Guidance

The module design corresponds to the security rules below. The term *shall* in this context specifically refers to a requirement for correct usage of the module in the Approved mode; all other statements indicate a security rule implemented by the module.

1. The module clears previous authentications on power cycle.
2. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
3. Power up self-tests do not require any operator action.
4. Data output is inhibited during key generation, self-tests, zeroization, and error states.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
7. The module does not support a maintenance interface or role.
8. The module does not support manual key entry.
9. The module does not output intermediate key values.
10. The module requires two independent internal actions to be performed prior to outputting plaintext CSPs.
11. The Crypto-Officer shall verify that the firmware image to be loaded on the module is a FIPS validated image. If any non-validated firmware image is loaded the module will no longer be a FIPS validated module.
12. The Crypto-Officer shall retain control of the module while zeroization is in process.
13. If the module loses power and then it is restored, then a new key shall be established for use with the AES GCM encryption/decryption processes.
14. The operator shall ensure that the number of 64-bit blocks encrypted by the same key does not exceed 2^20 with a single Triple-DES key when Triple-DES is the encryption algorithm for SSH.
15. Virtual Chassis is not supported in FIPS mode and shall not be configured on the modules.
16. RSA key generated shall only be 2048 bits or greater.
17. The module shall only be used with CMVP FIPS 140-2 validated modules when supporting the MACsec protocol for providing Peer, Authenticator functionality.
18. The link between the Peer and Authenticator, used in the MACsec communication, should be secure to prevent the possibility for an attacker to introduce foreign equipment into the local area network.
19. 3-key Triple-DES has been implemented in the module and is FIPS approved until December 31, 2023. Should the CMVP disallow the usage of Triple-DES post December 31, 2023, then users must not configure Triple-DES.

6.1 Cryptographic-Officer Guidance

The Crypto-Officer must check to verify the firmware image on the device is the FIPS 140-2 validated image. If the image is the FIPS 140-2 validated image, then proceed to section 6.1.2.

6.1.1 Installing the FIPS-Approved firmware image

Download the validated firmware image from the https://www.juniper.net/support/downloads/junos.html. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives. Select the validated firmware image. Download the firmware image to a local host or to an internal software distribution site.

Connect to the console port on the device from your management device and log in to the Junos OS CLI. Copy the firmware package to the device to the /var/tmp/ directory. Install the downloaded firmware image on the device:

user@device> request vmhost software add /var/tmp/*package*.tgz.

NOTE: If you need to terminate the installation, do not reboot your device; instead, finish the installation and then issue the request system software delete *package*.tgz command, where *package*.tgz is, for example, junos-vmhost-install-mx-x86-64-20.3R1.8.tgz. This is your last chance to stop the installation.

Reboot the device to load the installation and start the new firmware image:

user@device> request vmhost reboot

After the reboot has completed, log in and use the show version command to verify that the new version of the firmware is successfully installed.

Also install the fips-mode package and jpfe-fips package needed for enabling FIPS mode and running KATS respectively. These packages are part of the downloaded firmware. The following are the commands used for installing these packages:

user@device >request system software add optional://fips-mode.tgz

user@device >request system software add optional://jpfe-fips.tgz

6.1.2 **Enabling FIPS-Approved Mode of Operation**

The Crypto-Officer is responsible for initializing the module in a FIPS-Approved mode of operation. The FIPS-Approved mode of operation is not automatically enabled. The Crypto-Officer shall place the module in the FIPS-Approved mode by first zeroizing the device to delete all keys and CSPs. The instructions for zeroizing the module are in section 1.3 of this document. Next, the Crypto-Officer shall follow the steps found in the *Junos OS FIPS Evaluated Configuration Guide for ACX5448-M Devices, Release 20.3R1* document Chapter 2 to place the module into a FIPS-Approved mode of operation. The steps from the aforementioned document are repeated below:

To enable FIPS mode in Junos OS on the device:

1. Zeroize the device as explained in Section 1.3.

2. Login to the device with crypto-officer credentials and enter configuration mode:
   crypto-officer@device> edit
   Entering configuration mode
   [edit]
   crypto-officer@device#

3. Enable FIPS mode on the device by setting the FIPS level to 1, and verify the level:

   [edit]
   crypto-officer@device # **set system fips chassis level 1**

   [edit]
   crypto-officer@device # **show system fips**
   chassis level 1;

4. Commit the configuration
   [edit]
   crypto-officer@device# **commit**
   configuration check succeeds
   Generating RSA key /etc/ssh/fips_ssh_host_key
   Generating RSA2 key /etc/ssh/fips_ssh_host_rsa_key
   Generating ECDSA key /etc/ssh/fips_ssh_host_ecdsa_key
   [edit]
   'system'
   reboot is required to transition to FIPS level 1
   commit complete

5. Reboot the device:
   [edit]
   crypto-officer@device# **run request vmhost reboot**
   Reboot the system ? [yes,no] (no) **yes**

   During the reboot, the device runs Known Answer Tests (KATS). It returns a login prompt:

   crypto-officer@device:fips>

6. After the reboot has completed, log in and use the "show version" command to verify the firmware version is the validated version.

   crypto-officer@device:fips> show version

6.1.3 Placing the Module in a Non-Approved Mode of Operation

As Crypto-Officer, the operator needs to disable the FIPS-Approved mode of operation on the device to return it to a non-Approved mode of operation. To disable FIPS-Approved mode on the device, the device must be zeroized. Follow the steps found in section 1.3 to zeroize the device.

6.1.4 Entering Keys and CSPs via the Serial Interface

The Crypto-Officer must use a non-networked GPC when entering keys or CSPs (such as MACsec CAK and CKN values).

6.2 User Guidance

The user should verify that the module is operating in the desired mode of operation (FIPS-Approved mode or non-Approved mode) by observing the command prompt when logged into the device. If the string ":fips" is present, then the device is operating in a FIPS-Approved mode. Otherwise it is operating in a non-Approved mode.

All FIPS users, including the Crypto Officer, must observe security guidelines at all times.

All FIPS users must:

- Keep all passwords confidential.
- Store devices and documentation in a secure area.
- Deploy devices in secure areas.
- Check audit files periodically.
- Conform to all other FIPS 140-2 security rules.
- Follow these guidelines:
  - Users are trusted.
  - Users abide by all security guidelines.
  - Users do not deliberately compromise security.
  - Users behave responsibly at all times.

7 References and Definitions

The following standards are referred to in this Security Policy.

Table 19 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*

Table 20 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CAK	Connectivity Association Key
CKN	Connectivity Association Key Name
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
ICV	Integrity Check Value (i.e. Tag)
ICK	Integrity Check Key
KEK	Key Encrypting Key
MACsec	Media Access Control Security
MD5	Message Digest 5
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
SCB	Switch Control Board
SHA	Secure Hash Algorithms
SSH	Secure Shell
Triple-DES	Triple - Data Encryption Standard

Table 21 – Datasheet

Model	Title	URL
ACX5448-M	ACX5448-M 5G UNIVERSAL ROUTING PLATFORM	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000644-en.pdf