Juniper Networks

MX240, MX480, and MX960 3D Universal Edge Routers with the Multiservices MPC and Junos 14.2X4-D10.7

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Version: 0.8

Date: July 27, 2016

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

Table of Contents

List of Tables

List of Figures

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Juniper Networks MX Series 3D Universal Edge Routers with the Multiservices MPC (the "MX Series"). The MX 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.

The MX Series includes three models: the MX960, MX480, and MX240, each loaded with the MS-MPC, which provides hardware acceleration for an array of packet processing-intensive services such as Session Border Control functions, stateful firewall, NAT, flow monitoring, and anomaly detection. This integration allows customers to eliminate external firewalls that consume router ports and additional management resources. The FIPS validated version of firmware is JUNOS 14.2X4-D10.7 with the following packages:

- Junos OS package – jinstall64-14.2X4-D10.7-domestic-signed.tgz
- FIPS Mode package – fips-mode-i386-14.2X4-D10.7-signed.tgz
- JPFE FIPS Package – jpfe-fips-i386-14.2X4-D10.7-signed.tgz.

The cryptographic module is defined as a multiple-chip standalone module that executes JUNOS-FIPS firmware on any of the MX Series routers listed below. The cryptographic boundary for the MX Series is defined as follows for the validation:

- the outer edge of the chassis includes the Routing Engine (RE), the MS-MPC, Switch Control Board (SCB), slot cover in the following configurations:
  - For MX240 (2 available RE slots, 2 additional slots): 1 SCB, 1 Routing Engine, at least 1 and up to 2 MS-MPCs. All empty module bays must have a slot cover installed for proper cooling air circulation.
  - MX480 (2 available RE slots, 6 additional slots): 1 SCB, 1 RE, at least 1 and up to 4 MS-MPCs. All empty module bays must have a slot cover installed for proper cooling air circulation.
  - For MX960 (2 available RE slots, 12 additional slots): 1 SCB, 1 RE, at least 1 and up to 4 MS-MPCs. All empty module bays must have a slot cover installed for proper cooling air circulation.
- includes the inverse three-dimensional space where non-crypto-relevant line cards fit, with the backplane port serving as the physical interface
- excluding the power distribution module on the rear of the device

The cryptographic module is defined as a multiple-chip standalone module that executes JUNOS-FIPS firmware on any of the Juniper Networks MX 3D Universal Edge Routers listed in the table below.

Table 1 – Cryptographic Module Hardware Configurations

Chassis PN	Power PN	SCB PN	RE PN	MS PN
MX240	PWR-MX480-2400-DC-S PWR-MX480-2520-AC-S	SCBE2-MX SCBE-MX SCB-MX	RE-S-1800X4-XXG Note: XX = 8, 16 or 32 GB memory	MS-MPC-128

MX480	PWR-MX480-2400-DC-S PWR-MX480-2520-AC-S	SCBE2-MX SCBE-MX SCB-MX	RE-S-1800X4-XXG Note: XX = 8, 16 or 32 GB memory	MS-MPC-128
MX960	PWR-MX960-4100-DC-S PWR-MX960-DC-S PWR-MX960-4100-AC-S PWR-MX960-AC-S	SCBE2-MX SCBE-MX SCB-MX	RE-S-1800X4-XXG Note: XX = 8, 16 or 32 GB memory	MS-MPC-128
Tamper Label				
JNPR-FIPS-TAMPER-LBLS 520-052564				

The module is designed to meet FIPS 140-2 Level 2 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 limited 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 this module is 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.

1.1 Hardware and Physical Cryptographic Boundary

The cryptographic modules' operational environment is a limited operational environment.

The image below depicts the physical boundary of the modules, including the Routing Engine, MS-MPC, and SCB.

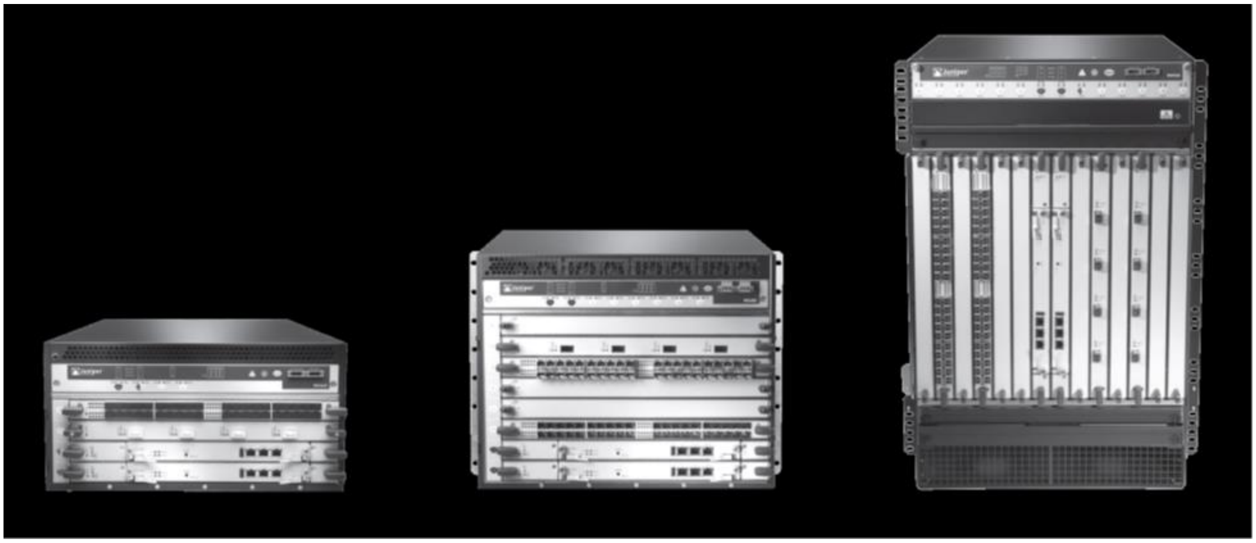

Figure 1 – Physical Cryptographic Boundary (Left: MX240, Center: MX480, Right MX960)

Table 3 - Ports and Interfaces

Port	Description	Logical Interface Type
Ethernet (data)	LAN Communications	Control in, Data in, Data out
Ethernet (mgmt.)	Remote Management	Control in, Data in, Data out, Status out
Serial	Console serial port	Control in, Status out
Power	Power connector	Power
Reset Button	Reset	Control in
LED	Status indicator lighting	Status out
USB	Disabled	N/A
Chassis Cluster Control	Disabled	N/A

1.2 Modes of Operation

The Crypto-Officer places the module in an Approved mode of operation by following the instructions in *Junos® OS for MX240, MX480, and MX960 3D Universal Edge Routers with Mutiservices MPC, Release 14.2X4-D10*. The steps are as follows:

1. ınstall the Junos 14.2X4-D10.7 firmware image
2. Install the FIPS mode package

3. Install the JUNOS Packet Forwarding Engine (JPFE) FIPS package
4. Run ‘set system fips level 1’

No further configuration is necessary for the purpose of placing it in and Approved mode.

The Crypto-Officer should also ensure that the backup image of the firmware is also Junos 14.2X4-D10.7 by issuing the ‘request system snapshot’ command.

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@mx240:fips#) and the output of the “show version” command will include “JUNOS Packet Forwarding Engine Support (fips) [14.2X4-D10.7]”.

The module supports three Approved modes of operation. The three modes are identified as Standard, Reduced Throughput, and Recovery.

In the Standard and Reduced Throughput Approved modes, the module supports the Approved and allowed algorithms and protocols identified in Table 4, Table 5, and Table 6. The services available in these modes are described in Table 9 and Table 11.

The Reduced Throughput mode is automatically selected by the module at power-up when the RE self-tests pass, at least one MS-MIC (each MS-MPC contains 4 MS-MICs) card passes its self-tests, and at least one MS-MIC card fails its self-tests. In this mode, the module offers reduced throughput VPN services.

In the Recovery Approved mode, the module supports the OpenSSL, SSH, and LibMD algorithms in Table 4; the algorithms in Table 5, and the SSH protocol in Table 6. The Recovery mode is automatically selected by the module at power-up if all of the MS cards fail their power-up self-tests but the RE self-tests pass. In this mode, the module does not offer VPN services. The services available in the Recovery mode are described in Table 10 and Table 11.

1.2.1 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 2.1 as well as the algorithms supported in the Approved mode of operation.

2 Cryptographic Functionality

The module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below. Table 6 summarizes the high level protocol algorithm support. The module does not implement algorithms that require vendor affirmation.

Table 4 - Approved and CAVP Validated Cryptographic Functions

Implementation	Algorithm	Mode	Key Size/Function	Strength	Cert
IKE	Triple-DES	CBC	168-bit (3 key) Encrypt/Decrypt	112	2168
	AES	CBC	128-bit Encrypt/Decrypt	128	3957
			192-bit Encrypt/Decrypt	192	
			256-bit Encrypt/Decrypt	256	
	SHA-1			80	3264
	SHA-256			128	
	SHA-384			192	
	HMAC-SHA-1		160-bit	128	2578
	HMAC-SHA-256		256-bit	256	
	HMAC-SHA-384		384-bit	256	
	IKE v1/v2 KDF (CVL Certificate)			112-192	792
	ECDSA	P-256: KeyGen		128	870
		P-384: KeyGen		192	
	RSA	2048: SigGen with SHA-256, SigVer with SHA-256		112	2020
	DSA	2048: KeyGen		112	1079
	DRBG	DRBG	HMAC-SHA-256	256	1158
IPsec ESP	Triple-DES	CBC	168-bit (3 key) Encrypt/Decrypt	112	2166
	AES	CBC	128-bit Encrypt/Decrypt	128	3955
			192-bit Encrypt/Decrypt	192	
			256-bit Encrypt/Decrypt	256	
	SHA-256			128	3261
	HMAC-SHA-256		256-bit	128	2575
OpenSSL	Triple-DES	CBC	168-bit (3 key) Encrypt/Decrypt	112	2167
	AES	CBC CTR	128-bit Encrypt/Decrypt	128	3956
			192-bit Encrypt/Decrypt	192	
			256-bit Encrypt/Decrypt	256	
	SHA-1			80	3262
	SHA-256			128	
	SHA-384			192	
	SHA-512			256	
	HMAC-SHA-1		160-bit	128	2576
	HMAC-SHA-256		256-bit	256	

	HMAC-SHA-512	512-bit	256	
	RSA	2048: KeyGen	112	2019
	ECDSA	P-256: KeyGen, SigGen with SHA-256, SigVer with SHA-256	128	869
		P-384: KeyGen, SigVer with SHA-384	192	
		P-521: KeyGen, SigVer with SHA-512	256	
	DSA	2048: KeyGen	112	1078
	DRBG	HMAC-SHA-256	256	1157
SSH KDF	SSHv2 KDF (CVL Certificate)		128, 192, 256	791
LibMD	SHA-1		80	3263
	SHA-256		128	
	SHA-512		256	
	HMAC-SHA-1	Password length (used for password obfuscation)	N/A Used for password obfuscation	2577
	HMAC-SHA-256			

Table 5 - Non-Approved but Allowed Cryptographic Functions

Algorithm	Reference
Non-SP 800-56A Compliant Diffie-Hellman	[IG] D.8 Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength).
Non-SP 800-56A Compliant Elliptic Curve Diffie-Hellman	[IG] D.8 EC Diffie-Hellman (key agreement; key establishment methodology provides 128, 192, or 256 bits of encryption strength).
NDRNG	[IG] 7.11 Hardware Non-Deterministic RNG used to seed the FIPS Approved DRBG.
HMAC-SHA-1-96 (HMAC Cert. #2578)	[IG] A.8 Hash Message Authentication Code truncated to 96-bits. Allowed for use in FIPS mode.

Table 6 - Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
IKEv1/v2	Group 14 (modp 2048) Group 19 (P-256) Group 20 (P-384)	RSA 2048 Pre-Shared Key	3 Key Triple-DES CBC AES CBC 128 AES CBC 192 AES CBC 256	HMAC-SHA-1-96 HMAC-SHA-256-128 HMAC-SHA-384-192

IPsec ESP	IKEv1/v2 with optional: • Group 14 (modp 2048) • Group 19 (P-256) • Group 20 (P-384)	IKEv1/v2	3 Key Triple-DES CBC AES CBC 128 AES CBC 192 AES CBC 256	HMAC-SHA-256-128
SSHv2	ECDH-sha2-nistp256 ECDH-sha2-nistp384 ECDH-sha2-nistp521	Host (module): ECDSA P-256 Client (user): ECDSA P-256 ECDSA P-384 ECDSA P-521	3 Key Triple-DES CBC AES CTR 128 AES CTR 192 AES CTR 256 AES CBC 128 AES CBC 192 AES CBC 256	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512

The IKE and SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In Table 6 above, each column of options for a given protocol is independent, and may be used in any viable combination.

These protocols have not been reviewed or tested by the CAVP and CMVP.

2.1 Disallowed Algorithms

These algorithms 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.

- ssh-dss
- ssh-rsa
- dh-group1-sha1
- hmac-md5
- hmac-ripemd160
- umac-128
- umac-64
- arcfour
- blowfish
- cast128

2.2 Critical Security Parameters

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

Table 7 - Critical Security Parameters (CSPs)

Name	Description and usage
DRBG_Seed	Seed material used to seed or reseed the DRBG
DRBG_State	Values V and Key which comprise the HMAC_DRBG state
SSH PHK	SSH Private host key. 1st time SSH is configured, the keys are generated. ECDSA P-256. Used to identify the host.
SSH DH	Ephemeral EC Diffie-Hellman private key used in SSH. ECDH P-256, P-384, or P-521
SSH-SEK	SSH Session Key; Session keys used with SSH. 3-Key Triple-DES, AES-128, AES-192, or AES-256 with HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-512.
ESP-SEK	IPSec ESP Session Keys. 3-Key Triple-DES, AES-128, AES-192, or AES-256 with HMAC-SHA-

	256-128.
IKE-PSK	Pre-Shared Key used to authenticate IKE connections.
IKE-Priv	IKE Private Key. RSA 2048.
IKE-SKEYI	IKE SKEYI. IKE secret used to derive IKE and IPsec ESP session keys.
IKE-SEK	IKE Session Keys. 3-Key Triple-DES, AES-128, AES-192, or AES-256 with HMAC-SHA-1-96, HMAC-SHA-256-128, or HMAC-SHA-384-192.
IKE-DH-PRI	Ephemeral Diffie-Hellman or EC Diffie-Hellman private key used in IKE. DH 2048 modp, ECDH P-256, or ECDH P-384
User Password	Passwords used to authenticate Users to the module.
CO Password	Passwords used to authenticate COs to the module.

Table 8 - Public Keys

Name	Description and usage
SSH-PUB	SSH Public Host Key used to identify the host. ECDSA P-256.
SSH-DH-PUB	Ephemeral EC Diffie-Hellman public key used in SSH key establishment. ECDH P-256, P-384 , or P-521
IKE-PUB	IKE Public Key RSA 2048.
IKE-DH-PUB	Ephemeral Diffie-Hellman or EC Diffie-Hellman public key used in IKE key establishment. DH 2048 modp, ECDH P-256, or ECDH P-384
Auth-UPub	User Authentication Public Keys. Used to authenticate users to the module. ECDSA P-256, P-384, or P-521
Auth-COPub	CO Authentication Public Keys. Used to authenticate CO to the module. ECDSA P-256, P-384, or P-521
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: Cryptographic 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 either identity-based operator authentication.

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

The User role monitors the router via the console or SSH. The user role may not 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 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 and P-384). The probability of a success with multiple consecutive attempts in a one-minute period is $5.6e7/(2^{128})$.

3.3 Services

All services implemented by the module are listed in the tables below. Table 12 lists the access to CSPs by each service.

Table 9 - Standard and Reduced Throughput Mode Authenticated Services

Service	Description	CO	User
Configure security	Security relevant configuration	x	
Configure	Non-security relevant configuration	x	
Secure Traffic	IPsec protected routing	x	
Status	Show status	x	x

Zeroize	Destroy all CSPs	x	
SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	x	x
IPsec connect	Initiate IPsec connection (IKE)	x	
Console access	Console monitoring and control (CLI)	x	x
Remote reset	Software initiated reset	x	

Table 10 - Recovery Mode Authenticated Services

Service	Description	CO	User
Configure security	Security relevant configuration	x	
Configure	Non-security relevant configuration	x	
Status	Show status	x	x
Zeroize	Destroy all CSPs	x	
SSH connect	Initiate SSH connection for SSH monitoring and control (CLI)	x	x
Console access	Console monitoring and control (CLI)	x	x
Remote reset	Software initiated reset	x	

Table 11 - 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 12 - CSP Access Rights within Services

	CSPs												
Service	DRBG_Seed	DRBG_State	SSH PHK	SSH DH	SSH-SEK	ESP-SEK	IKE-PSK	IKE-Priv	IKE-SKEYI	IKE-SEK	IKE-DH-PRI	User Password	CO Password
Configure security	--	E	GW	--	--	--	RW	GW	--	--	--	RW	RW
Configure	--	--	--	--	--	--	--	--	--	--	--	--	--
Secure traffic	--	--	--	--	--	E	--	--	--	E	--	--	--
Status	--	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
SSH connect	--	E	E	GE	GE	--	--	--	--	--	--	E	E

IPsec connect	--	E	--	--	--	G	E	E	GE	G	GE	--	--
Console access	--	--	--	--	--	--	--	--	--	--	--	--	--
Remote reset	GEZ	GZ	--	Z	Z	Z	--	--	Z	Z	Z	--	--
Local reset	GEZ	GZ	--	Z	Z	Z	--	--	Z	Z	Z	--	--
Traffic	--	--	--	--	--	--	--	--	--	--	--	--	--
LED Status	--	--	--	--	--	--	--	--	--	--	--	--	--

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.

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.

On power up or reset, the module performs the self-tests described below. All KATs for the selected Approved mode of operation must be completed successfully prior to any other use of cryptography by the module. If one of the Routing Engine/Control Plane KATs fails, the module enters the Error state. If one or more of the IPsec ESP KATs fails, the module selects the Reduced Throughput or Recover Approved mode of operation.

The module performs the following power-up self-tests:

Routing Engine/Control Plane:

Library	Test	Console Output
All	Firmware Integrity check using ECDSA P-256 with SHA-256	Verified manifest signed by PackageProductionEc_2016
LibMD	HMAC-SHA-1 KAT	HMAC-SHA1 Known Answer Test
	HMAC-SHA-256 KAT	HMAC-SHA2-256 Known Answer Test
	SHA-512 KAT	SHA-2 Known Answer Test
OpenSSL	SP 800-90A HMAC DRBG KAT - Initialize, re-seed, and generate functions	NIST 800-90 HMAC DRBG Known Answer Test
	ECDSA P-256 with SHA-256 Sign/Verify Pair-wise Consistency Test	FIPS ECDSA Known Answer Test
	ECDH P-256 Compute Shared Secret KAT	FIPS ECDH Known Answer Test
	RSA 2048 with SHA-256 Sign and Verify KAT	FIPS RSA Known Answer Test
	3 Key Triple-DES Enc/Dec KAT	Start to test DES3 CBC ENC ... Start to test DES3 CBC DEC ... DES3-CBC Known Answer Test
	HMAC-SHA-1 KAT	HMAC-SHA1 Known Answer Test
	HMAC-SHA-256 KAT	HMAC-SHA2-256 Known Answer Test
	HMAC-SHA-384 KAT	HMAC-SHA2-384 Known Answer Test
	HMAC-SHA-512 KAT	HMAC-SHA2-512 Known Answer Test
	AES CBC 128, 192, 256 Enc/Dec KAT	Start to test AES CBC ENC, KeySize = 16 ... Start to test AES CBC DEC, KeySize = 16 ... Start to test AES CBC ENC, KeySize = 24 ... Start to test AES CBC DEC, KeySize = 24 ... Start to test AES CBC ENC, KeySize = 32 ... Start to test AES CBC DEC, KeySize = 32 ... AES-CBC Known Answer Test
OpenSSH (reported under	SSHv2 KDF KAT	KDF-SSH Known Answer Test

OpenSSL)		
IKE	SP 800-90A HMAC DRBG KAT - Initialize, re-seed, and generate functions	NIST 800-90 HMAC DRBG Known Answer Test
	3 Key Triple-DES Enc/Dec KAT	Start to test DES3 CBC ENC ... Start to test DES3 CBC DEC ... DES3-CBC Known Answer Test
	HMAC-SHA-1 KAT	HMAC-SHA1 Known Answer Test
	HMAC-SHA-256 KAT	HMAC-SHA2-256 Known Answer Test
	HMAC-SHA-384 KAT	HMAC-SHA2-384 Known Answer Test
	AES CBC 128, 192, 256 Enc/Dec KAT	Start to test AES CBC ENC, KeySize = 16 ... Start to test AES CBC DEC, KeySize = 16 ... Start to test AES CBC ENC, KeySize = 24 ... Start to test AES CBC DEC, KeySize = 24 ... Start to test AES CBC ENC, KeySize = 32 ... Start to test AES CBC DEC, KeySize = 32 ... AES-CBC Known Answer Test
	RSA 2048 with SHA-256 Sign and Verify KAT	FIPS RSA Known Answer Test
	IKEv1 KDF KAT	KDF-IKE-V1 Known Answer Test
	IKEv2 KDF KAT	KDF-IKE-V2 Known Answer Test
All	Verification of a limited operational environment Critical Function Test	Expect an exec Authentication error... exec: /opt/sbin/kats/cannot-exec.real: Authentication error

IPsec ESP:

Test	**Log Output**
3 Key Triple-DES Enc/Dec KAT	Start to test DES3 CBC ENC ... station 281, testing SAE engine no. 0 ... station 281, testing SAE engine no. 4 ... station 281, testing SAE engine no. 8 ... station 281, testing SAE engine no. 1 ... station 281, testing SAE engine no. 5 ... station 281, testing SAE engine no. 9 ... station 281, testing SAE engine no. 2 ... station 281, testing SAE engine no. 6 ... station 281, testing SAE engine no. 10 ... station 281, testing SAE engine no. 3 ... station 281, testing SAE engine no. 7 ... station 281, testing SAE engine no. 11 ... Start to test DES3 CBC DEC ... station 281, testing SAE engine no. 0 ... station 281, testing SAE engine no. 4 ... station 281, testing SAE engine no. 8 ... station 281, testing SAE engine no. 1 ... station 281, testing SAE engine no. 5 ...

	station 281, testing SAE engine no. 9 ... station 281, testing SAE engine no. 2 ... station 281, testing SAE engine no. 6 ... station 281, testing SAE engine no. 10 ... station 281, testing SAE engine no. 3 ... station 281, testing SAE engine no. 7 ... station 281, testing SAE engine no. 11 ... DES3-CBC Known Answer Test
HMAC-SHA-256 KAT	Start to test HMAC-SHA2-256 ... station 281, testing SAE engine no. 0 ... station 281, testing SAE engine no. 4 ... station 281, testing SAE engine no. 8 ... station 281, testing SAE engine no. 1 ... station 281, testing SAE engine no. 5 ... station 281, testing SAE engine no. 9 ... station 281, testing SAE engine no. 2 ... station 281, testing SAE engine no. 6 ... station 281, testing SAE engine no. 10 ... station 281, testing SAE engine no. 3 ... station 281, testing SAE engine no. 7 ... station 281, testing SAE engine no. 11 ... HMAC-SHA2-256 Known Answer Test
AES CBC 128, 192, 256 Enc/Dec KAT	Start to test AES CBC ENC, KeySize = 16 ... station 281, testing SAE engine no. 0 ... station 281, testing SAE engine no. 4 ... station 281, testing SAE engine no. 8 ... station 281, testing SAE engine no. 1 ... station 281, testing SAE engine no. 5 ... station 281, testing SAE engine no. 9 ... station 281, testing SAE engine no. 2 ... station 281, testing SAE engine no. 6 ... station 281, testing SAE engine no. 10 ... station 281, testing SAE engine no. 3 ... station 281, testing SAE engine no. 7 ... station 281, testing SAE engine no. 11 ... Start to test AES CBC DEC, KeySize = 16 ... station 281, testing SAE engine no. 0 ... station 281, testing SAE engine no. 4 ... station 281, testing SAE engine no. 8 ... station 281, testing SAE engine no. 1 ... station 281, testing SAE engine no. 5 ... station 281, testing SAE engine no. 9 ... station 281, testing SAE engine no. 2 ... station 281, testing SAE engine no. 6 ... station 281, testing SAE engine no. 10 ... station 281, testing SAE engine no. 3 ... station 281, testing SAE engine no. 7 ... station 281, testing SAE engine no. 11 ...

	Start to test AES CBC ENC, KeySize = 24 ... station 281, testing SAE engine no. 0 ... station 281, testing SAE engine no. 4 ... station 281, testing SAE engine no. 8 ... station 281, testing SAE engine no. 1 ... station 281, testing SAE engine no. 5 ... station 281, testing SAE engine no. 9 ... station 281, testing SAE engine no. 2 ... station 281, testing SAE engine no. 6 ... station 281, testing SAE engine no. 10 ... station 281, testing SAE engine no. 3 ... station 281, testing SAE engine no. 7 ... station 281, testing SAE engine no. 11 ... Start to test AES CBC DEC, KeySize = 24 ... station 281, testing SAE engine no. 0 ... station 281, testing SAE engine no. 4 ... station 281, testing SAE engine no. 8 ... station 281, testing SAE engine no. 1 ... station 281, testing SAE engine no. 5 ... station 281, testing SAE engine no. 9 ... station 281, testing SAE engine no. 2 ... station 281, testing SAE engine no. 6 ... station 281, testing SAE engine no. 10 ... station 281, testing SAE engine no. 3 ... station 281, testing SAE engine no. 7 ... station 281, testing SAE engine no. 11 ... Start to test AES CBC ENC, KeySize = 32 ... station 281, testing SAE engine no. 0 ... station 281, testing SAE engine no. 4 ... station 281, testing SAE engine no. 8 ... station 281, testing SAE engine no. 1 ... station 281, testing SAE engine no. 5 ... station 281, testing SAE engine no. 9 ... station 281, testing SAE engine no. 2 ... station 281, testing SAE engine no. 6 ... station 281, testing SAE engine no. 10 ... station 281, testing SAE engine no. 3 ... station 281, testing SAE engine no. 7 ... station 281, testing SAE engine no. 11 ... Start to test AES CBC DEC, KeySize = 32 ... station 281, testing SAE engine no. 0 ... station 281, testing SAE engine no. 4 ... station 281, testing SAE engine no. 8 ... station 281, testing SAE engine no. 1 ... station 281, testing SAE engine no. 5 ... station 281, testing SAE engine no. 9 ... station 281, testing SAE engine no. 2 ... station 281, testing SAE engine no. 6 ...

	station 281, testing SAE engine no. 10 ... station 281, testing SAE engine no. 3 ... station 281, testing SAE engine no. 7 ... station 281, testing SAE engine no. 11 ... AES-CBC Known Answer Test

The module also performs the following conditional self-tests:

- Continuous RNG Test on the SP 800-90A HMAC-DRBGs
- Continuous RNG test on the NDRNG
- Pairwise consistency test when generating ECDSA and RSA key pairs.
- Pairwise consistency test when generating Diffie-Hellman (DSA) key pairs.
- Firmware Load Test (ECDSA P-256 with SHA-256 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. Tamper evident seals allow the operator to verify that only the approved ports are utilized. These seals are not factory-installed and must be applied by the Cryptographic Officer. (Seals are available for order from Juniper using part number JNPR-FIPS-TAMPER-LBLS.)

The Cryptographic Officer is responsible for securing and having control at all times of any unused seals and the direct control and observation of any changes to the module such as reconfigurations where the tamper evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

5.1 General Tamper Seal Placement and Application Instructions

A tamper seal must be placed over the USB port on the RE.

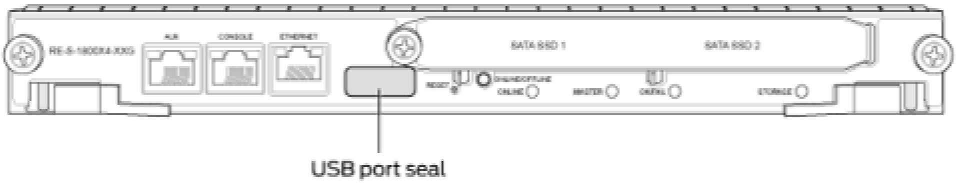

Figure 2 – Tamper Seal Location

The Cryptographic Officer should observe the following instructions:

- Handle the seals with care. Do not touch the adhesive side.
- Before applying a seal, ensure the location of application is clean, dry, and clear of any residue.
- Place the seal on the module, applying firm pressure across it to ensure adhesion. Allow at least 1 hour for the adhesive to cure.

6 Security Rules and Guidance

The module design corresponds to the security rules below. The term *must* 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 actions prior to outputting plaintext CSPs.

7 References and Definitions

The following standards are referred to in this Security Policy.

Table 13 – 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 14 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
ICV	Integrity Check Value (i.e. Tag)
IKE	Internet Key Exchange Protocol
IOC	Input/Output Card
IPsec	Internet Protocol Security
MD5	Message Digest 5
MIC	Modular Interface Card
MPC	Modular Port Concentrator
MS	Multiservices
NPC	Network Processing Card
RE	Routing Engine
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
SCB	Switch Control Board
SHA	Secure Hash Algorithms
SPC	Services Processing Card
SSH	Secure Shell
Triple-DES	Triple - Data Encryption Standard

Table 15 – Datasheets

Model	Title	URL
MX240 MX480 MX960	MX240, MX480, MX960 3D Universal Edge Routers	https://www.juniper.net/us/en/local/pdf/datasheets/1000208-en.pdf
MS-MPC	MX Series MS-MPC and MS-MIC Service Cards	http://www.juniper.net/documentation/en_US/junos15.1/topics/concept/ms-mic-and-mpc-overview.html