Juniper Express 4 MACsec Cryptographic Module

Software version: 1.0
Hardware version: JTAG ID 20611361

FIPS 140-3 Non-Proprietary Security Policy

Version 1.1

Last update: 2024-10-10

Prepared by:

atsec information security corporation

4516 Seton Center Parkway, Suite 250

Austin, TX 78759

www.atsec.com

Prepared for:

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089

www.juniper.net

Table of Contents

List of Tables

List of Figures

1 GENERAL

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Juniper Express 4 MACsec Cryptographic Module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for a Security Level 1 software-hybrid module.

This Security Policy has a one-to-one mapping to the [SP 800-140B] starting with section B.2.1 named "General" that maps to section 1 in this document and ending with section B.2.12 named "Mitigation of other attacks" that maps to section 12 in this document.

This Non-Proprietary Security Policy may be reproduced and distributed, but only whole and intact and including this notice. Other documentation is proprietary to their authors.

1.2 How this Security Policy was Prepared

In preparing the Security Policy document, the laboratory formatted the vendor-supplied documentation for consolidation without altering the technical statements therein contained. The further refining of the Security Policy document was conducted iteratively throughout the conformance testing, wherein the Security Policy was submitted to the vendor, who would then edit, modify, and add technical contents. The vendor would also supply additional documentation, which the laboratory formatted into the existing Security Policy, and resubmitted to the vendor for their final editing.

1.3 Security Levels

The following sections describe the cryptographic module and how it conforms to the FIPS 140-3 specification in each of the required areas.

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services and Authentication	1
5	Software/Firmware Security	1
6	Operational Environment	1
7	Physical Security	1
8	Non-invasive Security	N/A
9	Sensitive Security Parameter Management	1
10	Self-Tests	1
11	Life-cycle Assurance	1
12	Mitigation of Other Attacks	N/A
Overall Security Level		1

Table 1 - Security Levels

2 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 Module Embodiment

The Juniper Express 4 MACsec Cryptographic Module (hereafter referred to as "the module") is a software-hybrid module.

The module is composed by the MACsec blocks in hardware (contained in the Juniper Networks® Express 4 processor), which provides the AES GCM and XPN algorithm implementations for encrypting and decrypting MACsec traffic, and a device driver in software, which provides the functionality to comply with FIPS 140-3 requirements (i.e. integrity test, self-tests), as well as the API to configure the hardware component.

The module is also bound to the following cryptographic modules:

- Junos® OS Evolved Kernel Cryptographic Module Version 2.0 (validated under FIPS certificate #4776), which provides the integrity check utility that is invoked by the module to check the integrity of the module's software component.
- Junos® OS Evolved OpenSSL Cryptographic Module Version 3.0.8 (validated under FIPS certificate #4775) to provide the algorithm implementation for the integrity test.

For the purpose of the FIPS 140-3 validation, the module is a software-hybrid, multi-chip standalone cryptographic module validated at overall security level 1.

2.2 Module Design, Components, Versions

The diagram below shows the components that comprise the cryptographic module (in yellow), its cryptographic boundary (enclosed by dotted blue boxes) , and the interfaces with the operational environment.

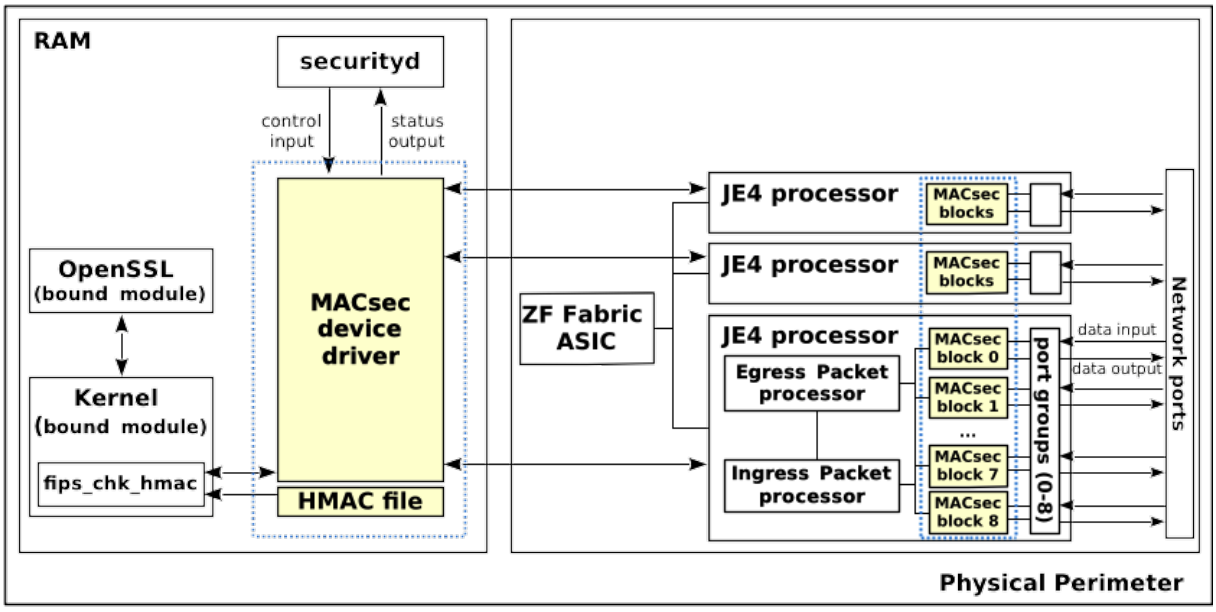

Figure 1 – Cryptographic Boundary

2.2.1 Module Components

Table 2 below enumerates the components that comprise the module with their versions and their location in the target platform.

Component Type	Version	Components	Description
Software	**1.0**	**/usr/lib64/libmacsecv2.so**	MACsec device driver shared library.
		/usr/lib64/.libmacsecv2.so.hmac	Integrity check HMAC value for the shared library.
Hardware	**JTAG ID 20611361**	**Juniper Express 4 MACsec blocks**	MACsec blocks are part of the Juniper Express 4 processor. Each MACsec block implements AES GCM and AES XPN encryption and decryption.

Table 2 – Cryptographic Module Components

2.3 Tested Operational Environments

The module has been tested on the following platforms with the corresponding module variants and configuration options:

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	Junos® OS Evolved 22.4	Juniper Networks® Packet Transport Router Model PTX10001-36MR	Intel® Xeon® D-2163IT	Not applicable

Table 3 – Tested Operational Environments

2.4 Modes of Operation

The module supports only the approved mode of operation. When the module starts up successfully, after passing all the pre-operational self-tests and conditional cryptographic algorithm self-tests (CASTs), the module is operating in the approved mode of operation.

The module does not implement a degraded mode of operation.

2.5 Security Functions

2.5.1 Approved Algorithms

Table 4 below lists all security functions of the module, including specific strengths employed for approved services.

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use
#A4089	AES [FIPS197], [SP800-38D]	GCM with external IV	128, 256-bit keys with key strength of 128 or 256 bits	Symmetric encryption Symmetric decryption

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use
#A4089	AES [FIPS197], [IEEE 802.1AE]	XPN with external IV and salt	128, 256-bit keys with key strength of 128 or 256 bits	Symmetric encryption Symmetric decryption

Table 4 – Approved Algorithms provided by the module

Table 5 below lists the approved algorithms provided by the bound OpenSSL module that are used by the module to perform integrity tests.

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use
#A4246, #A4247, #A4248, #A4249	HMAC [FIPS198-1], [SP800-38D]	SHA-256	256-bit key with key strength of 256 bits	Integrity test

Table 5 – Approved Algorithms provided by the bound OpenSSL module

2.5.2 Non-Approved Algorithms Allowed in the Approved Mode of Operation

The module does not implement non-approved algorithms allowed in the approved mode of operation.

2.5.3 Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

The module does not implement non-approved algorithms.

2.5.4 Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

The module does not implement non-approved algorithms.

3 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

Ports and interfaces implemented are shown in the following table. The Control Output interface is omitted because the module does not implement it.

Network ports and the power supply port correspond to the Juniper Express 4 processor where the MACsec blocks are contained.

All data output via data output interface is inhibited when the module is performing self-tests or zeroization, or when the module is in the error state.

Logical Interface	Physical Port	Data that passes over port/interface
Data Input	Network ports	Decrypted/encrypted data received from network ports, API input parameters for data input.
Data Output	Network ports	Encrypted/decrypted data sent to network ports.
Control Input	None	API function calls, API input parameters for control input.
Status Output	None	API return codes, API output parameters for status output.
Power Input	Power supply port	N/A

Table 6 – Ports and Interfaces

4 ROLES, SERVICES AND AUTHENTICATION

4.1 Roles

The module supports the Crypto Officer role only. This sole role is implicitly assumed by the operator of the module when performing a service. The module does not support concurrent operators.

Role	Service	Input	Output
Crypto Officer (CO)	Symmetric encryption for AES-128-GCM AES-256-GCM	Plaintext, AES key, Secure Channel Identifier (SCI), Packet Number (PN)	Ciphertext, Authentication Tag
	Symmetric decryption for AES-128-GCM AES-256-GCM	Ciphertext, AES key, Secure Channel Identifier (SCI), Packet Number (PN), Authentication Tag	Plaintext
	Symmetric encryption for AES-128-XPN AES-256-XPN	Plaintext, AES key, Short Secure Channel Identifier (SSCI), Packet Number (PN), salt	Ciphertext, Authentication Tag
	Symmetric decryption for AES-128-XPN AES-256-XPN	Ciphertext, AES key, Short Secure Channel Identifier (SSCI), Packet Number (PN), salt, Authentication Tag	Plaintext
	Show module name and version	None	Module name and version
	Show status	None	Return codes and/or log messages
	Self-tests	None	Pass/fail
	Zeroization	Port group ID	Pass/fail

Table 7 – Role, Service Commands, Input and Output

4.2 Authentication

The module does not implement authentication.

4.3 Services

The module only provides approved services, which are shown in Table 8.

4.3.1 Service Indicator

The module provides an approved service indicator as specified in the “Indicator” column in Table 8.

4.3.2 Approved Services

The table below shows the services available in the Approved mode. For each service, the table lists the associated cryptographic algorithm(s), the role to perform the service, the cryptographic keys or SSPs involved, and their access type(s). The following convention is used to specify access rights to an SSP:

- **G = Generate**: The module generates or derives the SSP.
- **R = Read**: The SSP is read from the module (e.g. the SSP is output).
- **W = Write**: The SSP is updated, imported, or written to the module.
- **E = Execute**: The module uses the SSP in performing a cryptographic operation.

- **Z = Zeroize**: The module zeroizes the SSP.
- **N/A**: the calling application does not access any SSP or key during its operation.

The details of the approved cryptographic algorithms including the CAVP certificate numbers can be found in Table 4.

The module provides API functions to access the registers of the MACsec blocks used to perform encryption (macsecv2_drv_rx_reg_port_config_rd) and decryption (macsecv2_drv_rx_reg_port_config_rd) services. The value 1 in the register position corresponding to the MACsec block determines the service indicator.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
			Cryptographic Module Services			
Symmetric encryption	Perform AES encryption	AES-GCM, AES-XPN	AES key	CO	W, E	macsecv2_drv_tx_reg_port_config_rd() returns 1 in bit corresponding to the MACsec block.
Symmetric decryption	Perform AES decryption	AES-GCM, AES-XPN	AES key	CO	W, E	macsecv2_drv_rx_reg_port_config_rd() returns 1 in bit corresponding to the MACsec block.
			Other services			
Show status	Return the module status	N/A	None	CO	N/A	None
Self-test	Perform the CASTs and the integrity test	AES-GCM, AES-XPN	None	CO	N/A	None
Zeroization	Zeroize all SSPs	N/A	All SSPs	CO	Z	None
Show module name and version	Return module name and version information	N/A	None	CO	N/A	None

Table 8 – Approved Services

4.3.3 Non-Approved Services

The module does not implement non-approved services.

5 SOFTWARE/FIRMWARE SECURITY

5.1 Integrity Techniques

The integrity of the module is ensured with the HMAC-SHA-256 value stored in the corresponding /usr/lib64/.libmacsecv2.so.hmac file that is computed at build time for the shared library. During Pre-Operational Self-Tests, the module invokes the fips_chk_hmac utility provided by the bound Kernel module (and whose cryptographic functionality is provided by the bound OpenSSL module) to calculate the HMAC value of the shared library, and then compares it with the prestored value. If the two HMAC values do not match, the test fails and the module enters the error state.

The integrity of the fips_chk_hmac utility itself is performed before the integrity tests of the module, and ensured with the HMAC-SHA2-256 value stored in the corresponding .hmac file that is computed at build time of the utility. The fips_chk_hmac utility calculates the HMAC value, and then compares it with the prestored value. If the two HMAC values do not match, the test fails and the module enters the error state.

5.2 On-demand Integrity Tests

Integrity tests are performed as part of the Pre-Operational Self-Tests, and can be invoked by powering-off and reloading the module which cause the module to run the power-up tests again.

5.3 Executable Code

The module consists of the device driver that controls the Juniper Express 4 MACsec blocks, in the form of a shared library as stated in Table 2.

6 OPERATIONAL ENVIRONMENT

6.1 Applicability

The module operates in a modifiable operational environment per FIPS 140-3 level 1 specifications. The module runs on a commercially available general-purpose operating system executing on the hardware specified in Table 3.

6.2 Policy and Requirements

The module shall be installed as stated in Section 11 . If properly installed, the operating system provides process isolation and memory protection mechanisms that ensure appropriate separation for memory access among the processes on the system. Each process has control over its own data and uncontrolled access to the data of other processes is prevented.

The module does not support concurrent operators .

The module does not have the capability of loading software or firmware from an external source.

Instrumentation tools like the ptrace system call, gdb and strace utilities, userspace live patching, as well as other tracing mechanisms offered by the Linux environment such as ftrace or systemtap, shall not be used in the operational environment. The use of any of these tools implies that the cryptographic module is running in a non-tested operational environment.

7 PHYSICAL SECURITY

The Juniper Express 4 processor (an ASIC silicon) is the hardware that contains the MACsec blocks that constitute the hardware component of the module. The embodiment of the chip is a single chip consisting of production-grade components. The coating is a standard sealing coat applied over the single chip. The module provides no additional physical security techniques.

Figure 2 - Juniper Express 4 processor

The module inherits the physical characteristics of the host running it. Figure 3 illustrates the Juniper Networks® Packet Transport Router Model PTX10001-36MR that represents the testing platform and includes the hardware component of the cryptographic module. The router includes three Juniper Express 4 ASIC chips to provide forwarding traffic and supporting MACsec for its 36 multi-rate ports.

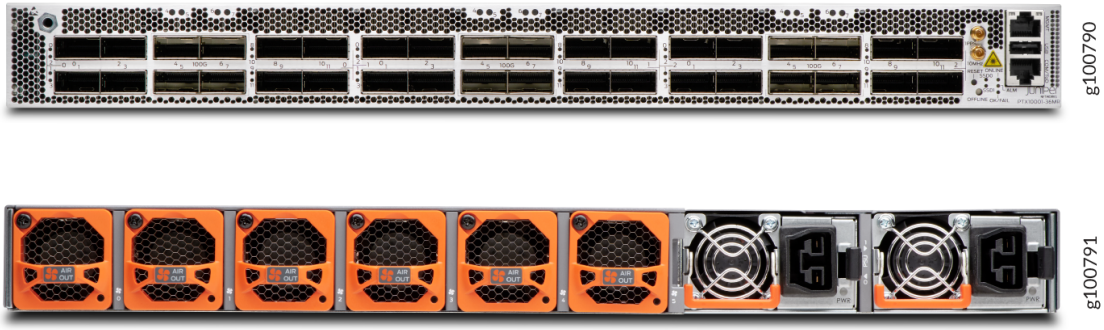

Figure 3 - Packet Transport Router Model PTX10001-36MR

8 NON-INVASIVE SECURITY

The module does not implement any non-invasive security mechanism, and therefore this section is not applicable.

9 SENSITIVE SECURITY PARAMETER MANAGEMENT

Table 9 summarizes the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module.

Key /SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import /export	Establishment	Storage	Zeroization	Use & Related Keys
AES key	128, 256 bits	AES-GCM, AES-XPN #A4089	N/A	**Import:** CM from TOEPP Path. Passed into the module via API parameters in plaintext (P) form. **Export:** N/A	N/A	MACsec block registers	macsecv2_drv_port_tx_sa_delete	**Use:** Symmetric encryption; Symmetric decryption; **Related SSPs:** N/A

Table 9 - SSPs

9.1 Random Number Generation

The module does not provide this security function.

9.2 SSP Generation

The module does not implement any SSP generation methods.

9.3 Key Agreement

The module does not support any approved key agreement methods.

9.4 Key Transport

The module does not support any key transport methods.

9.5 SSP Entry and Output

The module only supports SSP entry from the calling application running on the same operational environment. This corresponds to manual distribution, electronic entry/output (“CM Software to/from App via TOEPP Path”) per FIPS 140-3 IG 9.5.A Table 1. There is no entry of cryptographically protected SSPs.

The module does not output any SSPs.

9.6 SSP Storage

The module does not perform persistent storage of SSPs. The SSPs are temporarily stored in RAM for the device driver and registers for the Juniper Express 4 MACsec blocks. SSPs are provided to the module by the calling process and are destroyed when released by the appropriate zeroization function calls.

9.7 SSP Zeroization

The RAM occupied by SSPs is allocated by regular memory allocation operating system calls. The module calls internally the appropriate zeroization functions (i.e. memset) to zeroize any intermediate values used to configure the MACsec blocks and before returning to the calling application. The

zeroization functions overwrite the memory occupied by SSPs with “zeros” and deallocate the memory with the regular memory deallocation operating system call.

The module also zeroizes the registers when the MACsec block is no longer used when the macsecv2_drv_port_tx_sa_delete() function is invoked. The completion of this function will indicate that the zeroization of the SSPs included in the MACsec block finished successfully.

10 SELF-TESTS

The module performs the pre-operational and conditional cryptographic algorithms self-tests automatically when the module is loaded into memory. These self-tests ensure that the module is not corrupted and that the cryptographic algorithms work as expected. While the module is executing the pre-operational and the conditional cryptographic algorithms self-tests, services are not available, and input and output are inhibited. The module is not available for use by the calling application until the self-tests are completed successfully. If any of the self-tests fails, an error message is returned and the module transitions to error state.

See Section 10.4 for descriptions of possible self-test errors and recovery procedures.

10.1 Pre-operational Tests

The module performs a pre-operational software integrity test automatically when the module is powered on before the module transitions into the operational state. The details on the integrity test are specified in Section 5.1.

10.2 Conditional Tests

Table 10 lists the cryptographic algorithm self-tests (CASTs). The CASTs for the integrity mechanism are performed by the bound Kernel module, which provides that functionality. The details of the integrity test are provided in Section 5.1.

Each KAT includes comparison of the calculated output with the expected known answer, hard coded as part of the test vectors used in the test. Data output through the data output interface is inhibited during the self-tests. If the values do not match, the KAT fails and the module transitions to the error state.

Algorithm	Power-Up Tests
AES	• KAT AES GCM mode with 128 and 256 bit keys, encryption and decryption (separately tested). • KAT AES XPN mode with 128 and 256 bit keys, encryption and decryption (separately tested).

Table 10 - Conditional Cryptographic Algorithms Self-Tests performed by the module

KATs for the HMAC algorithm used in this module are performed by the respective bound modules.

10.2.1 Pairwise Consistency Tests

The module does not perform any pairwise consistency test.

10.3 Periodic/On-demand Self-Tests

On-demand self-tests can be invoked by powering-off and reloading the module which cause the module to run the pre-operational and conditional cryptographic algorithms self-tests.

10.4 Error States

When the module fails any pre-operational self-test, the module will enter the Error state. Any further cryptographic operation is inhibited. The calling application can obtain the module state by calling the macsecv2_drv_fips_kat_ok() and the macsecv2_drv_integrity_chk_ok() API functions. The function will return a boolean code indicating whether the CAST or the integrity tests passed or failed.

The Crypto Officer can recover from the Error state by restarting the hardware platform on which the module is running.

Error State	Cause of Error	Status Indicator
Error state	Failure of CAST	macsecv2_drv_fips_kat_ok() function returns false.
	Failure of integrity tests	macsecv2_drv_integrity_chk_ok() function returns false.

Table 11 - Error States

11 LIFE-CYCLE ASSURANCE

11.1 Delivery and Operation

11.1.1 Module Installation

The binary of the module is contained in the base Junos Evolved installation image. The Crypto Officer shall follow this Security Policy to configure the operational environment and install the module to be operated as a FIPS 140-3 validated module.

11.1.2 End of Life Procedures

As the module does not persistently store SSPs, secure sanitization of the module consists of unloading the module. This will zeroize all SSPs in volatile memory.

11.2 Crypto Officer Guidance

11.2.1 Verification of the Module Installation

The module is already pre-installed on the image file (junos-evo-install-ptx-fixed-x86-64-22.4R2.11-S1-EVO.iso). The crypto officer is responsible to verify the correct installation of the module by executing the following command:

```
show macsec drv version
```

Verify that the command returns the following name and version of the software and hardware components of the module, which matches the versions shown in Table 2:

```
Junos OS Evolved MACsec Cryptographic Driver Library, version 1.0 : ASIC JTAG ID 20611361
```

11.2.2 AES GCM IV

The AES GCM IV generation is compliant with IEEE 802.1AE and shall only be used for the MACsec protocol to be compliant with [FIPS140-3_IG] IG C.H, provision 1.c (“MACsec protocol IV generation”).

The module is part of the Juniper Packet Transport Router Model PTX10001-36MR, which supports MACsec using static connectivity association key (CAK) security mode. In this mode, a pre-shared key (PSK) is exchanged between the devices on each end of the point-to-point Ethernet link. Each appliance plays the role of either the Peer or the Authenticator in the context of the MACsec protocol. No authentication server is involved.

When supporting the MACsec protocol in the approved mode, the module should only be used together with the same appliance or other appliances that are also FIPS 140-3 validated and operating in the approved mode. In addition, the link between the Peer and the Authenticator should be secured to prevent the possibility for an attacker to introduce foreign equipment into the local area network.

In line with the MACsec protocol, the IV has a length of 96 bits and it is constructed externally by concatenating:

- For AES-128-GCM and AES-256-GCM: the 64-bit Secure Channel Identifier (SCI) and the 32-bit packet number (PN)
- For AES-128-XPN and AES-256-XPN: the 32-bit Short Secure Channel Identifier (SSCI), the 64-bit extended packet number (XPN) and a 96-bit salt.

In case the module's power is lost and then restored, the key used for the AES GCM encryption or decryption shall be redistributed.

12 MITIGATION OF OTHER ATTACKS

The module does not implement any mitigation mechanism.

13 APPENDIX A - GLOSSARY AND ABBREVIATIONS

AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions
API	Application Program Interface
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
ECB	Electronic Code Book
EE	Electronic Entry
FIPS	Federal Information Processing Standards Publication
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
IG	Implementation Guidance
KAT	Known Answer Test
MD	Manual Distribution
NIST	National Institute of Science and Technology
PAA	Processor Algorithm Acceleration
PCT	Pair-wise Consistency Test
SHA	Secure Hash Algorithm
SCI	Secure Channel Identifier
SSCI	Short Secure Channel Identifier
TOEPP	Tested Operational Environment's Physical Perimeter
XPN	Extended Packet Number

14 APPENDIX B – REFERENCES

IEEE-802.1AE	**IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security** https://1.ieee802.org/security/802-1ae **December 2018**
FIPS140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** March 2019 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
FIPS140-3_IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program** October 2022 https://csrc.nist.gov/csrc/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf
FIPS197	**Advanced Encryption Standard** November 2001 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS198-1	**The Keyed Hash Message Authentication Code (HMAC)** July 2008 http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
KERNEL-SP	**Junos® OS Evolved Kernel Cryptographic Module version 2.0 - FIPS 140-3 Non-Proprietary Security Policy** August 2023 https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp4776.pdf
OPENSSL-SP	**Junos® OS Evolved OpenSSL Cryptographic Module version 3.0.8 - FIPS 140-3 Non-Proprietary Security Policy** August 2023 https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp4775.pdf
SP800-38Arev1	**NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques** December 2001 https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
SP800-38D	**NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC** November 2007 http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
SP800-140B	**NIST Special Publication 800-140B - CMVP Security Policy Requirements** **March 2020** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140B.pdf