Ruckus Wireless LLC

Ruckus FastIron ICXTM 7550/7650/7850 Series Switch/Router

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This is a non-proprietary cryptographic module security policy for Ruckus FastIron ICX™ 7550/7650/7850 Series Switch/Router (hereinafter referred to as the module). The firmware version running on each module is IronWare OS 10.0.10. This security policy describes how the module meets the FIPS 140-3 Level 1 security requirements, and how to operate the module in an approved mode. This security policy may be freely distributed.

FIPS 140-3 (Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-3 standard and validation program is available on the NIST website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	2
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 Level	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module delivers the performance, flexibility, and scalability required for enterprise access deployment.
Module Type: Hardware

Module Embodiment: MultiChipStand

Module Characteristics:

Cryptographic Boundary:

The Tested Operational Environment Physical Perimeter (TOEPP) is defined as the entire chassis unit's physical perimeter encompassing the "top," "front," "left," "right," "rear" and "bottom" surfaces of the case as shown in the figures below and in the Physical Security section. The cryptographic boundary encompasses the entire TOEPP. This section illustrates the module hardware with the help of photographs.

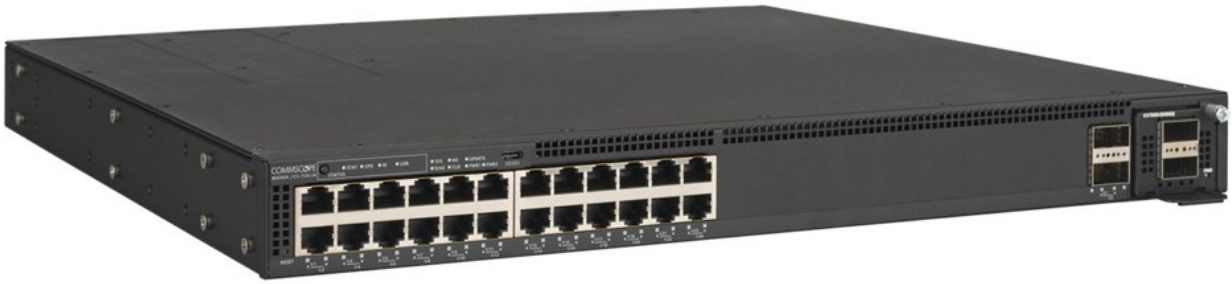

Figure 1: ICX 7550-24

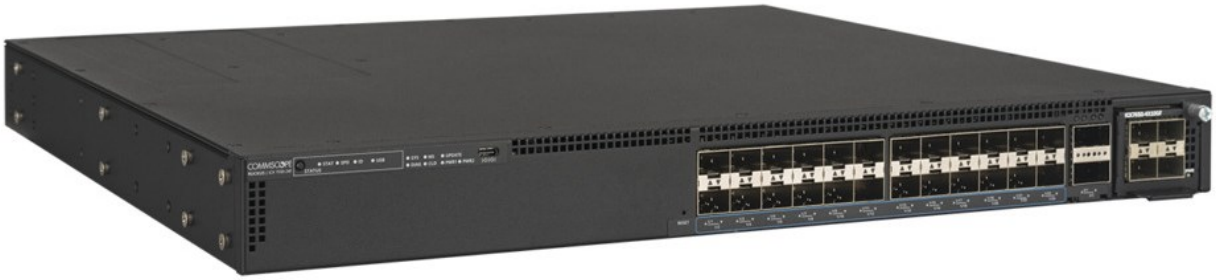

Figure 2: ICX 7550-24F

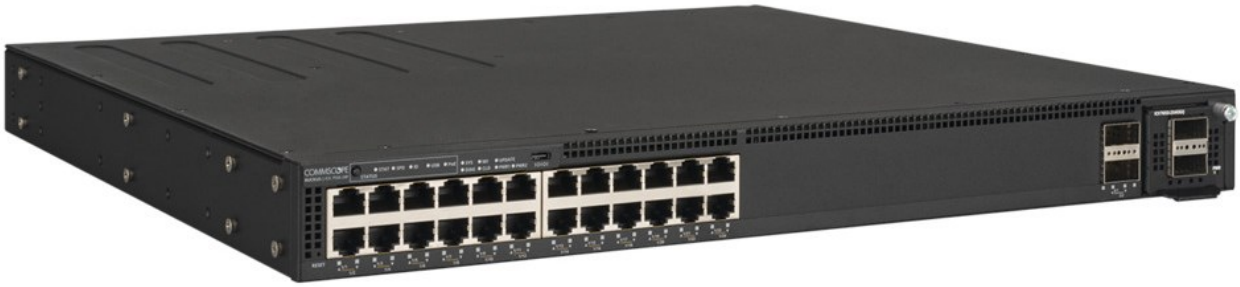

Figure 3: ICX 7550-24P

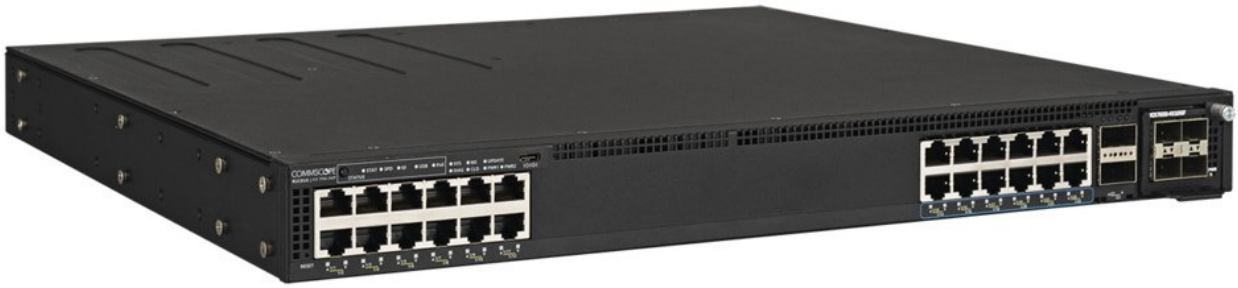

Figure 4: ICX 7550-24ZP

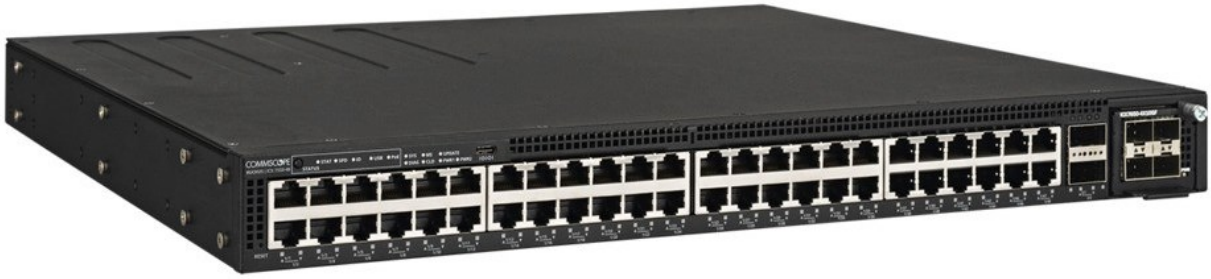

Figure 5: ICX 7550-48

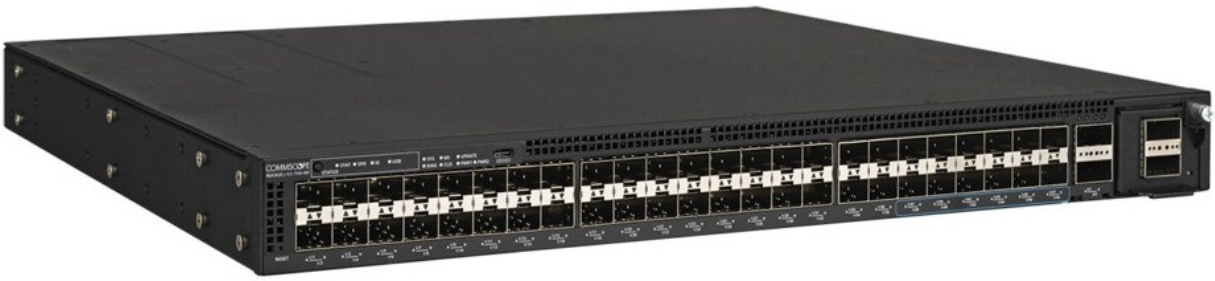

Figure 6: ICX 7550-48F

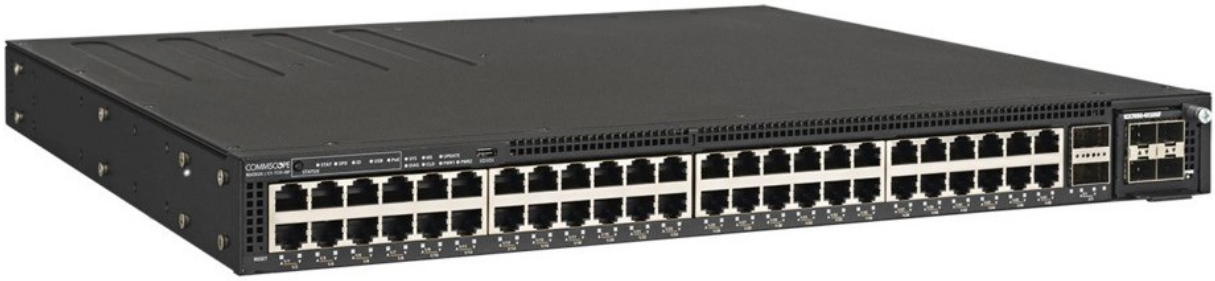

Figure 7: ICX 7550-48P

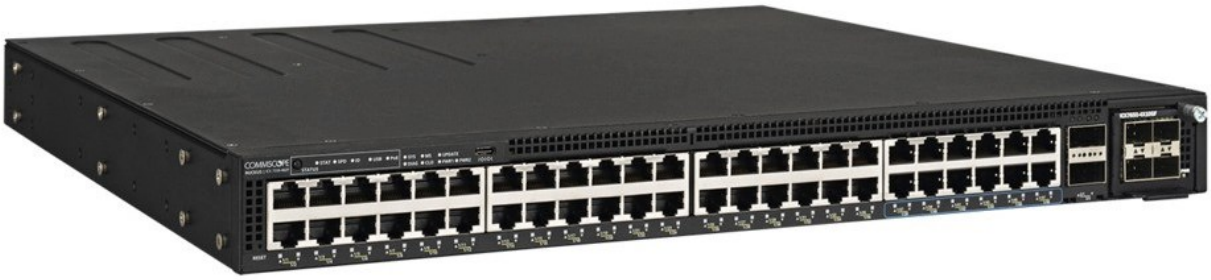

Figure 8: ICX 7550-48ZP

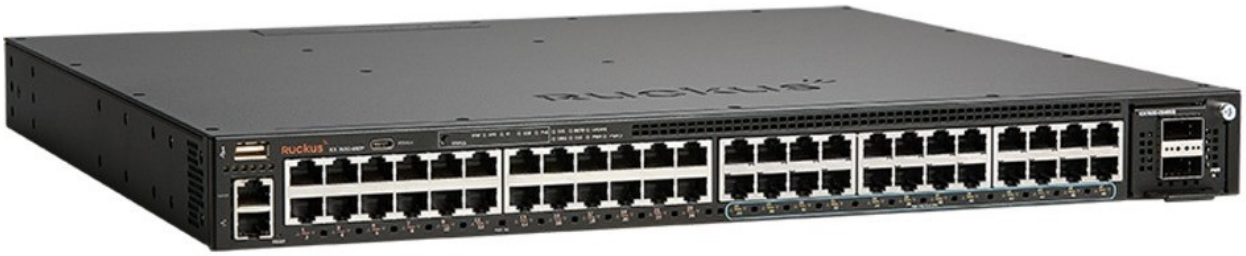

Figure 9: ICX 7650-48ZP

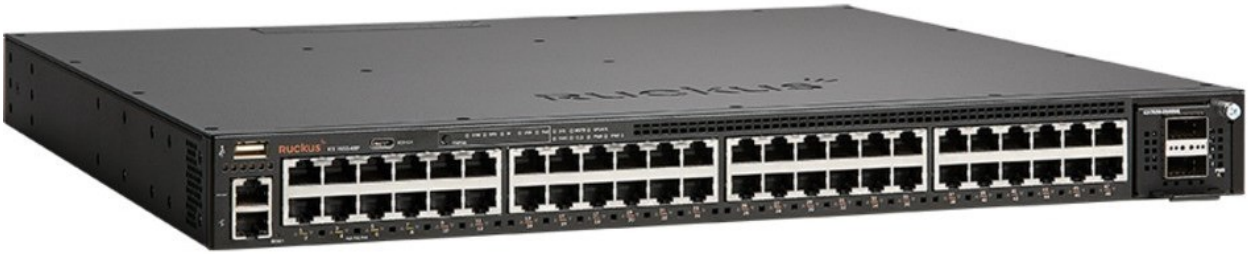

Figure 10: ICX 7650-48P

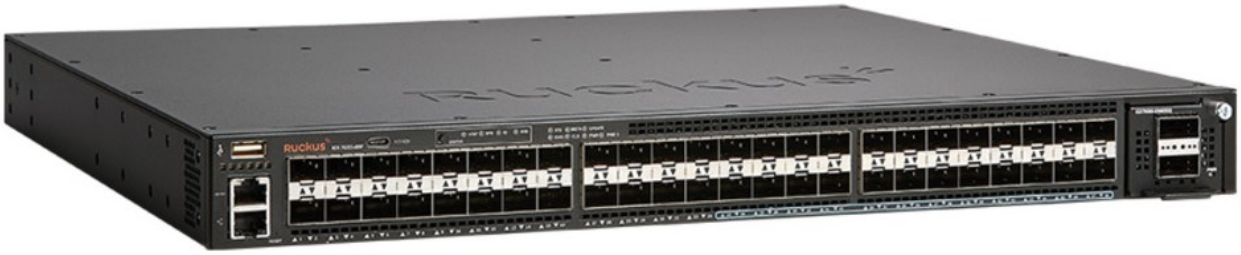

Figure 11: ICX 7650-48F

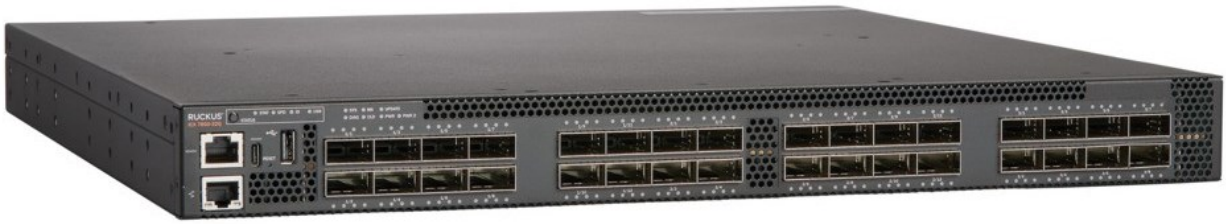

Figure 12: ICX 7850-32Q

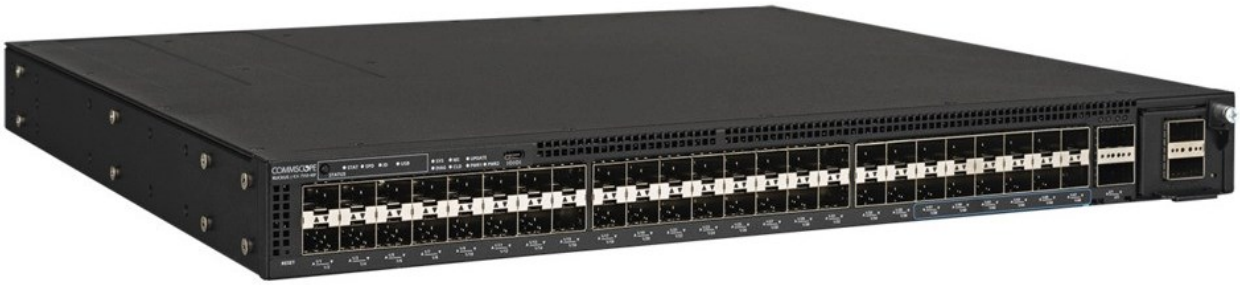

Figure 13: ICX 7850-48FS

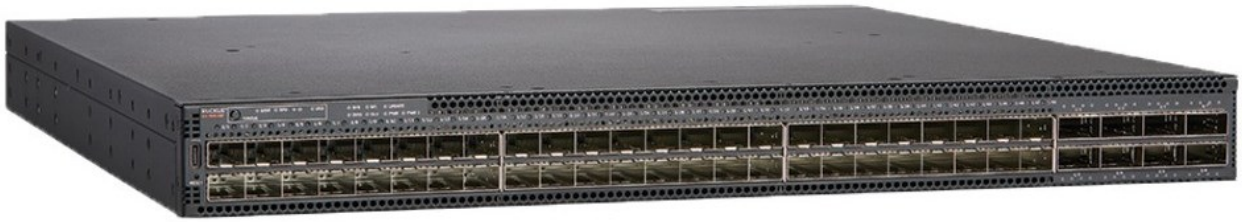

Figure 14: ICX 7850-48F

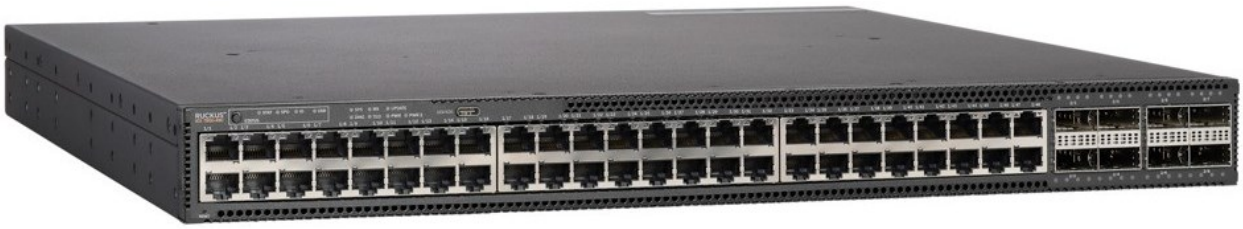

Figure 15: ICX 7850-48C

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
ICX-7550-24	ICX-7550-24	IronWare OS 10.0.10	ARM Cortex A72 (ARMv8)	
ICX-7550-24P	ICX-7550-24P	IronWare OS 10.0.10	ARM Cortex A72 (ARMv8)	
ICX-7550-24ZP	ICX-7550-24ZP	IronWare OS 10.0.10	ARM Cortex A72 (ARMv8)	
ICX-7550-24F	ICX-7550-24F	IronWare OS 10.0.10	ARM Cortex A72 (ARMv8)	
ICX-7550-48	ICX-7550-48	IronWare OS 10.0.10	ARM Cortex A72 (ARMv8)	
ICX-7550-48P	ICX-7550-48P	IronWare OS 10.0.10	ARM Cortex A72 (ARMv8)	
ICX-7550-48ZP	ICX-7550-48ZP	IronWare OS 10.0.10	ARM Cortex A72 (ARMv8)	
ICX-7550-48F	ICX-7550-48F	IronWare OS 10.0.10	ARM Cortex A72 (ARMv8)	
ICX-7650-48P	ICX-7650-48P	IronWare OS 10.0.10	ARM Cortex A57 (ARMv8)	
ICX-7650-48ZP	ICX-7650-48ZP	IronWare OS 10.0.10	ARM Cortex A57 (ARMv8)	
ICX-7650-48F	ICX-7650-48F	IronWare OS 10.0.10	ARM Cortex A57 (ARMv8)	
ICX-7850-32Q	ICX-7850-32Q	IronWare OS 10.0.10	ARM Cortex A57 (ARMv8)	
ICX-7850-48FS	ICX-7850-48FS	IronWare OS 10.0.10	ARM Cortex A57 (ARMv8)	
ICX-7850-48F	ICX-7850-48F	IronWare OS 10.0.10	ARM Cortex A57 (ARMv8)	
ICX-7850-48C	ICX-7850-48C	IronWare OS 10.0.10	ARM Cortex A57 (ARMv8)	

Table 2: Tested Module Identification – Hardware

The module is a hardware module. The module's operational environment is limited. The module's firmware version running on each model is IronWare OS 10.0.10.

The distinguishing features of each Hardware Model are detailed below:

RUCKUS ICX 7550 SERIES

The RUCKUS ICX 7550 Series switches support up to 2 redundant hot swappable load sharing power supplies (AC or DC), up to 3 hot swappable fans (exhaust or intake airflow), one RJ-45 Ethernet port for out of band network management, one USB Type-C port for console management, one RJ-45 port for serial console management, and one USB port for external file storage.

The ICX 7550 offers two 40GbE QSFP+ or two 40/100 GbE QSFP28 uplink/stacking ports (see below for details)

One optional uplink/stacking module may also be installed.

	**RUCKUS ICX 7550 24 Gigabit Ports** • 24-port 10/100/1000 Mbps • 2-port 40 Gbps Uplink/Stack QSFP+, expansion module slot
	**RUCKUS ICX 7550 48 Gigabit Ports** • 48-port 10/100/1000 Mbps • 2-port 40 Gbps Uplink/Stack QSFP+, expansion module slot
	**RUCKUS ICX 7550 24 Gigabit Ports with POE** • 24-port 10/100/1000 Mbps 802.3at POE+ • 2-port 40 Gbps Uplink/Stack QSFP+, expansion module slot • 24-PoE port 802.3at, up to 30W per port, up to 1900W PoE budget • Perpetual and Fast-boot POE on all ports
	**RUCKUS ICX 7550 48 Gigabit Ports with POE** • 48-port 10/100/1000 Mbps 802.3at POE+ • 2-port 40 Gbps Uplink/Stack QSFP+, expansion module slot • 48-PoE port 802.3at, up to 30W per port, up to 1900W PoE budget • Perpetual and Fast-boot POE on all ports
	**RUCKUS ICX 7550 24 Multi-Gigabit Ports with POE** • 12-port 100/1000 Mbps/2.5 Gbps 802.3bt POE, • 12-port 100/1000 Mbps/2.5/5/10 Gbps 802.3bt POE • 2-port 40/100 Gbps Uplink/Stack QSFP28, expansion module slot • 24-PoE port 802.3bt, up to 90W per port, up to 1900W PoE budget • Perpetual and Fast-boot POE on all ports
	**RUCKUS ICX 7550 48 Multi-Gigabit Ports with POE** • 36-port 100/1000 Mbps/2.5 Gbps 802.3bt POE, • 12-port 100/1000 Mbps/2.5/5/10 Gbps 802.3bt POE • 2-ports 40/100 Gbps Uplink/Stack QSFP28, expansion module slot • 24-PoE port 802.3bt, up to 90W per port, up to 1900W PoE budget • Perpetual and Fast-boot POE on all ports
	**RUCKUS ICX 7550 24 Fiber Ports** • 24-port 1/10 Gbps • 2-ports 40/100 Gbps Uplink/Stack QSFP28, expansion module slot
	**RUCKUS ICX 7550 48 Fiber Ports** • 36-port 100/1000 Mbps SFP • 12-port 1/10 Gbps SFP+ • 2-ports 40/100 Gbps Uplink/Stack QSFP28, expansion module slot
	**RUCKUS ICX 7550 Rear View** • 2 hot-swap load sharing power supplies (N+1, choice of AC/DC and standard/reversed airflow) • 3 hot-swap fans (N+1 redundancy) • USB storage, RJ45 serial port, RJ45 Ethernet management port

Figure 16: ICX-7550 Series

Note: The USB Port for external file storage is functionally disabled

Ruckus ICX 7650

All Ruckus ICX 7650 models offer one modular slots in the front for interchangeable uplink modules, dual power supply slots, dual fan tray slots in the back, one RJ-45 Ethernet port for out-of-band network management, one USB Type-C port for console management, one RJ-45 port for serial console management, and one USB port for external file storage.

	**Ruckus ICX 7650-48P** • 48x 10/100/1000 Mbps RJ-45 ports with 40 supporting PoE+ and 8 supporting PoE+, UPoE and PoH • Can stack on 4x40G or 2x100G rear facing QSFP ports, these ports can also be used as 2x40G uplinks when the switch is standalone • One slot for 2x40G or 4x10G front facing module • Up to 1500W PoE budget • 2x hot-swappable load sharing power supplies and 2x hot- swappable fan assemblies with reversible airflow options
	**Ruckus ICX 7650-48ZP** • 24x 10/100/1000 Mbps RJ-45 PoE+ ports • 24x 100/1000 Mbps 2.5/5/10 Gbps RJ-45 PoE+/PoH/UPoE ports • Can stack on 4x40G or 2x100G rear facing QSFP ports, these ports can also be used as 2x40G or 2x100G uplinks when switch is standalone • One slot for 1x 100G or 2x40G or 4x10G front facing module • Up to 1500W PoE budget • 2x hot-swappable load sharing power supplies and 2x hot- swappable fan assemblies with reversible airflow options
	**Ruckus ICX 7650-48F** • 24x 100/1000 Mbps SFP ports • 24x 1000 Mbps / 10 Gbps SFP+ ports • Can stack on 4x40G or 2x100G rear facing QSFP ports, these ports can also be used as 2x40G or 2x100G uplinks when switch is standalone • One slot for 1x 100G or 2x40G or 4x10G front facing module • 2x hot-swappable load sharing power supplies and 2x hot- swappable fan assemblies with reversible airflow options
	**Ruckus ICX 7650 Rear View (all models)** The four rear facing QSFP ports can be configured as follows: • 4x 40G QSFP+ stacking / 2x 40G QSFP+ uplink ports or • 2x100G QSFP28 stacking/uplink ports • Note: Front-facing optional module only enabled when rear ports are used for stacking. ICX 7650-48P only supports 2x40G rear facing uplink ports

Figure 17: ICX-7650 Series

Note: The USB Port for external file storage is functionally disabled

RUCKUS ICX 7850

All RUCKUS ICX 7850 models offer, dual power supply slots, 5 or 6 fan tray slots in the back, one RJ-45 Ethernet port for out-of-band network management, one USB Type-C port for console management, one RJ-45 port for serial console management, and one USB Type A port for external file storage.

	**RUCKUS ICX 7850-32Q** • 32x 40/100 GbE QSFP28 ports supporting native 40 GbE or 100 GbE, or breakout* to 4x10 GbE or 4x25 GbE • Up to 8 of the rightmost QSFP28 ports as stacking ports • 2x hot-swappable load sharing power supplies and 6x hot- swappable fan assemblies with reversible airflow options (Power supplies and FAN airflows must be the same)
	**RUCKUS ICX 7850-48FS** • 48x 1/10 GbE SFP+ ports with 128/256 bit MACsec and LRM support • 8x 40/100 Gbps QSFP28 ports supporting native 40 GbE or 100 GbE, or breakout* to 4x10 GbE or 4x25 GbE • Up to 8 of the QSFP28 ports as stacking ports • 2x hot-swappable load sharing power supplies and 5x hot- swappable fan assemblies with reversible airflow options (Power supplies and FAN airflows must be the same)
	**RUCKUS ICX 7850-48F** • 48x 1/10/25 GbE SFP28 ports • 8x 40/100 GbE QSFP28 ports supporting native 40 GbE or 100 GbE, or breakout* to 4x10 GbE or 4x25 GbE • Up to 8 of the QSFP28 ports as stacking ports • 2x hot-swappable load sharing power supplies and 5x hot- swappable fan assemblies with reversible airflow options (Power supplies and FAN airflows must be the same)
	**RUCKUS ICX 7850-48C** • 48x 1/10G GbE RJ45 ports • 8x 40/100 Gbps QSFP28 ports supporting native 40 GbE or 100 GbE, or breakout* to 4x10 GbE or 4x25 GbE • Up to 8 of the QSFP28 ports as stacking ports • 2x hot-swappable load sharing power supplies and 5x hot- swappable fan assemblies with reversible airflow options (Power supplies and FAN airflows must be the same)

Figure 18: ICX-7850 Series

Note: The USB Port for external file storage is functionally disabled

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode of Operation	The module is always in the approved mode of operation after initial operations are performed.	Approved	Global indicator after module initialization. Please refer to Security Policy, section Life-Cycle Assurance for more information

Table 3: Modes List and Description

By default, the module is delivered in an un-initialized state but supports an approved mode of operation. Once the module is configured to operate in the approved mode of operation by following the steps in section " Life-Cycle Assurance" of this document by the Crypto Officer, the module can only operate in the approved mode. The module does not claim implementation of a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Crypto Library I

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5076	-	SP 800-38A
AES-CFB128	A5076	-	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A5076	-	SP 800-38B
AES-CTR	A5076	-	SP 800-38A
AES-ECB	A5076	-	SP 800-38A
AES-GCM	A5076	-	SP 800-38D
AES-KW	A5076	-	SP 800-38F
AES-KWP	A5076	-	SP 800-38F
Counter DRBG	A5076	-	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A5076	-	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A5076	-	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A5076	-	FIPS 186-5
HMAC-SHA-1	A5076	-	FIPS 198-1
HMAC-SHA2-256	A5076	-	FIPS 198-1
HMAC-SHA2-384	A5076	-	FIPS 198-1
HMAC-SHA2-512	A5076	-	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5076	-	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A5076	-	SP 800-56A Rev. 3
KDF SNMP (CVL)	A5076	-	SP 800-135 Rev. 1
KDF SP800-108	A5076	-	SP 800-108 Rev. 1
KDF SSH (CVL)	A5076	-	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-5)	A5076	-	FIPS 186-5
RSA SigGen (FIPS186-5)	A5076	-	FIPS 186-5
RSA SigVer (FIPS186-5)	A5076	-	FIPS 186-5
Safe Primes Key Generation	A5076	-	SP 800-56A Rev. 3
SHA-1	A5076	-	FIPS 180-4
SHA2-256	A5076	-	FIPS 180-4
SHA2-384	A5076	-	FIPS 180-4
SHA2-512	A5076	-	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A5076	-	SP 800-135 Rev. 1

Table 4: Approved Algorithms - Crypto Library I

Crypto Library II

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	AES 4550	-	SP 800-38A
AES-GCM	AES 4550	-	SP 800-38D

Table 5: Approved Algorithms - Crypto Library II

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	N/A	The module performs Cryptographic Key Generation (CKG) for asymmetric keys as detailed by example 1 in section 4 and section 5 of SP800-133r2

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
KAS-ECC (SSHv2)	CKG KAS-Full	Full KAS-ECC Key Agreement used for SSHv2 service	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength IG:IG D.F Scenario 2, Path 2, Split Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-ECC-SSC Sp800-56Ar3: (A5076) KDF SSH: (A5076) Counter DRBG: (A5076) CKG: ()
KAS-FFC (SSHv2)	CKG KAS-Full	Full KAS-FFC Key Agreement used for SSHv2 service	Caveat:Key establishment methodology provides between 112 and 200 bits of security strength IG:IG D.F Scenario 2, Path 2, Split Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-FFC-SSC Sp800-56Ar3: (A5076) Domain Parameter Generation Methods: MODP-2048, MODP-4096, MODP-8192 Safe Primes Key Generation: (A5076) Safe Prime Groups: MODP-2048, MODP-4096, MODP-

Name	Type	Description	Properties	Algorithms
				8192 KDF SSH: (A5076) Counter DRBG: (A5076) CKG: ()
KAS-ECC (TLSv1.2)	CKG KAS-Full	Full KAS-ECC Key Agreement used for TLSv1.2 service	Caveat:Key establishment methodology provides between 128 and 192 bits of security strength IG:IG D.F Scenario 2, Path 2, Split Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-ECC-SSC Sp800-56Ar3: (A5076) Domain Parameter Generation Methods: P-256, P-384 TLS v1.2 KDF RFC7627: (A5076) Counter DRBG: (A5076) CKG: ()
KAS-FFC (TLSv1.2)	CKG KAS-Full	Full KAS-FFC Key Agreement used for TLSv1.2 service	Caveat:Key establishment methodology provides 112 bits of security strength IG:IG D.F Path 2, Scenario 2, Split Key Confirmation:No Key Derivation:IG 2.4.B SP 800-135rev1 CVL	KAS-FFC-SSC Sp800-56Ar3: (A5076) Domain Parameter Generation Methods: ffdhe2048 Safe Primes Key Generation: (A5076) Safe Prime Groups: ffdhe2048 TLS v1.2 KDF RFC7627: (A5076) Counter DRBG: (A5076) CKG: ()
SSH-KTS (AES and HMAC)	KTS-Wrap	KTS via SSHv2 service by using AES and HMAC	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength Standard:SP 800-	AES-CBC: (A5076) AES-CTR: (A5076) HMAC-SHA-1: (A5076) HMAC-SHA2-256: (A5076)

Name	Type	Description	Properties	Algorithms
			38F IG D.G:"combination" method: use any approved symmetric encryption mode together with an approved authentication method	
TLS-KTS (AES and HMAC)	KTS-Wrap	KTS via TLS v1.2 service by using AES and HMAC	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength Standard:SP 800-38F IG D.G:"combination" method: use any approved symmetric encryption mode together with an approved authentication method	AES-CBC: (A5076) AES-ECB: (A5076) HMAC-SHA-1: (A5076) HMAC-SHA2-256: (A5076) HMAC-SHA2-512: (A5076)
TLS-KTS (AES-GCM)	KTS-Wrap	KTS via TLSv1.2 service by using AES-GCM	Caveat:Key establishment methodology provides between 128 and 256 bits of security strength Standard:SP 800-38F IG D.G:Uses a previously approved authenticated symmetric encryption mode	AES-GCM: (A5076)
MACSec-KTS (AES-KW)	KTS-Wrap	MACSec KeyWrap using AES-KW to	Security Strength:Provides 128 or 256 bits of	AES-KW: (A5076)

Name	Type	Description	Properties	Algorithms
		protect MACSec SAK	encryption strength	
MACSec-KTS (AES-KWP)	KTS-Wrap	MACSec KeyWrap using AES-KWP to protect MACSec SAK	Security Strength:Provides 128 or 256 bits of encryption strength	AES-KWP: (A5076)
SSH RSA KeyGen	CKG AsymKeyPair-KeyGen	RSA KeyGen for SSHv2	Keysize:112 bits encryption strength	RSA KeyGen (FIPS186-5): (A5076) Counter DRBG: (A5076) CKG: ()
SSH RSA SigGen	DigSig-SigGen	RSA SigGen for SSHv2		RSA SigGen (FIPS186-5): (A5076)
SSH RSA SigVer	DigSig-SigVer	RSA SigVer for SSHv2		RSA SigVer (FIPS186-5): (A5076)
SSH ECDSA KeyGen	CKG AsymKeyPair-KeyGen	ECDSA KeyGen for SSHv2	Keysize:128 to 192 bits encryption strength	ECDSA KeyGen (FIPS186-5): (A5076) Counter DRBG: (A5076) CKG: ()
SSH ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for SSHv2		ECDSA SigGen (FIPS186-5): (A5076)
SSH ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for SSHv2		ECDSA SigVer (FIPS186-5): (A5076)
TLS RSA KeyGen	CKG AsymKeyPair-KeyGen	RSA KeyGen for TLSv1.2	Keysize:112 bits encryption strength	Counter DRBG: (A5076) RSA KeyGen (FIPS186-5): (A5076) CKG: ()
TLS RSA SigGen	DigSig-SigGen	RSA SigGen for TLSv1.2		RSA SigGen (FIPS186-5): (A5076)
TLS RSA SigVer	DigSig-SigVer	RSA SigVer for TLSv1.2		RSA SigVer (FIPS186-5): (A5076)
TLS ECDSA KeyGen	CKG AsymKeyPair-KeyGen	ECDSA KeyGen for TLSv1.2	Keysize:128 to 192 bits encryption strength	Counter DRBG: (A5076) ECDSA KeyGen (FIPS186-5): (A5076) CKG: ()

Name	Type	Description	Properties	Algorithms
TLS ECDSA SigGen	DigSig-SigGen	ECDSA SigGen for TLSv1.2		ECDSA SigGen (FIPS186-5): (A5076)
TLS ECDSA SigVer	DigSig-SigVer	ECDSA SigVer for TLSv1.2		ECDSA SigVer (FIPS186-5): (A5076)
Block ciphers (SSHv2)	BC-UnAuth	Block ciphers for SSHv2 service		AES-CBC: (A5076) AES-CTR: (A5076)
Block ciphers (TLSv1.2)	BC-Auth BC-UnAuth	Block ciphers for TLSv1.2 service		AES-CBC: (A5076) AES-GCM: (A5076) AES-ECB: (A5076)
Block ciphers (SNMPv3)	BC-UnAuth	Block ciphers for SNMPv3 service		AES-CFB128: (A5076) KDF SNMP: (A5076)
Block ciphers (MACSec)	BC-Auth	Block ciphers for MACSec service		AES-ECB: (AES 4550) AES-GCM: (AES 4550) KDF SP800-108: (A5076)
MAC (SSHv2)	MAC	MAC for SSHv2 service		HMAC-SHA-1: (A5076) HMAC-SHA2-256: (A5076) HMAC-SHA2-512: (A5076) SHA-1: (A5076) SHA2-256: (A5076) SHA2-512: (A5076)
MAC (TLSv1.2)	MAC	Message Authentication for TLSv1.2 services		HMAC-SHA-1: (A5076) HMAC-SHA2-256: (A5076) HMAC-SHA2-384: (A5076) SHA-1: (A5076) SHA2-256: (A5076) SHA2-384: (A5076)

Name	Type	Description	Properties	Algorithms
MAC (SNMPv3)	MAC	Message Authentication for SNMPv3 services		HMAC-SHA-1: (A5076) HMAC-SHA2-256: (A5076) HMAC-SHA2-384: (A5076) HMAC-SHA2-512: (A5076) SHA-1: (A5076) SHA2-256: (A5076) SHA2-384: (A5076) SHA2-512: (A5076) KDF SNMP: (A5076)
DRBG Function	DRBG	Used for DRBG generation		Counter DRBG: (A5076)
SNMPv3 Keying Materials Development	KAS-135KDF	Keying materials, used to derive SNMP session keys		KDF SNMP: (A5076)
TLS Keying Materials Development	KAS-135KDF	Keying materials, used to derive TLS session keys		TLS v1.2 KDF RFC7627: (A5076)
Firmware Load Test	DigSig-SigVer	Signature Verification for firmware load test		RSA SigVer (FIPS186-5): (A5076)
MACSec-SAK-Integrity	MAC	Used to protect the integrity of SAK during key transmission		AES-CMAC: (A5076)
MACsec Keying Materials Development	KBKDF	MACsec session keying materials, used to derive MACsec session keys		KDF SP800-108: (A5076)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

Notes:

- The Module's AES-GCM implementation conforms to Implementation Guidance C.H scenario #1 following RFC 5288 for TLS. The Module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The keys for the client and server negotiated in the TLSv1.2 handshake process (client_write_key and server_write_key) are compared and the Module aborts the session if the key values are identical. The operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the Module being validated. The counter portion of the IV is set by the Module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the Module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.
- The module takes on the role of Authenticator (not by aid of RADIUS Authentication Server) reference to the MACsec protocol. The AES GCM IV construction is performed in compliance with IEEE 802.1AE and its amendments. The IV length used is 96 bits (per SP 800-38D and FIPS 140-3 IG C.H). If the module loses power, then new AES GCM keys should be established. The module should only be used with FIPS 140-3 validated modules when supporting the MACsec protocol for providing Peer, Authenticator functionality. The Peer and the Authenticator Modules Security Policies shall state that the link between the Peer and the Authenticator is protected by AES-KW/KWP (ACVP Cert. #A5076) to prevent the possibility for an attacker to introduce foreign equipment into the local area network.
- In accordance with FIPS 140-3 IG D.H, the cryptographic Module performs Cryptographic Key Generation as per section 5 in SP800-133 Rev2. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90A Rev1 DRBG.

2.8 RBG and Entropy

Cert Number	Vendor Name
E192	Ruckus Wireless LLC

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Ruckus IronWare 10.0.10 Entropy Source	Non-Physical	ARM Cortex A57 (ARMv8); ARM Cortex A72 (ARMv8)	8 bits	4 bits	N/A

Table 9: Entropy Sources

Ruckus FastIron™ IronWare 10.0.10 Entropy Source v1.0 is the entropy source used on each Ruckus FastIron ICX™ 7550, 7650, and 7850 Series Router with firmware IronWare OS 10.0.10 to seed the approved DRBG. The noise source of entropy is periodic sampling of the high-

precision CPU clock within the ARM CPU. There is no conditioning component applied on the output of the clock source. Health testing is implemented on the output of the noise source.

The entropy source provides a minimum entropy of 4 bits per sample with the sample size of 8 bits. The module makes repeated calls to the entropy source after which the random data is loaded into a buffer. This buffer is used by the DRBG to get entropy input. Buffer size is big enough that the overall effective entropy is more than that is required for the DRBG instantiation. Similar implementation is done for DRBG reseeding."

2.9 Key Generation

The module generates RSA, ECDSA, EC Diffie-Hellman, and Diffie-Hellman asymmetric key pairs compliant with FIPS 186-5, using a NIST SP 800-90Ar1 CTR DRBG for random number generation. In accordance with FIPS 140-3 IG D.H, the cryptographic module performs CKG for asymmetric keys as per section 5.1 of NIST SP 800-133rev2 (vendor affirmed) by obtaining a random bit string directly from an approved DRBG. The random bit string supports the required security strength requested by the calling application (without any V, as described in Additional Comments 2 of IG D.H.).

2.10 Key Establishment

The module provides the following key/SSP establishment services in the approved mode of operation:

- KAS-FFC Shared Secret Computation:
    - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-FFC shared secret computation. The shared secret computation provides between 112 and 152 bits of encryption strength.

- KAS-ECC Shared Secret Computation:
    - The module provides SP800-56Arev3 compliant key establishment according to FIPS 140-3 IG D.F scenario 2 path (2) with KAS-ECC shared secret computation. The shared secret computation provides between 128 and 256 bits of encryption strength.

2.11 Industry Protocols

The module supports SSHv2, TLS v1.2, SNMPv3 and MACSec industrial protocols. No parts of the SSH, TLS and SNMP protocols, other than the KDFs, have been tested by the CAVP and CMVP. Please refer to SSPs Table for more information.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Console port, Mgmt Port, PoE+ ports, Ethernet Ports, SPF/SFP+, QSFP+, and QSFP28 ports	Data Input	Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and MACSec service data.
Console port, Mgmt Port, PoE+ ports, Ethernet Ports, SPF/SFP+, QSFP+, and QSFP28 ports	Data Output	Data output from the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and MACSec service data.
Console port, Mgmt Port, PoE+ ports, Ethernet Ports, SPF/SFP+, QSFP+, and QSFP28 ports	Control Input	Control Data input into the module for all the services defined in Approved Services Table, including TLSv1.2, SSHv2, SNMPv3 and MACSec service data.
Console port, Mgmt Port, PoE+ ports, Ethernet Ports, SPF/SFP+, QSFP+, and QSFP28 ports and LEDs	Status Output	Status Information output from the module.
N/A	Control Output	N/A
Power	Power	Provide the Power Supply to the module.

Table 10: Ports and Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Table 2. The module provides physical ports which are mapped to logical interfaces provided by the module (data input, data output, control input, control output and status output) as above.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password-Based	The minimum length is eight (8) characters (94 possible characters). The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8) which is less than 1/1,000,000. As the module supports at most ten failed attempts to authenticate in a one-minute period, the probability of successfully	Password Based	The probability that a random attempt will succeed or a false acceptance will occur is 1/(94^8) which is less than 1/1,000,000. Please refer to Description section in this table for more details.	The probability of successfully authenticating to the module within one minute is 10/(94^8), which is less than 1/100,000. Please refer to Description section in this table for more details.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	authenticating to the module within one minute is 10/(94^8), which is less than 1/100,000. This calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total.			
RSA-Based Certificate	The modules supports RSA public-key based authentication mechanism using a minimum of RSA 2048 bits, which provides 112 bits of security strength. The probability that a random attempt will succeed is 1/(2^112) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^112), which is less than 1/100,000.	RSA SigVer (FIPS186-5) (A5076)	With a minimum modulus size of 2048, the probability that a random attempt will succeed is 1/(2^112) which is less than 1/1,000,000. Please refer to Description section in this table for more details.	For multiple attacks during a one-minute period, to exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 8.65x10^31 (2^112 /60 = 8.65 x 10^31) attempts per second. Please refer to Description section in this table for more details.
ECDSA-Based Certificate	The modules support ECDSA public-key based authentication mechanism using a	ECDSA SigVer (FIPS186-5) (A5076)	With a minimum curve of P-256, the probability that a random	For multiple attacks during a one-minute period, to exceed a one in

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	minimum of curve P-256, which provides 128 bits of security strength. The probability that a random attempt will succeed is 1/(2^128) which is less than 1/1,000,000. For multiple attacks during a one-minute period, as the module at its highest can support at most 17,000 new sessions per second to authenticate in a one-minute period, the probability of successfully authenticating to the module within a one minute period is 17,000 * 60 = 1,020,000/(2^128), which is less than 1/100,000.		attempt will succeed is 1/(2^128) which is less than 1/1,000,000. Please refer to Description section in this table for more details.	100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 5.67x10^36 (2^128 /60 = 5.67 x 10^36) attempts per second. Please refer to Description section in this table for more details.

Table 11: Authentication Methods

The module implements role-based authentication. The module supports the Crypto Officer role and the User role. The module also allows the concurrent operators.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	Password-Based RSA-Based Certificate ECDSA-Based Certificate
User	Role	User	Password-Based RSA-Based Certificate ECDSA-Based Certificate
Port Config Admin	Role	Port Config Admin	Password-Based RSA-Based Certificate ECDSA-Based Certificate

Table 12: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status	Provide Module's current status (return codes and/or syslog messages)	Global Indicator or syslog message	Command used to show Module's Status	Module's Operational Status	None	Crypto Officer Port Config Admin User
Show Version	Provide Module's name and version information	Console message	Command to show version	Module's ID and versioning information	None	Crypto Officer Port Config Admin User
Perform Self-Tests	Perform Self-Tests (Pre-operational self-test and Conditional Self-Tests)	Perform self-test completion message	Command to trigger Self-Test	Status of the self-tests results	None	Crypto Officer User Port Config Admin Unauthenticated
Perform Zeroization	Perform Zeroization	Syslog message	Command to zeroize the module	Status of the SSPs zeroization	None	Crypto Officer - DRBG Entropy Input: Z - DRBG Seed: Z - DRBG Internal State V value: Z - DRBG Key: Z - User Password: Z - Crypto Officer Password: Z - Port Config Admin Password: Z - Firmware Load Test Key: Z - SSH DH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: Z - SSH DH Public Key: Z - SSH Peer DH Public Key: Z - SSH DH Shared Secret: Z - SSH ECDH Private Key: Z - SSH ECDH Public Key: Z - SSH Peer ECDH Public Key: Z - SSH ECDH Shared Secret: Z - SSH ECDSA Private Key: Z - SSH ECDSA Public Key: Z - SSH RSA Private Key: Z - SSH RSA Public Key: Z - SSH Session Encryption Key: Z - SSH Session Authentication Key: Z - TLS DH Private Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS DH Public Key: Z - TLS Peer DH Public Key: Z - TLS DH Shared Secret: Z - TLS ECDH Private Key: Z - TLS ECDH Public Key: Z - TLS Peer ECDH Public Key: Z - TLS ECDH Shared Secret: Z - TLS ECDSA Private Key: Z - TLS ECDSA Public Key: Z - TLS RSA Private Key: Z - TLS RSA Public Key: Z - TLS Master Secret: Z - TLS Session Encryption Key: Z - SNMPv3 Authentication Secret: Z - SNMPv3 Encryption Key: Z - SNMPv3

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Integrity Key: Z - MACSec CAK: Z - MACSec ICK: Z - MACSec SAK: Z - MACSec KEK: Z
Crypto Officer Authentication	CO Role Authentication	N/A	CO Authentication Request	Status of the CO authentication	None	Crypto Officer - Crypto Officer Password: W,Z
User Authentication	User Role Authentication	N/A	User role authentication request	Status of the User role authentication	None	User - User Password: W,Z
Port Config Admin Authentication	Port Config Admin Role Authentication	N/A	Port Config Admin role authentication request	Status of the Port Config Admin role authentication	None	Port Config Admin - Port Config Admin Password: W,Z
Port Configuration Mangement	Perform Port Configuration	N/A	Commands to configure the port parameters of switch/router	Port configuration completion status information	None	Crypto Officer Port Config Admin
Account Mangement	Account Creation	N/A	Commands to create a new user account	Status of the new user accounts	None	Crypto Officer
Configure SSHv2 Function	Configure SSHv2 Function	Global Indicator and SSHv2 configuration success	Commands to configure SSHv2	Status of the completion of the SSHv2 configuration	SSH RSA KeyGen SSH ECDSA KeyGen DRBG Function	Crypto Officer - SSH RSA Private Key: G,W - SSH RSA Public Key: G,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		status message				- SSH ECDSA Private Key: G,W - SSH ECDSA Public Key: G,W - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E - DRBG Key: G,W,E
Run SSHv2 Function	Execute SSHv2 Function	Global Indicator and successful SSHv2 log message	Initiate SSHv2 tunnel establishment	Status of SSHv2 tunnel establishment	KAS-ECC (SSHv2) KAS-FFC (SSHv2) SSH-KTS (AES and HMAC) SSH RSA SigGen SSH RSA SigVer SSH ECDSA SigGen SSH ECDSA SigVer Block ciphers (SSHv2) MAC (SSHv2) DRBG Function	Crypto Officer - SSH DH Private Key: G,W,E,Z - SSH DH Public Key: G,R,W,E,Z - SSH Peer DH Public Key: W,E,Z - SSH DH Shared Secret: G,W,E,Z - SSH ECDH Private Key: G,W,E,Z - SSH ECDH Public Key: G,R,W,E,Z - SSH Peer ECDH Public Key: W,E,Z - SSH ECDH Shared Secret: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH RSA Private Key: E - SSH RSA Public Key: R,E - SSH ECDSA Private Key: E - SSH ECDSA Public Key: R,E - SSH Session Encryption Key: G,W,E,Z - SSH Session Authentication Key: G,W,E,Z - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E - DRBG Key: G,W,E - RADIUS Secret: W,E Port Config Admin - SSH DH Private Key: R,E - SSH DH Public Key: R,E - SSH Peer DH Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: R,E - SSH DH Shared Secret: R,E - SSH ECDH Private Key: R,E - SSH ECDH Public Key: R,E - SSH Peer ECDH Public Key: R,E - SSH ECDH Shared Secret: R,E - SSH RSA Private Key: R,E - SSH RSA Public Key: R,E - SSH ECDSA Private Key: R,E - SSH ECDSA Public Key: R,E - SSH Session Encryption Key: R,E - SSH Session Authentication Key: R,E - DRBG Entropy Input: R,E - DRBG Seed: R,E - DRBG Internal State V value: R,E - DRBG Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						R,E - RADIUS Secret: W,E User - SSH DH Private Key: R,E - SSH DH Public Key: R,E - SSH Peer DH Public Key: R,E - SSH DH Shared Secret: R,E - SSH ECDH Private Key: R,E - SSH ECDH Public Key: R,E - SSH Peer ECDH Public Key: R,E - SSH ECDH Shared Secret: R,E - SSH RSA Private Key: R,E - SSH RSA Public Key: R,E - SSH ECDSA Private Key: R,E - SSH ECDSA Public Key: R,E - SSH Session Encryption Key: R,E - SSH Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication Key: R,E - DRBG Entropy Input: R,E - DRBG Seed: R,E - DRBG Internal State V value: R,E - DRBG Key: R,E - RADIUS Secret: W,E
Configure SSL over TLSv1.2 Function	Configure SSL over TLSv1.2 Function	Global Indicator and TLS v1.2 configuration success status message	Commands to configure TLSv1.2	Status of the completion of TLSv1.2 configuration	TLS RSA KeyGen TLS ECDSA KeyGen DRBG Function	Crypto Officer - TLS RSA Private Key: G,W - TLS RSA Public Key: G,W - TLS ECDSA Private Key: G,W - TLS ECDSA Public Key: G,W - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG Internal State V value: G,W,E - DRBG Key: G,W,E
Run SSL over TLSv1.2 Function	Execute SSL over TLSv1.2 Function	Global Indicator and successful TLS v1.2	Commands to initiate TLSv1.2	Status of the completion of TLSv1.2	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) TLS-KTS	Crypto Officer - TLS DH Private Key: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		log message		establishment	(AES and HMAC) TLS-KTS (AES-GCM) TLS RSA KeyGen TLS RSA SigGen TLS RSA SigVer TLS ECDSA KeyGen TLS ECDSA SigGen TLS ECDSA SigVer Block ciphers (TLSv1.2) MAC (TLSv1.2) DRBG Function TLS Keying Materials Development	- TLS DH Public Key: G,R,W,E,Z - TLS Peer DH Public Key: W,E,Z - TLS DH Shared Secret: G,W,E,Z - TLS ECDH Private Key: G,W,E,Z - TLS ECDH Public Key: G,R,W,E,Z - TLS Peer ECDH Public Key: W,E,Z - TLS ECDH Shared Secret: G,W,E,Z - TLS RSA Private Key: E - TLS RSA Public Key: R,E - TLS Master Secret: G,W,E,Z - TLS Session Encryption Key: G,W,E,Z - TLS Session Authentication Key: G,W,E,Z - DRBG Entropy Input: G,W,E - DRBG Seed: G,W,E - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Internal State V value: G,W,E - DRBG Key: G,W,E - TLS ECDSA Private Key: E - TLS ECDSA Public Key: R,E
Configure MACSec Function	Configure MACSec Function	Global Indicator and MACSec configuration on success status message	Commands to configure MACSec service	Status of the completion of MACSec configuration	MACSec-KTS (AES-KW) MACSec-KTS (AES-KWP) Block ciphers (MACSec) MACSec-SAK-Integrity	Crypto Officer - MACSec CAK: W,E - MACSec ICK: G,W,E,Z - MACSec SAK: G,W,E,Z - MACSec KEK: G,W,E,Z
Run MACSec Function	Execute MACSec Function	Global Indicator and successful MACSec log message	Commands to initiate MACSec service	Status of the completion of MACSec establishment	MACSec-KTS (AES-KW) MACSec-KTS (AES-KWP) Block ciphers (MACSec) MACSec-SAK-Integrity MACsec Keying Materials Development	Crypto Officer - MACSec CAK: W,E - MACSec ICK: G,W,E,Z - MACSec SAK: G,W,E,Z - MACSec KEK: G,W,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Configure SNMPv3 Function	Configure SNMPv3 Function	Global Indicator and SNMPv3 configuration success status message	Commands to configure SNMPv3 service	Status of the completion of SNMPv3 configuration	Block ciphers (SNMPv3) MAC (SNMPv3)	Crypto Officer - SNMPv3 Authentication Secret: W,E - SNMPv3 Encryption Key: G,W,E,Z - SNMPv3 Integrity Key: G,W,E,Z
Run SNMPv3 Function	Execute SNMPv3 Function	Global Indicator and successful SNMPv3 log message	Commands to initiate SNMPv3 service	Status of the completion of SNMPv3 establishment	Block ciphers (SNMPv3) MAC (SNMPv3) SNMPv3 Keying Materials Development	Crypto Officer - SNMPv3 Authentication Secret: W,E - SNMPv3 Encryption Key: G,W,E,Z - SNMPv3 Integrity Key: G,W,E,Z
Firmware Load Test	Execute the Firmware Load Test	Global indicator and successful Firmware Loading status message	Commands to load new firmware image	Outcome of the Firmware Load Test	Firmware Load Test	Crypto Officer - Firmware Load Test Key: E

Table 13: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module also supports the firmware load test by using RSA 2048 bits with SHA2-256 (RSA Cert. #A5076) for the new validated firmware to be uploaded into the module. A Firmware Load Test Key was preloaded to the module's binary at the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate to the module before loading the firmware. This ensures that unauthorized access and use of the module is not performed. The module will load the new update upon reboot. The update attempt will be rejected if the verification fails.

4.6 Additional Information

The module supports unauthenticated service. The unauthenticated User/Operators can trigger the self-test service by power-cycling the module, and is able to observe the module's LEDs status.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs the Firmware Integrity tests by using CRC-32 during the Pre-Operational Self-Test. At Module's initialization, the integrity of the runtime executable binary file (SPR10010dufi.bin) is verified using the following two integrity check mechanisms to ensure that the module has not been tampered:

- Bootloader Integrity Test (CRC-32)
- Firmware Integrity Test (CRC-32)

If at the load time the CRC-32 value does not match the stored, known CRC-32 value, the module would enter to an Error state with all crypto functionality inhibited.

In addition, the module also supports the firmware load test detailed in the "External Software/Firmware Loaded" section above.

5.2 Initiate on Demand

Integrity test is performed as part of the Pre-Operational Self-Tests. It is automatically executed at power-on. The operator can power-cycle or reboot the module to initiate the firmware integrity test on-demand. This automatically performs the integrity test of all firmware components included within the boundary of the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

The module is a multi-chip standalone hardware cryptographic module. The module meets the FIPS 140-3 Level 1 security requirements as production grade components.

8 Non-Invasive Security

No approved non-invasive attack mitigation test metrics are defined at this time.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
DRAM	Volatile Memory	Dynamic
Flash	Non-Volatile Memory	Static

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Peer Public Key Input	External (Outside of the Module's Boundary)	Module	Plaintext	Automated	Electronic	
Module Public Key Output	Module	External (Outside of the Module's Boundary)	Plaintext	Automated	Electronic	
Password/Secret Input via SSHv2 encrypted by AES and HMAC	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	SSH-KTS (AES and HMAC)
Password/Secret Input via TLS v1.2 encrypted by AES and HMAC	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	TLS-KTS (AES and HMAC)

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Password/Secret Input via TLS v1.2 encrypted by AES-GCM	External (Outside of the Module's Boundary)	Module	Encrypted	Automated	Electronic	TLS-KTS (AES-GCM)
MACSec SAK Output encrypted by MACSec KEK using AES-KW	Module	External (Outside of the Module's Boundary)	Encrypted	Automated	Electronic	MACSec-KTS (AES-KW)
MACSec SAK Output encrypted by MACSec KEK using AES-KWP	Module	External (Outside of the Module's Boundary)	Encrypted	Automated	Electronic	MACSec-KTS (AES-KWP)

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization Command	CO issues zeroization service	the zeroization command will erase all SSPs stored in the DRAM or in the Flash of the module.	'fips zeroize all' Command

Table 16: SSP Zeroization Methods

Please note that the Firmware Load Test Key is only used for Firmware Load Test Authentication and not subject to the zeroization requirement.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Entropy Input	Used to seed the DRBG	960 - at least 256 bits	Entropy Input - CSP			DRBG Function
DRBG Seed	Used in DRBG Generation	384 bits - 384 bits	DRBG Seed - CSP			DRBG Function

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Internal State V value	Used in DRBG Generation	128 bits - 128 bits	DRBG Internal State V value - CSP			DRBG Function
DRBG Key	Used in DRBG Generation	256 bits - 256 bits	DRBG Key - CSP			DRBG Function
User Password	User authentication	8-60 Characters - 8-60 Characters	Authentication Data - CSP			
Crypto Officer Password	Crypto Officer authentication	8-60 Characters - 8-60 Characters	Authentication Data - CSP			
Port Config Admin Password	Port Config Admin authentication	8-60 Characters - 8-60 Characters	Authentication Data - CSP			
RADIUS Secret	RADIUS Server Authentication	8-64 Characters - 8-64 Characters	Authentication Data - CSP			
Firmware Load Test Key	Used for Firmware Load Test	2048 bits - 112 bits	Public Key - CSP			Firmware Load Test
SSH ECDH Private Key	Used to derive the SSH ECDH Shared Secret	Curves: 256, 384, 521 bits - 128 to 256 bits	Private Key - CSP	KAS-ECC (SSHv2)		KAS-ECC (SSHv2)
SSH ECDH Public Key	Used to derive SSH ECDH Shared Secret	Curves: 256, 384, 521 bits - 128-256 bits	Public Key - PSP		KAS-ECC (SSHv2)	
SSH Peer ECDH Public Key	Used to derive SSH ECDH Shared Secret	Curves: 256, 384, 521 bits - 128 to 256 bits	Public Key - PSP			KAS-ECC (SSHv2)
SSH ECDH Shared Secret	Used to derive SSH Session	Curves: 256, 384, 521 bits -	Shared Secret - CSP		KAS-ECC (SSHv2)	KAS-ECC (SSHv2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Encryption Keys, SSH Session Authentication Keys	128 to 256 bits				
SSH DH Private Key	Used to derive the SSH DH Shared Secret	MODP-2048, MODP-4096, MODP-8192 - 112-200 bits	Private Key - CSP	KAS-FFC (SSHv2)		KAS-FFC (SSHv2)
SSH DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-4096, MODP-8192 - 112-200 bits	Public Key - PSP		KAS-FFC (SSHv2)	
SSH Peer DH Public Key	Used to derive SSH DH Shared Secret	MODP-2048, MODP-4096, MODP-8192 - 112-200 bits	Public Key - PSP			KAS-FFC (SSHv2)
SSH DH Shared Secret	Used to derive SSH Session Encryption Keys, SSH Session Authentication Keys	MODP-2048, MODP-4096, MODP-8192 - 112-200 bits	Shared Secret - CSP		KAS-FFC (SSHv2)	KAS-FFC (SSHv2)
SSH RSA Private Key	Used for SSH session authentication	Modulus 2048 bits - 112 bits	Private Key - CSP	SSH RSA KeyGen		SSH RSA SigGen
SSH RSA Public Key	Used for SSH sessions authentication	Modulus 2048 bits - 112 bits	Public Key - PSP		SSH RSA KeyGen	

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SSH ECDSA Private Key	Used for SSH session authentication	Curve P-256/P-384 - 128-192 bits	Private Key - CSP	SSH ECDSA KeyGen		SSH ECDSA SigGen
SSH ECDSA Public Key	Used for SSH sessions authentication	Curve P-256/P-384 - 128-192 bits	Public Key - PSP		SSH ECDSA KeyGen	
SSH Session Encryption Key	Used for SSH Session confidentiality protection	128-256 bits - 128-256 bits	Session Key - CSP		KAS-ECC (SSHv2) KAS-FFC (SSHv2)	Block ciphers (SSHv2)
SSH Session Authentication Key	Used for SSH Session integrity protection	At least 160 bits - At least 160 bits	Session Key - CSP		KAS-ECC (SSHv2) KAS-FFC (SSHv2)	MAC (SSHv2)
TLS ECDH Private Key	Used to derive the TLS ECDH Shared Secret	Curves: 256, 384 bits - 128 to 192 bits	Private Key - CSP	KAS-ECC (TLSv1.2)		KAS-ECC (TLSv1.2)
TLS ECDH Public Key	Used to derive TLS ECDH Shared Secret	Curves: 256, 384 bits - 128 to 192 bits	Public Key - PSP		KAS-ECC (TLSv1.2)	
TLS Peer ECDH Public Key	Used to derive TLS ECDH Shared Secret	Curves: 256, 384 bits - 128 to 192 bits	Public Key - PSP			KAS-ECC (TLSv1.2)
TLS ECDH Shared Secret	Used to derive TLS Session Encryption Keys, TLS Session Authentication Keys	Curves: 256, 384 bits - 128 to 192 bits	Shared Secret - CSP		KAS-ECC (TLSv1.2)	KAS-ECC (TLSv1.2)
TLS DH Private Key	Used to derive the TLS DH Shared Secret	ffdhe2048 - 112 bits	Private Key - CSP	KAS-FFC (TLSv1.2)		KAS-FFC (TLSv1.2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS DH Public Key	Used to derive TLS DH Shared Secret	ffdhe2048 - 112 bits	Public Key - PSP		KAS-FFC (TLSv1.2)	
TLS Peer DH Public Key	Used to derive TLS DH Shared Secret	ffdhe2048 - 112 bits	Public Key - PSP			KAS-FFC (TLSv1.2)
TLS DH Shared Secret	Used to derive TLS Session Encryption Keys, TLS Session Authentication Keys	ffdhe2048 - 112 bits	Shared Secret - CSP		KAS-FFC (TLSv1.2)	KAS-FFC (TLSv1.2)
TLS RSA Private Key	Used for TLS session authentication	Modulus 2048 bits - 112 bits	Private Key - CSP	TLS RSA KeyGen		TLS RSA SigGen
TLS RSA Public Key	Used for TLS sessions authentication	Modulus 2048 bits - 112 bits	Public Key - PSP		TLS RSA KeyGen	
TLS ECDSA Private Key	Used for TLS session authentication	Curve P-256/P-384 - 128-192 bits	Private Key - CSP	TLS ECDSA KeyGen		TLS ECDSA SigGen
TLS ECDSA Public Key	Used for TLS sessions authentication	Curve P-256/P-384 - 128-192 bits	Public Key - PSP		TLS ECDSA KeyGen	
TLS Master Secret	Used to protect TLS Session. Pre-master secret	At least 112 bits - At least 112 bits	Master Secret - CSP		TLS Keying Materials Development	KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2)
TLS Session Encryption Key	Used to protect TLS Session. TLS Master secret	128-256 bits - 128-256 bits	Session Key - CSP		KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) TLS Keying Materials	Block ciphers (TLSv1.2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
					Development	
TLS Session Authentication Key	Used to protect TLS Session. TLS master secret	at least 112 bits - at least 112 bits	Session Key - CSP		KAS-ECC (TLSv1.2) KAS-FFC (TLSv1.2) TLS Keying Materials Development	MAC (TLSv1.2)
SNMPv3 Authentication Secret	Used for SNMPv3 user authentication	8-20 characters - N/A	Authentication Secret - CSP			
SNMPv3 Encryption Key	Used to protect SNMPv3 traffic confidentiality	128 bits - 128 bits	Encryption Key - CSP		SNMPv3 Keying Materials Development	Block ciphers (SNMPv3)
SNMPv3 Integrity Key	Used to secure SNMPv3 traffic integrity	At least 160 bits - At least 112 bits	Authentication Key - CSP		SNMPv3 Keying Materials Development	MAC (SNMPv3)
MACSec CAK	Used to derive MACSec ICK and MACSec KEK	128 bits - N/A	MACSec Secret - CSP			MACsec Keying Materials Development
MACSec ICK	Used to protect the MACSec Integrity	128 bits - 128 bits	Integrity Key - CSP		MACsec Keying Materials Development	MACSec-SAK-Integrity AES-CMAC (A5076)
MACSec SAK	Used to protect the MACSec traffic confidentiality	128 bits - 128 bits	Encryption Key - CSP		MACSec-KTS (AES-KW) MACSec-KTS (AES-KWP) TLS Keying Materials	Block ciphers (MACSec)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
					Development MACSec-SAK-Integrity	
MACSec KEK	Used to transport MACSec SAK to Peer	128 bits - 128 bits	Encryption Key - CSP		MACsec Keying Materials Development	MACSec-KTS (AES-KW) MACSec-KTS (AES-KWP)

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Entropy Input		DRAM:Plaintext	Until Reboot	Zeroization Command	DRBG Seed:Used With DRBG Internal State V value:Used With DRBG Key:Used With
DRBG Seed		DRAM:Plaintext	Until Reboot	Zeroization Command	DRBG Entropy Input:Used With DRBG Internal State V value:Used With DRBG Key:Used With
DRBG Internal State V value		DRAM:Plaintext	Until Reboot	Zeroization Command	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Key:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Key		DRAM:Plaintext	Until Reboot	Zeroization Command	DRBG Entropy Input:Used With DRBG Seed:Used With DRBG Internal State V value:Used With
User Password	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via TLS v1.2 encrypted by AES and HMAC Password/Secret Input via TLS v1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	
Crypto Officer Password	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via TLS v1.2 encrypted by AES and HMAC Password/Secret Input via TLS v1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	
Port Config Admin Password	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via TLS v1.2 encrypted	Flash:Plaintext		Zeroization Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	by AES and HMAC Password/Secret Input via TLS v1.2 encrypted by AES-GCM				
RADIUS Secret	Password/Secret Input via SSHv2 encrypted by AES and HMAC Password/Secret Input via TLS v1.2 encrypted by AES and HMAC Password/Secret Input via TLS v1.2 encrypted by AES-GCM	Flash:Plaintext		Zeroization Command	
Firmware Load Test Key		Flash:Plaintext		N/A	
SSH ECDH Private Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH ECDH Public Key:Paired With SSH Peer ECDH Public Key:Used With
SSH ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH ECDH Private Key:Paired With
SSH Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH ECDH Private Key:Used With
SSH ECDH Shared Secret		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH ECDH Private Key:Derived From SSH ECDH Public Key:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH DH Private Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH DH Public Key:Paired With SSH Peer DH Public Key:Used With
SSH DH Public Key	Module Public Key Output	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH DH Private Key:Paired With
SSH Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH DH Private Key:Used With
SSH DH Shared Secret		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH DH Private Key:Derived From SSH DH Public Key:Derived From
SSH RSA Private Key		Flash:Plaintext		Zeroization Command	SSH RSA Public Key:Paired With
SSH RSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	SSH RSA Private Key:Paired With
SSH ECDSA Private Key		Flash:Plaintext		Zeroization Command	SSH ECDSA Public Key:Paired With
SSH ECDSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	SSH ECDSA Private Key:Paired With
SSH Session Encryption Key		DRAM:Plaintext	While SSH tunnel is on	Zeroization Command	SSH Session Authentication Key:Used With
SSH Session Authentication Key		DRAM:Plaintext	While SSH	Zeroization Command	SSH Session Encryption

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			tunnel is on		Key:Used With
TLS ECDH Private Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS ECDH Public Key:Paired With TLS Peer ECDH Public Key:Used With
TLS ECDH Public Key	Module Public Key Output	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS ECDH Private Key:Paired With
TLS Peer ECDH Public Key	Peer Public Key Input	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS ECDH Private Key:Used With
TLS ECDH Shared Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS ECDH Private Key:Derived From TLS ECDH Public Key:Derived From
TLS DH Private Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS DH Public Key:Paired With TLS Peer DH Public Key:Used With
TLS DH Public Key	Module Public Key Output	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS DH Private Key:Paired With
TLS Peer DH Public Key	Peer Public Key Input	DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS DH Private Key:Used With
TLS DH Shared Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS DH Private Key:Derived From TLS DH

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Public Key:Derived From
TLS RSA Private Key		Flash:Plaintext		Zeroization Command	TLS RSA Public Key:Paired With
TLS RSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	TLS RSA Private Key:Paired With
TLS ECDSA Private Key		Flash:Plaintext		Zeroization Command	TLS ECDSA Public Key:Paired With
TLS ECDSA Public Key	Module Public Key Output	Flash:Plaintext		Zeroization Command	TLS ECDSA Private Key:Paired With
TLS Master Secret		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS ECDH Shared Secret:Derived From
TLS Session Encryption Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS Session Authentication Key:Used With
TLS Session Authentication Key		DRAM:Plaintext	While TLS tunnel is on	Zeroization Command	TLS Session Encryption Key:Used With
SNMPv3 Authentication Secret	Password/Secret Input via SSHv2 encrypted by AES and HMAC	DRAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command	SNMPv3 Encryption Key:Derive To SNMPv3 Integrity Key:Derive To
SNMPv3 Encryption Key		DRAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command	SNMPv3 Authentication Secret:Derived From
SNMPv3 Integrity Key		DRAM:Plaintext	While SNMPv3 tunnel is on	Zeroization Command	SNMPv3 Authentication Secret:Derived From SNMPv3 Encryption

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					Key:Used With
MACSec CAK	Password/Secret Input via SSHv2 encrypted by AES and HMAC	Flash:Plaintext	Until Zeroized	Zeroization Command	MACSec ICK:Derived From MACSec SAK:Derived From MACSec KEK:Derived From
MACSec ICK		DRAM:Plaintext	While MACSec session is on	Zeroization Command	MACSec KEK:Used With
MACSec SAK	MACSec SAK Output encrypted by MACSec KEK using AES-KW MACSec SAK Output encrypted by MACSec KEK using AES-KWP	DRAM:Plaintext	While MACSec session is on	Zeroization Command	MACSec CAK:Derived From
MACSec KEK		DRAM:Plaintext	While MACSec session is on	Zeroization Command	MACSec SAK:Encrypts

Table 18: SSP Table 2

9.5 Transitions

The module includes an implementation of SHA-1 for hashing and message authentication. This implementation will be non-Approved for all uses starting January 1, 2031. User should move to SHA2, which is available in this module."

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
CRC-32 (Bootloader)	N/A	KAT	SW/FW Integrity	Module is in normal state	The module performs the Bootloader integrity test

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
					by using CRC-32 at the power up
CRC-32 (Firmware)	N/A	KAT	SW/FW Integrity	Module is in normal state	The module performs the Firmware integrity test by using CRC-32 at the power up

Table 19: Pre-Operational Self-Tests

The modules perform the self-tests, including the pre-operational self-tests and conditional self-tests. The module runs all self-tests without operator intervention. In the event that a self-test fails, the module will enter an error state, output an error message and follow up with a module reboot. The module permits operators to initiate the pre-operational or conditional self-tests on demand for periodic testing of the module by rebooting the system (i.e., power-cycling).

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt KAT (A5076)	128 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CBC Decrypt KAT (A5076)	128 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
AES-GCM Authenticated Encrypt KAT (A5076)	128 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-GCM Authenticated Decrypt KAT (A5076)	128 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
AES-CMAC Encrypt KAT (A5076)	128 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up
AES-CMAC Decrypt KAT (5076)	128 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
Counter DRBG Instantiate/Generate/Reseed KAT (A5076)	AES-128	KAT	CAST	Module is in normal state	Instantiate, Generate, and Reseed KATs	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA-1 KAT (A5076)	SHA-1	KAT	CAST	Module is in normal state	HMAC-SHA-1	Power Up
HMAC-SHA2-256 KAT (A5076)	SHA2-256	KAT	CAST	Module is in normal state	HMAC-SHA2-256	Power Up
HMAC-SHA2-384 KAT (A5076)	SHA2-384	KAT	CAST	Module is in normal state	HMAC-SHA2-384	Power Up
HMAC-SHA2-512 KAT (A5076)	SHA2-512	KAT	CAST	Module is in normal state	HMAC-SHA2-512	Power Up
KAS-ECC-SSC Sp800-56Ar3 KAT (A5076)	P-256 Curve	KAT	CAST	Module is in normal state	Primitive Z KAT	Power Up
KAS-FFC-SSC Sp800-56Ar3 KAT (A5076)	MODP-2048	KAT	CAST	Module is in normal state	Primitive Z KAT	Power Up
ECDSA SigGen (FIPS186-5) KAT (A5076)	Curve P-256	KAT	CAST	Module is in normal state	N/A	Power Up
ECDSA SigVer (FIPS186-5) KAT (A5076)	Curve P-256	KAT	CAST	Module is in normal state	N/A	Power Up
RSA SigGen (FIPS186-5) KAT (A5076)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigGen KAT	Power Up
RSA SigVer (FIPS186-5) KAT (A5076)	2048 bit modulus with SHA2-256	KAT	CAST	Module is in normal state	RSA SigVer KAT	Power Up
KDF SNMP KAT (A5076)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF SSH KAT (A5076)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
TLS v1.2 KDF RFC7627 KAT (A5076)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
SHA-1 KAT (A5076)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
SHA2-256 KAT (A5076)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
SHA2-384 KAT (A5076)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
SHA2-512 KAT (A5076)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
ECDSA KeyGen (FIPS186-5) PCT (A5076)	Curve P-256	PCT	PCT	Module is in normal state	N/A	Performs all required pair-wise consistency tests on the newly generated keypairs before the first operational use.
RSA KeyGen (FIPS186-5) PCT (A5076)	2048 bit Modulus	PCT	PCT	Module is in normal state	RSA	Performs all required pair-wise consistency tests on the newly generated

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
						key pairs before the first operational use.
KAS-ECC-SSC Sp800-56Ar3 PCT (A5076)	Curve P-256 with SHA2-256	PCT	PCT	Module is in normal state	N/A	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
KAS-FFC-SSC Sp800-56Ar3 PCT (A5076)	MODP-2048	PCT	PCT	Module is in normal state	N/A	Performs all required pair-wise consistency tests on the newly generated key pairs before the first operational use.
RSA SigVer (FIPS186-5) Firmware Load Test	2048 bits with SHA2-256	KAT	SW/FW Load	Module is in normal state	N/A	When firmware has been uploaded to the module
KDF-SP800-108 KAT (A5076)	N/A	KAT	CAST	Module is in normal state	N/A	Power Up
AES-GCM Authenticated Encrypt KAT (AES 4550)	128 bits	KAT	CAST	Module is in normal state	Encrypt	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM Authenticated Decrypt KAT (AES 4550)	128 bits	KAT	CAST	Module is in normal state	Decrypt	Power Up
Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Power Up
Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source	Power Up
Entropy 90B Continuous Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	Module is in normal state	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long	Entropy data is generated from the Entropy Source - Continuous

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					period of time	
Entropy 90B Continuous Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	Module is in normal state	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source	Entropy data is generated from the Entropy Source - Continuous

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
CRC-32 (Bootloader)	KAT	SW/FW Integrity	Recommend 60 Days	Reboot
CRC-32 (Firmware)	KAT	SW/FW Integrity	Recommend 60 Days	Reboot

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
AES-CBC Decrypt KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
AES-GCM Authenticated Encrypt KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
AES-GCM Authenticated Decrypt KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
AES-CMAC Encrypt KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
AES-CMAC Decrypt KAT (5076)	KAT	CAST	Recommend 60 Days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG Instantiate/Generate/Reseed KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA-1 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-256 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-384 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
HMAC-SHA2-512 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
KAS-FFC-SSC Sp800-56Ar3 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
ECDSA SigGen (FIPS186-5) KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
ECDSA SigVer (FIPS186-5) KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
RSA SigGen (FIPS186-5) KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
RSA SigVer (FIPS186-5) KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
KDF SNMP KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
KDF SSH KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
TLS v1.2 KDF RFC7627 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
SHA-1 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
SHA2-256 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
SHA2-384 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
SHA2-512 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
ECDSA KeyGen (FIPS186-5) PCT (A5076)	PCT	PCT	Recommend 60 Days	Reboot
RSA KeyGen (FIPS186-5) PCT (A5076)	PCT	PCT	Recommend 60 Days	Reboot
KAS-ECC-SSC Sp800-56Ar3 PCT (A5076)	PCT	PCT	Recommend 60 Days	Reboot
KAS-FFC-SSC Sp800-56Ar3 PCT (A5076)	PCT	PCT	Recommend 60 Days	Reboot
RSA SigVer (FIPS186-5) Firmware Load Test	KAT	SW/FW Load	Recommend 60 Days	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDF-SP800-108 KAT (A5076)	KAT	CAST	Recommend 60 Days	Reboot
AES-GCM Authenticated Encrypt KAT (AES 4550)	KAT	CAST	Recommend 60 Days	Reboot
AES-GCM Authenticated Decrypt KAT (AES 4550)	KAT	CAST	Recommend 60 Days	Reboot
Entropy 90B Start-up Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
Entropy 90B Start-up Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A
Entropy 90B Continuous Repetition Count Test (RCT)	RCT	CAST	N/A	N/A
Entropy 90B Continuous Adaptive Proportion Test (APT)	APT	CAST	N/A	N/A

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	If self-test tests fail, the module is put into an error state	Self-test failure	Reboot the module	System Halt

Table 23: Error States

If any of the above-mentioned self-tests fail, the module reports the cause of the error and enters an error state. In the Error State, no cryptographic services are provided, and data output is prohibited. The only method to recover from the error state is to reboot the module and reperforming the self-tests, including the pre-operational software integrity test and the conditional CASTs. The module will only enter into the operational state after successfully passing the pre-operational firmware integrity test and the conditional CASTs. The table below shows the different causes that lead to the Error State and the status indicators reported.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module meets all the Level 1 requirements for FIPS 140-3. Follow the secure operations provided below to place the module in approved mode. Operating this module without maintaining the following settings will put the module operate in a non-compliant state.

The module runs firmware version IronWare OS 10.0.10. This is the only allowable firmware image for this current approved mode of operation. The Crypto Officer shall load the FIPS 140-3 validated firmware only to maintain validation. Any firmware/software loaded into this module

that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-3 validation.

The module is initiated into the approved mode of operation via the following procedures through the Command Line interface (CLI):

1. The Crypto Officer must login by using the default login password.
2. The Crypto Officer shall replace the default login password with a new one.
3. Enter into the configuration mode by using ‘conf t’ command.
4. Enable approved mode by using ‘fips enable’ command.
5. Create accounts for Port Config Admin role and User role respectively.
6. Configure SSH, TLS, SNMPv3 and MACSec services by using only approved algorithms listed above.
7. Configure the module as the MACSec Peer Authenticator in the MACSec service.
8. If using RADIUS server for roles authentication, please configure a secure TLS tunnel to secure traffic between the module and the RADIUS server. The RADIUS shared secret must be at least 8 characters long.
9. Disable the TFTP server.
10. Ensure that installed digital certificates are signed using approved algorithms.
11. Save the configuration.
12. Reload the module.
13. Verify the approved mode by using command ‘fips show’ (This command outputs the module’s status. After the approved mode was enabled, the output would be “approved *mode: Administrative status ON*”).
14. The Crypto Officer shall load the FIPS 140-3 validated firmware only to maintain validation.

Once the module has completed initialization into the approved mode of operation, the module automatically enforces a password change for the Crypto Officer. Any non-approved algorithms or security functions are rejected automatically by the module and an error message is output.

11.2 Administrator Guidance

No specific Administrator guidance.

11.3 Non-Administrator Guidance

No specific Non-Administrator guidance.

11.4 End of Life

Crypto Officers should follow the procedure below for the secure destruction of their module:

Note: This process will cause the module to no longer function after it has wiped all configurations and keys.

1. Access the module via SSH with Crypto Officer
2. Authenticate using proper credentials
3. Execute command: “fips zeroize all”
   a. Confirm command

Module will begin zeroization process and wipe all security parameters and configurations

12 Mitigation of Other Attacks

N/A for this module.