Ruckus FastIron ICX™ 7450 Series Switch/Router
Firmware Version: IronWare OS 09.0.10

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.5

Last Update Date: 10-04-2024

Prepared by:
Ruckus Wireless LLC
Salarpuria Supreme, #137, Marathahalli
Bangalore, Karnataka 560037
India
www.commscope.com

Table of Contents

1. General

This is a non-proprietary cryptographic module security policy for Ruckus FastIron ICX™ 7450 Series Switch/Router (hereinafter referred to as the module). The firmware version running on each module is IronWare OS 09.0.10. 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.

The table below indicates the actual security levels for each area of the module.

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	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

Table 1 - Security Levels

The module is designed to meet an overall security level 1.

2. Cryptographic Module Specification

Cryptographic Boundary

The module is a hardware, multi-chip standalone cryptographic module. The cryptographic boundary is defined as the module's chassis unit encompassing the "top," "front," "left," "right," "rear" and "bottom" surfaces of the case representing the module's physical perimeter. This section illustrates the module hardware with the help of photographs.

Figure 1 - Front/top side of ICX7450-48P with IPSec module inserted

Figure 2 - Back side of ICX7450-48P with IPSec module inserted

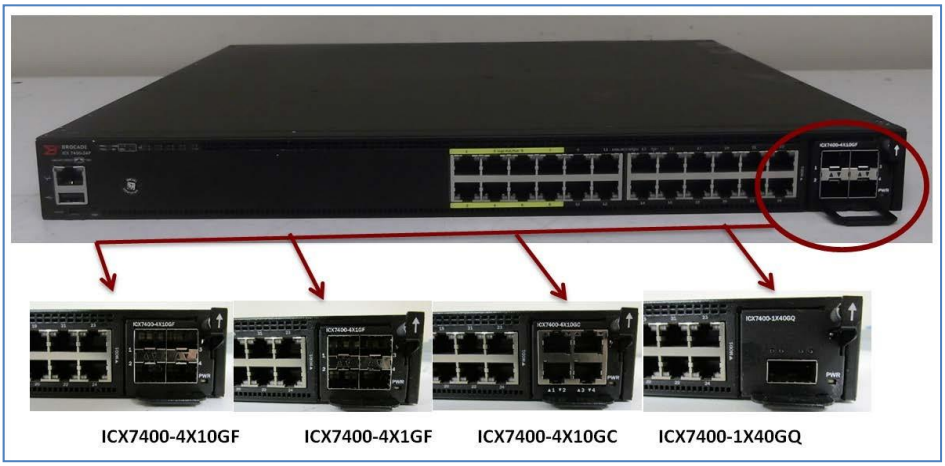


Figure 3 - Front/top side of ICX7450-24P with ICX7400-4X10GF, ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-1X40GQ and ICX7400-SERVICE MOD

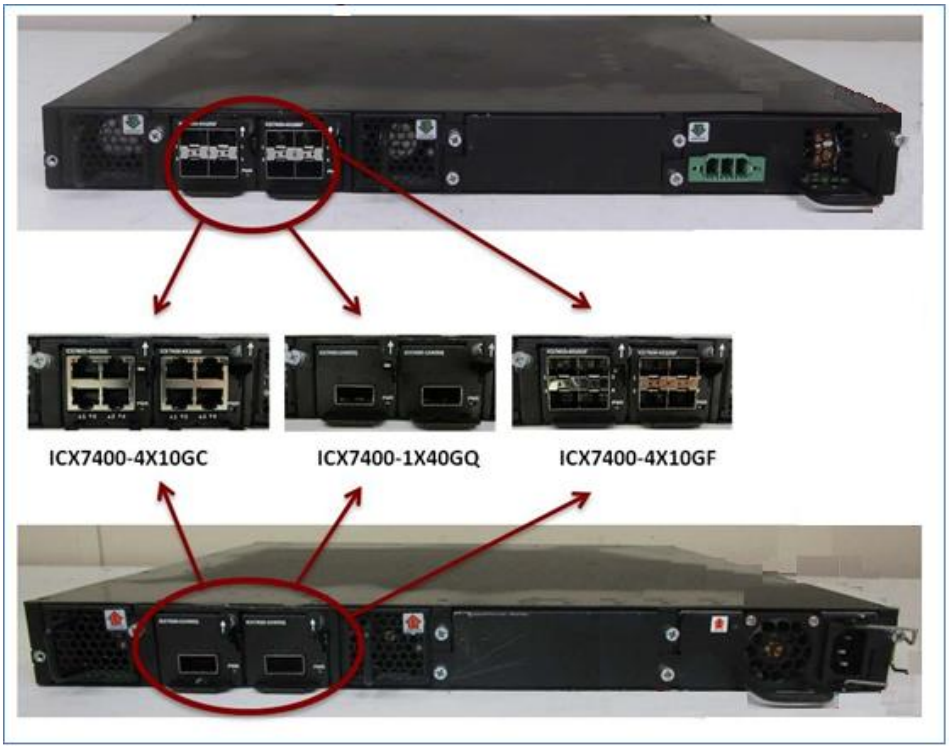


Figure 4- Back side of ICX7450-24P with ICX7400-4X10GC, ICX7400-1X40GQ and ICX7400-4X10GF

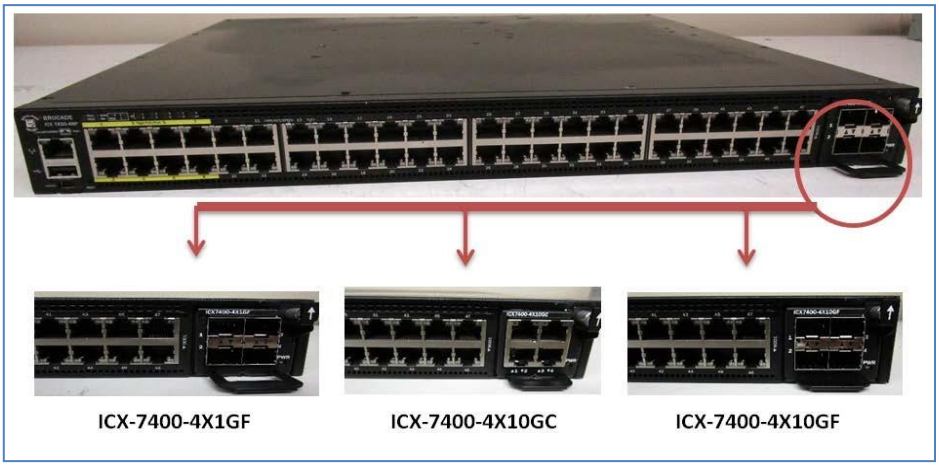
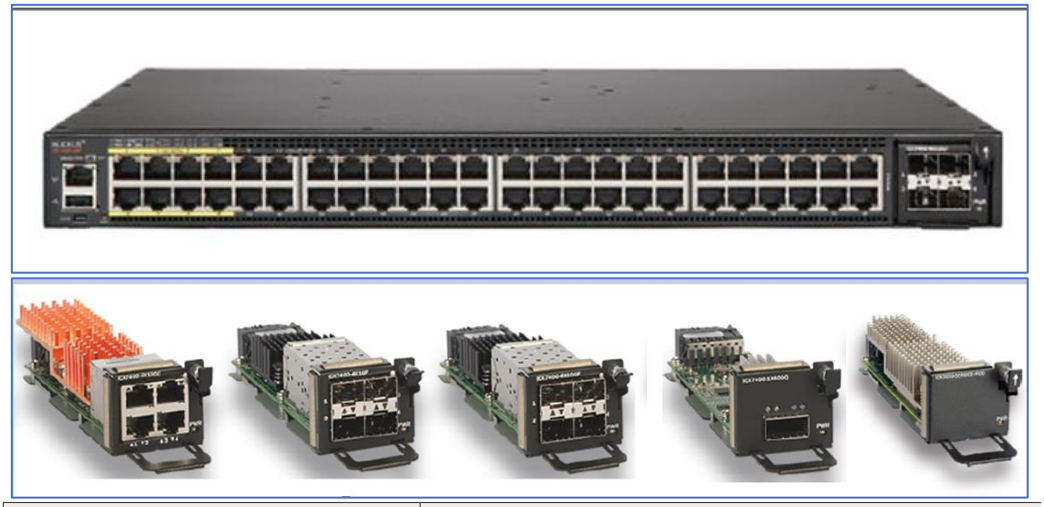


Figure 5 - Front/top side of ICX7450-48P with ICX74004X1GF, ICX7400-4X10GC and ICX7400-4X10GF



RUCKUS ICX7400-4X1GF Module	4-port 100 Mbps/1 GbE SFP
RUCKUS ICX7400-4X10GF Module	4-port 1/10 GbE SFP/SFP+ for uplink or stacking
RUCKUS ICX7400-4X10GC Module	4-port 1/10 GbE 10GBASE-T copper
RUCKUS ICX7400-1X40GQ Module	1-port 40 GbE QSFP+ for uplink or stacking
RUCKUS ICX7400-SERVICE-MOD Module	Service module for IPsec VPN encryption

Figure 6 - ICX7450-48P with ICX7400-4X1GF, ICX7400-4X10GF, ICX7400-4X10GC, ICX7400-1X40GQ, ICX7400-SERVICE-MOD

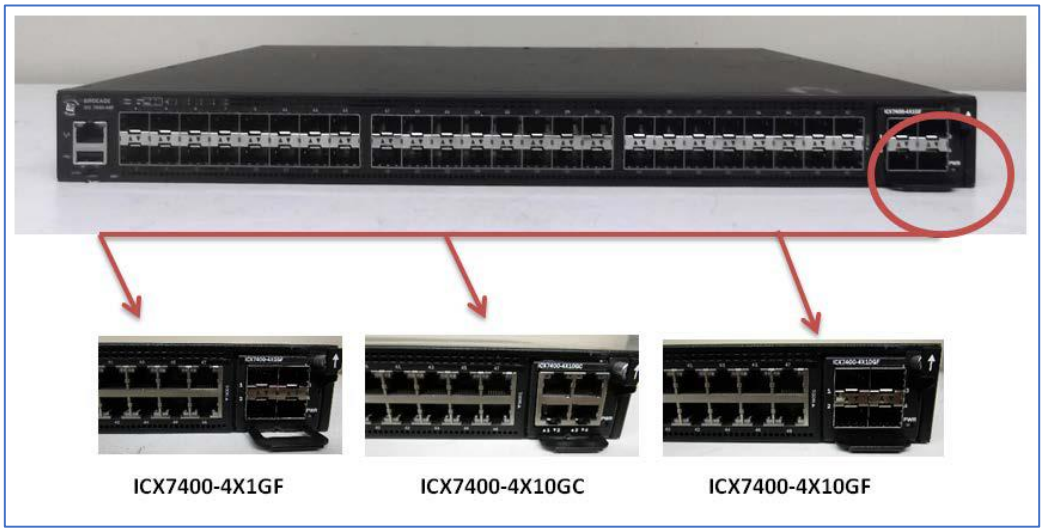


Figure 7 - Front/top side of ICX7450-48F with ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-4X10GF

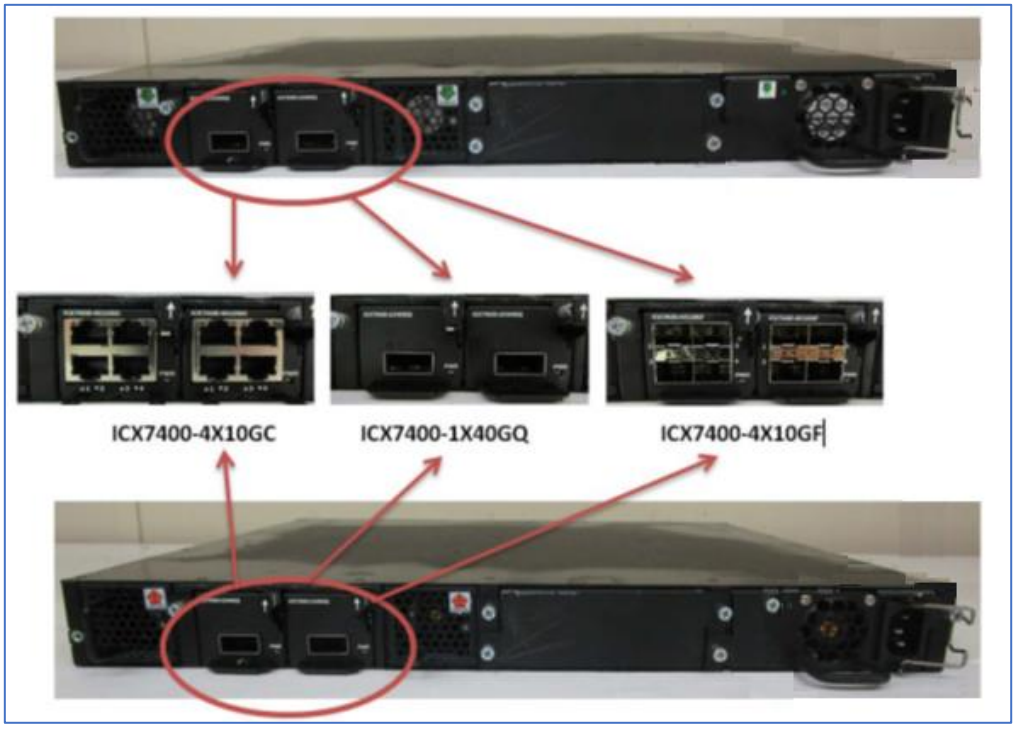


Figure 8 - Back side of ICX7450-48F with ICX7400-4X10GC, ICX7400-1X40GQ and ICX7400-4X10GF

The module delivers the performance, flexibility, and scalability required for enterprise access deployment. Table 2 below lists the model and firmware version included in this validation.

Hardware Model	Hardware [Part Numbers and Versions]	Firmware Version	Distinguishing Features
ICX7450-24P	ICX7450-24P-E2 with [ICX7400-4X1GF, ICX7400-4X10GF, ICX7400-4X10GC, ICX7400-1X40GQ, ICX7400-SERVICE-MOD]	IronWare OS 09.0.10	ICX7450-24P module has the following physical ports: • 1x RJ-45 Ethernet Mgmt port • 1x USB Type-C serial console port • 24x 10/100/1000 Mbps RJ-45 PoE+ ports In addition, each of the network modules has the following physical ports: • 4x 1GbE SFP ports on ICX7400-4X1GF • 4x 1GbE uplink/stacking SFP+ ports on ICX7400-4X10GF • 4x 1GbE 10GBASE-T copper Ethernet ports on ICX7400-4X10GC • 1x 4 GbE uplink/stacking QSFP+ ports on ICX7400-1X40GQ Please refer to Cryptographic Module Interfaces section for more information

Hardware Model	Hardware [Part Numbers and Versions]	Firmware Version	Distinguishing Features
ICX7450-48P	ICX7450-48P-E2 with [ICX7400-4X1GF, ICX7400-4X10GF, ICX7400-4X10GC, ICX7400-1X40GQ, ICX7400-SERVICE-MOD]	IronWare OS 09.0.10	ICX7450-48P module has the following physical ports: • 1x RJ-45 Ethernet Mgmt port • 1x USB Type-C serial console port • 48x 10/100/1000 Mbps RJ-45 PoE+ ports In addition, each of the network modules has the following physical ports: • 4x 1GbE SFP ports on ICX7400-4X1GF • 4x 1GbE uplink/stacking SFP+ ports on ICX7400-4X10GF • 4x 1GbE 10GBASE-T copper Ethernet ports on ICX7400-4X10GC • 1x 4 GbE uplink/stacking QSFP+ ports on ICX7400-1X40GQ Please refer to Cryptographic Module Interfaces section for more information
ICX7450-48F	ICX7450-48F-E2 with [ICX7400-4X1GF, ICX7400-4X10GF, ICX7400-4X10GC, ICX7400-1X40GQ, ICX7400-SERVICE-MOD]	IronWare OS 09.0.10	ICX7450-48F module has the following physical ports: • 1x RJ-45 Ethernet Mgmt port • 1x USB Type-C serial console port • 48x 1GbE SFP ports In addition, each of the network modules has the following physical ports: • 4x 1GbE SFP ports on ICX7400-4X1GF • 4x 1GbE uplink/stacking SFP+ ports on ICX7400-4X10GF • 4x 1GbE 10GBASE-T copper Ethernet ports on ICX7400-4X10GC • 1x 4 GbE uplink/stacking QSFP+ ports on ICX7400-1X40GQ Please refer to Cryptographic Module Interfaces section for more information

Table 2 – Tested Operational Environments

Modes of Operation

By default, the module is delivered with a non-approved mode of operation 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 "Secure Operation" 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.

The tables below list all approved or vendor-affirmed security functions of the module, including specific key size(s) (in bits unless noted otherwise) employed for Approved services, and implemented modes of operation. There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in these tables.

Approved Security Functions

The module implements the following approved cryptographic algorithms that have been ACVP certified.

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function /Notes
#A2345	AES • FIPS197 • SP800-38A	AES-ECB	128 and 256 bits	Data Encryption/Decryption
#A2345	AES • FIPS197 • SP800-38A	AES-CBC	128 and 256 bits	Data Encryption/Decryption
#A2345	AES • FIPS197 • SP800-38A	AES-CFB128	128 and 256 bits	Data Encryption/Decryption
#A2345	AES • FIPS197 • SP800-38A	AES-CTR	128 and 256 bits	Data Encryption/Decryption
#A2345	AES • FIPS197 • SP 800-38D	AES-GCM	128 and 256 bits	Authenticated Encryption/Decryption
#A2345	AES • FIPS197 • FIPS800-38B	AES-CMAC	128 bits	Assurance of the authenticity
#A2345	AES • SP800-38F	AES-KW	128 bits	Authenticated Encryption/Decryption
#A2345	AES • SP800-38F	AES-KWP	128 bits	Authenticated Encryption/Decryption
#A2345	DRBG • SP800-90Arev1	CTR_DRBG (AES-256 bits)	N/A	Deterministic Random Bit Generation
#A2345	ECDSA • FIPS186-4	ECDSA KeyGen	Curves: P-256, P-384	ECDSA Key Generation
#A2345	ECDSA • FIPS186-4	ECDSA SigGen	Curves: P-256, P-384	ECDSA Digital Signature Generation

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function /Notes
#A2345	ECDSA • FIPS186-4	ECDSA SigVer	Curves: P-256, P-384	ECDSA Digital Signature Verification
#A2345	KAS-ECC-SSC • SP800-56Arev3	KAS-ECC-SSC Scheme: Ephemeral Unified	KAS-ECC-SSC with Curves P-256, P-384, P-521	KAS-ECC Shared Secret Computation
#A2345	KAS • SP800-56Arev3	KAS (ECC) Scheme: ephemeralUnified KAS Role: initiator, responderP KAS (KAS-SSC Cert. #A2345, CVL Cert. #A2345	KAS-ECC with Curves P-256, P-384, P-521; Key establishment methodology provides between 128 and 256 bits of encryption strength	Key Agreement Scheme per SP800-56Arev3 with key derivation function (SP800-135rev1) Note: The module's KAS (ECC) implementation is FIPS140-3 IG D.F Scenario 2 (path 2) compliant
#A2345	KAS-FFC-SSC • SP800-56Arev3	KAS-FFC-SSC Scheme: dhEphem	MODP-2048, MODP-4096, MODP-8192	KAS-FFC Shared Secret Computation
#A2345	KAS • SP800-56Arev3	KAS (FFC) Scheme: dhEphem KAS (KAS-SSC Cert. #A2345, CVL Cert. #A2345	KAS-FFC with MODP-2048, MODP-4096, MODP-8192 Key establishment methodology provides between 112 and 200 bits of encryption strength	Key Agreement Scheme per SP800-56Arev3 with key derivation function (SP800-135rev1) Note: The module's KAS (ECC) implementation is FIPS140-3 IG D.F Scenario 2 (path 2) compliant
#A2345	KBKDF • SP800-108rev1	KDF Mode: Counter	N/A	SP800-108Rev1 Compliant Key Derivation Function (KDF)
#A2345	KDF SSH (CVL) • SP800-135rev1	SSHv2 KDF	N/A	SP800-135Rev1 Compliant Key Derivation Function (KDF) for SSHv2
#A2345	KDF TLS (CVL) • SP800-135rev1	TLSv1.1/1.2 KDF	N/A	SP800-135rev1 Compliant Key Derivation Function (KDF) for TLSv1.1/1.2
#A2345	KDF SNMP (CVL) • SP800-135rev1	SNMPv3 KDF	N/A	SP800-135rev1 Compliant Key Derivation Function (KDF) for SNMPv3
#A2345	KDF IKEv2 (CVL) • SP800-135rev1	IKEv2 KDF	N/A	SP800-135rev1 Compliant Key Derivation Function (KDF) for IKEv2

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function /Notes
#A2345	KTS (MACSec) • SP800-38F	KTS (AES Cert. #A2345)	Key establishment methodology provides 128 bits of encryption strength	Key Transport using AES-KW/KWP in MACSec
#A2345	KTS (SSH) SP800-38F	KTS (AES Cert. #A2345 and HMAC Cert. #A2345)	Key establishment methodology provides 128 or 256 bits of encryption strength	Key Transport using AES and HMAC in SSH
#A2345	KTS (TLS) • SP800-38F	KTS (AES Cert. #A2345 and HMAC Cert. #A2345)	Key establishment methodology provides 128 or 256 bits of encryption strength	Key Transport using AES and HMAC in TLS
#A2345	KTS (TLS) • SP800-38F	KTS (AES-GCM Cert. #A2345)	Key establishment methodology provides 128 or 256 bits of encryption strength	Key Transport using AES-GCM in TLS
#A2345	SHS • FIPS180-4	SHA-1 Message Length: 0-51200 Increment 8	N/A	Secure hashing Note: SHA-1 is not used for digital signature generation
#A2345	SHS • FIPS180-4	SHA2-256 Message Length: 0-51200 Increment 8	N/A	Secure hashing
#A2345	SHS • FIPS180-4	SHA2-384 Message Length: 0-51200 Increment 8	N/A	Secure hashing
#A2345	HMAC • FIPS198-1	HMAC-SHA-1	At least 160 bits	Hash based message authenticate code generation and verification
#A2345	HMAC • FIPS198-1	HMAC-SHA2-256	At least 160 bits	Hash based message authenticate code generation and verification
#A2345	HMAC • FIPS198-1	HMAC-SHA2-384	At least 160 bits	Hash based message authenticate code generation and verification
#A2345	RSA • FIPS186-4	RSA KeyGen Mode: B.3.3	Modulus: 2048 bits	Key Generation
#A2345	RSA • FIPS186-4	RSA SigGen (PKCS 1.5)	Modulus: 2048 bits	Signature Generation
#A2345	RSA • FIPS186-4	RSA Sigver (PKCS 1.5)	Modulus: 2048 bits	Signature Verification

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function /Notes
#A2345	Safe Primes Key Generation • SP800-56Arev3	N/A	Safe Prime Groups: MODP-2048, MODP-4096, MODP-8192	KAS-FFC Keypair domain parameters generation
Vendor Affirmed	CKG • SP800-133rev2	N/A	N/A	Vendor Affirmed Cryptographic Key Generation (CKG) compliant with SP800-133rev2 and IG D.H The cryptographic module performs Cryptographic Key Generation (CKG) for asymmetric keys as per sections 4 and 5 in SP800-133rev2 (vendor affirmed). A seed (i.e., the random value) used in asymmetric key generation is a direct output from SP800-90Arev1 CTR_DRBG

Table 3 - Approved Algorithms (Crypto Library I)

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function /Notes
AES #4550	AES • FIPS197 • SP800-38A	AES-ECB	128 bits	ECB is a pre-requisite algorithm for GCM
AES #4550	AES • FIPS197 • SP800-38D	AES-GCM	128 bits	Authenticated Encryption/Decryption in MACSec

Table 4 - Approved Algorithms (Crypto Library II)

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function /Notes
AES #5074	AES • FIPS197 • SP800-38A	AES-ECB	128 bits	ECB is a pre-requisite algorithm for GCM
AES #5074	AES • FIPS197 • SP800-38D	AES-GCM	128 bits	Authenticated Encryption/Decryption in IPSec/IKE

Table 5 - Approved Algorithms (Crypto Library III)

Notes:

- There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in Tables 3-5.

- The module's AES-GCM implementation conforms to IG 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 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's AES-GCM implementation conforms to IG C.H scenario #1 following RFC 7296 for IPSec/IKE. The module uses RFC 7296 compliant IPSec/IKE to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. The operations of one of the two parties involved in the IKE key establishment scheme shall be performed entirely within the cryptographic boundary of the module being validated. 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 AES GCM IV is generated internally in the cryptographic module in accordance with IEEE 802.1AE and its amendments. The IV length used is 96 bits (per SP800-38D and FIPS 140-3 IG C.H). The AES GCM IV construction is performed in compliance with IEEE 802.1AE and its amendments. 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 should be secured to prevent the possibility for an attacker to introduce foreign equipment into the local area network.
- No parts of the SSH, TLS, SNMP and IKEv2 protocols, other than the KDFs, have been tested by the CAVP and CMVP.

As the module can only be operated in the Approved mode of operation, and any algorithms not listed in the tables 3-5 above will be rejected by the module while in the approved mode, the tables defined in SP800-140B for the following categories are missing from this document.

- Non-Approved Algorithms Allowed in Approved Mode of Operation
- Non-Approved Algorithms Allowed in Approved Mode of Operation with No Security Claimed
- Non-Approved Algorithms Not Allowed in Approved Mode of Operation

3. Cryptographic Module Interfaces

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-3 defined logical interfaces: Data Input, Data Output, Control Input, Control Output (N/A) and Status Output. The logical interfaces and their mapping are described in the following table. Please note that the module doesn't support Control Output logical interface.

Physical Port	Logical Interface	Data that passes over port/interface
Console port, Mgmt port, SFP/SFP+ ports, QSFP+ ports, Ethernet ports	Data Input	SSH, TLS, SNMPv3, IPSec/IKEv2 or MACSec traffic
Console port, Mgmt port, SFP/SFP+ ports, QSFP+ ports, Ethernet ports	Data Output	SSH, TLS, SNMPv3, IPSec/IKEv2 or MACsec traffic
Console port, Mgmt port, SFP/SFP+ ports, QSFP+ ports, Ethernet ports	Control Input	Control Input
Console port, Mgmt port, SFP/SFP+ ports, QSFP+ ports, Ethernet ports, and LEDs	Status Output	Status information
N/A	Control Output	NA
Power	N/A	Provides the power supply to the module

Table 6 – Ports and Interfaces

4. Roles, Services, and Authentication

The module supports role-based authentication. In approved mode, the cryptographic module supports the following roles:

1. **Crypto Officer Role**: The Crypto Officer role has complete access to the system. The Crypto Officer is the only role that can perform firmware loading, security functions configuration (SSHv2, TLSv1.1/v1.2, SNMPv3, IPSec/IKEv2 and MACSec) and account management. A crypto officer can create additional accounts thereby creating additional crypto officers.
2. **Port Config Admin Role**: The Port Config Admin role has read and write access for configuring specific ports but not for global (system-wide) parameters.
3. **User Role**: The User role on the device has read-only privileges and no configuration mode access.

The module does not support the maintenance role.

For all other services, an operator must authenticate to the module as described in Table below. The module provides services for remote communication (SSHv2 and SNMPv3) for management and configuration of cryptographic functions.

The following subsections describe services available to operators based on role.

Role	Service	Input	Output
Crypto Officer	Perform Self-test	Command to trigger self-test	The self-tests completion status information
Crypto Officer	Perform Zeroization	Command to zeroize the module	The zeroization completion status information

Role	Service	Input	Output
Crypto Officer	Update Firmware	Command to upload a new validated firmware	The firmware update completion status information
Crypto Officer	CO Authentication	CO role authentication request	Status of the CO role authentication
Crypto Officer	Configuration Management	Commands to configure the module	Status of the completion of network related configuration
Crypto Officer	Configure RADIUS Server	Commands to configure RADIUS Server	Status of the completion of RADIUS Server configuration
Crypto Officer	Configure SSHv2 Function	Commands to configure SSHv2 function	Status of the completion of SSHv2 configuration
Crypto Officer	Configure SSL over TLSv1.1/1.2 Function	Commands to configure SSL over TLSv1.1/2 function	Status of the completion of SSL over TLSv1.1/1.2 configuration
Crypto Officer	Configure SNMPv3 Function	Commands to configure SNMPv3 function	Status of the completion of SNMPv3 configuration
Crypto Officer	Configure IPsec/IKE Function	Commands to configure IPSec/IKE function	Status of the completion of IPSec/IKE configuration
Crypto Officer	Configure MACSec Function	Commands to configure MACSec function	Status of the completion of MACSec configuration
Crypto Officer	Account management	Command to create user account	The status of the new user accounts
Crypto Officer	Show Version	Command to show version	Module's name and versioning information
Crypto Officer	Show Status	Command to get the status of the module	Module's current status information
Crypto Officer	Port Configuration Management	Commands to configure the port parameters of switch/router	Port configuration completion status information
Crypto Officer	Run SSHv2 Function	Initiate SSHv2 tunnel establishment request	Status of SSHv2 tunnel establishment
Crypto Officer	Run SSL over TLSv1.1/v1.2 Function	Initiate SSL over TLSv1.1/v1.2 tunnel establishment request	Status of TLSv1.1/v1.2 tunnel establishment
Crypto Officer	Run SNMPv3 Function	Initiate SNMPv3 tunnel establishment request	Status of SNMPv3 tunnel establishment
Crypto Officer	Run IPSec/IKE Function	Initiate IPsec/IKE tunnel establishment request	Status of IPSec/IKE tunnel establishment
Crypto Officer	Run MACSec Function	Initiate MACSec tunnel establishment request	Status of MACSec tunnel establishment

Table 7 - Roles, Service Commands, Input and Output (Crypto Officer role)

Role	Service	Input	Output
User	Show Version	Command to show version	Module's name and versioning information
User	Show Status	Command to get the status of the module	Module's current status information
User	User Authentication	User role authentication request	Status of the User role authentication
User	Run SSHv2 Function	Initiate SSHv2 tunnel establishment request	Status of SSHv2 tunnel establishment

Table 8 - Roles, Service Commands, Input and Output (User role)

Role	Service	Input	Output
Port Config Admin	Show Version	Command to show version	Module's name and versioning information
Port Config Admin	Show Status	Command to get the status of the module	Module's current status information

Role	Service	Input	Output
Port Config Admin	Port Config Admin Authentication	Port Config Admin role authentication request	Status of the Port Config Admin role authentication
Port Config Admin	Port Configuration Management	Commands to configure the port parameters of switch/router	Port configuration completion status information
Port Config Admin	Run SSHv2 Function	Initiate SSHv2 tunnel establishment request	Status of SSHv2 tunnel establishment

Table 9 - Roles, Service Commands, Input and Output (Port Config Admin role)

Role	Authentication Method	Authentication Strength
Crypto Officer, User, Port Config Admin	Password-based authentication	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. The probability of successfully authenticating to the module within one minute is $10/(94^8)$, which is less than 1/100,000. The configuration supports at most ten failed attempts to authenticate in a one-minute period. 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
Crypto Officer, User, Port Config Admin	RSA-based authentication	RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength, which means an attacker would have a 1 in 2112 chance of randomly obtaining the key, which is much stronger than the one in a million chances required by FIPS 140-3. 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 (2112 /60 = 8.65 x 1031) attempts per second, which is less than 1/100,000
Crypto Officer, User, Port Config Admin	ECDSA-based authentication	When configuring the smallest curve P-256, the probability that a random attempt will succeed, or a false acceptance will occur is 1/2^128, which is less than 1/1,000,000. 256 attempts are allowed in a one-minute period. Therefore, the probability of a random success in a one-minute period is 256/2^128, which is less than 1/100,000

Table 10 – Roles and Authentication

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Perform Self-test	The module runs pre-operational self-tests and conditional algorithm Self-tests (CASTs)	N/A	N/A	Crypto Officer	N/A	Self-test completion message
Perform Zeroization	Zeroize service destroys all SSPs in the module	N/A	ALL	Crypto Officer	Z	Zeroize completion message
Update Firmware	The module's firmware is updated to a new version	RSA SigVer	Firmware Load Test Key	Crypto Officer	E	Global indicator and Firmware update completion message
Show Status	Provide module's name and current status information	N/A	N/A	Crypto Officer; User; Port Config Admin	R	N/A

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Show Version	Provide modules version information	N/A	N/A	Crypto Officer; User; Port Config Admin	R	N/A
CO Authentication	CO role authentication	N/A	Crypto Officer Password	Crypto Officer	G, R, W, E	N/A
User Authentication	User role authentication	N/A	User Password	User	G, R, W, E	N/A
Port Config Admin Authentication	Port Config Admin role authentication	N/A	Port Config Admin Password	Port Config Admin	G, R, W, E	N/A
Configure SSHv2 Function	Configure SSHv2 Function	AES-CBC, AES-CTR, CKG, CTR_DRBG, KDF SSH, HMAC-SHA-1, HMAC-SHA2-256, KAS-ECC-SSC, KAS (ECC), KAS-FFC-SSC, KAS (FFC), KTS, ECDSA KeyGen, ECDSA SigGen, ECDSA SigVer, RSA KeyGen, RSA SigGen, RSA SigVer, Safe Primes KeyGen	DRBG Entropy Input, DRBG Seed, DRBG Internal State V value, DRBG Key, SSH ECDSA Private Key, SSH ECDSA Public Key, SSH RSA Private Key, SSH RSA Public Key, SSH DH Private Key, SSH DH Public Key, SSH DH Shared Secret Key, SSH ECDH Private Key, SSH ECDH Public Key, SSH ECDH Shared Secret Key, SSH Session Encryption Key, SSH Session Integrity Key	Crypto Officer	R, W, G	Global indicator and SSH connection success log message
Configure SSL over TLSv1.1/v1.2 Function	Configure TLSv1.1/v1.2 Function	AES-ECB, AES-CBC, AES-GCM, CKG, CTR_DRBG, KDF TLS, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, KAS-ECC-SSC,	DRBG Entropy Input, DRBG Seed, DRBG Internal State V value, DRBG Key, TLS ECDSA Private Key, TLS ECDSA Public Key, TLS RSA Private Key, TLS RSA Public Key, TLS DH Private Key, TLS DH Public key, TLS DH Shared Secret, TLS ECDH Private Key, TLS ECDH Public key,	Crypto Officer	R, W, G	Global indicator and TLS connection success log message

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
		KAS (ECC), KAS-FFC-SSC, KAS (FFC), KTS, ECDSA KeyGen, ECDSA SigGen, ECDSA SigVer, RSA KeyGen, RSA SigGen, RSA SigVer, Safe Primes KeyGen	TLS ECDH Shared Secret, TLS Pre-Master Secret, TLS Master Secret, TLS Session Encryption Key, TLS Session Integrity Key			
SNMPv3 Function Configuration	Configure SNMPv3 Function	AES-CFB128, KDF SNMP, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	SNMPv3 User Authentication Secret, SNMPv3 Session Encryption Key, SNMPv3 Session Integrity Key	Crypto Officer	R, W, G	Global indicator and SNMPv3 connection success log message
Configure IPsec/IKEv2 Function	Configure IPSec/IKEv2 Function	AES-CBC, AES-GCM, CKG, CTR_DRBG, KDF IKEv2, ECDSA KeyGen, ECDSA SigGen, ECDSA SigVer, HMAC-SHA2-256, HMAC-SHA2-384, KAS-ECC-SSC, KAS (ECC), KAS-FFC-SSC, KAS (FFC), RSA KeyGen, RSA SigGen, RSA SigVer, Safe Primes KeyGen	DRBG Entropy Input, DRBG Seed, DRBG Internal State V value, DRBG Key, IPSec/IKE Pre-shared Secret, IPSec/IKE ECDH Private Key, IPSec/IKE ECDH Public Key, IPSec/IKE ECDH Shared Secret, IPSec/IKE DH Private Key, IPSEC/IKE DH Public key, IPSec/IKE DH Shared Secret, IPSec/IKE RSA Private Key, IPSec/IKE RSA Public Key, IPSec/IKE ECDSA Private Key, IPSEC/IKE ECDSA Public Key, IPSec/IKE Session Encryption Key, IPSec/IKE Session Integrity Key	Crypto Officer	G, R, W	Global indicator and IPSec/IKE connection success log message
Configure MACSec Function	Configure MACSec Function	AES-CMAC; AES-GCM; AES-KW; AES-KWP; KBKDF;	MACSec CAK; MACSec ICK; MACSec KEK; MACSec SAK	Crypto Officer	G, R, W	Global indicator and MACSec connection success log message

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
		KTS				
Port Configuration Management	Perform Port Configuration	N/A	Crypto Officer Password; Port Config Admin Password	Crypto Officer; Port Config Admin	R, E	N/A
Account management	Account Creation	N/A	Crypto Officer Password; User Password; Port Config Admin Password	Crypto Officer	W	N/A
Run SSHv2 Function	Negotiation and encrypted data transport via SSH	AES-CBC, AES-CTR, CKG, CTR_DRBG, KDF SSH, HMAC-SHA-1, HMAC-SHA2-256, KAS-ECC-SSC, KAS (ECC), KAS-FFC-SSC, KAS (FFC), KTS, ECDSA KeyGen, ECDSA SigGen, ECDSA SigVer, RSA KeyGen, RSA SigGen, RSA SigVer, Safe Primes KeyGen	DRBG Entropy Input, DRBG Seed, DRBG Internal State V value, DRBG Key, SSH ECDSA Private Key, SSH ECDSA Public Key, SSH RSA Private Key, SSH RSA Public Key, SSH DH Private Key, SSH DH Public Key, SSH DH Shared Secret Key, SSH ECDH Private Key, SSH ECDH Public Key, SSH ECDH Shared Secret Key, SSH Session Encryption Key, SSH Session Integrity Key	Crypto Officer	R, W, G	Global indicator and SSH connection success log message
Run SSL over TLSv1.1/v1.2 Function	Negotiation and encrypted data transport via SSL (TLSv1.1/v1.2)	AES-ECB, AES-CBC, AES-GCM, CKG, CTR_DRBG, KDF TLS, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, KAS-ECC-SSC, KAS (ECC), KAS-FFC-SSC, KAS (FFC), KTS, ECDSA KeyGen,	DRBG Entropy Input, DRBG Seed, DRBG Internal State V value, DRBG Key, TLS ECDSA Private Key, TLS ECDSA Public Key, TLS RSA Private Key, TLS RSA Public Key, TLS DH Private Key, TLS DH Public key, TLS DH Shared Secret, TLS ECDH Private Key, TLS ECDH Public key, TLS ECDH Shared Secret, TLS Pre-Master Secret, TLS Master Secret, TLS Session Encryption Key, TLS Session Integrity Key	Crypto Officer	R, W, G	Global indicator and TLS connection success log message

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
		ECDSA SigGen, ECDSA SigVer, RSA KeyGen, RSA SigGen, RSA SigVer, Safe Primes KeyGen				
Run SNMPv3 Function	Negotiation and encrypted data transport via SNMPv3	AES-CFB128, KDF SNMP, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384	SNMPv3 User Authentication Secret, SNMPv3 Session Encryption Key, SNMPv3 Session Integrity Key	Crypto Officer	R, W, G	Global indicator and SNMPv3 connection success log message
Run IPSec/IKEv2 Function	Negotiation and encrypted data transport via IPSec	AES-CBC, AES-GCM, CKG, CTR_DRBG, KDF IKEv2, ECDSA KeyGen, ECDSA SigGen, ECDSA SigVer, HMAC-SHA2-256, HMAC-SHA2-384, KAS-ECC-SSC, KAS (ECC), KAS-FFC-SSC, KAS (FFC), RSA KeyGen, RSA SigGen, RSA SigVer, Safe Primes KeyGen	DRBG Entropy Input, DRBG Seed, DRBG Internal State V value, DRBG Key, IPSec/IKE Pre-shared Secret, IPSec/IKE ECDH Private Key, IPSec/IKE ECDH Public Key, IPSec/IKE ECDH Shared Secret, IPSec/IKE DH Private Key, IPSEC/IKE DH Public key, IPSec/IKE DH Shared Secret, IPSec/IKE RSA Private Key, IPSec/IKE RSA Public Key, IPSec/IKE ECDSA Private Key, IPSEC/IKE ECDSA Public Key, IPSec/IKE Session Encryption Key, IPSec/IKE Session Integrity Key	Crypto Officer	R, E	Global indicator and IPSec/IKE connection success log message
Run MACSec Function	Negotiation and encrypted data transport via MACSec	AES-CMAC, AES-GCM, AES-KW, AES-KWP, KTS, KBKDF	MACSec CAK, MACSec ICK, MACSec KEK, MACSec SAK	Crypto Officer	R, E	Global indicator and MACSec connection success log message

Table 11 - Approved Services

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 = Zeroise: The module zeroises the SSP

Unauthenticated Services
The services for someone without an authorized role are to view the status output from the module's LEDs and to cycle power the module.

5. Software/Firmware Security

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 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 by using RSA 2048 bits with SHA2-256 (RSA Cert. #A2345) 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 binary the factory and used for firmware load test. In order to load new firmware, the Crypto Officer must authenticate into the module before loading any 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.

Integrity Test 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

The module is a hardware module. The module's operational environment is non-modifiable. The module's firmware version running on each model is IronWare OS 09.0.10. Any other firmware loaded into these modules is out of the scope of this validation and requires a separate FIPS 140-3 validation.

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 equipment.

8. Non-Invasive Security

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

9. Sensitive Security Parameter Management

Key/SSP Name/Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
DRBG Entropy Input	384 bits	N/A	Generated from noise source	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to seed the DRBG
DRBG Seed	256 bits	DRBG Cert. #A2345	Internally Derived from entropy input string as defined by SP800-90Arev1	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used DRBG generation
DRBG Internal State V value	256 bits	DRBG Cert. #A2345	Internally Derived from entropy input string as defined by SP800-90Arev1	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used DRBG generation
DRBG Key	256 bits	DRBG Cert. #A2345	Internally Derived from entropy input string as defined by SP800-90Arev1	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used DRBG generation
Port Config Admin Password	8 to 60 Characters	N/A	N/A	Import: Encrypted by SSH session key Export: No	MD/EE	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for Port Config Admin authentication
Crypto Officer Password	8 to 60 Characters	N/A	N/A	Import: Encrypted by SSH session key Export: No	MD/EE	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for Crypto Officer authentication
User Password	8 to 60 Characters	N/A	N/A	Import: Encrypted by SSH session key Export: No	MD/EE	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for User authentication
RADIUS Secret	8 to 64 Characters	N/A	N/A	Import: Encrypted by SSH session key Export: No	MD/EE	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for RADIUS Server authentication
SSH ECDSA Private Key	P-256, P-384	CKG, DRBG, ECDSA KeyGen, ECDSA SigGen Cert. #A2345	Internally generated conformant to SP800-133r2 (CKG) using FIPS 186-4 ECDSA key generation method, and the random value used in key generation is generated using	Import: No Export: No	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SSH authentication

Key/SSP Name/Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
			SP800-90Arev1 DRBG					
SSH ECDSA Public Key	P-256, P-384	ECDSA SigVer Cert #A2345	Internally derived per the FIPS 186-4 ECDSA key generation method	Import: No Export: to the SSH peer application	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SSH authentication
SSH RSA Private Key	2048 bits	CKG, DRBG, RSA KeyGen, RSA SigGen Cert. #A2345	Internally generated conformant to SP800-133r2 (CKG) using FIPS 186-4 RSA key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SSH authentication
SSH RSA Public Key	2048 bits	RSA SigVer Cert #A2345	Internally derived per the FIPS 186-4 RSA key generation method	Import: No Export: to SSH peer application	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SSH authentication
SSH DH Private Key	MODP-2048, 4096, 8192 bits	CKG, DRBG, KAS-FFC-SSC Cert. #A2345	Internally generated. conformant to SP800-133r2 (CKG) using SP800-56Arev3 Diffie-Hellman key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive SSH DH Shared secret
SSH DH Public Key	MODP-2048, 4096, 8192 bits	KAS-FFC-SSC Cert. #A2345	Internally derived internally per the Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to SSH peer application	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive SSH DH Shared secret
SSH DH Shared Secret	MODP-2048, 4096, 8192 bits	KAS-FFC-SSC Cert. #A2345	Internally derived using SP800-56A rev3 EC Diffie-Hellman shared secret computation	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive SSH Session Encryption Key, SSH Session Integrity Key
SSH ECDH Private Key	P-256, P-384, P-521	CKG, DRBG, KAS-ECC-SSC Cert. #A2345	Internally generated. conformant to SP800-133r2 (CKG) using SP800-56Arev3 EC Diffie-Hellman key generation method, and the random value used in key generation	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive SSH ECDH Shared secret

Key/SSP Name/Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
			is generated using SP800-90Arev1 DRBG					
SSH ECDH Public Key	P-256, P-384, P-521	KAS-ECC-SSC Cert. #A2345	Internally derived internally per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to SSH peer application	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive SSH ECDH Shared secret
SSH ECDH Shared Secret	P-256, P-384, P-521	KAS-ECC-SSC Cert. #A2345	Internally derived using SP800-56A rev3 EC Diffie-Hellman shared secret computation	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive SSH Session Encryption Key SSH Session Integrity Key
SSH Session Encryption Key	128, 256 bits	AES-CTR, KDF SSH, KTS Cert. #A2345	Internally derived via key derivation function defined in SP800-135rev1 KDF (SSHv2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SSH session confidentiality protection
SSH Session Integrity Key	At least 160 bits	HMAC-SHA-1, HMAC-SHA2-256, KDF SSH Cert. #A2345	Internally derived via key derivation function defined in SP800-135rev1 KDF (SSHv2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SSH session integrity protection
IPSec/IKE Pre-Shared Secret	8 to 60 Characters	N/A	N/A	Import: Encrypted by SSH session key Export: No	MD/EE	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to authenticate IPsec/IKE peer
IPSec/IKE ECDH Private Key	P-256, P-384	CKG, DRBG, KAS-ECC-SSC Cert. #A2345	Internally generated. conformant to SP800-133r2 (CKG) using SP800-56Arev3 EC Diffie-Hellman key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive IPSec/IKE ECDH Shared secret
IPSec/IKE ECDH Public Key	P-256, P-384	KAS-ECC-SSC Cert. #A2345	Internally derived internally per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to the IPSec/IKE peer application	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive IPSec/IKE ECDH Shared secret
IPSec/IKE ECDH Shared Secret	P-256, P-384	KAS-ECC-SSC Cert. #A2345	Internally derived using SP800-56A rev3 EC Diffie-Hellman shared secret computation	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive IPSec/IKE Session Encryption Key, IPSec/IKE session Integrity Key

Key/SSP Name/Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
IPSec/IKE DH Private Key	MODP-2048	CKG, DRBG, KAS-FFC-SSC Cert. #A2345	Internally generated. conformant to SP800-133r2 (CKG) using SP800-56Arev3 Diffie-Hellman key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive IPSec/IKE DH Shared secret
IPSec/IKE DH Public key	MODP-2048	CKG, DRBG, KAS-FFC-SSC Cert. #A2345	Internally derived internally per the Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to IPSec/IKE peer application	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive IPSec/IKE DH Shared secret
IPSec/IKE DH Shared Secret	MODP-2048	KAS-FFC-SSC Cert. #A2345	Internally derived using SP800-56Arev3 Diffie-Hellman shared secret computation	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive IPSec/IKE Session Encryption Key, IPSec/IKE Session Integrity Key
IPSec/IKE RSA Private Key	2048 bits	CKG, DRBG, RSA KeyGen, RSA SigGen Cert. #A2345	Internally generated conformant to SP800-133r2 (CKG) using FIPS 186-4 RSA/RSA key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for IPSec/IKE authentication
IPSec/IKE RSA Public Key	2048 bits	CKG, DRBG, RSA KeyGen RSA SigVer Cert. #A2345	Internally derived per the FIPS 186-4 RSA key generation method	Import: No Export: to IPSec/IKE peer application	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for IPSec/IKE authentication
IPSec/IKE ECDSA Private Key	P-256, P-384	CKG, DRBG, ECDSA KeyGen, ECDSA SigGen Cert. #A2345	Internally generated conformant to SP800-133r2 (CKG) using FIPS 186-4 ECDSA key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for IPSec/IKE authentication
IPSec/IKE ECDSA Public Key	P-256, P-384	CKG, DRBG, ECDSA KeyGen,	Internally derived per the FIPS 186-4	Import: No	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP)	Used for IPSec/IKE authentication

Key/SSP Name/Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
		ECDSA SigVer Cert. #A2345	ECDSA key generation method	Export: to IPSec/IKE peer application			Zeroization Command	
IPSec/IKE Session Encryption Key	128, 256 bits	AES-CBC Cert. #A2345, AES-GCM Cert. #5074	Internally derived via key derivation function defined in SP800-135rev1 KDF (IKEv2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for IPSec/IKE session confidentiality protection
IPSec/IKE Session Integrity Key	At least 160 bits	HMAC-SHA2-256, HMAC-SHA2-384 Cert. #A2345	Internally derived via key derivation function defined in SP800-135rev1 KDF (IKEv2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for IPSec/IKE session integrity protection
SNMPv3 User Authentication Secret	8 to 20 characters	N/A	Please see Establishment	Import: Encrypted by SSH session key Export: No	MD/EE	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	SNMPv3 User Authentication
SNMPv3 Session Encryption Key	128 bits	AES-CFB128, KDF SNMP Cert. #A2345	Internally derived via key derivation function defined in SP800-135rev1 KDF (SNMPv3)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SNMPV3 session confidentiality protection
SNMPv3 Session Integrity Key	At least 160 bits	HMAC-SHA-1, KDF SNMP Cert. #A2345	Internally derived via key derivation function defined in SP800-135rev1 KDF (SNMPv3)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for SNMPv3 session integrity protection

Key/SSP Name/Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
TLS ECDSA Private Key	P-256, P-384	CKG, DRBG, ECDSA KeyGen, ECDSA SigGen Cert. #A2345	Internally generated conformant to SP800-133r2 (CKG) using FIPS 186-4 ECDSA key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for TLS authentication
TLS ECDSA Public Key	P-256, P-384	ECDSA SigVer Cert. #A2345	Internally derived per the FIPS 186-4 ECDSA key generation method	Import: No Export: to TLS peer application	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for TLS authentication
TLS RSA Private Key	2048 bits	CKG, DRBG, RSA KeyGen, RSA SigGen, Cert. #A2345	Internally generated conformant to SP800-133r2 (CKG) using FIPS 186-4 RSA key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for TLS authentication
TLS RSA Public Key	2048 bits	RSA SigVer Cert. #A2345	Internally derived per the FIPS 186-4 RSA key generation method	Import: No Export: to TLS peer application	N/A	Flash (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for TLS authentication
TLS DH Private Key	MODP-2048	CKG, DRBG, KAS-FFC-SSC Cert. #A2345	Internally generated. conformant to SP800-133r2 (CKG) using SP800-56Arev3 Diffie-Hellman key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS DH Shared secret
TLS DH Public Key	MODP-2048	KAS-FFC-SSC Cert. #A2345	Internally derived internally per the Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to TLS peer application	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS DH Shared secret
TLS DH Shared Secret	MODP-2048	KAS-FFC-SSC Cert. #A2345	Internally derived using SP800-56A rev3	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP)	Used to derive TLS Session Encryption

Key/SSP Name/Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
			Diffie-Hellman shared secret computation				Zeroization Command	Key, TLS Session Integrity Key
TLS ECDH Private Key	P-256, P-384	CKG, DRBG, KAS-ECC-SSC Cert. #A2345	Internally generated. conformant to SP800-133r2 (CKG) using SP800-56Arev3 EC Diffie-Hellman key generation method, and the random value used in key generation is generated using SP800-90Arev1 DRBG	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS ECDH Shared Secret
TLS ECDH Public key	P-256, P-384	KAS-ECC-SSC Cert. #A2345	Internally derived internally per the EC Diffie-Hellman key agreement (SP800-56Arev3)	Import: No Export: to TLS peer application	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS ECDH Shared secret
TLS ECDH Shared Secret	P-256, P-384	KAS-ECC-SSC Cert. #A2345	Internally derived using SP800-56A rev3 EC Diffie-Hellman shared secret computation	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS Session Encryption Key, TLS Session Integrity Key
TLS Pre-Master Secret	256 bits	N/A	Internally derived via key derivation function defined in SP800-135rev1 KDF (TLSv1.1/1.2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to derive TLS Session Encryption Key, TLS Session Integrity Key
TLS Master Secret	48 bytes	N/A	Internally derived via key derivation function defined in SP800-135rev1 KDF (TLSv1.1/1.2)	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	TLS pre master secret, TLS Encryption Key TLS Session Integrity Key
TLS Session Encryption Key	128 or 256 bits	AES-ECB, AES-CBC, AES-GCM, KDF TLS, KTS Cert. #A2345	Internally derived via key derivation function defined in SP800-135 rev1 KDF TLSv1.1/1.2 KDF	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for TLS session confidentiality protection
TLS Session Integrity Key	At least 160 bits	KDF TLS HMAC-SHA2-256, HMAC-SHA2-384 Cert. #A2345	Internally derived via key derivation function defined in SP800-135 rev1 KDF TLSv1.1/1.2	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for TLS session integrity protection
MACSec CAK	128 bits	N/A	N/A	Import: Encrypted by SSH session key Export: No	MD/EE	Flash (plaintext)	Explicit zeroization by zeroization command	Used to derive MACSec ICK and MACSec KEK

Key/SSP Name/Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroization	Use & related Keys
MACSec ICK	128 bits	AES-CMAC, KBKDF Cert. #A2345	Internally derived using SP800-108 KDF	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	used for MACSec Peer authentication
MACSec KEK	128 bits	AES-KW, AES-KWP, KBKDF, KTS Cert. #A2345	Internally derived using SP800-108 KDF	Import: No Export: No	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used to transport MACSec SAK to MACSec Peer
MACSec SAK	128 bits	AES-CMAC KBKDF, Cert. #A2345 AES-GCM AES Cert: #4550	Internally derived using SP800-108 KDF	Import: No Export: Encrypted by MACSec KEK	N/A	DRAM (plaintext)	Zeroized by SSP (CSP/PSP) Zeroization Command	Used for MACSec session protection
Firmware Load Test Key	2048 bits	RSA SigVer, SHA2-256 Cert. #A2345	Pre-loaded at the factory (in the module's executable binary)	N/A	N/A	Flash (Plaintext)	N/A	User for Firmware load test

Table 12 - SSPs

Notes:

1. The module uses procedural zeroization to explicitly zeroize all SSPs listed in Table 12.
2. The zeroization operations shall be performed under the control of the CO role by using the CLI command "fips zeroize all"
3. To initiate zeroization, see Section End of Life / Sanitization in this document for more details.
4. The zeroized SSPs cannot be retrieved or reused. Once the command is initiated, the SSPs are overwritten with 0s.

RBG Entropy Source.

Entropy sources	Minimum number of bits of entropy	Details
ENT (NP). Periodic sampling of the high-precision CPU clock within the ARM CPU is the only single entropy source used to seed the SP800-90Arev1 DRBG (DRBG Cert. #A2345)	256 bits	The system tick clock/register as the single entropy source to provide the sufficient entropy to seed the SP800-90Arev1 DRBG (DRBG Cert. #A2345). The entropy source was directly used to seed the DRBG without the entropy conditioning process. Please refer to entropy report for details

Table 13 – Non-Deterministic Random Number Generation Specification

10. Self-Test

The modules perform the following 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).

Pre-Operational Self-Tests:

- **Pre-Operational Firmware Integrity Test**
  - BootLoader Integrity Test (CRC-32)
  - Firmware Integrity Test (CRC-32)
- **No Pre-Operational Bypass Test**
- **No Pre-Operational Critical Functions Test**

Conditional Self-Tests

- **Conditional Cryptographic Algorithm Tests:**
  - AES-CBC 128 bits encryption KAT
  - AES-CBC 128 bits decryption KAT
  - AES-CMAC 128 bits encryption KAT
  - AES-CMAC 128 bits decryption KAT
  - AES-GCM 128 bits authenticated encryption KAT
  - AES-GCM 128 bits authenticated decryption KAT
  - CTR_DRBG Instantiate KAT
  - CTR_DRBG Generate KAT
  - CTR_DRBG Reseed KAT

  Note: DRBG Health Tests as specified in SP800-90Arev1 Section 11.3 are performed
  - ECDSA P-256 with SHA2-256 SigGen KAT
  - ECDSA P-256 with SHA2-256 SigVer KAT
  - HMAC-SHA-1 KAT
  - HMAC-SHA2-256 KAT
  - HMAC-SHA2-384 KAT
  - KAS-FFC-SSC Primitive KAT
  - KAS-ECC-SSC Primitive KAT
  - RSA 2048 bits modulus with SHA2-256 SigGen KAT
  - RSA 2048 bits modulus with SHA2-256 SigVer KAT
  - SHA-1 KAT
  - SHA2-256 KAT
  - SHA2-384 KAT
  - KBKDF KAT
  - KDF SSH KAT
  - KDF SNMP KAT
  - KDF IKEv2 KAT
  - KDF TLS KAT
  - SP800-90B Entropy Source start-up health tests:
    - Repetition Count Test (RCT)
    - Adaptive Proportion Test (APT)
  - SP800-90B Entropy Source Continuous Health Tests:
    - Repetition Count Test (RCT)
    - Adaptive Proportion Test (APT)

In addition, the module also performs the Conditional Cryptographic Algorithm Self-tests to the following two AES-GCM algorithms:

- AES-GCM 128 bits authenticated encryption KAT for AES Cert. #4550
- AES-GCM 128 bits authenticated decryption KAT for AES Cert. #4550
- AES-GCM 128 bits authenticated encryption KAT for AES Cert. #5074
- AES-GCM 128 bits authenticated decryption KAT for AES Cert. #5074

- **Conditional Pair-Wise Consistency Tests:**
  - RSA PCT
  - ECDSA PCT
  - KAS-ECC PCT
  - KAS-FFC PCT

- **Conditional Firmware Load Test**
  - Firmware Load Test (RSA 2048 bits modulus with SHA2-256)

- **No Conditional Manual Entry Test**
- **No Conditional Bypass Test**
- **No Conditional Critical Function Test**

Error Handling

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.

Cause of Error	Error State Indicator
Pre-operational Firmware Integrity Test Fails	FIPS: Crypto module POST Failed
Conditional CAST Fails	FIPS Fatal Cryptographic Module Failure. Reason: <Reason String>
Conditional PCT Fails	Pairwise consistency check failed
Firmware Load Test Fails	FIPS: Firmware Integrity Test: *Package Checksum Verification: FAIL*

Table 14 – Error State Indicators

Periodic/On-Demand Self-Test

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). The full suite of self-tests is then executed. The same procedure may be employed by the operator to perform periodic self-tests.

In addition, the Crypto Officer shall perform the periodic test on demand no more than 10 days to ensure all components are functioning correctly.

11. Life-cycle Assurance

The module is designed to handle the various stages of a module's life-cycle. The sections below highlight the details for each stage.

Secure Operation

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 remove the module from the approved mode of operation. The module runs firmware version IronWare OS 09.0.10. 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.

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 upon the first-time authentication.
3. The Crypto Officer shall create the account for Port Config Admin role and User role respectively.
4. Enter into the configuration mode by using 'conf t' command.
5. Enable approved mode by using 'fips enable' command.
6. Configure SSH, TLS, SNMPv3, MACSec, IPSec/IKE and Radius services by using only approved algorithms listed in Tables 3, 4 and 5 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*").

Once the module has completed initialization into the approved mode of operation, the module automatically enforces a password change for the Crypto Officer. The default login password won't be accepted by the module. Any non-approved algorithms or security functions are rejected automatically by the module and an error message is output.

End of Life / Sanitization

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.

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

12. Mitigation of Other Attacks

This module is not designed to mitigate against any other attacks outside of the FIPS 140-3 scope.

I. Terms and Definitions

Term	Meaning
FIPS	Federal Information Processing Standard
Approved mode	Device actively running in FIPS 140-3 compliant manner
CC	Common Criteria
HMAC	Keyed-Hash Message Authentication Code (RFC2104)
POST	Power-on Self-Test
PKI	Public Key Infrastructure
PSK	Pre-shared keys
RSA	Rivest, Shamir and Aldeman Public/Private Key
RNG	Random Number Generator
SSL	Secure Socket Layer, used in HTTPS protocol for payload encryption.
TLS	Transport Layer Security, successor to SSL, used in HTTPS protocol for payload encryption.
KAT	Known Answer Test
DSS	Digital Signature Standard
DSA	Digital Signature Algorithm, proposed by NIST in 1991 for FIPS 186-x
DES	Data Encryption Standard (single DES should not be used see TDEA)
NDPP	Network Devices Protection Profile
DRBG	Deterministic Random Bits Generator

ACVP	Automated Cryptographic Validation Program
NDcPP	Network Device collaborative protection profile