Brocade® 7840 Extension Switch

FIPS 140-2
Non-Proprietary
Security Policy

Document Version 1.0

Brocade Communications

January 14th, 2016

Document History

Version	Summary of Changes	Publication Date
1.0	Initial Release	January 14, 2016

Table of Contents

Table of Tables

Table of Figures

1 Module Overview

The Brocade 7840 is a multiple-chip standalone cryptographic module, as defined by FIPS 140-2. The cryptographic boundary of the 7840 Extension Switch is the outer perimeter of the metal chassis including the removable cover. The power supply units are not included in the cryptographic boundary. The module is a Fibre Channel and/or Gigabit Ethernet routing switch that provides secure network services and network management.

For the module to operate in a FIPS approved mode of operation, the tamper evident seals supplied in FIPS Kit P/N Brocade XBR-000195 must be installed as defined in Appendix A.

The Crypto-Officer is responsible for storing and controlling the inventory of any unused seals. The unused seals shall be stored in plastic bags in a cool, dry environment between 60° and 70° F (15° to 20° C) and less than 50% relative humidity. Rolls should be stored flat on a slit edge or suspended by the core.

The Crypto-Officer shall maintain a serial number inventory of all used and unused tamper evident seals. The Crypto-Officer shall periodically monitor the state of all applied seals for evidence of tampering. A seal serial number mismatch, a seal placement change, a checkerboard destruct pattern that appears in peeled film and adhesive residue on the substrate are evidence of tampering. The Crypto-Officer shall periodically view each applied seal under a UV light to verify the presence of a UV wallpaper pattern. The lack of a wallpaper pattern is evidence of tampering. The Crypto-Officer is responsible for returning a module to a FIPS approved state after any intentional or unintentional reconfiguration of the physical security measures.

A validated module configuration is comprised of Fabric OS v7.4.0 (P/N: 51-1001672-01) installed on, a switch or backbone and a set of installed blades. The below platforms may be used in a validated module configuration:

Firmware
Fabric OS v7.4.0

Table 1 - Firmware Version

Switch	SKU	Part Number	Brief Description
7840	BR-7840-0002	80-1008000-01	7840, 42P, 24 16G LW SFPS, 0 1/10/40GBE SFP

Table 2 - Switch Platforms

Figure 1 - Brocade 7840

Figure 1 illustrates the Brocade 7840 cryptographic module.

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	NA
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	NA

Table 3 - Module Security Level Specification

3 Modes of Operation

3.1 Approved mode of operation

The cryptographic module supports the following Approved algorithms:

Approved Algorithm	Description	Certificate Number
AES	128, 192, and 256-bit keys (ECB, CBC)	2876, 2892, 2893
AES	256-bit key (CBC, GCM)	3130
AES	256-bit keys (ECB, GCM)	3132
ECDSA	P-256 NOTE: P-384 and P-521 are latent functionality i.e. not available in any services in FIPS mode or non-FIPS mode	518, 522, 523
HMAC	HMAC-SHA1, 224, 256, 384, 512 (160-bit key)	1814, 1828, 1829, 1952
DRBG	SP800-90A CTR_DRBG (AES-256-CTR)	635, 670, 671, 672
RSA	2048-bit and 3072-bit keys	1514, 1522, 1523
SHS	SHA-1, 224, 256, 384, 512	2417, 2435, 2436, 2571
Triple-DES	KO 1, 2 CBC mode (192-bit key) NOTE: Two-key Triple-DES is latent functionality i.e. not available in any services in FIPS mode or non-FIPS mode.	1719, 1723, 1724
CVL	ECC CDH Primitive (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength) P-256, P-384, P-521	311, 318, 320
CVL	TLS v1.0/1.1 and v1.2 NOTE: SSL “is not” supported in FIPS mode.	312, 319, 321
CVL	SSHv2	312, 319, 321
CVL	IKEv2	396

Table 4 - Approved Algorithms available in firmware

Users should reference the transition tables that will be available at the CMVP: (http://csrc.nist.gov/groups/STM/cmvp/)

The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

FIPS Approved mode enables:

- HTTP TLS v1.0/1.1 and TLS v1.2
- SSHv2
- IKEv2

The following non-Approved algorithms and protocols are allowed within the Approved mode of operation:

- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- EC Diffie-Hellman (CVL Certs. #311, #318 and #320, key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength)
- HMAC-MD5 to support RADIUS authentication
- NDRNG – used for seeding the Approved DRBG
- MD5 -used for password hash (Note: The use of MD5 does not provide cryptographic protection, and is considered as plaintext)

The initial state of the cryptographic module is not in a FIPS-compliant state. The cryptographic module contains four default accounts: root, factory, admin, and user. Each default account has a public, default password.

The cryptographic module may be configured for FIPS mode via execution of the following procedure:

1) Login as root
2) Set ciphers to FIPS compliant ciphers
3) Perform zeroization operation
4) Power cycle the module
5) Login as root and change passwords for all existing user accounts
6) Disable Telnet and HTTP
7) Enable HTTPS
8) Enforce Secure Config Upload/Download
9) Do not use FTP
    a) Support Save
    b) FW Download
10) Disable MD5 and SHA1 hash and 0-3 within authentication protocols; Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) and FCAP.
11) Configure to use SHA256 as the signature algorithm for FCAP authentication with group 4.
12) Disable Management Interface IPSec/IKEv2

13) Disable In-Band Management Interface
14) Disable In-Flight Encryption
15) Disable TACACS+ authspec mode
16) Confirm that LDAP CA certificate is RSA 2048 signed with SHA256
17) Confirm that SNMP has been changed to "No Access" for SNMP SET Security
18) Enable Self-Tests
    a) Use CLI command:
       "`fipscfg --enable selftests –dp`"
19) Within RADIUS, configure to only use PEAP MS-CHAP V2 [NOTE: The operator may choose to encrypt with AES-256]
20) Install removable front cover(s) (as applicable) and apply tamper labels as per Appendix A
21) Disable Boot PROM access
22) Disable Factory role access
23) Login as Admin
24) Disable Root access
25) Enable FIPS:
    a) Use CLI command:
       "`fipscfg --enable fips –dp`"
26) Power-cycle the module
27) Note: Externally generated RSA key pairs shall only be imported if they are RSA 2048
28) After certificate operations (e.g. importing) view "`fips --verify fips`" to validate FIPS
29) Execute "`fipscfg --enable SHA256`" for SSHv2 sessions with RSA 2048 keys and signed/verified with SHA256 [NOTE: The operator can use either ECDSA or RSA]
30) Verify FIPS mode and examine that all verifications pass.
    a) Use CLI command:
       "`fips ––verify –dp`"
31) SSHv2 clients and server should support the Diffie-Hellman-group-exchange-256 and the ability to sign/verify with SHA256 to connect to the switch unless ECDSA is implemented

NOTE: Once the Crypto-Officer has executed the procedure above, the cryptographic module can no longer operate in a non-FIPS mode of operation.

The operator can determine if the cryptographic module is running in FIPS (Approved) vs. non-FIPS (non-Approved) mode via execution of the CLI command, "`fipscfg --show`" service. The module will return the following as an indicator for the FIPS Mode of Operation: "FIPS mode is: Enabled". When operating in the non-Approved mode of operation the following will be displayed "FIPS mode is: Disabled."

3.2 Non-Approved mode of operation

NOTICE: The module provides the following non-FIPS approved algorithms only in non-FIPS mode of operation. The use of any such service is an explicit violation of this Security Policy and is explicitly disallowed by this Security Policy;

- aes-128-ecb (non-compliant)
- aes-192-cbc (non-compliant)
- aes-192-ecb (non-compliant)
- aes-256-ecb (non-compliant)
- bf
- bf-cbc
- bf-cfb
- bf-ecb
- bf- ofb
- cast
- cast-cbc
- cast5-cbc
- cast5-cfb
- cast5-ecb
- cast5-ofb
- des
- des-cbc
- des-cfb
- des-ecb
- des-ede
- des-ede-cbc
- des-ede-cfb
- des-ede-ofb
- des-ede3
- des-ede3-cfb
- des-ede3-ofb
- des-ofb
- des3
- desx
- rc2
- rc2-40-cbc
- rc2-64-cbc
- rc2-cbc
- rc2-cfb
- rc2-ecb
- rc2-ofb
- rc4
- rc4-40
- md2
- md4
- md5
- ripemd160
- aes-128-ctr (non-compliant)
- aes-192-ctr (non-compliant)
- aes-256-ctr (non-compliant)
- arcfour256
- arcfour128
- cast128-cbc
- arcfour
- hmac-md5
- umac-64
- hmac-ripemd160
- hmac-sha-1-96 (non-compliant)
- hmac-md5-96
- SNMPv3 KDF (non-compliant)
- RSA key size < 2048 bits (for SSHv2 and TLS)
- DH key size < (2048 bits for SSHv2)
- IKEv2 (non-compliant): DH 2048 keys with SHA-1 (non-compliant) for key exchange and HMAC-SHA-512 (non-compliant) for IKEv2 protocol
- DH-CHAP: Diffie Hellman with NULL DH, 1024, 1280, 1536 and 2048 keys with MD5 and SHA-1 (non-compliant) hash algorithm

Crypto Function/Service	Role	Additional Details
Cipher suites for SSL and TLS	Crypto-Officer	aes-128-ecb (non-compliant), aes-192-cbc (non-compliant), aes-192-ecb (non-compliant), aes-256-ecb (non-compliant), bf, bf-cbc, bf-cfb, bf-ecb, bf- ofb, cast, cast-cbc, cast5-cbc, cast5-cfb, cast5-ecb, cast5-ofb, des, des-cbc, des-cfb, des-ecb, des-ede, des-ede-cbc, des-ede-cfb, des-ede-ofb, des-ede3, des-ede3-cfb, des-ede3-ofb, des-ofb, des3, desx, rc2, rc2-40-cbc, rc2-64-cbc, rc2-cbc, rc2-cfb, rc2-ecb, rc2-ofb, rc4, rc4-40
Message Digests for SSL and TLS	Crypto-Officer	md2, md4, ripemd160
Message authentication algorithms and ciphers for configuring SSHv2	Crypto-Officer	Ciphers: aes-128-ctr (non-compliant), aes-192-ctr (non-compliant), aes-256-ctr (non-compliant), arcfour256, arcfour128, bf-cbc, cast128-cbc, arcfour Macs: hmac-md5, umac-64, hmac-ripemd160, hmac-sha-1-96 (non-compliant), hmac-md5-96
Common Certificates for FCAP and HTTPS	Crypto-Officer	FCAP and HTTPS are supported with certificates of any size (512 to 2048 and above) signed with MD5, SHA-1 (non-compliant), SHA-256 (non-compliant)
SNMP	Crypto-Officer	SNMPv1 and SNMPv3 KDF (non-compliant); Algorithms: SHA-1 (non-compliant) and MD5
RADIUS or LDAP	Crypto-Officer	PAP and CHAP authentication method for RADIUS (all considered as plaintext) RADIUS and LDAP are supported with CA certificates of any size (512 to 2048 and above) signed with MD5, SHA-1 (non-compliant), SHA-256 (non-compliant) LDAP uses TLS connections in non-FIPS mode without certificates
Telnet	Crypto-Officer	N/A – No algorithms (plaintext)
HTTP	Crypto-Officer	N/A – No algorithms (plaintext)
FTP	Crypto-Officer	Config Upload, Config Download, Support Save, FW Download, autoftp
FCIP IKEv2 or IPSec	Crypto-Officer	Management Interface IPSec/IKEv2 (disabled for management interface) Ciphers: aes-256-gcm (non-compliant)
In-Band Management Interface	Crypto-Officer	N/A – No algorithms (plaintext)
RSA	Crypto-Officer	RSA key size < 2048 bits for SSHv2 and TLS
Diffie-Hellman	Crypto-Officer	DH key size < 2048 bits for SSHv2

In-Flight Encryption	Crypto-Officer	IKEv2: DH 2048 keys with SHA-1 (non-compliant) for key exchange and HMAC-SHA-512 (non-compliant) for IKEv2 protocol DH-CHAP: Diffie Hellman with NULL DH, 1024, 1280, 1536 and 2048 keys with MD5 and SHA-1 (non-compliant) hash algorithm FCAP: Certificates with any key size signed by MD5, SHA-1 (non-compliant), SHA-256 (non-compliant)
TACACS+ authspec mode	Crypto-Officer	PAP or CHAP authspec is supported

Table 5 - Services in Non-Approved Mode of Operation

4 Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

- Fiber Channel: Data Input, Data Output, Control Input, Status Output
- 1 GbE, 10 GbE & 40 GbE: Data Input, Data Output, Control Input, Status Output
- Ethernet Ports: Control Input, Status Output
- Serial port: Control Input, Status Output
- USB: Data Input, Data Output, Status Output
    - Brocade USB flash device, XBR-DCX-0131
- Power Supply Connectors: Power Input
- LEDs: Status Output

4.1 LED Indicators

Port side:

- System Status LED (1 per module)
- System Power LED (1 per module)
- Management port Ethernet:
    - Ethernet Link LED (1)
    - Ethernet Status LED (1)
- FC Port Status LED (one for each FC port)
- 40 GbE FCIP Port Status (one for each FCIP port)
- 1/10 GbE FCIP Port Status (one for each FCIP port)

Non-port side:

- Power supply AC input status LED (one per power supply)
- Power supply DC output status LED (one per power supply)
- Fan status LED (one per fan)

Model	Port/Interface Type								
	Fibre Channel Ports	40 GbE ports	1 GbE & 10 GbE	Management port Ethernet	Serial Port	USB	Power Supply Connectors	FAN FRU	LED (total)
7840	24	2	16	1	1	1	2	3	51

Table 6 - Port/Interface Quantities

5 Identification and Authentication Policy

5.1 Assumption of Roles

The cryptographic module supports the following operator roles listed in the table below. The cryptographic module enforces the separation of roles using role-based operator authentication. An operator must enter a username and its password to log in. The username is an alphanumeric string of maximum 40 characters. The password is an alphanumeric string of 8 to 40 characters chosen from 96 printable and human-readable characters. Upon correct authentication, the role is selected based on the username of the operator and the context of the module. At the end of a session, the operator must log-out. The module supports a maximum of 256 operators, five Radius servers and five LDAP servers that may be allocated the following roles:

Role	Type of Authentication	Authentication Data	FOS RBAC Role
Admin (Crypto-Officer)	Role-based operator authentication	Username and Password	Admin
User (User role)	Role-based operator authentication	Username and Password	User, BasicSwitchAdmin, SwitchAdmin, Operator
Security Admin	Role-based operator authentication	Username and Password	SecurityAdmin
Fabric Admin	Role-based operator authentication	Username and Password	FabricAdmin
Maximum Permissions (for a user-defined role)	Role-based operator authentication	Username and Password	N/A
LDAP Server	Role-based operator authentication	LDAP Root CA certificate	N/A
RADIUS Server	Role-based operator authentication	RADIUS Shared Secret	N/A
Host/Server/Peer Switch	Role-based operator authentication	PKI (FCAP) or Shared Secret (DH-CHAP)	N/A
IKEv2 Peer	Role-based operator authentication	IKEv2 Authentication Key	N/A

Table 7 - Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/96^8 which is less than 1/1,000,000. The module can be configured to restrict the number of consecutive failed authentication attempts. If the module is not configured to restrict failed authentication attempts, then the maximum attempts possible within one minute is 20. The probability of successfully authenticating to the module within one minute is 20/96^8 which is less than 1/100,000.
Digital Signature Verification (PKI)	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^112 which is less than 1/1,000,000. The module will restrict the number of consecutive failed authentication attempts to 10. The probability of successfully authenticating to the module within one minute is 10/2^112 which is less than 1/100,000.
Knowledge of a Shared Secret	The probability that a random attempt will succeed or a false acceptance will occur is 1/96^8 which is less than 1/1,000,000. The maximum possible authentication attempts within a minute are 16 attempts. The probability of successfully authenticating to the module within one minute is 16/96^8 which is less than 1/100,000.
Knowledge of IKEv2 Authentication Key	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^512, which is less than 1/1,000,000. The maximum attempts allowed in a one minute period are equal to one attempt. If an authentication error is detected, the session goes into a fault state, and no new attempts are allowed. Therefore, the probability of a random success in a one minute period is 1/2^512, which is less than 1/100,000.

Table 8 - Strengths of Authentication Mechanisms

Service Name	Description	FOS Interface
Fabric Element Authentication	Fabric element authentication, including selection of authentication protocols, protocol configuration selection and setting authentication secrets.	authutil secauthsecret
FIPSCfg	Control FIPS mode operation and related functions.	fipscfg
Zeroize	Zeroize all CSPs.	fipgscfg --zeroize
FirmwareManagement	Control firmware management.	firmwarecommit firmwaredownload firmwaredownloadstatus
IKEv2 Negotiation - IPsec Traffic	Negotiate IKEv2 sessions, key security associations for IPsec	portcfg ipsec-policy portcfg fciptunnel
PKI	PKI configuration functions, including FOS switch certificates and SSL certificates.	seccertutil
RADIUS	RADIUS configuration functions.	aaaconfig
LDAP	LDAP configuration functions.	aaaconfig
UserManagement	User and password management.	passwd passwdconfig userconfig
SSHv2 and TLS	Crypto configuration	seccryptocfg

Table 9 - Service Descriptions

6 Access Control Policy

6.1 Roles and Services

Services \ Roles	User	Admin (Crypto-Officer)	FabricAdmin	SecurityAdmin	Maximum Permissions	LDAP Server	RADIUS Server	Host Server / Peer Switch	IKEv2 Peer
Fabric Element Authentication		X		X	X			X	
FIPSCfg		X		X	X				
Zeroize		X		X	X				
FirmwareManagement	X	X	X	X	X				
PKI	X	X	X	X	X				
RADIUS		X		X	X		X		
LDAP		X		X	X	X			
UserManagement		X		X	X				
IKEv2 Negotiation-IPsec Traffic		X		X					X
SSHv2 and TLS	X	X		X					

Table 10 - Services Authorized for Roles

6.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2. Self-tests may be initiated by power-cycling the module.
- Show Status: This service is met through the various status outputs provided by the services provided above, as well as the LED interfaces.

6.3 Definition of Critical Security Parameters (CSPs)

DH Private Keys:

- DH Private Keys for use with 2048 bit modulus

FCSP Private Key:

- Fibre-Channel Security Protocol (FCSP) CHAP Secret

FCAP Private Key:

- Fibre-Channel Authentication Protocol (FCAP) Private Key (RSA 2048)

SSHv2 / SCP/ SFTP CSPs:

- SSHv2/SCP/SFTP Session Keys – 128, 192, and 256 bit AES CBC or Triple-DES 3 key CBC
- SSHv2/SCP/SFTP Authentication Key [HMAC-SHA-1 (160 bits)]
- SSHv2 KDF Internal State
- SSHv2 DH Shared Secret Key (2048 bit)
- SSHv2 ECDH Shared Secret Key (P-256, P-384 and P-521)
- SSHv2 ECDH Private Key (P-256, P-384 and P-521)
- SSHv2 2048 RSA Private Key
- SSHv2 ECDSA Private Key (P-256)
- Value of K during SSHv2 P-256 ECDSA session

TLS CSPs:

- TLS Private Key (RSA 2048)
- TLS Pre-Master Secret
- TLS Master Secret
- TLS KDF Internal State
- TLS Session Keys – 128, 256 bit AES CBC, Triple-DES 3 key CBC
- TLS Authentication Key for HMAC-SHA-1 (160 bits), HMAC-SHA-256, HMAC-SHA-384

DRBG Seed Material/Internal State:

- DRBG Seed Material
- DRBG Internal State (V and Key)

Passwords:

- Passwords

Radius Secret:

- RADIUS Secret

IKEv2 and IPsec CSPs:

- DH Private Key (256 bits) (Used in IKEv2)
- DH Shared Secret (2048 bits) (Used in IKEv2)
- IKEv2 AES-256-GCM Encrypt/Decrypt Keys
- ESP AES-256-GCM Encrypt/Decrypt Keys
- IKEv2 KDF State
- IKEv2 Authentication Key

DRBG Internal State and Entropy Data (On Cavium):

- DRBG Internal State (V and key) (On Cavium)
- Entropy Data (On Cavium)

6.4 Definition of Public Keys

DH Public Keys:

- DH Public Key (2048 bit modulus)
- DH Peer Public Key (2048 bit modulus)

FCAP Public Keys:

- FCAP Public Key (RSA 2048)
- FCAP Peer Public Key (RSA 2048)

TLS Public Keys:

- TLS Public Key (RSA 2048)
- TLS Peer Public Key (RSA 2048)

Firmware Download Public Key:

- FW Download Public Key (RSA 2048)

SSHv2 Public Keys:

- SSHv2 RSA 2048 bit Public Key
- SSHv2 ECDSA Public Key (P-256)
- SSHv2 ECDH Public Key (P-256, P-384 and P-521)

LDAP Root CA Certificate:

- LDAP Root CA certificate (RSA 2048)

IKEv2 and IPSEC Public Keys:

- DH Public Key (Used in IKEv2)
- DH Peer Public Key (Used in IKEv2)

6.5 Definition of CSPs Modes of Access

Table below defines the relationship between access to CSPs and the different module services. Please see Section 6.3 and Section 6.4 for explicit designation of CSPs and Public Keys. The modes of access shown in the table are defined as follows:

- R: Read
- W: Write
- N: No Access
- Z: Zeroize (Session Termination, "secauthsecret –remove" command and "fipscfg –zeroize" command)

Services \ CSPs	SSHv2/SCP/SFTP CSPs	DH Private Keys	TLS CSPs	DRBG Seed Material/Internal State	DRBG Internal State and Entropy Data (On Cavium)	Passwords	RADIUS Secret	FCAP Private Key	FCSP CHAP Secret	IKEv2 and IPsec CSPs
Fabric Element Authentication	N	N	N	RW	N	N	N	RW	RW	N
FIPSCfg	N	N	N	N	N	N	N	N	N	N
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
FirmwareManagement	R	R	N	N	N	N	N	N	N	N
PKI	RW	RW	N	RW	N	N	N	N	N	N
RADIUS	N	N	N	N	N	RW	RW	N	N	N
LDAP	N	N	N	N	N	N	N	N	N	N
UserManagement	N	N	RW	RW	N	RW	N	N	N	N
IKEv2 Negotiation – IPsec Traffic	N	N	N	N	RW	N	N	N	N	RW
SSHv2 and TLS	RW	RW	RW	N	N	RW	N	N	N	N

Table 11 - CSP Access Rights within Roles & Services

Services \ Public Keys	DH Public Keys	FCAP Public Keys	TLS Public Keys	Firmware Download Public Key	SSHv2 Public Keys	LDAP Root CA Certificate	IKEv2 and IPSEC Public Keys
Fabric Element Authentication	RW	RW	N	N	N	N	N
FIPSCfg	N	N	N	N	N	N	N
Zeroize	N	N	N	N	N	N	N
FirmwareManagement	N	N	N	RW	N	N	N
PKI	N	N	RW	N	RW	N	N
RADIUS	N	N	N	N	N	N	N
LDAP	N	N	N	N	N	RW	N
UserManagement	N	N	N	N	N	N	N
IKEv2 Negotiation – IPsec Traffic	RW	N	N	RW	N	N	RW
SSHv2 and TLS	RW	RW	RW	N	RW	R	N

Table 12 - Public Key Access Rights within Roles & Services

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device supports a limited operational environment; only trusted, validated code RSA signed may be executed.

8 Security Rules

The cryptographic modules' design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS140-2 Level 2 module.

1) The cryptographic module shall provide role-based authentication.
2) When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3) The cryptographic module shall perform the following tests:
    a) Power up Self-Tests:
        i) Cryptographic algorithm tests:
            (1) Three Key Triple-DES CBC KAT Encrypt
            (2) Three Key Triple-DES CBC KAT Decrypt

(3) AES (128, 192, 256) CBC KAT Encrypt
(4) AES (128, 192, 256) CBC KAT Decrypt
(5) AES (256) GCM KAT Encrypt
(6) AES (256) GCM KAT Decrypt
(7) HMAC SHA-1 KAT
(8) HMAC SHA-256 KAT
(9) HMAC SHA-384 KAT
(10) HMAC SHA-512 KAT
(11) DRBG KAT
(12) SHA-1 KAT
(13) SHA-256 KAT
(14) SHA-384 KAT
(15) SHA-512 KAT
(16) RSA 2048 SHA-256 Sign KAT
(17) RSA 2048 SHA-256 Verify KAT
(18) SP800-135 SSHv2 KDF KAT
(19) SP800-135 TLS 1.0 KDF KAT
(20) SP800-135 TLS 1.2 KDF KAT
(21) SP800-135 IKEv2 KDF KAT
(22) ECDSA KAT
(23) ECDH KAT (Primitive "Z" Computation KAT)

ii) Firmware Integrity Test (128-bit EDC)
iii) Critical Functions Tests:
(1) RSA 2048 Encrypt/Decrypt

b) Conditional Self-Tests:
i) Continuous Random Number Generator (RNG) test – performed on non-approved RNG.
ii) Continuous Random Number Generator test – performed on DRBG (CTR_DRBG, AES-256).
iii) RSA 2048 SHA-256 Pairwise Consistency Test (Sign/Verify)
iv) RSA 2048 Pairwise Consistency Test (Encrypt/Decrypt)
v) ECDSA Pairwise Consistency Test (Sign/Verify)
vi) Firmware Load Test (RSA 2048 with SHA-256 Signature Verification)
vii) Bypass Test: N/A
viii) Manual Key Entry Test: N/A

4) At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test.
5) Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
6) Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

7) The module does not support a maintenance role or maintenance interface.

8) The serial port may only be accessed by the Crypto-Officer when the Crypto-Officer is physically present at the cryptographic boundary, via a direct connection without any network access or other intervening systems.

9) The following protocols have not been reviewed or tested by the CAVP nor CMVP:

   i) TLS v1.0/1.1

   ii) SSHv2

   iii) TLS v1.2

   iv) IKEv2

10) The module complies with FIPS 140-2 Implementation Guidance, Section A.5, Key/IV Pair Uniqueness Requirements from SP 800-38D:

    The AES GCM session key is established via the IKEv2 KDF (internally). The 96-bit IV is also constructed internally (deterministically) as per FIPS 140-2 IG A.5 Scenario 3. The fixed field (64-bits) is randomly generated bits from the SP 800-90A DRBG; this is an acceptable construction of the fixed field as per SP 800-38D Section 8.2.1 which states "the entire fixed field may consist of arbitrary bits when there is only one context to identify, such as when a fresh key is limited to a single session of a communications protocol".

    Furthermore, this is satisfactory because as per the implementation guidance "just the fact that the modules can possibly have at least 2^32 different names will be sufficient to meet this requirement." The invocation field is a separate 32-bit deterministic non-repetitive counter which increments by one. The implementation of the deterministic non-repetitive counter management logic inside the module ensures that after 2^31 operations, a new AES GCM session key and IV must be created (i.e. IKE V2 renegotiation is automatically enforced which results in new GCM Key and new IV). The IV restoration conditions are satisfied for the deterministic non-repetitive counter as per the IG A.5 bullet 3: The GCM key and IV are session specific; if the module loses power the implementation is required to renegotiate a new IKE session and thus a new GCM key and IV will be created.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with tamper evident seals.
- Tamper evident seals.

9.2 Operator Required Actions

The operator is required to inspect the tamper evident seals, periodically, per the guidance provided in the user documentation.

Physical Security Mechanisms	Recommended Frequency of Inspection / Test	Inspection / Test Guidance Details
Tamper Evident Seals	12 months	Reference Appendix A for a description of tamper label application for all evaluated platforms.

Table 13 - Inspection/Testing of Physical Security Mechanisms

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

Table 14 - Mitigation of Other Attacks

11 Definitions and Acronyms

10 GbE	10 Gigabit Ethernet
AES	Advanced Encryption Standard
Blade	Any functional assembly that can be installed in a chassis, excluding power and fan FRUs
Cavium	This is a reference to multi-core MIPS64 processor component manufactured by Cavium, Inc. which is used on this hardware product.
CBC	Cipher Block Chaining
CLI	Command Line interface
CSP	Critical Security Parameter
DH	Diffie-Hellman
FIPS	Federal Information Processing Standard
FOS	Fabric Operating System
FRU	Field Replaceable Unit
GbE	Gigabit Ethernet
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
NOS	Network Operating System
NTP	Network Time Protocol
PKI	Public Key Infrastructure
PROM	Programmable Read-Only Memory
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SCP	Secure Copy Protocol
SHA	Secure Hash Algorithm
SSHv2	Secure Shell Protocol
Triple-DES	Triple Data Encryption Standard
TLS	Transport Layer Security Protocol

12 Brocade Abbreviations

0 1/10/40GBE SFP	Zero SFP devices provided
16GB	16 Gigabit
42P	42 Ports
BR	Brocade
FC	Fibre Channel
FCIP	Fiber Channel over Internet Protocol
GBE	Gigabit Ethernet
LWL	Long Wave Length
SFP	Small form-factor pluggable

13 Appendix A: Tamper Label Application

Use ethyl alcohol to clean the surface area at each tamper evident seal placement location. Prior to applying a new seal to an area that shows seal residue, use consumer strength adhesive remove to remove the seal residue. Then use ethyl alcohol to clean off any residual adhesive remover before applying a new seal.

Twenty-seven (27) tamper evident seals are required to complete the physical security requirements for the Brocade 7840. Steps 1 – 5 below, detail the tamper evident seal placement for the Brocade 7840 module.

1. Apply two (2) seals to the front side of the module. See Figure 2 for correct seal placement.
2. Apply twelve (12) seals to the back side of the module. See Figure 3 for correct seal placement.
3. Apply five (5) seals to the left side of the module. These seals will wrap around to the bottom of the module. See Figure 4 for correct seal placement.
4. Apply five (5) seals to the right side of the module. These seals will wrap around to the bottom of the module. See Figure 5 for correct seal placement.
5. Apply three (3) seals to the bottom side of the module near the front side. See Figure 6 for correct seal placement.

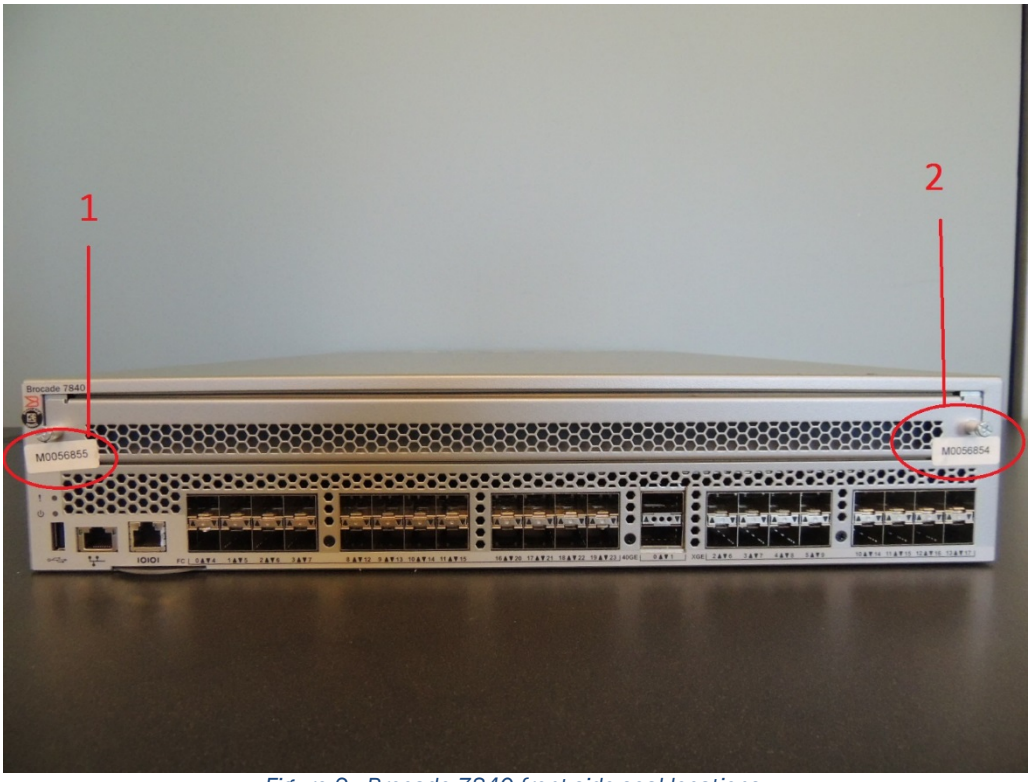

Figure 2 - Brocade 7840 front side seal locations

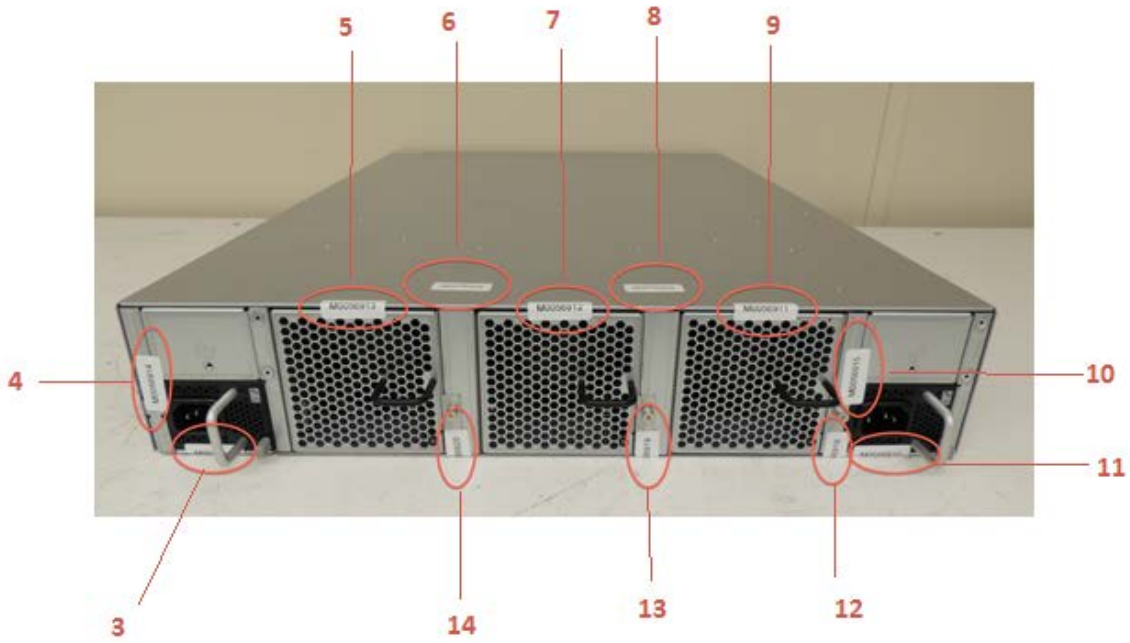

Figure 3 - Brocade 7840 back side seal locations

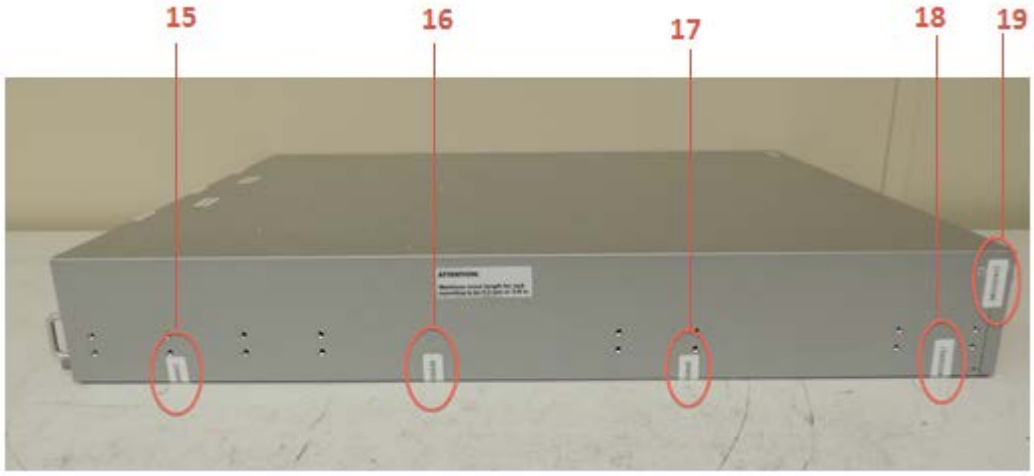

Figure 4 - Brocade 7840 left side seal locations

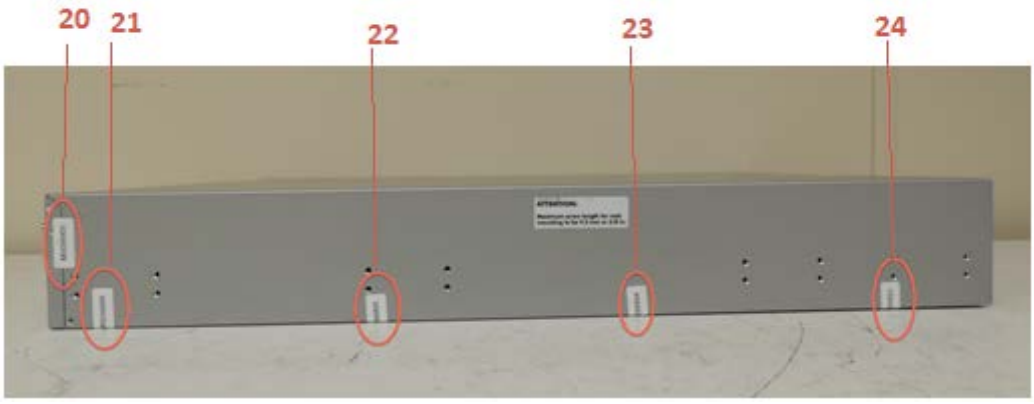

Figure 5 - Brocade 7840 right side seal locations

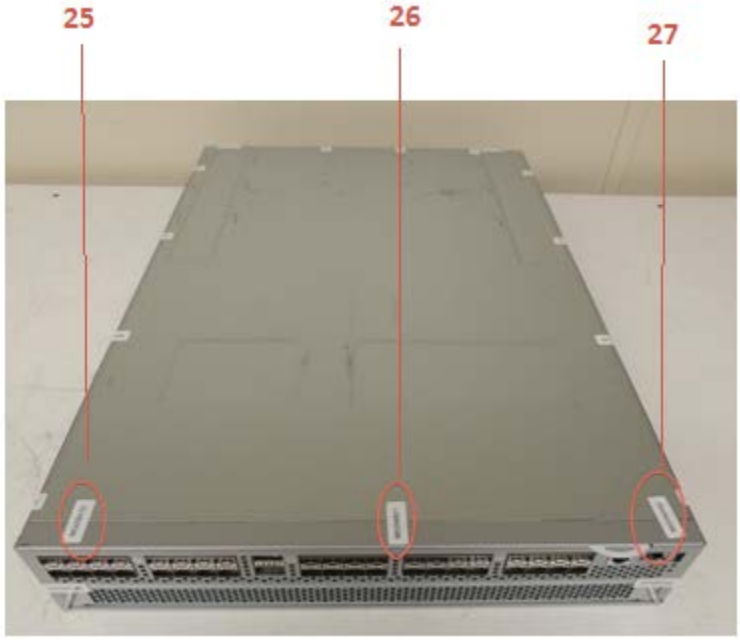

Figure 6 - Brocade 7840 bottom side seal locations

14 Appendix B: Block Diagram

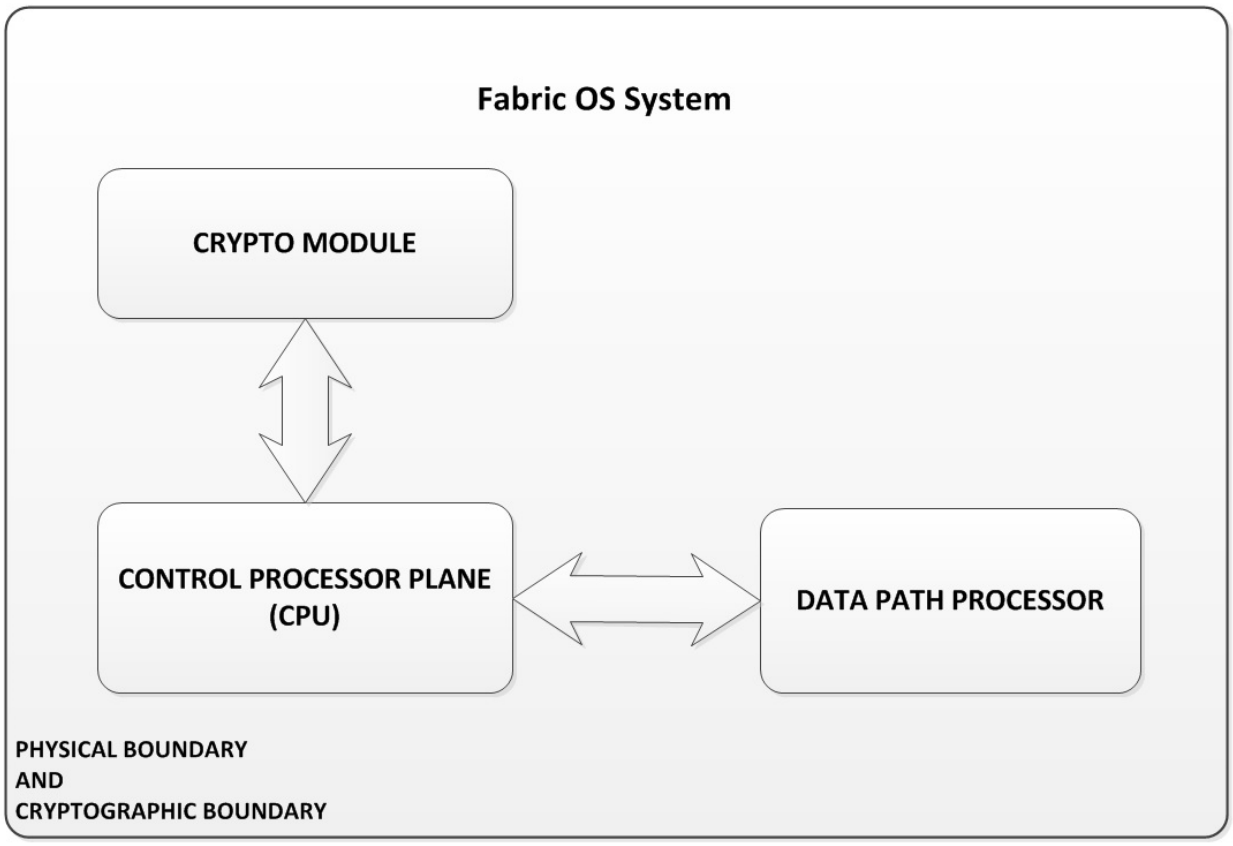

Figure 7 - Block Diagram

15 Appendix C: Critical Security Parameters & Public Keys

The module supports the following CSPs:

1. DH Private Keys for use with 2048 bit modulus
- Description: Used in DHCHAP, and SSHv2 to establish a shared secret
- Generation: Internally, using the SP800-90A DRBG (AES-256-CTR DRBG)
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination and "fipscfg -zeroize" command

2. Fibre-Channel Security Protocol (FCSP) CHAP Secret
- Description: Shared secret used for authentication in FC-Security Protocol
- Generation: N/A
- Storage: Plaintext in RAM, Compact Flash
- Entry: Configured by an operator during the secauthsecret command
- Output: N/A
- Key-To-Entity: User
- Destruction: "secauthsecret -remove" command and "fipscfg -zeroize" command

3. Fibre-Channel Authentication Protocol (FCAP) Private Key (RSA 2048)
- Description: PKI based authentication for peer FC switches
- Generation: Internally, using the SP800-90A DRBG (AES-256-CTR DRBG)
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

4. SSHv2/SCP/SFTP Session Keys - 128, 192, and 256 bit AES CBC or Triple-DES 3 key CBC
- Description: AES or Triple-DES encryption key used to secure SSHv2/SCP/SFTP sessions
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

5. SSHv2/SCP/SFTP Authentication Key [HMAC-SHA-1 (160 bits)]
- Description: Session authentication key used to authenticate and provide integrity of SSHv2 session
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

6. SSHv2 KDF Internal State
- Description: Used to generate Host encryption and authentication key
- Generation: Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: RAM in plaintext

- Entry: N/A
- Output: N/A
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

7. SSHv2 DH Shared Secret Key (2048 bit)
- Description: Shared secret from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Destruction: Session termination or "fipscfg -zeroize" command

8. SSHv2 ECDH Shared Secret Key (P-256, P-384 and P-521)
- Description: Shared secret from the ECDH Key Agreement primitive. Used in SSHv2 KDF to derive (client and server) session keys
- Generation: N/A
- Establishment: SSHv2 ECDH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Destruction: Session termination or "fipscfg -zeroize" command

9. SSHv2 ECDH Private Key (P-256, P-384 and P-521)
- Description: ECDH private key (NIST defined P curves)
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Entry: N/A as per IG 7.7
- Output: N/A as per IG 7.7
- Storage: Plaintext in RAM
- Key-To-Entity: Process
- Destruction: Session termination or "fipscfg -zeroize" command

10. SSHv2 2048 RSA Private Key
- Description: Used to authenticate SSHv2 server to client
- Generation: SP800-90A DRBG
- Storage: RAM in plaintext
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

11. SSHv2 ECDSA Private Key (P-256)
- Description: Used to authenticate SSHv2 server to client
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Storage: RAM in plaintext
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

12. Value of K during SSHv2 P-256 ECDSA session
- Description: Used to generate keys that signs and verify
- Generation: ECC standard
- Storage: RAM in plaintext
- Entry: N/A
- Output: N/A
- Key-To-Entity: User

- Destruction: Session termination or "fipscfg -zeroize" command

13. TLS Private Key (RSA 2048)
- Description: RSA key used to establish TLS sessions (decrypt padded TLS Pre-Master secret key block)
- Generation: Internally, using the SP800-90A DRBG
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

14. TLS Pre-Master Secret
- Description: Secret value used to establish the Session and Authentication key
- Generation: N/A
- Establishment: RSA key wrapped over TLS session; allowed as per FIPS 140-2 IG D.9
- Storage: Plaintext in RAM
- Entry: RSA key wrapped (after padding to block size) during TLS handshake
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

15. TLS Master Secret
- Description: 48 bytes secret value used to establish the Session and Authentication key
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 and 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

16. TLS KDF Internal State
- Description: values of the KDF internal state
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

17. TLS Session Keys - 128, 256 bit AES CBC, Triple-DES 3 key CBC
- Description: Triple-DES or AES key used to secure TLS sessions
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination and "fipscfg -zeroize" command

18. TLS Authentication Key for HMAC-SHA-1 (160 bits), HMAC-SHA-256, HMAC-SHA-384
- Description: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 key used to provide data authentication for TLS sessions
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination and "fipscfg -zeroize" command

19. DRBG Seed Material
- Description: Seed material for SP800-90A DRBG (AES-256-CTR DRBG)
- Generation: Internally generated; raw random data from NDRNG
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: Session termination or "fipscfg -zeroize" command

20. DRBG Internal State (V and Key)
- Description: SP800-90A DRBG (AES-256-CTR DRBG) Internal State
- Generation: SP800-90A DRBG seeded by raw random data from NDRNG
- Establishment: N/A
- Storage: RAM (plaintext)
- Entry: N/A
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

21. Passwords
- Description: Password used to authenticate operators (8 to 40 characters)
- Generation: N/A
- Storage: MD5 digest (plaintext) in Compact Flash
- Entry: Configured by the operator during account maintenance and authentication
- Output: N/A
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

22. RADIUS Secret
- Description: Used to authenticate the RADIUS Server (8 to 40 characters)
- Generation: N/A
- Storage: Plaintext in RAM and Compact Flash
- Entry: Configured by an operator during the "aaaconfig - add" command
- Output: CLI through "aaaconfig -show" and "configupload"
- Key-To-Entity: User
- Destruction: "fipscfg -zeroize" command

23. DH Private Key (256 bits) (Used in IKEv2)
- Description: Used in IKEv2 Diffie-Hellman to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Establishment: N/A
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SPI
- Destruction: KDF completion or session termination

24. DH Shared Secret (2048 bits) (Used in IKEv2)
- Description: Shared secret from the DH Key agreement primitive - (K) and (H) used in in IKEv2.
- Generation: N/A
- Establishment: IKEv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Storage: Plaintext in RAM

- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SPI
- Destruction: Session termination

25. IKEv2 AES-256-GCM Encrypt/Decrypt Keys
- Description: Symmetric keys used for AES-256 encrypt/decrypt
- Generation: N/A
- Establishment: DH Key Agreement and IKEv2 KDF (SP800-135 Section4.1.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Storage: Cavium key memory
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SA Number
- Destruction: Session termination

26. ESP AES-256-GCM Encrypt/Decrypt Keys
- Description: Symmetric keys used for AES-256 encrypt/decrypt
- Generation: N/A
- Establishment: DH Key Agreement and IKEv2 KDF (SP800-135 Section4.1.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Blitzer FPGA key memory
- Entry: N/A
- Output: N/A
- Key-To-Entity: ESP SA Number
- Destruction: Session termination

27. IKEv2 KDF State
- Description: values of the IKEv2 KDF internal state
- Generation: N/A
- Establishment: IKEv2 KDF (SP800-135 Section4.1.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: N/A
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SA control memory
- Destruction: Session termination

28. IKEv2 Authentication Key
- Description: Pre-shared secret key used for IKEv2 session authentication (512 bits)
- Generation: N/A
- Establishment: Encrypted/authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9.
- Storage: Plaintext in RAM
- Entry: Encrypted/authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9.
- Output: N/A
- Key-To-Entity: IKEv2 SA control memory
- Destruction: Session termination

29. DRBG Internal State (V and Key) (On Cavium)
- Description: SP800-90A DRBG (AES-256-CTR DRBG) Internal State
- Generation: SP800-90A DRBG seeded by raw random data from NDRNG
- Establishment: N/A
- Storage: Cavium
- Entry: N/A
- Output: N/A
- Key-To-Entity: OpenSSL context per core
- Destruction: Session termination

30. Entropy Data (on Cavium)
- Description: Seed material for SP800-90A DRBG (AES-256-CTR DRBG)
- Generation: internally generated; raw random data from NDRNG

- Establishment: N/A
- Storage: Cavium
- Entry: N/A
- Output: N/A
- Key-To-Entity: Cavium Random Number Memory
- Destruction: DRBG Instantiation

- - - - - - - - - - - - PUBLIC KEYS - - - - - - - - - - - -

31. DH Public Key (2048 bit modulus)
- Description: Used to establish shared secrets (SSHv2 and DHCHAP)
- Generation: SP800-90A DRBG
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: plaintext
- Key-To-Entity: User

32. DH Peer Public Key (2048 bit modulus)
- Description: Used to establish shared secrets (SSHv2 and DHCHAP)
- Generation: N/A
- Storage: Plaintext in RAM
- Entry: plaintext
- Output: N/A

33. FCAP Public Key (RSA 2048)
- Description: PKI based authentication for peer FC switches
- Generation: N/A
- Storage: Plaintext in DRAM
- Entry: plaintext
- Output: plaintext
- Key-To-Entity: User

34. FCAP Peer Public Key (RSA 2048)
- Description: PKI based authentication for peer FC switches
- Generation: N/A
- Storage: Plaintext in DRAM
- Entry: plaintext
- Output: N/A
- Key-To-Entity: User

35. TLS Public Key (RSA 2048)
- Description: Used by client to encrypt TLS Pre-Master Secret
- Generation: SP800-90A DRBG
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: plaintext
- Key-To-Entity: User

36. TLS Peer Public Key (RSA 2048)
- Description: Used to authenticate the client
- Generation: N/A
- Storage: Plaintext in Compact Flash
- Entry: Plaintext during TLS handshake protocol
- Output: N/A
- Key-To-Entity: User

37. FW Download Public Key (RSA 2048)
- Description: Used to update the FW of the module.
- Generation: N/A Generated outside the module
- Storage: Plaintext in Compact Flash

- Entry: Through firmwarekeyupdate cmd or through FW Update.
- Output: Through firmwarekeyshow cmd
- Key-To-Entity: User

38. SSHv2 RSA 2048 bit Public Key
- Description: Used to authenticate the SSHv2 server to the client
- Generation: SP800-90A DRBG
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: plaintext during SSHv2 handshake
- Key-To-Entity: User

39. SSHv2 ECDSA Public Key (P-256)
- Description: Used to authenticate SSHv2 server to client
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Storage: Plaintext in Compact Flash
- Entry: N/A
- Output: plaintext during SSHv2 handshake
- Key-To-Entity: User

40. LDAP ROOT CA certificate (RSA 2048)
- Description: Used to authenticate LDAP server
- Generation: N/A
- Storage: Plaintext in Compact Flash
- Entry: Plaintext
- Output: N/A
- Key-To-Entity: User

41. DH Public Key (2048-bit) (Used in IKEv2)
- Description: Used in IKEv2 Diffie-Hellman to establish a shared secret
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Establishment: N/A
- Storage: Cavium
- Entry: N/A
- Output: N/A
- Key-To-Entity: IKEv2 SPI

42. DH Peer Public Key (2048-bit) (Used in IKEv2)
- Description: Used in IKEv2 Diffie-Hellman to establish a shared secret
- Generation: N/A
- Establishment: N/A
- Storage: Cavium
- Entry: IKEv2
- Output: N/A
- Key-To-Entity: IKEv2 SPI

43. SSHv2 ECDH Public Key (P-256, P-384 and P-521)
- Description: ECDH public key (NIST defined P curves)
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A.
- Establishment: N/A
- Entry: N/A
- Output: Plaintext
- Storage: Plaintext in RAM
- Key-To-Entity: Process
- Destruction: N/A