Brocade® DCX, DCX 8510-8, DCX-4S and DCX 8510-4 Backbones, 6510 and 6520 FC Switches, and 7800 Extension Switch

FIPS 140-2

Non-Proproprietary

Security Policy

Document Version 1.0

Brocade Communications Systems, Inc.

January 20, 2017

Document History

Version	Publication Date	Summary of Changes
1.0	January 20, 2017	Initial Release

Table of Contents

Table of Tables

Table of Figures

1 Module Overview

The Brocade 6510, 6520, 7800, DCX, DCX 8510-8, DCX-4S and DCX 8510-4 are multiple-chip standalone cryptographic modules, as defined by FIPS 140-2. The cryptographic boundary for DCX, DCX 8510-8, DCX-4S and DCX 8510-4 backbone is the outer perimeter of the metal chassis including the removable cover, control processor blades, core switch blades, and port blades or filler panels. The cryptographic boundary of the 6510 FC Switch, 6520 FC Switch, and 7800 is the outer perimeter of the metal chassis including the removable cover. The module is a Fiber Channel and/or Gigabit Ethernet routing switch that provides secure network services and network management.

For each 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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

1.1 Brocade 6510 FC Switch

Figure below illustrates the Brocade 6510 FC Switch cryptographic module.

Figure 1 - Brocade 6510 FC Switch

Switch	SKU	Part Number	Brief Description
Brocade 6510	BR-6510-48-16G-R	80-1005272-03	Brocade 6510, 48 ports 16G configuration (minimal 24 ports + 24-port POD licenses) with port[2] side air flow - Forty-eight (48) ports are enabled: Factory installed, two licenses BR-MIDR12POD-01 to enable 24 additional ports - Quantity of 48, 16GB SFPs - Quantity of 2 Power Supply and Fan Assembly (XBR-5100-0001)

Table 2 – Brocade 6510 FC Switches (Validated 6510 Configurations)

Table below lists power supply and fan assemblies supported on Brocade 6510 FC Switches:

SKU	Part Number	Description
XBR-5100-0001	80-1001304-02	Brocade 5100 Power Supply/Fan FRU, Port-side exhaust airflow

Table 3 - Brocade 6510 FC Switch Supported Power Supplies and Fan Assemblies

Table below lists software licenses supported on Brocade 6510 FC Switches:

SKU	Part Number	Description
BR-MIDR12POD-01	80-1005356-02	Software, POD license, 12 Port On-Demand internal support part

Table 4 - Brocade 6510 FC Switch Software Licenses

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

1.2 Brocade 6520 FC Switch

Figure below illustrates the Brocade 6520 cryptographic module.

Figure 2 - Brocade 6520

Switch	SKU / Part Number	Brief Description
Brocade 6520	BR-6520-96-16G-R / 80-1007257-03	Brocade 6520, 96 ports 16G configuration (minimal 48 ports + 48-port POD license) with port side air flow - Forty-eight additional ports are enabled by software POD license SW-ENTPOD2-01. - Quantity of 96, 16GB, Short Wavelength (SWL) SFPs - Quantity of three fan FRUs (XBR-FAN-80-R) and - Quantity of two 1100W AC power supplies (XBR-1100WPSAC-R)

Table 5 – Brocade 6520 FC Switches (Validated Brocade 6520 Configurations)

Table below lists power supplies supported on Brocade 6520 FC Switches:

SKU	Part Number	Brief Description
XBR-1100WPSAC-R	80-1007263-01	FRU 1100W AC Power Supply, Port side exhaust airflow

Table 6- Brocade 6520 FC Switch Supported Power Supplies

Table below lists fan assemblies supported on Brocade 6520 FC Switches:

SKU	Part Number	Brief Description
XBR-FAN-80-R	80-1004580-02	Fan FRU, 80MM, Port side exhaust airflow

Table 7 - Brocade 6520 FC Switch Supported Fan Assemblies

Table below lists software licenses supported on Brocade 6520 FC Switches:

SKU	Part Number	Brief Description
SW-ENTPOD2-01	80-1007272-01	Software, Port On Demand, enable forty-eight (48) ports

Table 8 - Brocade 6520 FC Switch Software Licenses

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

1.3 Brocade 7800 Extension Switch

Figure below illustrates the Brocade 7800 cryptographic module.

Figure 3 - Brocade 7800

Switch	SKU	Part Number	Brief Description

Brocade 7800	BR-7800F-0001	80-1006977-02	Brocade 7800, 22 ports 16G configuration (baseline + 16 ports Upgrade License; with upgrade package XBR-7800UG-0001)
			- SW-7800UG-01 licenses
			- Provides 22 ports,
			  - Quantity of 16, Fiber Channel optical ports, and
			  - Quantity of 6, 1Gbps Ethernet ports
			- Quantity of 16, 8GB Short Wavelength (SWL) SFPs

Table 9 – Brocade 7800 Extension Switch (Validated Brocade 7800 Configurations)

Table below lists upgrade packages for Brocade 7800 Extension Switch. These upgrade packages include software licenses and optics supported on Brocade 7800 Extension Switch:

SKU	Part Number	Brief Description
XBR-7800UG-0001	80-1002820-02	Software, 7800 upgrade package: - This upgrade package includes POD software license and optics components Software POD license component: - All total 16 (4 + 12) Fiber Channel optical ports are enabled - POD license enables 12 additional ports - Base unit of this device comes with 4 minimal ports enabled - Also, all total 6 (2 + 4) 1GbE Ethernet ports are enabled - POD license enables 4 additional ports - Base unit of this device comes with 2 minimal ports enabled Optics components: - This package will also include twelve 8GB Short Wavelength SFP optics

Table 10 – Brocade 7800 Upgrade Packages (software licenses and optics)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

1.4 Brocade DCX-4S, DCX 8510-4, DCX and DCX 8510-8 Backbones

Brocade DCX-4S, DCX 8510-4, DCX and DCX 8510-8 refer to four distinct 8 Gbps and 16 Gbps core Fiber Channel switch configurations. These configurations are based on selected chassis, a common Control Processor blade, four different (8 Gbps and 16 Gbps) Core blades; a selection of 8/16 Gbps FC port blades and an optional FC extender blade.

Backbone models are described in the table below:

Backbone	SKU	Part Number	Brief Description
Brocade DCX	BR-DCX-0002[1]	80-1006752-01	Brocade DCX configuration, 2 Power Supplies, 0 Ports, 2 Control Processor blades (CP8), 2 Core blades (CR8), 0 SFPs, Enterprise Bundle[2], 2 WWN
Brocade DCX-4S	BR-DCX4S-0002[1]	80-1006772-01	Brocade DCX-4S configuration, 2 Power Supplies, 0 Port, 2 Control Processor blades (CP8), 2 Core blades (CR4S-8), 0 SFPs, BR, Enterprise Bundle[2]
Brocade DCX 8510-4	BR-DCX8514-0002[1]	80-1006964-01	Brocade DCX8510-4 configuration, 2 Power Supplies, 0 Ports, 2 Control Processor blades, 2 16G Core blades, 0 SFPs, Enterprise Bundle[2]
Brocade DCX 8510-8	BR-DCX8518-0001[1]	80-1007025-01	Brocade DCX8510-8 configuration, 2 Power Supplies, 0 Ports, 2 Control Processor blades (CP8), 2 16GB Core blades (CR16-8), 0 SFPs, Enterprise Bundle[2]

Table 11 - Backbone Models

Notes for table above:

1. SKU refers to a bundled / combined package which include chassis and minimal required line cards / blades.
2. Enterprise Software License Bundle: Adaptive Networking, Extended Fabrics, Advance Performance Monitoring, Trunking, Fabric Watch, Server Application Optimized.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

The blades listed below may be used in backbone-based validated module configurations:

Blade	Acronym	Part Number	Brief Description
CP8 Control Processor Blade	CP8	80-1006794-01	FRU, Control Processor blade for DCX product (for DCX, DCX-4S, DCX8510-4 and DCX8510-8)
CR16-4 Core Switch Blade	CR16-4	80-1004897-01	FRU, Core blade for DCX8510-4
CR16-8 Core Switch Blade	CR16-8	80-1004898-01	FRU, Core blade for DCX8510-8
CR4S-8 Core Switch Blade	CR4S-8	80-1006771-01	FRU, Core blade for DCX-4S
CR8 Core Switch Blade	CR8	80-1006750-01	FRU, Core blade for DCX
FC16-32 Port Blade	FC16-32	80-1005166-02	FRU, Port blade with 32 FC Ports for DCX8510-4 or DCX-8510-8 configurations, with 16G SFP
FC16-48 Port Blade	FC16-48	80-1005187-02	FRU, Port blade with 48 FC Ports for DCX8510-4 or DCX-8510-8 configurations, with 16G SFP
FC8-16 Port Blade	FC8-16	80-1006936-01	FRU, Port blade with 16 FC Ports for DCX or DCX-4S configurations, with 8G SFP
FC8-32 Port Blade	FC8-32	80-1006779-01	FRU, PORT BLADE, 32 FC Ports for DCX or DCX-4S configurations, with 8G SFP
FC8-48 Port Blade	FC8-48	80-1006823-01	FRU, PORT BLADE, 48 FC Ports for DCX or DCX-4S configurations, with 8G SFP
FC8-64 Port Blade	FC8-64	80-1007000-01	FRU, PORT BLADE, 64 Ports for DCX or DCX-4S configurations, with 8G SFP
FX8-24 Port Blade	FX8-24	80-1007017-01	FRU, Extender blade, 8G X 12 Ports, 10x1GBE, 2X10GBE
DCX/DCX 8510-8 Filler Panel	DCX/DCX 8510-8 Filler Panel	49-1000016-04	Filler Panel (for DCX and DCX8510-8)
DCX-4S Backbone Filler Panel	DCX-4S Filler Panel	49-1000064-02	Filler Panel (for DCX-4S)
DCX-4S/DCX 8510-4 Filler Panel	DCX-4S/DCX 8510-4 Filler Panel	49-1000294-05	Filler Panel (for DCX-4S and DCX8510-4)

Table 12 - Supported Blades

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 4, illustrates representative configurations of the DCX-4S (left image) and DCX (right image) cryptographic modules. These are not the only possible configurations. Other possible configurations can be created by utilizing other compatible blades as listed in Table 12.

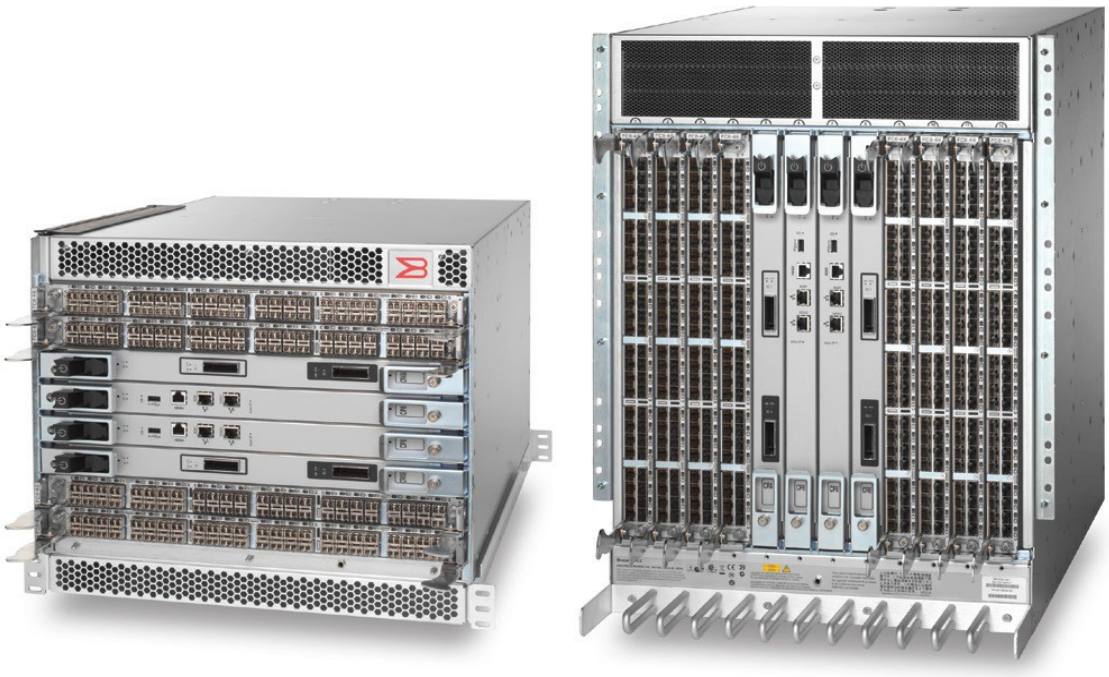

Figure 4 - DCX-4S and DCX

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 5 illustrates representative configurations of the DCX 8510-4 (left image) and DCX 8510-8 (right image) cryptographic modules. These are not the only possible configurations. Other possible configurations can be created by utilizing other compatible blades as listed in Table 12.

Figure 5 - DCX 8510-4 and DCX 8510-8

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

1.4.1 Validated modules

Validated DCX configurations are listed below.

Configuration Reference	SKU / Part Number	Quantity	Description
DCX (Configuration)	BR-DCX-0002 / 80-1006752-01	1	Brocade DCX chassis which includes: - Quantity of 2 Power Supplies (SKU=DCX, DCX-4S + 8510 2000W POWER SUPPLY, P/N=80-1001273-03) - Quantity of 2 Control Processor blades (SKU=CP8, P/N=80-1006794-01) - Quantity of 2 Core blades (SKU=CR8, P/N=80-1006750-01)
	FC8-32 / 80-1006779-01	1	FC8-32 Port Blade

Table 13 - Validated DCX Configurations

Validated DCX-4S configurations are listed below.

Configuration Reference	SKU / Part Number	Quantity	Description
DCX-4S (Configuration 1)	BR-DCX4S-0002 / 80-1006772-01	1	Brocade DCX-4S chassis which includes: - Quantity of 2 Power Supplies (SKU=DCX, DCX-4S + 8510 2000W POWER SUPPLY, P/N=80-1001273-03) - Quantity of 2 Control Processor blades (SKU=CP8, P/N=80-1006794-01) - Quantity of 2 Core blades (SKU=CR4S-8, P/N=80-1006771-01)
	FC8-32 / 80-1006779-01	1	FC8-32 Port Blade
	FC8-48 / 80-1006823-01	1	FC8-48 Port Blade
DCX-4S (Configuration 2)	BR-DCX4S-0002 / 80-1006772-01	1	Brocade DCX-4S chassis which includes: - Quantity of 2 Power Supplies (SKU=DCX, DCX-4S + 8510 2000W POWER SUPPLY, P/N=80-1001273-03) - Quantity of 2 Control Processor blades (SKU=CP8, P/N=80-1006794-01) - Quantity of 2 Core blades (SKU=CR4S-8, P/N=80-1006771-01)
	FC8-16 / 80-1006936-01	1	FC8-16 Port Blade
	FC8-48 / 80-1006823-01	1	FC8-48 Port Blade

Table 14 - Validated DCX-4S Configurations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Validated DCX 8510-4 configurations are listed below.

Configuration Reference	SKU / Part Number	Quantity	Description
DCX 8510-4 (Configuration 1)	BR-DCX8514-0002 / 80-1006964-01	1	Brocade DCX chassis which includes: - Quantity of 2 Power Supplies (SKU=DCX, DCX-4S + 8510 2000W POWER SUPPLY, P/N=80-1001273-03) - Quantity of 2 Control Processor blades (SKU=CP8, P/N=80-1006794-01) - Quantity of 2 Core blades (SKU=CR16-4, P/N=80-1004897-01)
	FC16-48 / 80-1005187-02	1	FC16-48 Port Blade
	FC8-64 / 80-1007000-01	1	FC8-64 Port Blade

Table 15 - Validated DCX 8510-4 Configurations

Validated DCX 8510-8 configurations are listed below.

Configuration Reference	SKU / Part Number	Quantity	Description
DCX 8510-8 (Configuration)	BR-DCX8518-0001 / 80-1007025-01	1	Brocade DCX chassis which includes: - Quantity of 2 Power Supplies (SKU=DCX, DCX-4S + 8510 2000W POWER SUPPLY, P/N=80-1001273-03) - Quantity of 2 Control Processor blades (SKU=CP8, P/N=80-1006794-01) - Quantity of 2 Core blades (SKU=CR16-8, P/N=80-1004898-01)
	FC16-32 / 80-1005166-02	1	FC16-32 Port Blade
	FX8-24 / 80-1007017-01	1	Extender blade

Table 16 - Validated DCX 8510-8 Configurations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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 17 - Module Security Level Specification

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

3 Modes of Operation

3.1 Approved mode of operation

3.1.1 Algorithm certificates

3.1.1.1 Brocade 6510 and Brocade 7800

Approved Algorithm	Description	Certificate Number
AES Note: AES-ECB mode is latent functionality i.e. not used in FIPS Approved mode of operation. It is used in non-Approved FIPS mode.	ECB (e/d; 128 , 192 , 256); CBC (e/d; 128 , 192 , 256);	2876
CVL	ECC CDH Primitive (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength) Curves tested: P-256 P-384 P-521	311
CVL	TLS v1.0/1.1 and v1.2 KDF NOTE: SSL “is not” supported in FIPS mode. TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384))	312
CVL	SSHv2 KDF SSH (SHA 1 , 224 , 256 , 384 , 512)	312
DRBG	SP800-90A CTR_DRBG (AES-256-CTR) CTR_DRBG: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256)	670
ECDSA NOTE: P-384 and P-521 are latent functionality i.e. not available in any services in FIPS mode or non-FIPS mode	P-256 FIPS186-4: PKG: CURVES(P-256 P-384 P-521 TestingCandidates) PKV: CURVES(P-256 P-384 P-521) SigGen: CURVES(P-256: (SHA-256, 384, 512) SigVer: CURVES(P-256: (SHA-256, 384, 512))	942
HMAC NOTE: HMAC-SHA224 and HMAC-SHA512 are latent functionality, i.e. not available and not used in any services in FIPS mode or non-FIPS modes.	HMAC-SHA-1, 224, 256, 384, 512 (160-bit key) HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS) HMAC-SHA224 (Key Size Ranges Tested: KS<BS) HMAC-SHA256 (Key Size Ranges Tested: KS<BS) HMAC-SHA384 (Key Size Ranges Tested: KS<BS) HMAC-SHA512 (Key Size Ranges Tested: KS<BS)	1814

Approved Algorithm	Description	Certificate Number
RSA NOTE: 3072-bit key is latent functionality, i.e. not available and not used in any services in FIPS mode or non-FIPS modes. NOTE: Signature Generation and Signature Verification utilizing SHA-224, SHA-384 and SHA-512 are latent functionalities, i.e. not available and not used in any services in FIPS mode.	2048-bit and 3072-bit keys FIPS186-4: 186-4KEY(gen): FIPS186-4_Fixed_e (65537) ; PGM (ProbPrimeCondition): 2048, 3072 PPTT:(C.2) ALG [RSASSA-PKCS1_V1_5] SIG(gen) (2048 SHA(224 , 256 , 384 , 512)) (3072 SHA(224 , 256 , 384 , 512)) SIG (Ver) (1024 SHA(224 , 256 , 384 , 512)) (2048 SHA(224 , 256 , 384 , 512)) (3072 SHA(224 , 256 , 384 , 512))	2234
SHS NOTE: SHA-224, SHA-384 and SHA-512 are latent functionalities i.e. not available in any services in FIPS mode	SHA-1, 224, 256, 384, 512 SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)	2417
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. TCBC(KO 1 e/d,)	1719

Table 18 - Approved Algorithms available in firmware on Brocade 6510 and Brocade 7800

FIPS Approved mode enables:

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

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.

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 Cert. #311, key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength)
- HMAC-MD5 to support RADIUS authentication (HMAC-MD5 is not exposed to the operator)
- 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)

3.1.1.2 Brocade 6520 and Brocade DCX Control Processor (CP) blade

Approved Algorithm	Description	Certificate Number
AES Note: AES-ECB mode is latent functionality, i.e. not used in FIPS Approved mode of operation. It is used in non-Approved FIPS mode.	ECB (e/d; 128 , 192 , 256); CBC (e/d; 128 , 192 , 256);	2893
CVL	ECC CDH Primitive (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength) Curves tested: P-256 P-384 P-521	320
CVL	TLS v1.0/1.1 and v1.2 KDF NOTE: SSL “is not” supported in FIPS mode. TLS(TLS1.0/1.1 TLS1.2 (SHA 256 , 384))	321
DRBG	SP800-90A CTR_DRBG (AES-256-CTR) CTR_DRBG: [Prediction Resistance Tested: Enabled; BlockCipher_Use_df: (AES-256)	671
ECDSA NOTE: P-384 and P-521 are latent functionality, i.e. not available in any services in FIPS mode or non-FIPS mode	P-256 FIPS186-4: PKG: CURVES(P-256 P-384 P-521 TestingCandidates) PKV: CURVES(P-256 P-384 P-521) SigGen: CURVES(P-256: (SHA-256, 384, 512) SigVer: CURVES(P-256: (SHA-256, 384, 512))	943
HMAC NOTE: HMAC-SHA224 and HMAC-SHA512 are latent functionality, i.e. not available and not used in any services in FIPS mode or non-FIPS modes.	HMAC-SHA-1, 224, 256, 384, 512 (160-bit key) HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS) HMAC-SHA224 (Key Size Ranges Tested: KS<BS) HMAC-SHA256 (Key Size Ranges Tested: KS<BS) HMAC-SHA384 (Key Size Ranges Tested: KS<BS) HMAC-SHA512 (Key Size Ranges Tested: KS<BS)	1829

Approved Algorithm	Description	Certificate Number
RSA NOTE: 3072-bit key is latent functionality, i.e. not available and not used in any services in FIPS mode or non-FIPS modes. NOTE: Signature Generation and Signature Verification utilizing SHA-224, SHA-384 and SHA-512 are latent functionalities, i.e. not available and not used in any services in FIPS mode.	2048-bit and 3072-bit keys FIPS186-4: 186-4KEY(gen): FIPS186-4_Fixed_e (65537) ; PGM(ProbPrimeCondition): 2048 , 3072 PPTT:(C.2) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (2048 SHA(224, 256, 384, 512)) (3072 SHA(224 ,256 ,384 ,512)) SIG(Ver) (1024 SHA(224 , 256 , 384 , 512)) (2048 SHA(224, 256, 384, 512)) (3072 SHA(224, 256, 384, 512))	2235
SHS NOTE: SHA-224, SHA-384 and SHA-512 are latent functionalities i.e. not available in any services in FIPS mode	SHA-1, 224, 256, 384, 512 SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)	2436
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.	1724

Table 19 - Approved Algorithms available in firmware on Brocade 6520 and DCX Control Processor (CP) blade

FIPS Approved mode enables:

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

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.

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 Cert. #320, key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength)
- HMAC-MD5 to support RADIUS authentication (HMAC-MD5 is not exposed to the operator)
- 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)

3.1.2 Invoking FIPS Approved mode

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 SHA-1 hash and 0-3 within authentication protocols; Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) and FCAP.
11) Configure to use SHA-256 as the signature algorithm for FCAP authentication with group 4.
12) Do not define FCIP IKEv2 or IPSec policies
13) Disable Management Interface IPSec/IKEv2
14) Disable In-Band Management Interface
15) Disable In-Flight Encryption
16) Disable TACACS+ authspec mode
17) Confirm that LDAP CA certificate is RSA 2048 signed with SHA-256
18) Confirm that SNMP has been changed to “No Access” for SNMP SET Security
19) Enable Self-Tests
    a) `“fipscfg --enable selftests”`
20) For RADIUS authentication, configure the RADIUS server with PEAP-MSCHAPv2 mode and shared secret.
    a) **Note 1**: PEAP-MSCHAPv2 is used for authentication via RADIUS server. TLSv1.0 is the secure tunnel established between the cryptographic module and the RADIUS server; all PEAP-MSCHAPv2 data is securely tunneled via the TLSv1.0 secure tunnel.

       This is a protocol that relies on the strength of TLSv1.0, which is utilizing RSA 2048 with SHA-256 and FIPS Approved cipher suites (AES, HMAC-SHA-1).
    b) **Note 2**: TLSv1.2 is not supported for RADIUS.
21) Install removable front cover(s) (as applicable) and apply tamper labels as per Appendix A
22) Disable Boot PROM access

23) Disable Factory role access
24) Login as Admin
25) Disable Root access
26) Enable FIPS:
    a) `"fipscfg --enable fips"`
27) Power-cycle the module
28) Note: Externally generated RSA key pairs shall only be imported if they are RSA 2048
29) After certificate operations (e.g. importing) view "`fips --verify fips`" to validate FIPS
30) Execute "`fipscfg --enable SHA256`" for SSHv2 sessions with RSA 2048 keys and signed/verified with SHA-256 [NOTE: The operator can use either ECDSA or RSA]
31) Verify FIPS mode and examine that all verifications pass.
    a) `"fipscfg --verify fips"`
32) SSHv2 clients and server should support the Diffie-Hellman-group-exchange-256 and the ability to sign/verify with SHA-256 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."

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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)
- blowfish
- blowfish-cbc
- blowfish-cfb
- blowfish-ecb
- blowfish-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 sizes 1024 and 2048 (non-compliant) (for SSHv2 and TLS)
- DH key size < 2048 bits (for SSHv2)
- DH-CHAP: Diffie Hellman with NULL DH, 1024, 1280, 1536 and 2048 keys with MD5 and SHA-1 (non-compliant) hash algorithm
- SHA-1 (non-compliant)
- SHA-224 (non-compliant)
- SHA-256 (non-compliant)
- SHA-384 (non-compliant)
- SHA-512 (non-compliant)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Crypto Function/Service	User Role Change Access	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) blowfish, blowfish-cbc, blowfish-cfb, blowfish-ecb, blowfish- 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 and hash algorithms for SSL and TLS	Crypto-Officer	md2, md4, ripemd160, SHA-1 (non-compliant), SHA-224 (non-compliant), SHA-384 (non-compliant) and SHA-512 (non-compliant)
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, blowfish-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 (plaintext) 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) LDAP is 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
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	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 20 - 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: 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

1) Blades:
    a) Blade Power LED
    b) Blade Status LED
    c) Fiber Channel port status LED
    d) Fiber Channel port speed LED
    e) USB port Status LED
    f) Active CP LED
    g) Ethernet port (SERVICE) Link LED
    h) Ethernet port (SERVICE) Activity LED
    i) Ethernet port (MGMT) Link LED
    j) Ethernet port (MGMT) Activity LED
    k) ICL port LINK LED
    l) ICL port ATTN LED

2) Backbone:
    a) WWN Status Interface LED
    b) FAN power LED
    c) FAN status LED

3) Switches:
    a) Switch Power LED
    b) Switch Status LED
    c) Ethernet port Link LED
    d) Ethernet port Activity LED
    e) Gigabit Ethernet (GE) port status LED
    f) Gigabit Ethernet (GE) port activity LED
    g) Fiber Channel port status LED

Model	Port/Interface Type						
	Fiber Channel Ports	1 GbE & 10 GbE	Ethernet	Serial Port	USB	Power Supply Connectors	LED
DCX-4S	256	24	4	2	2	2	4
DCX	512	24	4	2	2	4	30
DCX 8510-4	192	12	4	2	2	2	4
DCX 8510-8	384	12	4	2	2	4	30
6510	48	0	1	1	1	2	54
6520	96	0	1	1	1	2	107
7800	16	8	1	1	1	2	32

Table 21 - Port/Interface Quantities

Blade	LED
CP8 Control Processor	8
CR16-4 Core Switch Blade	4
CR16-8 Core Switch Blade	4
CR4S-8 Core Switch Blade	6
CR8 Core Switch Blade	4
FC16-32 Port Blade	34
FC16-48 Port Blade	50
FC8-16 Port Blade	18
FC8-32 Port Blade	34
FC8-48 Port Blade	50
FC8-64 Port Blade	66
FX8-24 Port Blade	26

Table 22 - DCX-4S, DCX, DCX 8510-4, and DCX 8510-8 blade LED counts

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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

Table 23 - Roles and Required Identification and Authentication

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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.

Table 24 - Strengths of Authentication Mechanisms

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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
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 25 - Service Descriptions

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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
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			
SSHv2 and TLS	X	X		X				

Table 26 - 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.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

6.3 Definition of Critical Security Parameters (CSPs)

DH Private Keys:

- DH Private Keys for use with 2048 bit modulus

FCSP CHAP Secret:

- Fiber-Channel Security Protocol (FCSP) CHAP Secret

FCAP Private Key:

- Fiber-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

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)

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	Passwords	RADIUS Secret	FCAP Private Key	FCSP CHAP Secret
Fabric Element Authentication	N	N	N	RW	N	N	RW	RW
FIPSCfg	N	N	N	N	N	N	N	N
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z
FirmwareManagement	R	R	N	N	N	N	N	N
PKI	RW	RW	N	RW	N	N	N	N
RADIUS	N	N	N	N	RW	RW	N	N
LDAP	N	N	N	N	N	N	N	N
UserManagement	N	N	RW	RW	RW	N	N	N
SSHv2 and TLS	RW	RW	RW	N	RW	N	N	N

Table 27 - 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
Fabric Element Authentication	RW	RW	N	N	N	N
FIPSCfg	N	N	N	N	N	N
Zeroize	N	N	N	N	N	N
FirmwareManagement	N	N	N	RW	N	N
PKI	N	N	RW	N	RW	N
RADIUS	N	N	N	N	N	N
LDAP	N	N	N	N	N	RW
UserManagement	N	N	N	N	N	N
SSHv2 and TLS	RW	RW	RW	N	RW	R

Table 28 - 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) HMAC SHA-1 KAT
            (6) HMAC SHA-256 KAT
            (7) HMAC SHA-384 KAT
            (8) HMAC SHA-512 KAT
            (9) DRBG KAT
            (10) SHA-1 KAT
            (11) SHA-256 KAT
            (12) SHA-384 KAT
            (13) SHA-512 KAT
            (14) RSA 2048 SHA-256 Sign KAT
            (15) RSA 2048 SHA-256 Verify KAT
            (16) SP800-135 SSHv2 KDF KAT
            (17) SP800-135 TLS 1.0 KDF KAT
            (18) SP800-135 TLS 1.2 KDF KAT
            (19) ECDSA KAT
            (20) 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/v1.1

ii) SSHv2

iii) TLS v1.2

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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 29 - Inspection/Testing of Physical Security Mechanisms

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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 30 - Mitigation of Other Attacks

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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
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
POD	Ports on Demand licensing
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

16GB	16 Gigabit
2 CORE	Two core switch blades
8GB	8 Gigabit
BR	Brocade
CP8	8G Control Processor blade
CR16-4	16G core switch blade for DCX 8510-4 backbone
CR16-8	16G core switch blade for DCX 8510-8 backbone
CR4S-8	8G Core Switch Blade for DCX -4S backbone
CR8	8G Core Switch Blade for DCX backbone
FC	Fiber Channel
FC8-16	8G, 16-port, Fiber Channel port blade
FCIP	Fiber Channel over Internet Protocol
FX8-24	8G, 24 port, Extension blade
GBE	Gigabit Ethernet
GE	Gigabit Ethernet
ICL	Inter-Chassis Link
LIC	License
LWL	Long Wavelength
MGMT	Management
POD	Ports on Demand, Defines the size of an upgrade license. For example, a 24-Port POD License allows the user to enable twenty-four additional ports
SFP	Small form-factor pluggable
SWL	Short Wavelength
UPG	Upgrade
WWN	World Wide Name card

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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.

13.1 Brocade DCX and DCX 8510-8 Backbone

Twenty-two (22) tamper evident seals are required to complete the physical security requirements total. See Figure 6 to Figure 11 for directions.

- Apply three (3) seals to the right side of the chassis.

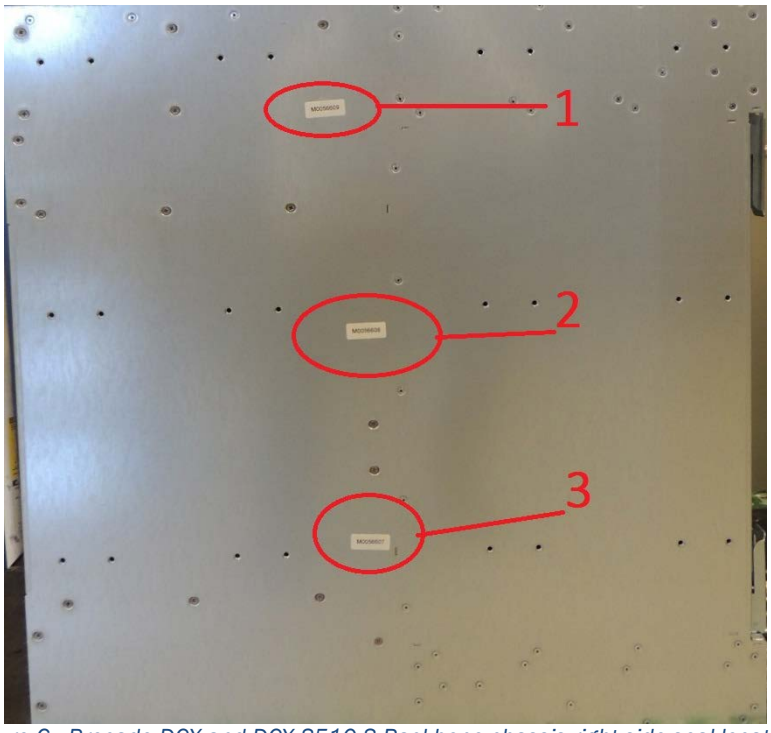

Figure 6 - Brocade DCX and DCX 8510-8 Backbone chassis right side seal location

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

- Apply twelve (12) seals to the front side of the chassis.

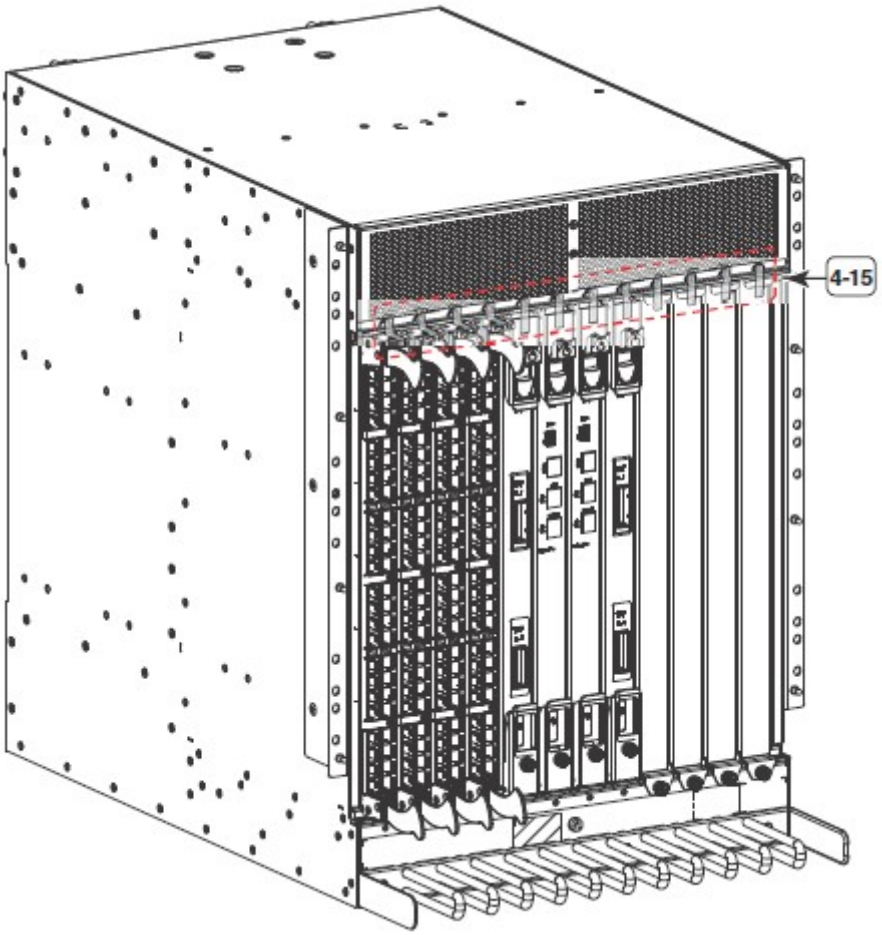

Figure 7 - Brocade DCX and DCX 8510-8 Backbone front side seal locations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

- Apply seven (7) seals to the back side of the chassis

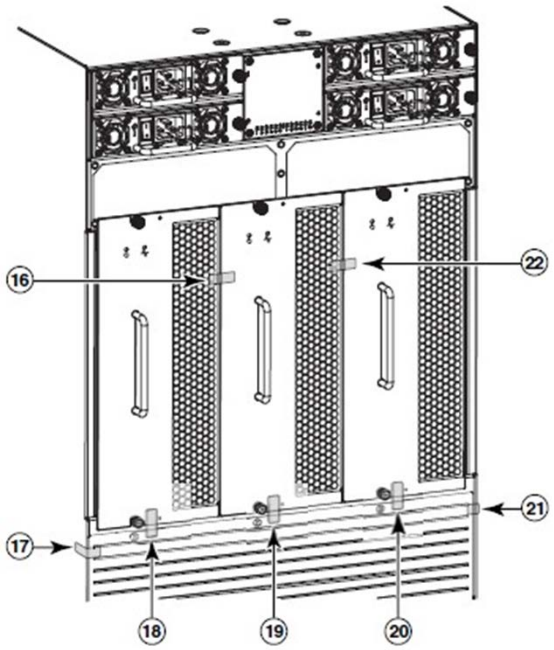

Figure 8 - Brocade DCX and DCX 8510-8 Backbone back side seal locations

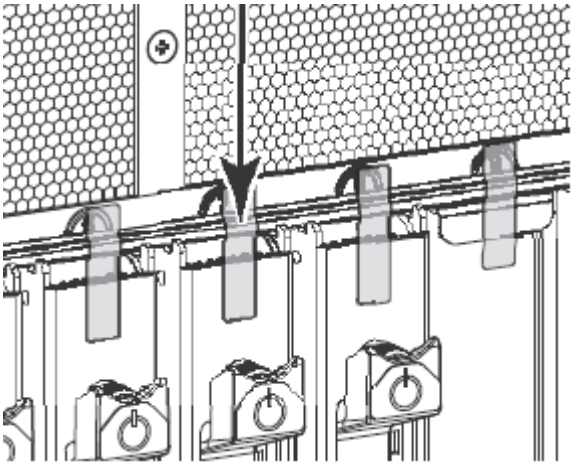

Figure 9 - Brocade DCX and DCX 8510-8 Backbone flat ejector handle seal application on the port side

Next page →

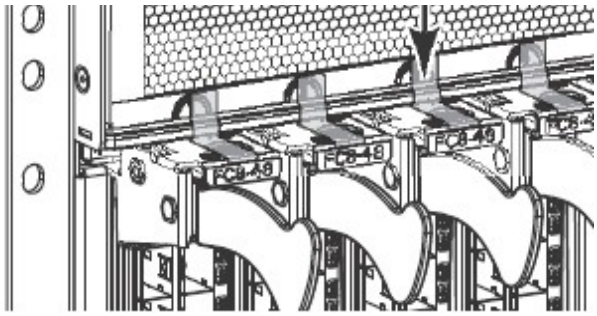

Figure 10 - Brocade DCX and DCX 8510-8 Backbone stainless steel handle seal application on the port side

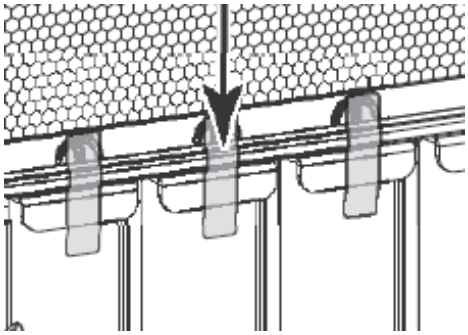

Figure 11 - Brocade DCX and DCX 8510-8 Backbone filler panel seal application on the port side

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.2 Brocade DCX-4S and DCX 8510-4 Backbone

Nineteen (19) tamper evident seals are required to complete the physical security requirements total. See Figure 12 through Figure 17 for directions.

- Apply fourteen (14) seals to the backbone front side of the chassis.

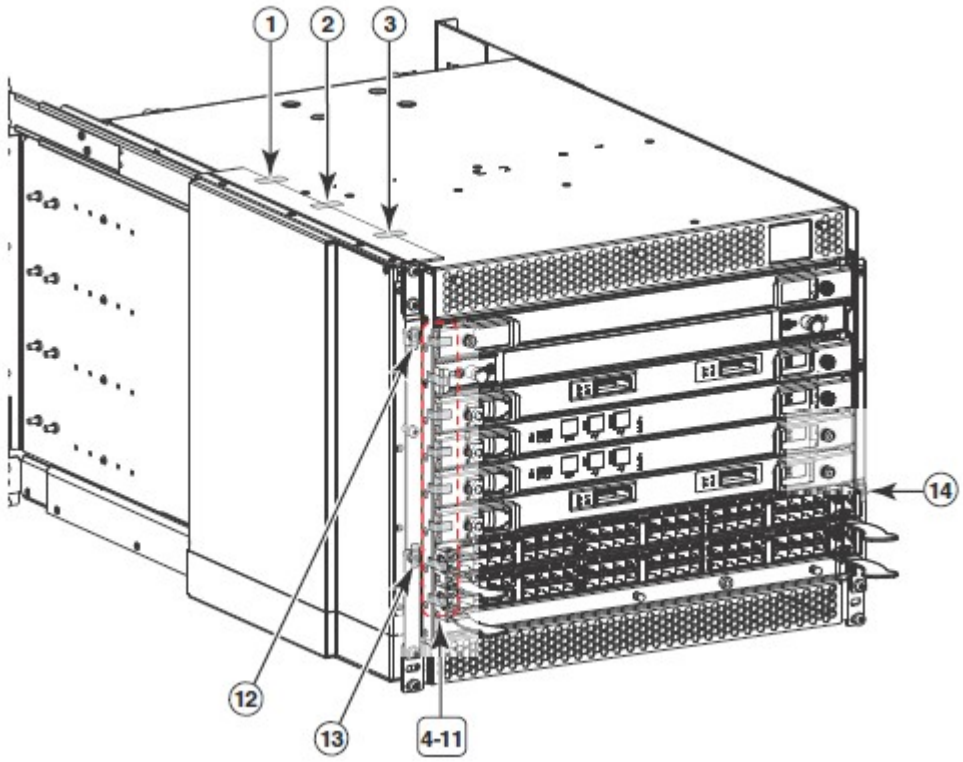

Figure 12 - Brocade DCX-4S and DCX 8510-4 Backbone front side seal locations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

- Apply five (5) seals to the back side of the chassis

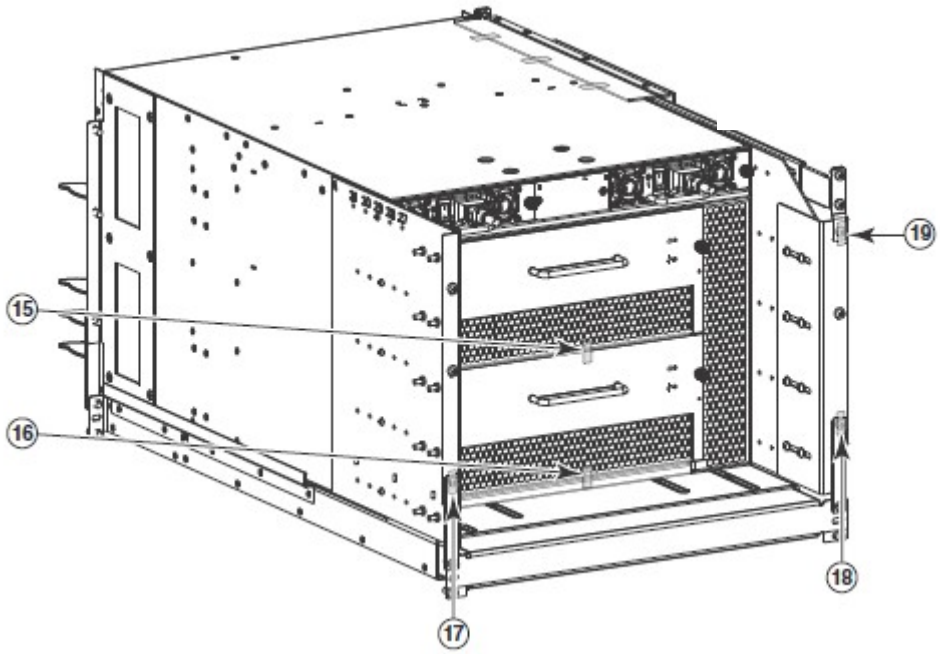

Figure 13 - Brocade DCX-4S and DCX 8510-4 Backbone back side seal locations

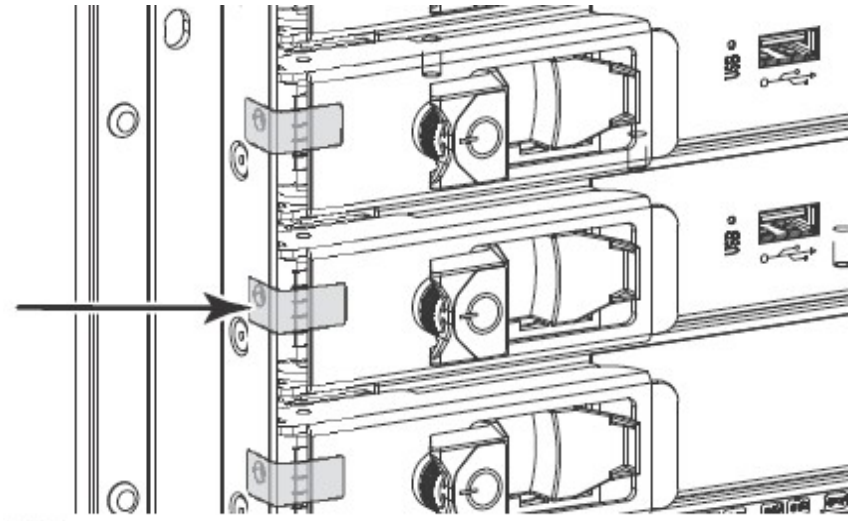

Figure 14 - Brocade DCX-4S and DCX 8510-4 Backbone flat ejector handle seal application

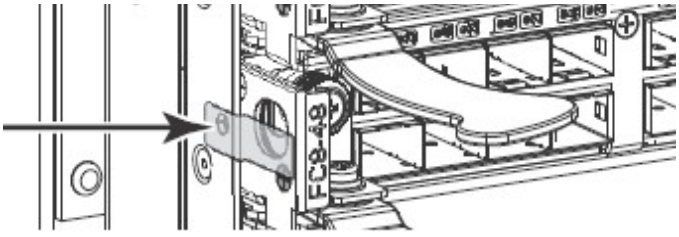

Figure 15 - Brocade DCX-4S and DCX 8510-4 Backbone stainless steel ejector handle seal application

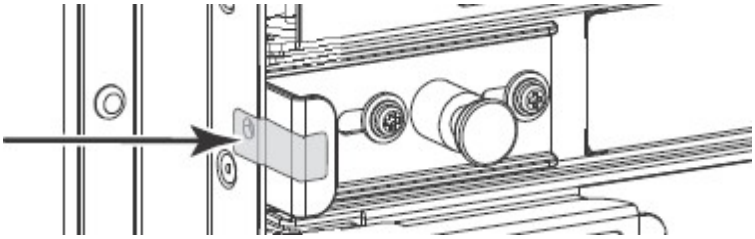

Figure 16 - Brocade DCX-4S and DCX 8510-4 Backbone filler panel (PN 49-1000294-05) seal application

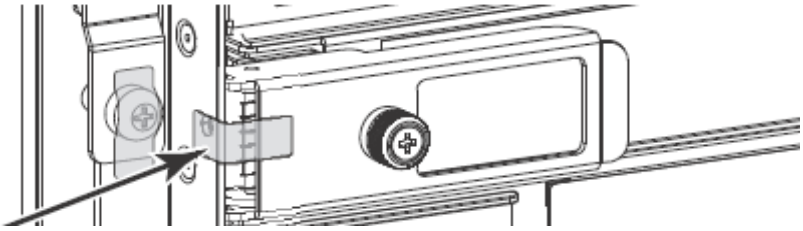

Figure 17 - Brocade DCX-4S Backbone filler panel (PN 49-1000064-02) seal application

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.3 Brocade 6510 FC Switch

Two tamper evident seals are required to complete the physical security requirements. See Figure 18 through Figure 20 for directions.

- Apply one (1) seal to the left side. See Figure 18.

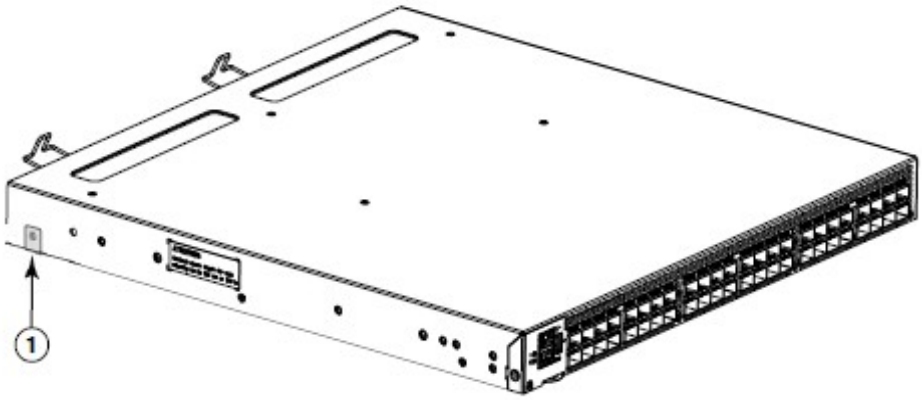

Figure 18 - Brocade 6510 left side seal application

- Apply one (1) seal to the right side. See Figure 19.

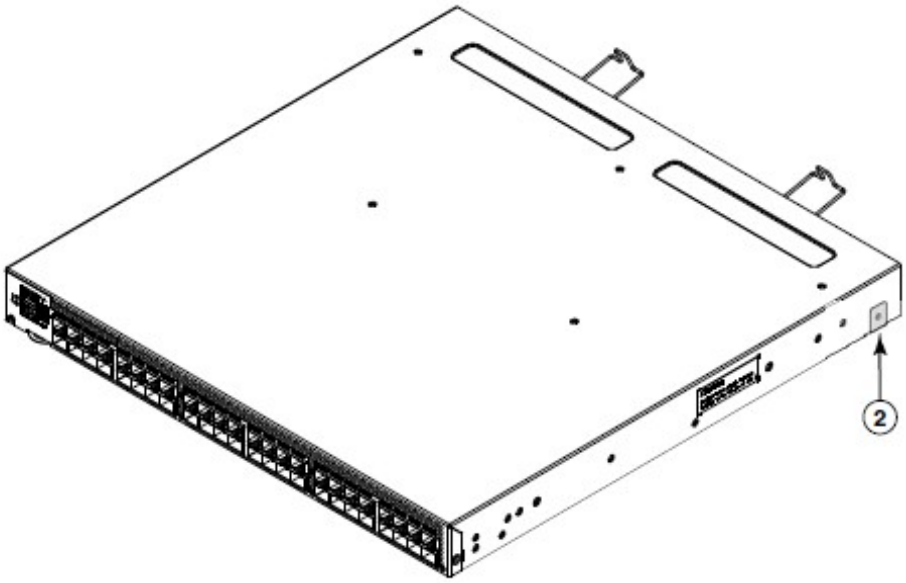

Figure 19 - Brocade 6510 right side seal application

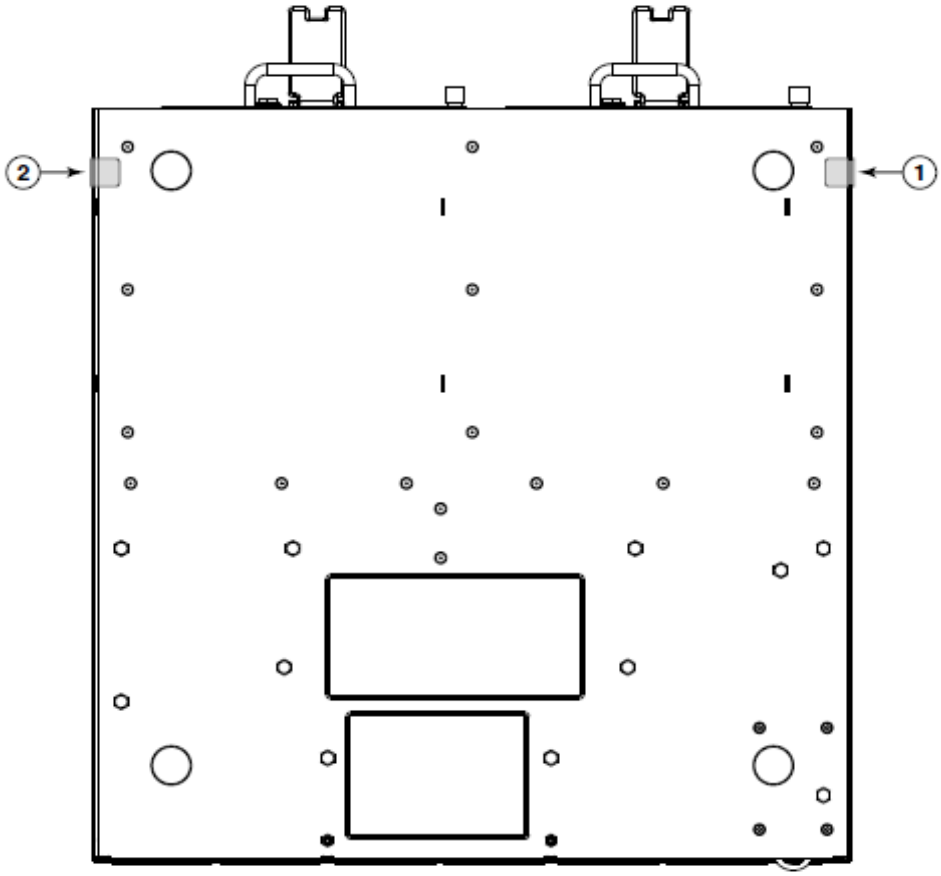

Figure 20 - Brocade 6510 bottom seal locations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.4 Brocade 6520 FC Switch

Twenty-six (26) tamper evident seals are required to complete the physical security requirements. See Figure 21 through Figure 24 for seal placement directions.

1. Relative to the left side of the Brocade 6520, apply four (4) seals along the left bottom side of the chassis. Make a 90 degree bend from the left side to the bottom side of the chassis. See Figure 21 for details on how to position each seal.
2. Relative to the left side of the Brocade 6520, apply one (1) seal vertically, on the left side of the switch, over the seam between the top cover and the front panel of the switch. Do not allow the seal to cover either of the rack mount screw holes on the left side of the switch. See Figure 21 for details on how to position each seal.

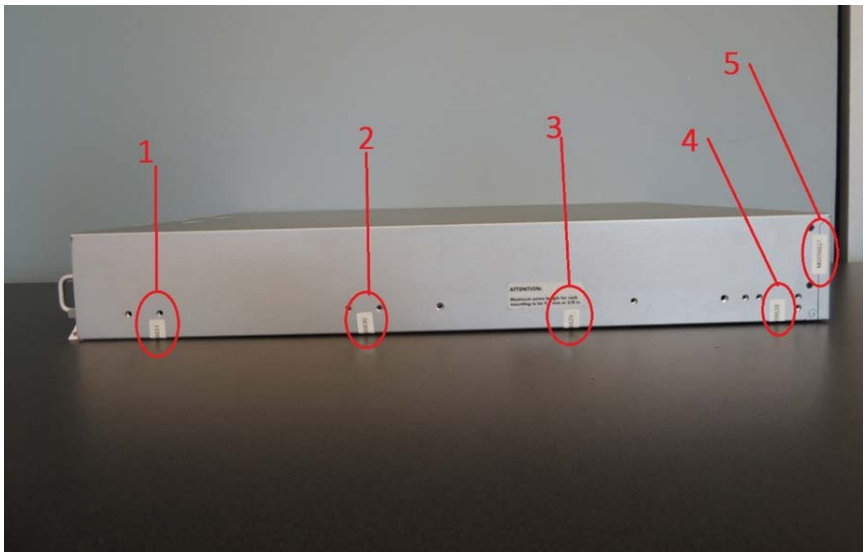

Figure 21 - Brocade 6520 left side seal locations

3. Relative to the right side of the Brocade 6520, apply four (4) seals along the right bottom side of the chassis. Make a 90 degree bend from the right side to the bottom side of the chassis. See Figure 23 for details on how to position each seal.
4. Relative to the right side of the Brocade 6520, apply one (1) seal vertically, on the right side of the switch, over the seam between the top cover and the front panel of the switch. Do not allow the seal to cover either of the rack mount screw holes on the left side of the switch. See Figure 22 for details on how to position each seal.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

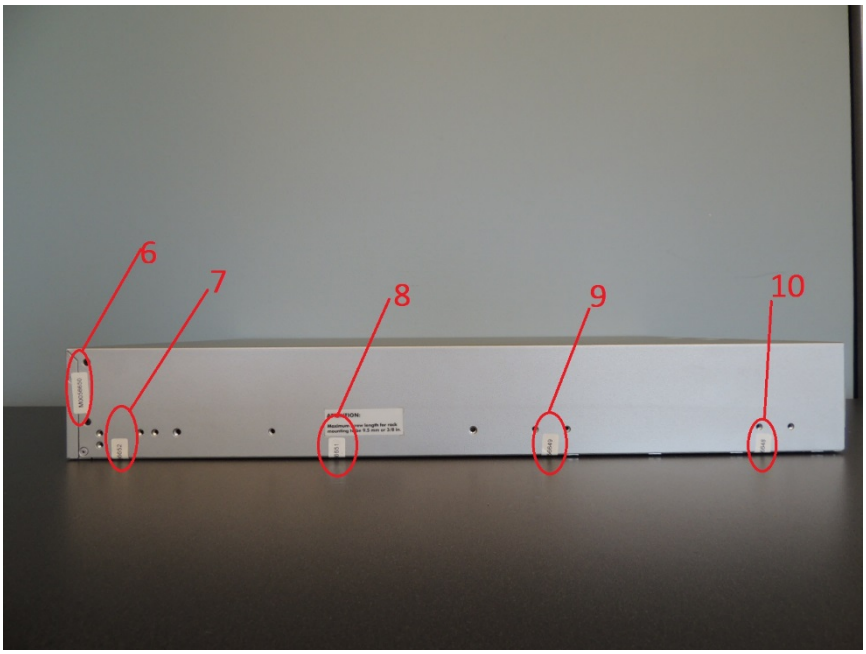

Figure 22 - Brocade 6520 right side seal locations

5. Relative to the non-port side of the Brocade 6520, apply one (1) seal over the seam between the top cover and the grill of the each of the three (3) FAN FRUs. Each seal makes a 90 bend from the top of the switch and the grill of each FAN FRU. See Figure 23 for details on how to position each seal. Apply two (2) seals over the flathead screws on the top cover near the FAN FRUs. See Figure 24 for details on how to position each seal. Five (5) seals are required to complete this step.
6. Relative to the non-port side of the Brocade 6520, apply two (2) seals over the seam between the chassis and the AC power module on the left non-port side of the chassis. See Figure 23 for details on how to position each seal.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

7. Relative to the non-port side of the Brocade 6520, apply two (2) seals over the seam between the chassis and the AC power module on the right non-port side of the chassis. See Figure 23 for details on how to position each seal.
8. Relative to the non-port side of the Brocade 6520, apply one (1) seal to the flange of each of the three (3) FAN FRUs and the bottom of the switch. Each seal makes a 90 bend from the bottom of the switch to the flange of each FAN FRU. See Figure 23 for details on how to position each seal. Three (3) seals are required to complete this step.

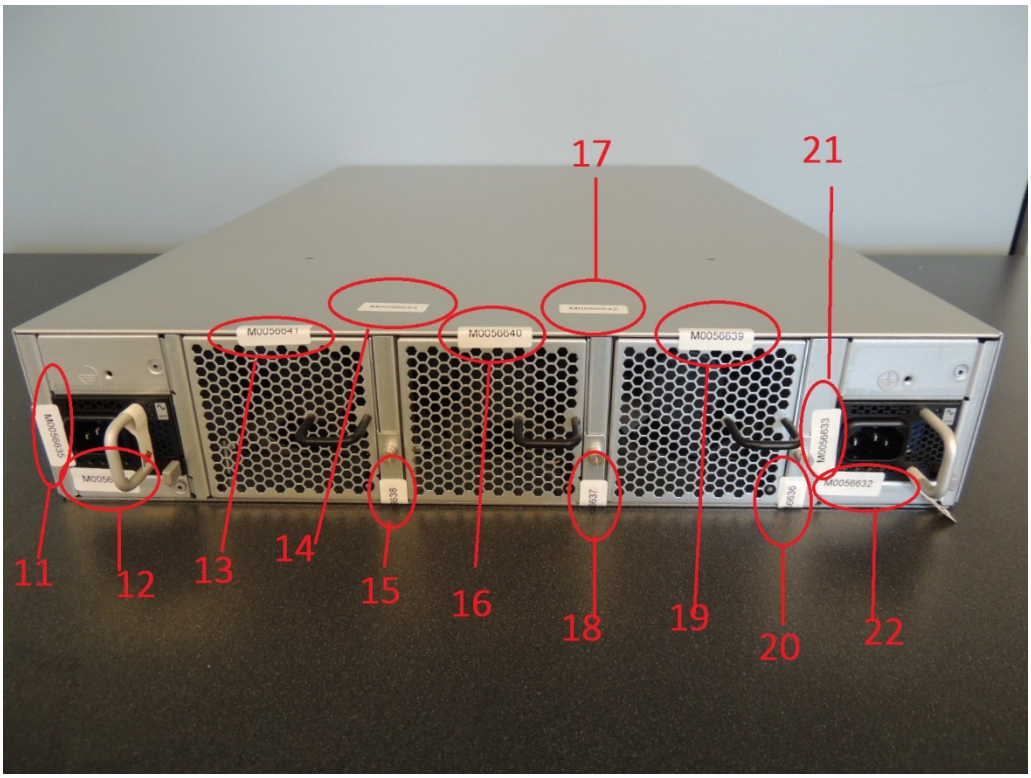

Figure 23 - Brocade 6520 top and non-port side seal locations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

9. Relative to the bottom side of the Brocade 6520, apply four (4) seals diagonally, on the bottom side of the switch, over the seam between the front panel and the bottom panel of the switch. See Figure 24 for details on how to position each seal.

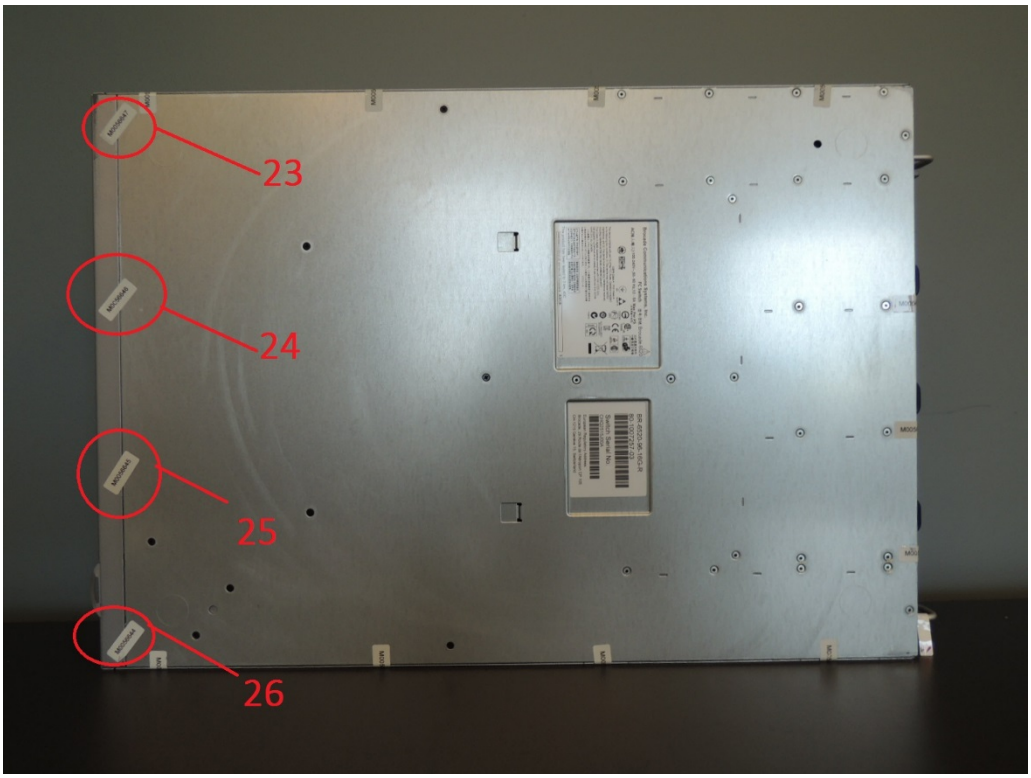

Figure 24 - Brocade 6520 bottom side seal locations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.5 Brocade 7800 Extension Switch

Two (2) tamper evident seals are required to complete the physical security requirements. See Figure 25 through Figure 27 for seal placement.

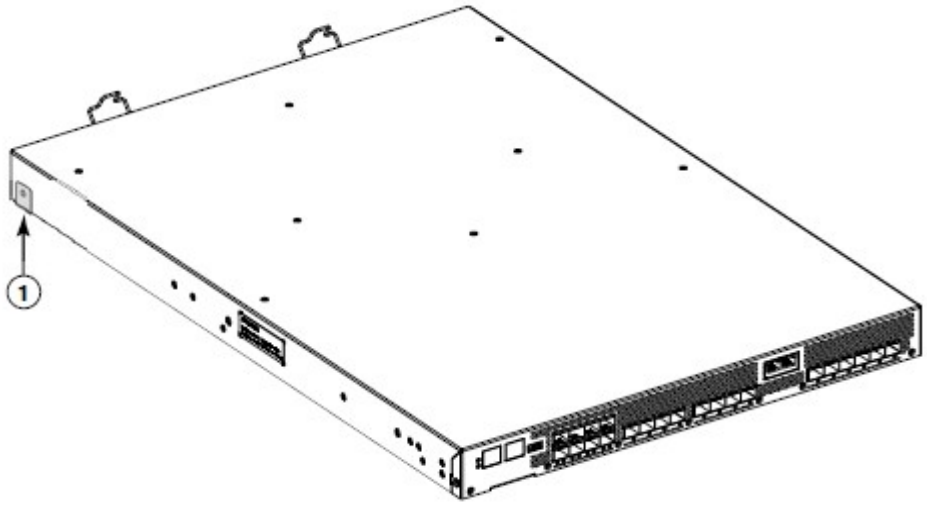

Figure 25 - Brocade 7800 left side seal locations

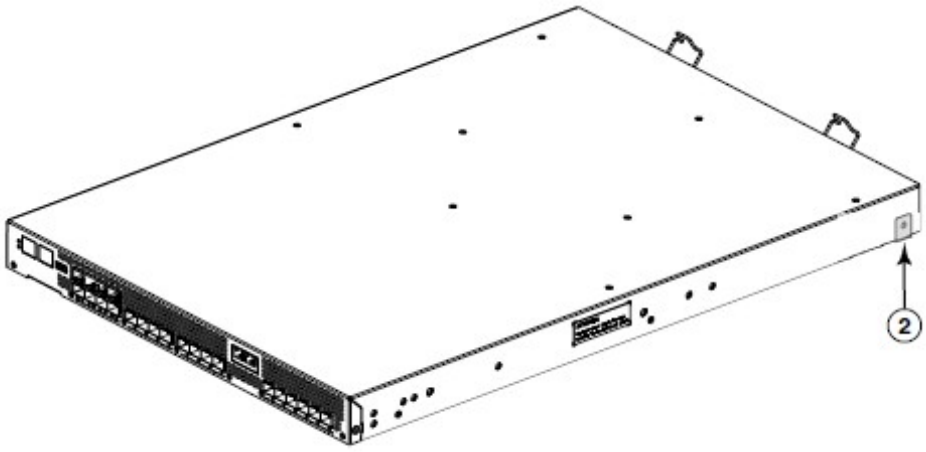

Figure 26 - Brocade 7800 right side seal locations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

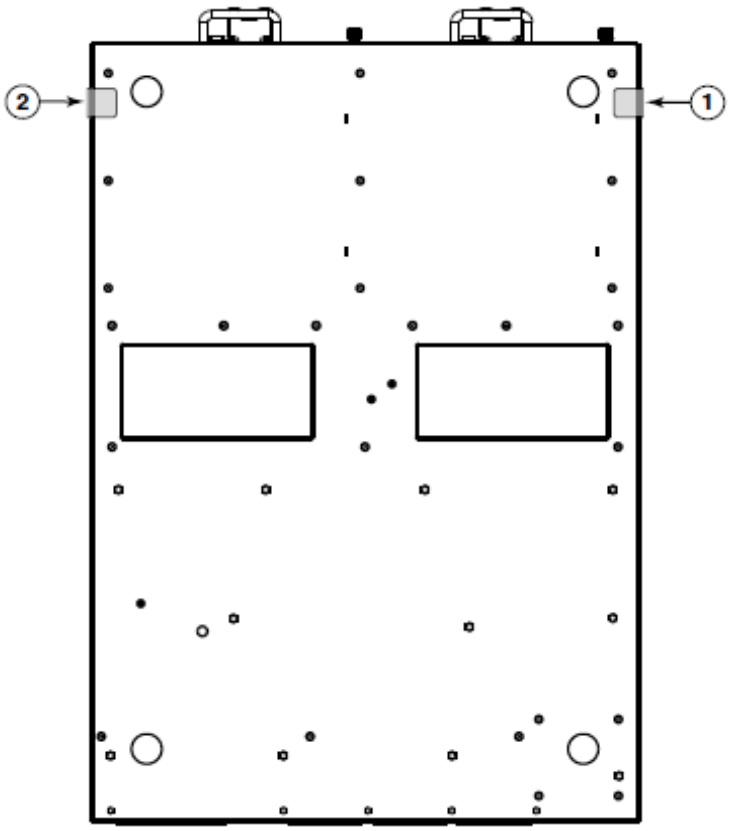

Figure 27 - Brocade 7800 bottom seal locations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

14 Appendix B: Block Diagram

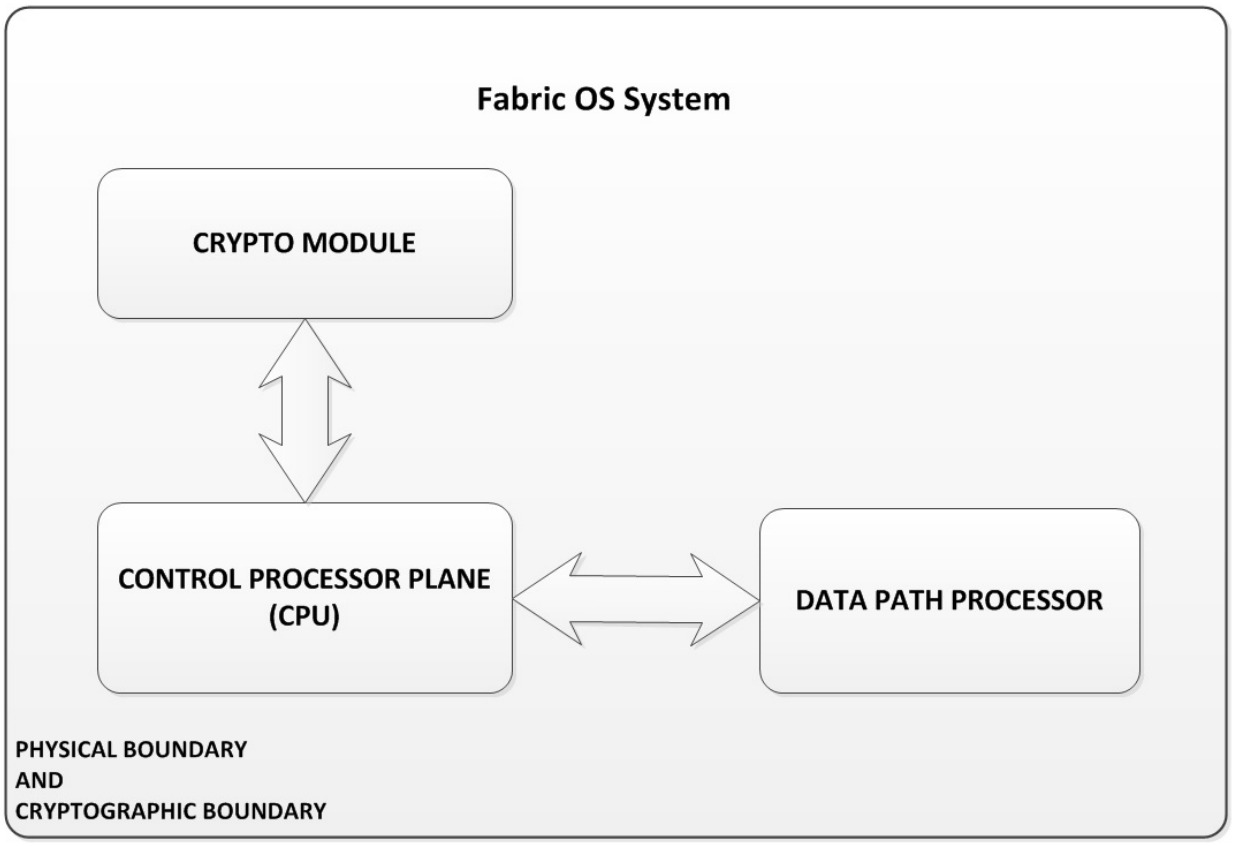

Figure 28 - Block Diagram

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

15 Appendix C: Critical Security Parameters and 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. Fiber-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. Fiber-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 performing the "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

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

23. 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

24. 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

25. 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

26. 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

27. 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

28. 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

29. 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

30. 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

31. 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

32. 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

33. 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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.