Brocade® DCX, DCX 8510-8, DCX-4S and DCX 8510-4 Backbones; 6510 FC Switch; and 7800 Extension Switch with Fabric OS v7.0.0b or Fabric OS v7.0.0b1 Firmware Security Policy

Document Version 2.0

Brocade Communications

August 29, 2012
Table of Contents

1. MODULE OVERVIEW .................................................................................................................. 4
2. SECURITY LEVEL ..................................................................................................................... 10
3. MODES OF OPERATION ......................................................................................................... 10
   APPROVED MODE OF OPERATION ......................................................................................... 10
   NON-APPROVED MODE OF OPERATION ............................................................................... 12
4. PORTS AND INTERFACES ................................................................................................. 13
   LED INDICATORS .................................................................................................................. 13
   DCX-4S, DCX, DCX 8510-4, AND DCX 8510-8 BLADE LED COUNTS: ............................. 14
5. IDENTIFICATION AND AUTHENTICATION POLICY ......................................................... 15
   ASSUMPTION OF ROLES ................................................................................................. 15
6. ACCESS CONTROL POLICY .......................................................................................... 17
   ROLES AND SERVICES ....................................................................................................... 17
   UNAUTHENTICATED SERVICES ......................................................................................... 17
   DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPs) ....................................... 17
   DEFINITION OF PUBLIC KEYS: ......................................................................................... 18
   DEFINITION OF CSPS MODES OF ACCESS .................................................................. 18
7. OPERATIONAL ENVIRONMENT ....................................................................................... 19
8. SECURITY RULES ............................................................................................................. 19
9. PHYSICAL SECURITY POLICY ..................................................................................... 20
   PHYSICAL SECURITY MECHANISMS ............................................................................. 20
   OPERATOR REQUIRED ACTIONS .................................................................................... 20
10. MITIGATION OF OTHER ATTACKS POLICY ................................................................. 20
11. DEFINITIONS AND ACRONYMS .................................................................................. 21
12. BROCADE ABBREVIATIONS ...................................................................................... 21

APPENDIX A: TAMPER LABEL APPLICATION ...................................................................... 23
   BROCADE DCX AND DCX 8510-8 BACKBONE .............................................................. 23
   BROCADE DCX-4S AND DCX 8510-4 BACKBONE ....................................................... 27
   BROCADE 6510 ................................................................................................................ 29
   BROCADE 7800 ................................................................................................................ 31
Table of Tables

Table 1 Firmware Version ........................................................................................................ 4
Table 2 Switch Platforms ......................................................................................................... 4
Table 3 Backbone Models ........................................................................................................ 5
Table 4 Supported Blades ......................................................................................................... 6
Table 5 Backbone Blade Support Matrix .................................................................................... 6
Table 6 Module Security Level Specification ............................................................................ 10
Table 7 Approved Algorithms available in firmware ............................................................... 10
Table 8 Port/Interface Quantities ............................................................................................. 14
Table 9 Blade LED Count ......................................................................................................... 14
Table 10 Roles and Required Identification and Authentication ............................................. 15
Table 11 Strengths of Authentication Mechanisms ................................................................. 16
Table 12 Service Descriptions ................................................................................................. 16
Table 13 Services Authorized for Roles .................................................................................... 17
Table 14 CSP Access Rights within Roles & Services ............................................................... 18
Table 15 Public Key Access Rights within Roles & Services ..................................................... 19
Table 16 Inspection/Testing of Physical Security Mechanisms .................................................. 20

Table of Figures

Figure 1 DCX-4S and DCX .......................................................................................................... 8
Figure 2 DCX 8510-4 and DCX 8510-8 ................................................................................... 9
Figure 3 Brocade 6510 ........................................................................................................... 9
Figure 4 Brocade 7800 ........................................................................................................... 9
Figure 5 Brocade DCX and DCX 8510-8 Backbone chassis right side seal locations ................ 23
Figure 6 Brocade DCX and DCX 8510-8 Backbone port side seal locations ......................... 24
Figure 7 Brocade DCX and DCX 8510-8 Backbone non-port side seal locations ................. 25
Figure 8 Brocade DCX and DCX 8510-8 Backbone flat ejector handle seal application .......... 25
Figure 9 Brocade DCX and DCX 8510-8 Backbone stainless steel handle seal application ...... 26
Figure 10 Brocade DCX and DCX 8510-8 Backbone filler panel seal application ................. 26
Figure 11 Brocade DCX-4S and DCX 8510-4 Backbone port side seal locations .................... 27
Figure 12 Brocade DCX-4S and DCX 8510-4 Backbone non-port side seal locations ........... 28
Figure 13 Brocade DCX-4S and DCX 8510-4 Backbone flat ejector handle seal application .... 28
Figure 14 Brocade DCX-4S and DCX 8510-4 Backbone stainless steel ejector handle seal application .......................................................................................................................... 28
Figure 15 Brocade DCX-4S and DCX 8510-4 Backbone filler panel (PN 49-1000294-05) seal application ................................................................. 28
Figure 16 Brocade DCX-4S Backbone filler panel (PN 49-1000064-02) seal application .......... 28
Figure 17 Brocade 6510 top left port side seal application ...................................................... 29
Figure 18 Brocade 6510 top right port side seal application ................................................... 29
Figure 19 Brocade 6510 bottom seal application .................................................................... 30
Figure 20 Brocade 7800 top left port side seal application ...................................................... 31
Figure 21 Brocade 7800 top right port side seal application .................................................... 31
Figure 22 Brocade 7800 bottom seal application ................................................................... 32
1. Module Overview

The Brocade 6510, 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 6510 FC Switch and 7800 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 each module to operate in a FIPS approved mode of operation, the tamper evident seals supplied in Brocade XBR-000195 must be installed as defined in Appendix A.

The security 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 security officer shall maintain a serial number inventory of all used and unused tamper evident seals. The security 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 security officer shall periodically inspect 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 security 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 either Fabric OS v7.0.0b (P/N 63-1000968-01) or Fabric OS v7.0.0b1 (P/N 63-1001098-01) installed on a switch or backbone and a set of installed blades. The following platforms may be used in a validated module configuration:

<table>
<thead>
<tr>
<th>Firmware</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric OS v7.0.0b</td>
<td>63-1000968-01</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Fabric OS v7.0.0b1</td>
<td>63-1001098-01</td>
</tr>
</tbody>
</table>

**Table 1** Firmware Version

<table>
<thead>
<tr>
<th>Switch</th>
<th>Part Number</th>
<th>Brief Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6510</td>
<td>80-1005232-02¹</td>
<td>6510,24P,16GB SFP,NON-PORT² SIDE AIR FLOW</td>
</tr>
<tr>
<td></td>
<td>80-1005267-02¹</td>
<td>6510,24P,16GB SFP,PORT SIDE² AIR FLOW</td>
</tr>
<tr>
<td></td>
<td>80-1005268-02¹</td>
<td>6510,24P,8GB SFP,NON-PORT SIDE AIR FLOW</td>
</tr>
<tr>
<td></td>
<td>80-1005269-02¹</td>
<td>6510,24P,8GB SFP,PORT SIDE AIR FLOW</td>
</tr>
<tr>
<td></td>
<td>80-1005271-02</td>
<td>6510,48P,16GB SFP,NON-PORT SIDE AIR FLOW, 24-PORT POD LICENSE</td>
</tr>
<tr>
<td></td>
<td>80-1005272-02</td>
<td>6510,48P,16GB SFP, PORT SIDE AIR FLOW, 24-Port POD LICENSE</td>
</tr>
<tr>
<td>7800</td>
<td>80-1002607-06</td>
<td>7800, UPG LIC, 22P, 16 8 SWL</td>
</tr>
<tr>
<td></td>
<td>80-1002608-06</td>
<td>7800, UPG LIC, 22P, 16 8 LWL</td>
</tr>
<tr>
<td></td>
<td>80-1002609-06</td>
<td>7800, 6P, 8GB SWL SFP</td>
</tr>
</tbody>
</table>

**Table 2** Switch Platforms

Table Notes

2. Port side and non-port side air flow indicates whether the fan direction causes air to be drawn into the port side air vents or exhausted from the port side air vents.
<table>
<thead>
<tr>
<th>Backbone</th>
<th>Part Number</th>
<th>Brief Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCX</td>
<td>80-1001064-08 80-1001064-09&lt;sup&gt;1&lt;/sup&gt;</td>
<td>DCX,2PS,0P,2CP,2 CORE,0SFP</td>
</tr>
<tr>
<td></td>
<td>80-1004920-02 80-1004920-03&lt;sup&gt;1&lt;/sup&gt;</td>
<td>DCX,2PS,0P,2CP,2 CORE,0 SFP,ENT BUN&lt;sup&gt;2&lt;/sup&gt;,2 WWN</td>
</tr>
<tr>
<td>DCX-4S</td>
<td>80-1002071-08 80-1002071-09&lt;sup&gt;1&lt;/sup&gt;</td>
<td>DCX-4S,2PS,0P,2CP,2 CORE,0SFP</td>
</tr>
<tr>
<td></td>
<td>80-1002066-08 80-1002066-09&lt;sup&gt;1&lt;/sup&gt;</td>
<td>DCX-4S,2PS,0P,2CP,2 CORE,0SFP,BR,ENT BUN&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
<tr>
<td>DCX 8510-4</td>
<td>80-1004697-02 80-1004697-03&lt;sup&gt;1&lt;/sup&gt;</td>
<td>DCX8510-4,2PS,0P,2CP,2 16G CORE,0SFP</td>
</tr>
<tr>
<td></td>
<td>80-1005158-02 80-1005158-03&lt;sup&gt;1&lt;/sup&gt;</td>
<td>DCX8510-4,2PS,0P,2CP,2 16G CORE,0SFP,ENT BUN&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
<tr>
<td>DCX 8510-8</td>
<td>80-1004917-02 80-1004917-03&lt;sup&gt;1&lt;/sup&gt;</td>
<td>DCX8510-8,2PS,0P,2CP,2 16GB,0SFP,ENT BUN&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
</tbody>
</table>

Table 3 Backbone Models

Table Notes

1. Assemblies are equivalent with one exception. The higher dash level assembly incorporated an upgraded blower assembly within the fan module. This change is not security relevant.

2. Enterprise Software License Bundle: Adaptive Networking, Extended Fabrics, Advance Performance Monitoring, Trunking, Fabric Watch, Server Application Optimized
The blades listed below may be used in backbone-based validated module configurations:

<table>
<thead>
<tr>
<th>Blade</th>
<th>Acronym *</th>
<th>Part Number</th>
<th>Brief Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP8 Control Processor Blade</td>
<td>CP8</td>
<td>80-1001070-06</td>
<td>FRU, CP BLADE, DCX</td>
</tr>
<tr>
<td>CR16-4 Core Switch Blade</td>
<td>CR16-4</td>
<td>80-1004897-01</td>
<td>FRU, CORE BLADE, DCX8510-4</td>
</tr>
<tr>
<td>CR16-8 Core Switch Blade</td>
<td>CR16-8</td>
<td>80-1004898-01</td>
<td>FRU, CORE BLADE, DCX8510-8</td>
</tr>
<tr>
<td>CR4S-8 Core Switch Blade</td>
<td>CR4S-8</td>
<td>80-1002000-02</td>
<td>FRU, CORE BLADE, DCX-4S</td>
</tr>
<tr>
<td>CR8 Core Switch Blade</td>
<td>CR8</td>
<td>80-1001071-02</td>
<td>FRU, CORE BLADE, DCX</td>
</tr>
<tr>
<td>FC8-16 Port Blade</td>
<td>FC8-16</td>
<td>80-1001066-01</td>
<td>FRU, PORT BLADE, 16P, DCX, 8G SFP</td>
</tr>
<tr>
<td>FC8-32 Port Blade</td>
<td>FC8-32</td>
<td>80-1001067-01</td>
<td>FRU, PORT BLADE, 8P, DCX, 8G SFP</td>
</tr>
<tr>
<td>FC8-48 Port Blade</td>
<td>FC8-48</td>
<td>80-1001453-01</td>
<td>FRU, PORT BLADE, 48P, DCX, 8G SFP</td>
</tr>
<tr>
<td>FC8-64 Port Blade</td>
<td>FC8-64</td>
<td>80-1003887-01</td>
<td>FRU, PORT BLADE, 48P, DCX, 8G SFP</td>
</tr>
<tr>
<td>FCOE10-24 Port Blade</td>
<td>FCOE10-24</td>
<td>80-1002762-04</td>
<td>FRU, FCOE BLADE, 10GE X 24P</td>
</tr>
<tr>
<td>FR4-18i Port Blade</td>
<td>FR4-18i</td>
<td>80-1000233-10</td>
<td>FRU, FCIP BLADE, 4G X 16P, 2X16GE</td>
</tr>
<tr>
<td>FX8-24 Port Blade</td>
<td>FX8-24</td>
<td>80-1002839-02</td>
<td>FRU, EXT BLADE, 8G X 12P, 10X1GGE, 2X1GGE</td>
</tr>
<tr>
<td>DCX/DCX 8510-8 Filler Panel</td>
<td>DCX/DCX 8510-8 Filler Panel</td>
<td>49-1000016-04</td>
<td>FILLER PANEL</td>
</tr>
<tr>
<td>DCX-4S Backbone Filler Panel</td>
<td>DCX-4S Backbone Filler Panel</td>
<td>49-1000064-02</td>
<td>FILLER PANEL</td>
</tr>
<tr>
<td>DCX-4S/DCX 8510-4 Filler Panel</td>
<td>DCX-4S/DCX 8510-4 Filler Panel</td>
<td>49-1000294-05</td>
<td>FILLER PANEL</td>
</tr>
</tbody>
</table>

Table 4 Supported Blades

* NOTICE: Acronym referenced in Table 5 below

Each backbone model supports a selected set of blades:

<table>
<thead>
<tr>
<th>Backbone Model</th>
<th>Blades (max count)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCX (12 slots) **</td>
<td>CP8 (2), CR8 (2), FC8-16 (8), FC8-32 (8), FC8-48 (8), FC8-64 (8), FC10-6 (1), FR4-18i (4), FX8-24 (1), FCOE10-24 (1), DCX/DCX 8510-8 Filler Panel (10)</td>
</tr>
<tr>
<td>DCX 8510-8 (12 slots) **</td>
<td>CP8 (2) **, CR16-8 (2), FC8-64 (8), FC16-32 (8), FC16-48 (8), FX8-24 (1), DCX/DCX 8510-8 Filler Panel (10)</td>
</tr>
<tr>
<td>DCX-4S (8 slots) **</td>
<td>CP8 (2), CR4S-8 (2), FC8-16 (4), FC8-32 (4), FC8-48 (4), FC8-64 (4), FC10-6 (1), FR4-18i (4), FX8-24 (1), FCOE10-24 (1), DCX-4S Backbone Filler Panel (6), DCX-4S/DCX 8510-4 Filler Panel (6)</td>
</tr>
<tr>
<td>DCX 8510-4 (8 slots) **</td>
<td>CP8 (2), CR16-4 (2), FC8-64 (4), FC16-32 (4), FC16-48 (4), FX8-24 (1), DCX-4S/DCX 8510-4 Filler Panel (6)</td>
</tr>
</tbody>
</table>

Table 5 Backbone Blade Support Matrix

** NOTICE: Each Backbone Model shall be fully populated with a minimum of two CP8 Control Processor Blades (Part Number: 80-1001070-06), with every remaining slot populated with a blade as per Table 5 above.
The name of a backbone-based validated module configuration is formed by a concatenation of part numbers of the specific set of blades installed in the backbone.

For the DCX and DCX 8510-8 platforms:
<Backbone PN><Slot 1 PN><Slot 2 PN>....<Slot 12 PN>

For the DCX-4S and DCX 8510-4 platforms:
<Backbone PN><Slot 1 PN><Slot 2 PN>....<Slot 8 PN>
Figure 1 and Figure 2 illustrate representative configurations of the DCX and DCX 8510 cryptographic modules. These are not the only possible configurations. Other possible configurations can be created by utilizing the blade and support matrix information in Table 4 and Table 5.
Figure 2 DCX 8510-4 and DCX 8510-8

Figure 3 and Figure 4 illustrate the Brocade 6510 and Brocade 7800 cryptographic modules.

Figure 3 Brocade 6510

Figure 4 Brocade 7800
2. Security Level

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

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

Table 6 Module Security Level Specification

3. Modes of Operation

Approved mode of operation

The cryptographic module supports the following Approved algorithms:

<table>
<thead>
<tr>
<th>Approved Algorithm</th>
<th>Fabric OS v7.0.0b</th>
<th>Fabric OS v7.0.0b1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triple-DES</td>
<td>Cert. #652, #1043</td>
<td>Cert. #652, #1043</td>
</tr>
<tr>
<td>AES</td>
<td>Cert. #731, #1595, #1596</td>
<td>Cert. #731, #1595, #1596</td>
</tr>
<tr>
<td>SHS [SHA-1]</td>
<td>Cert. #749, #1408</td>
<td>Cert. #749, #1408</td>
</tr>
<tr>
<td>SHS [SHA-256]</td>
<td>Cert. #749, #1408</td>
<td>Cert. #749, #1408</td>
</tr>
<tr>
<td>SHS [SHA-512]</td>
<td>Cert. #1407, #1408</td>
<td>Cert. #1407, #1408</td>
</tr>
<tr>
<td>HMAC SHA-1</td>
<td>Cert. #397, #933, #934</td>
<td>Cert. #397, #933, #934</td>
</tr>
<tr>
<td>HMAC SHA 256</td>
<td>Cert. #397, #933, #934</td>
<td>Cert. #397, #933, #934</td>
</tr>
<tr>
<td>HMAC SHA 512</td>
<td>Cert. #933, #934</td>
<td>Cert. #933, #934</td>
</tr>
<tr>
<td>RNG</td>
<td>Cert. #426, #854</td>
<td>Cert. #426, #854</td>
</tr>
<tr>
<td>RSA</td>
<td>Cert. #778, #779</td>
<td>Cert. #1048, #1049</td>
</tr>
</tbody>
</table>

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

- RSA Key Wrapping (key establishment methodology; 1024-bit keys provide 80 bits of encryption strength)
• Diffie-Hellman (DH) with 1024 bit or 2048 bit modulus (key agreement; key establishment methodology provides 80 bits of encryption strength)
• SNMPv3 (Cryptographic functionality does not meet FIPS requirements and is considered plaintext)
• HMAC-MD5 to support RADIUS authentication
• NDRNG – used for seeding Approved RNG
• SSHv2 KDF
• TLS KDF with HMAC-MD5
• TLS
• SSHv2
• RSA Key Transport (Key establishment methodology; 1024-bit keys provide 80-bits of encryption strength for TLS, use 2048-bit keys for SSH public key authentication)
• MD5 (used for password hash)
• RADIUS PEAP MS-CHAP V2
• Non-deterministic random number generator for seeding ANSI X9.31 DRNG

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) Perform zeroization operation
2) Change passwords for all existing user accounts.
3) Disable Telnet, HTTP, Remote Procedure Call (RPC)
4) Enable HTTPS, Secure-RPC
5) Do not use FTP
   a) Config Upload
   b) Config Download
   c) Support Save
   d) FW Download
6) Disable Root Access
7) Disable Boot PROM Access
8) Do not use MD5 within Authentication Protocols; Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) and FCAP.
9) Do not define FCIP IKE or IPSec policies.
10) Disable Management Interface IPSec/IKE
11) Disable In-Band Management Interface
12) Disable In-Flight Encryption
13) Configure LDAP to use certificate-based authentication.
14) Configure SNMP Access List for read-only access.
15) Enable Self-Tests
16) Within Radius, only use PEAP MS-CHAP V2. Configure RADIUS Server to only use PEAP MS-CHAP V2.
17) Enable Signed FW Download
18) Install removable front cover (as applicable) and apply tamper labels
19) Enable FIPS mode via the "fipscfg – enable fips" command
The operator can determine if the cryptographic module is running in FIPS vs. non-FIPS 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.”

Non-Approved mode of operation
In non-Approved mode, an operator will have no access to CSPs used within the Approved mode. When switching between FIPS and non-FIPS mode of operation, the operator is required to perform zeroization of the module’s plaintext CSPs.

The following cipher suites are allowed in non-FIPS mode for configuring SSL and TLS:

The following message digest functions are allowed in non-FIPS mode: md2,md4,md5,md5

The following message authentication algorithms and ciphers are allowed in non-FIPS mode for configuring SSH:
Macs:hmac-md5,hmac-sha1,umac-64,hmac-ripemd160,hmac-sha1-96,hmac-md5-96
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, Data Output, Status Input
- LEDs: Status Output (1)

LED Indicators

1) Blades
   a) Blade Power LED
   b) Blade Status LED
   c) Fibre Channel port status LED
   d) Fibre 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
### Port/Interface Quantities

<table>
<thead>
<tr>
<th>Model</th>
<th>Fibre Channel</th>
<th>1 GbE &amp; 10 GbE</th>
<th>Ethernet</th>
<th>Serial Port</th>
<th>USB</th>
<th>Power Supply Connectors</th>
<th>LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCX-4S</td>
<td>256</td>
<td>24</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>DCX</td>
<td>512</td>
<td>24</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>30</td>
</tr>
<tr>
<td>DCX 8510-4</td>
<td>192</td>
<td>12</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>DCX 8510-8</td>
<td>384</td>
<td>12</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>30</td>
</tr>
<tr>
<td>6510</td>
<td>48</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>54</td>
</tr>
<tr>
<td>7800</td>
<td>16</td>
<td>8</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>32</td>
</tr>
</tbody>
</table>

Table 8 Port/Interface Quantities

### DCX-4S, DCX, DCX 8510-4, and DCX 8510-8 blade LED counts:

<table>
<thead>
<tr>
<th>Blade</th>
<th>LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP8 Control Processor</td>
<td>8</td>
</tr>
<tr>
<td>CR16-4 Core Switch Blade</td>
<td>4</td>
</tr>
<tr>
<td>CR16-8 Core Switch Blade</td>
<td>4</td>
</tr>
<tr>
<td>CR4S-8 Core Switch Blade</td>
<td>6</td>
</tr>
<tr>
<td>CR8 Core Switch Blade</td>
<td>4</td>
</tr>
<tr>
<td>FC10-6 Port Blade</td>
<td>8</td>
</tr>
<tr>
<td>FC16-32 Port Blade</td>
<td>34</td>
</tr>
<tr>
<td>FC16-48 Port Blade</td>
<td>50</td>
</tr>
<tr>
<td>FC8-16 Port Blade</td>
<td>18</td>
</tr>
<tr>
<td>FC8-32 Port Blade</td>
<td>34</td>
</tr>
<tr>
<td>FC8-48 Port Blade</td>
<td>50</td>
</tr>
<tr>
<td>FC8-64 Port Blade</td>
<td>66</td>
</tr>
<tr>
<td>FCOE10-24 Port Blade</td>
<td>26</td>
</tr>
<tr>
<td>FR4-18i Port Blade</td>
<td>20</td>
</tr>
<tr>
<td>FX8-24 Port Blade</td>
<td>26</td>
</tr>
</tbody>
</table>

Table 9 Blade LED Count
5. Identification and Authentication Policy

Assumption of Roles

The cryptographic module supports for operator roles. The cryptographic module shall enforce 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 eight to 40 characters randomly chosen from the 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:

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

Table 10 Roles and Required Identification and Authentication
### Authentication Mechanism

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Strength of Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>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 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 $1/100,000$.</td>
</tr>
<tr>
<td>Digital Signature Verification (PKI)</td>
<td>The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{80}$ 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 $10/2^{80}$ which is less than $1/100,000$.</td>
</tr>
<tr>
<td>Knowledge of a Shared Secret</td>
<td>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 is 16. The probability of successfully authenticating to the module within one minute is $16/96^8$ which is less than $1/100,000$.</td>
</tr>
</tbody>
</table>

**Table 11 Strengths of Authentication Mechanisms**

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
<th>FOS Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Element Authentication</td>
<td>Fabric element authentication, including selection of authentication protocols, protocol configuration selection and setting authentication secrets.</td>
<td>authutil  secauthsecret</td>
</tr>
<tr>
<td>FIPSCfg</td>
<td>Control FIPS mode operation and related functions</td>
<td>fipscfg</td>
</tr>
<tr>
<td>Zerize</td>
<td>Zerize all CSPs</td>
<td>fipgscfg --zeroize</td>
</tr>
<tr>
<td>FirmwareManagement</td>
<td>Control firmware management.</td>
<td>firmwarecommit  firmwareownload firmwareownloadstatus</td>
</tr>
<tr>
<td>PKI</td>
<td>PKI configuration functions, including FOS switch certificates and SSL certificates.</td>
<td>seccertutil</td>
</tr>
<tr>
<td>RADIUS</td>
<td>RADIUS configuration functions.</td>
<td>aaaconfig</td>
</tr>
<tr>
<td>LDAP</td>
<td>LDAP configuration functions.</td>
<td>aaaconfig</td>
</tr>
<tr>
<td>UserManagement</td>
<td>User and password management.</td>
<td>passwd  passwdconfig  userconfig</td>
</tr>
</tbody>
</table>

**Table 12 Service Descriptions**
6. Access Control Policy

Roles and Services

<table>
<thead>
<tr>
<th>Service</th>
<th>User</th>
<th>Admin</th>
<th>FabricAdmin</th>
<th>SecurityAdmin</th>
<th>Maximum Permissions</th>
<th>LDAP Server</th>
<th>RADIUS Server</th>
<th>Host Server/Peer Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Element Authentication</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FiPSCfg</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zer0ize</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FirmwareManagement</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKI</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>UserManagement</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 13 Services Authorized for Roles

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.

Definition of Critical Security Parameters (CSPs)

- DH Private Keys for use with 1024 bit or 2048 bit modulus
- Fibre-Channel Security Protocol (FCSP) CHAP Secret
- Fibre-Channel Authentication Protocol (FCAP) Private Key (RSA 1024, 2048)
- SSH/SCP/SFTP Session Keys - 128, 192, and 256 bit AES CBC or TDES 3 key CBC
- SSH/SCP/SFTP Authentication Key for HMAC-SHA-1
- SSH KDF Internal State
- SSH DH Shared Secret 1024 – 8192 bits
- SSH 2048 RSA Private Key
- TLS Private Key (RSA 1024)
- TLS Pre-Master Secret
- TLS Master Secret
- TLS PRF Internal State
- TLS Session Keys – 128, 256 bit AES CBC, TDES 3 key CBC
- TLS Authentication Key for HMAC-SHA-1
• RNG Seed Material
• ANSI X9.31 DRNG Internal State
• Passwords
• RADIUS Secret
• RPC Shared Secret

**Definition of Public Keys:**

The following are the public keys contained in the module:

- DH Public Key (1024 bit or 2048 bit modulus)
- DH Peer Public Key (1024 bit or 2048 bit modulus)
- FCAP Public Key (RSA 1024)
- FCAP Peer Public Key (RSA 1024)
- TLS Public Key (RSA 1024)
- TLS Peer Public Key (RSA 1024)
- FW Download Public Key (RSA 1024)
- SSH RSA 1024/2048 bit Public Key
- LDAP ROOT CA certificate (RSA 1024)

**Definition of CSPs Modes of Access**

Table 12 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- **R**: Read
- **W**: Write
- **N**: No Access
- **Z**: Zeroize

<table>
<thead>
<tr>
<th>Fabric Element Authentication</th>
<th>SSH/SCP/SFTP CSPs</th>
<th>TLS CSPs</th>
<th>RNG Seed Material/Internal State</th>
<th>Passwords</th>
<th>RADIUS Secret</th>
<th>FCAP Private Key</th>
<th>FCAP CHAP Secret</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPSCfg</td>
<td>N</td>
<td>N</td>
<td>RW</td>
<td>N</td>
<td>N</td>
<td>RW</td>
<td>RW</td>
</tr>
<tr>
<td>Zeroize</td>
<td>Z</td>
<td>Z</td>
<td>Z</td>
<td>N</td>
<td>Z</td>
<td>Z</td>
<td>Z</td>
</tr>
<tr>
<td>FirmwareManagement</td>
<td>R</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>PKI</td>
<td>RW</td>
<td>N</td>
<td>RW</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>RADIUS</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>RW</td>
<td>RW</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>UserManagement</td>
<td>N</td>
<td>RW</td>
<td>RW</td>
<td>RW</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

**Table 14 CSP 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 signed by RSA 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) TDES CBC KAT (encrypt/decrypt)
         (2) AES CBC KAT (encrypt/decrypt)
         (3) HMAC SHA-1 KAT
         (4) HMAC SHA-256 KAT
         (5) HMAC SHA-512 KAT
         (6) ANSI X9.31 DRNG KAT
         (7) SHA-1 KAT
         (8) SHA-256 KAT
         (9) SHA-512 KAT
         (10) RSA 1024 SHA-1 Sign/Verify KAT
      ii) Firmware Integrity Test (128-bit EDC)
iii) Critical Functions Tests:
   (1) RSA 2048 Encrypt/Decrypt KAT
   b) Conditional Self-Tests:
      i) Continuous Random Number Generator (RNG) test – performed on non-approved RNG.
      ii) Continuous Random Number Generator test – performed on ANSI X9.31 DRNG.
      iii) RSA 1024/2048 SHA-1 Pairwise Consistency Test (Sign/Verify)
      iv) RSA 1024/2048 Pairwise Consistency Test (Encrypt/Decrypt)
      v) Firmware Load Test (RSA 1024 SHA-1 Signature Verification
      vi) Bypass Test: N/A
      vii) 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.

9. Physical Security Policy

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.

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

<table>
<thead>
<tr>
<th>Physical Security Mechanisms</th>
<th>Recommended Frequency of Inspection/Test</th>
<th>Inspection/Test Guidance Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tamper Evident Seals</td>
<td>12 months</td>
<td>Reference Appendix A for a description of tamper label application for all evaluated platforms.</td>
</tr>
</tbody>
</table>

Table 16 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.
11. Definitions and Acronyms

10 GbE  10 Gigabit Ethernet
AES    Advanced Encryption Standard
Blade  Blade server
CBC    Cipher Block Chaining
CLI    Command Line Interface
CSP    Critical Security Parameter
DH     Diffie-Hellman
FIPS   Federal Information Processing Standard
FOS    Fabric Operating System
GbE    Gigabit Ethernet
HMAC   Hash Message Authentication Code
HTTP   Hyper Text Transfer Protocol
KAT    Known Answer Test
LED    Light Emitting Diode
LDAP   Lightweight Directory Access Protocol
MAC    Message Authentication Code
NTP    Network Time Protocol
NOS    Network Operating System
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
SSH    Secure Shell Protocol
TDES   Triple Data Encryption Standard
TLS    Transport Layer Security Protocol

12. Brocade Abbreviations

24P    24 ports
48P    48 ports
16GB   16 Gigabit
8GB    8 Gigabit
SFP    Small form-factor pluggable
LWL    long wave length
SWL    Short wave length
LIC    License
UPG    Upgrade
2PS    Two power supply modules
OP     No port blades
0SFP   Zero SFP devices provided
2CP    Two Control processor blades (see Table 4)
2 CORE Two core switch blades (see Table 4)
ENT BUN Enterprise Software License Bundle: Adaptive Networking, Extended Fabrics, Advance
Performance Monitoring, Trunking, Fabric Watch, Server Application Optimized (see foot note for
Table 2 & 3)
BR     Brocade
WWN    World Wide Name card
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

<table>
<thead>
<tr>
<th>FC</th>
<th>Fibre Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCIP</td>
<td>Fiber Channel over Internet Protocol</td>
</tr>
<tr>
<td>GE</td>
<td>Gigabit Ethernet</td>
</tr>
<tr>
<td>GBE</td>
<td>Gigabit Ethernet</td>
</tr>
<tr>
<td>CP8</td>
<td>8G Control Processor blade</td>
</tr>
<tr>
<td>CR8</td>
<td>8G Core Switch Blade for DCX backbone</td>
</tr>
<tr>
<td>CR4S-8</td>
<td>8G Core Switch Blade for DCX -4S backbone</td>
</tr>
<tr>
<td>CR16-8</td>
<td>16G core switch blade for DCX 8510-8 backbone</td>
</tr>
<tr>
<td>CR16-4</td>
<td>16G core switch blade for DCX 8510-4 backbone</td>
</tr>
<tr>
<td>FC8-16</td>
<td>8G, 16-port, Fibre Channel port blade</td>
</tr>
<tr>
<td>FR4-18i</td>
<td>4G, 18 port, FCIP, routing and extension blade</td>
</tr>
<tr>
<td>FCOE</td>
<td>Fiber Channel over Ethernet</td>
</tr>
<tr>
<td>FCOE10-24</td>
<td>10G, 24 port, FCOE blade</td>
</tr>
<tr>
<td>FX8-24</td>
<td>8G, 24 port , Extension blade</td>
</tr>
<tr>
<td>ICL</td>
<td>Inter-Chassis Link</td>
</tr>
<tr>
<td>MGMT</td>
<td>Management</td>
</tr>
</tbody>
</table>
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.

**Brocade DCX and DCX 8510-8 Backbone**

Twenty-two tamper evident seals are required to complete the physical security requirements.

Figure 5 Brocade DCX and DCX 8510-8 Backbone chassis right side seal locations
Apply twelve seals are to the port side of the chassis.

Figure 6 Brocade DCX and DCX 8510-8 Backbone port side seal locations
Figure 7 Brocade DCX and DCX 8510-8 Backbone non-port side seal locations

Apply seven seals are to the non-port side of the chassis

Figure 8 Brocade DCX and DCX 8510-8 Backbone flat ejector handle seal application
Figure 9 Brocade DCX and DCX 8510-8 Backbone stainless steel handle seal application

Figure 10 Brocade DCX and DCX 8510-8 Backbone filler panel seal application
Brocade DCX-4S and DCX 8510-4 Backbone

Nineteen tamper evident seals are required to complete the physical security requirements.

Figure 11 Brocade DCX-4S and DCX 8510-4 Backbone port side seal locations

Apply fourteen seals are to the port side of the chassis

Apply five seals are to the non-port side of the chassis
Figure 12 Brocade DCX-4S and DCX 8510-4 Backbone non-port side seal locations

Figure 13 Brocade DCX-4S and DCX 8510-4 Backbone flat ejector handle seal application

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

Figure 15 Brocade DCX-4S and DCX 8510-4 Backbone filler panel (PN 49-1000294-05) seal application

Figure 16 Brocade DCX-4S Backbone filler panel (PN 49-1000064-02) seal application
Brocade 6510

Two tamper evident seals are required to complete the physical security requirements.

Figure 17 Brocade 6510 top left port side seal application

Figure 18 Brocade 6510 top right port side seal application
Figure 19 Brocade 6510 bottom seal application
Brocade 7800

Two tamper evident seals are required to complete the physical security requirements.

Figure 20 Brocade 7800 top left port side seal application

Figure 21 Brocade 7800 top right port side seal application
Figure 22 Brocade 7800 bottom seal application1024