Brocade Encryption Switch/FS8-18 Cryptographic Module Security Policy

Document *Version 2.3*

Brocade Communications

December 15, 2009

TABLE OF CONTENTS

1. Module Overview

Brocade has implemented a Fibre-channel and Gigabit Ethernet data at-rest encryption module in two configurations, the FS8-18 Cryptographic Module and the Brocade Encryption Switch (BES) Cryptographic Module.

The FS8-18 Cryptographic Module configuration (P/N 60-1001078-01 Rev. B and C) provides the ability to expand a Brocade director chassis to include a Fibre Channel data encryption capability.

The Brocade Encryption Switch (BES) Cryptographic Module configuration (P/N 60-1001079-01 Rev. B and C) supports a standalone Fibre Channel data encryption capability.

The cryptographic modules provide services to secure data storage in a data center fabric. The module supports Brocade encryption devices, encrypting data between any two ports in the fabric. Each module provides up to 96 Gbps of encryption bandwidth. Brocade modules can be deployed as highly-available, fabric-based products that interoperate with existing storage and servers to provide high speed encryption.

The cryptographic module is defined by the following components:

- Motherboard (PCB)
- Metal Enclosure - Top and bottom metal covers with tamper labels
- Mounting tray
- Components contained by the metal enclosure

The images in Figures 1 and 2 show several components mounted outside of the metal covers; these components are **NOT** part of the

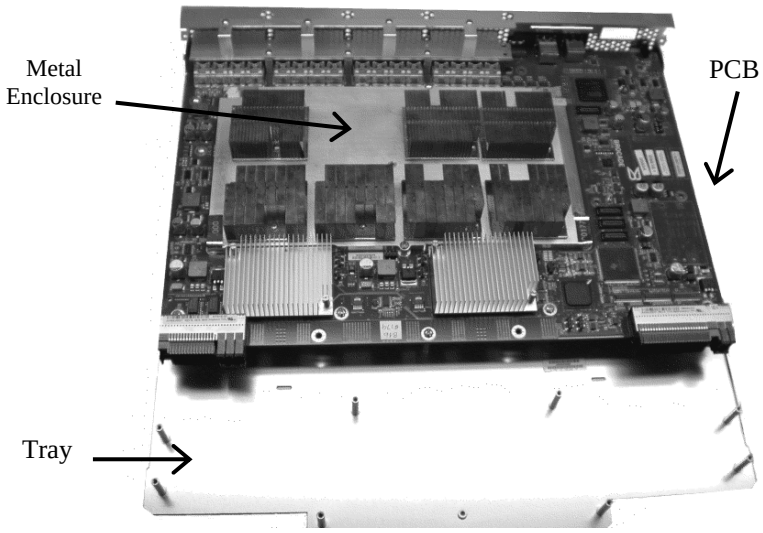


Figure 1 -BES Configuration

cryptographic module.

- Heat sinks
- Physical port adapters
- Exposed components

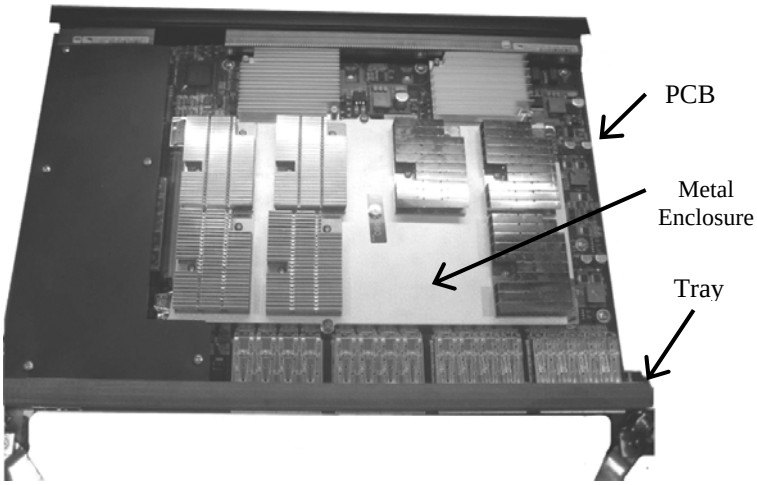


Figure 2 - FS8-18 Configuration

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

2. Modes of Operation

Approved mode of operation

The cryptographic module will only support an Approved mode of operation and implements the following Approved algorithms:

- AES GCM (AES Cert. #851, vendor affirmed)

- AES (Cert. #596, Cert. #851)
- DRNG (Cert. #358)
- HMAC-SHA-1 (Cert. #346)
- HMAC-SHA-512 (Cert. #346)
- SHA-1 (Cert. #844)
- SHA-1, SHA-256, SHA-512 (Cert. #645)
- RSA Verify 1024 (Cert. #407)
- RSA Sign/Verify (Cert. #337)

The following non-Approved algorithms will also be supported:

- RSA Encrypt/Decrypt for key transport within TLS (Provides 112 bits of security strength for key establishment)
- TLS
- MD5 to support TLS
- NDRNG
- Elliptic Curve Cryptography – Cofactor Diffie-Hellman (ECC-CDH) with p-521 curve (Non-compliant; No security is intended to be provided by this function; it is implemented for compatibility. Services utilizing this function are provided through a TLS session.)
- AES Key Wrap per the AES Key Wrap Specification (AES Cert. #596, key wrapping; key establishment methodology provides 256 bits of encryption strength)

3. Ports and Interfaces

The cryptographic module ports and interfaces are defined as the exposed end points of traces of the motherboard that connect enclosed components to exterior logic devices and physical connectors. The cryptographic module provides the following physical ports and logical interfaces:

Table 2 - Ports and Interfaces

Name	Type
FC Switch ASIC	Data Input, Data Output, Status Output
Gig-E	Data Output, Control Input, Status Output
Power	Power Input
PCI-e	Data Input, Control Input, Status Output
Reset	Control Input

4. Identification and Authentication Policy

Assumption of roles

The module supports two operator roles: the Cryptographic Officer and User. The cryptographic module shall enforce the separation of roles using identity-based operator authentication. The operators authenticate to the module by means of RSA digital signature verification using 2048-bit keys.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Cryptographic Officer	Identity-based operator authentication	Digital signature verification
User	Identity-based operator authentication	Digital signature verification

Table 4– Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Digital signature verification	Signatures are generated and verified using RSA 2048-bit keys, which are known to have an effective strength of 112-bits. 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 supports 10 consecutive failed authentication attempts. The probability of successfully authenticating to the module within one minute is 10/2^112 which is less than 1/100,000.

5. Access Control Policy

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

CSP / Key	Algorithm	Storage	Establishment	Generation
Crypto-Module (CM) Private Key: Used to authenticate the module.	RSA	Plaintext	N/A	Internal DRNG
Data Encryption Keys: Used for data confidentiality.	AES	Plaintext	N/A	Internal DRNG

CSP / Key	Algorithm	Storage	Establishment	Generation
Master Key: Used for DEK confidentiality.	AES	Plaintext	Entry: TLS Session	Internal DRNG
Link Key: Used for DEK confidentiality.	AES	Plaintext	Entry: TLS Session	N/A
TLS Encryption Key: Used for session confidentiality.	AES	Plaintext	Agreement: TLS Session Handshake	N/A
TLS Authentication Key: Used for session integrity.	HMAC	Plaintext	Agreement: TLS Session Handshake	N/A
TLS Pre-Shared Key: Used to establish TLS session keys.	KDF	Plaintext	Agreement: TLS Session Handshake	N/A
DRNG State: Used for random number generation.	DRNG	Plaintext	N/A	Internal NDRNG

Definition of Public Keys:

The following are the public keys contained in the module:

- Brocade Certificate Public Key: Used to verify firmware image integrity.
- Crypto-Module (CM) Public Key: Supports the authentication of the Crypto-Module.
- Crypto-Officer (CO) Public Key: Used to authenticate the Cryptographic Officer.
- Peer Device Public Key: Used to authenticate the peer device as FIPS user.
- Recovery Share Public Keys: Used to authenticate Recovery Cards.
- User Public Key: Used to authenticate the FIPS user.

Table 5 defines the relationship between access to CSPs and the different module services:

Table 5 – CSP Access Rights within Roles & Services

C.O.	User	Un-Authenticated	Service	Cryptographic Keys and CSPs Accessed by Service
X			Enable: Authorize the module to perform services	Use TLS Encryption Key Use TLS Authentication Key Use TLS Pre-Shared Key
X			Create KEK Wrapping Key	Use TLS Encryption Key Use TLS Authentication Key Use CM Private Key
X			Create RSA Key Transport Shared Secret	Use TLS Encryption Key Use TLS Authentication Key Use CM Private Key
X			Manage Master Key: Import or Export the Master Key	Use TLS Encryption Key Use TLS Authentication Key Read Master Key Import Master Key
X			Import Certificate	Use TLS Encryption Key Use TLS Authentication Key
X			Manage KEK: Import, export, create or delete KEKs	Use TLS Encryption Key Use TLS Authentication Key Use KEK Wrapping Key Delete Master Key or Link Key Create Master Key

C.O.	User	Un-Authenticated	Service	Cryptographic Keys and CSPs Accessed by Service
X			Install Manufacturing Public Key	Use TLS Encryption Key Use TLS Authentication Key
X			Create Link Key	Use TLS Encryption Key Use TLS Authentication Key Create Link Key
X			Firmware Load	Use TLS Encryption Key Use TLS Authentication Key
	X		Configure Encryption Service Rules: Specifies the policy for LUN encryptions. The service allows the configuration of alternating bypass.	Use TLS Encryption Key Use TLS Authentication Key Use Master Key, DEK, Link Key
	X		Commit Encryption Service Rules: Commits to the policy for LUN encryptions, results in creation, wrapping, import and export of DEKs. The service allows the configuration of alternating bypass.	Use TLS Encryption Key Use TLS Authentication Key Use Master Key, DEK, Link Key
		X	Initialize: Used to initialize and configure the module for operation.	Create CM Private Key
		X	Export Certificate: Export the specified X.509 certificates	N/A
		X	Zeroize: Destroy all plaintext CSPs contained within the module.	Destroy All CSPs
		X	Zeroize by tamper: Destroy all plaintext CSPs contained within the module by removing a cover of the module.	Destroy All CSPs
		X	Self-Tests: This service executes the suite of self-tests required by FIPS 140-2.	N/A

C.O.	User	Un-Authenticated	Service	Cryptographic Keys and CSPs Accessed by Service
		X	Show Status: Indicates the current module operational status.	N/A

6. Operational Environment

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

Note: Loading non-validated firmware will invalidate the module's FIPS 140-2 validation. There will be no assurance provided regarding compliant operation.

7. Security Rules

The cryptographic module's 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 FIPS 140-2 Level 3 module.

1. The module shall only support an Approved mode of operation. The module is initialized and configured to operate once initialized using the cryptographic configuration initialization service.
2. The unauthorized operator shall not have access to any of the module's cryptographic services.
3. The cryptographic module shall perform the following Self Tests:

   Power-On Self-Tests:

   - FW Integrity Tests:
     - RSA signature verification
     - FW Integrity Test (16-bit EDC)
   - Cryptographic Algorithm Tests:
     - AES GCM KAT
     - AES KAT
     - AES Key Wrap KAT

- DRNG KAT
- HMAC-SHA-1 KAT
- HMAC-SHA-512 KAT
- SHA-1, 256, and 512 KAT
- RSA Sign/Verify KAT
- RSA Encrypt/Decrypt KAT
- ECC-CDH KAT
- KDF KAT

Conditional Tests:

- FW Load Test (RSA signature verification)
- Continuous Test for the DRNG and NDRNG
- Alternating Bypass Test
- Pair-wise Consistency Tests

3. 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-tests.
4. Data output shall be inhibited during self-tests and error states.
5. Data output shall be logically disconnected from the processes performing key generation, zeroization, and key entry.
6. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

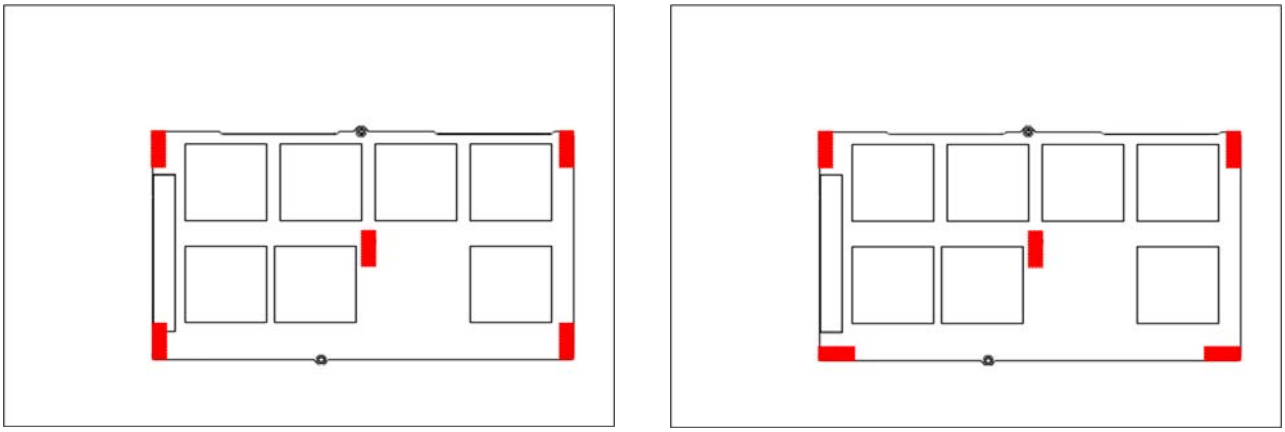
8. Physical Security Policy

Physical Security Mechanisms

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

- Production-grade components and opaque enclosure.
- Tamper response mechanism protecting the removable cover.

- Tamper labels and hard, opaque removable cover. Placement of labels is shown in red in Figure 2.



FS8-18 Configuration **BES Configuration**

Figure 3 - Tamper Label Placement on Cryptographic Boundary

9. Mitigation of Other Attacks Policy

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