EMC2
where information lives

FIPS 140-2 Non-Proprietary Security Policy

4 Gb/s FC I/O Module with Encryption from EMC

Document Version 1.0

September 1, 2011

Prepared For:

EMC Corporation
176 South Street
Hopkinton, MA 01748
www.emc.com

Prepared By:

Apex Assurance Group, LLC
530 Lytton Avenue, Ste 200
Palo Alto, CA 94301
www.apexassurance.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the 4 Gb/s FC I/O Module with Encryption from EMC.

Table of Contents

1 Introduction 5
1.1 About FIPS 140........ 5
1.2 About this Document........ 5
1.3 External Resources........ 5
1.4 Notices........ 5
1.5 Acronyms........ 5

2 4 Gb/s FC I/O Module with Encryption from EMC........ 7
2.1 Product Overview 7
2.2 Cryptographic Module Specification........ 7
2.2.1 Validation Level Detail 7
2.2.2 Approved Algorithms and Implementation Certificates 8
2.2.3 Non-Approved Algorithms 8
2.3 Module Interfaces........ 8
2.4 Roles, Services, and Authentication........ 9
2.4.1 Operator Services and Descriptions 9
2.5 Physical Security 10
2.6 Operational Environment 10
2.7 Cryptographic Key Management........ 11
2.8 Self-Tests........ 12
2.8.1 Power-On Self-Tests........ 12
2.8.2 Conditional Self-Tests........ 12
2.9 Mitigation of Other Attacks........ 12

3 Guidance and Secure Operation........ 13
3.1 Crypto Officer Guidance 13
3.2 User Guidance 13

List of Tables

Table 1 – Acronyms and Terms....6
Table 2 – Validation Level by DTR Section....8
Table 3 – Algorithm Certificates....8
Table 4 – Logical Interface / Physical Interface Mapping....9
Table 5 – Operator Services and Descriptions....10
Table 6 – Module Keys/CSPs....11

List of Figures

Figure 1 – Physical Boundary....7

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic products to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment of Canada (CSEC) Cryptographic Module Validation Program (CMVP) owns the FIPS 140 program. The CMVP accredits independent testing labs to perform FIPS 140 testing; the CMVP also validates test reports for all products pursuing FIPS 140 validation. *Validation* is the term given to a product that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at
http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the 4 Gb/s FC I/O Module with Encryption solution from EMC provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

EMC's 4 Gb/s FC I/O Module with Encryption line card may also be referred to as the "module" in this document.

1.3 External Resources

The EMC website (http://www.emc.com) contains information on the full line of products from EMC, including a detailed overview of the 4 Gb/s FC I/O Module with Encryption solution. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/) contains links to the FIPS 140-2 certificate and EMC contact information.

1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DTR	Derived Testing Requirement
FIPS	Federal Information Processing Standard
FC	Fibre Channel
GPC	General Purpose Computer
GPOS	General Purpose Operating System
I/O	Input/Output
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
QSFP	Quad Small Form-Factor Pluggable
XTS	Xor-Encrypt-Xor-based Tweaked CodeBook with CipherText Stealing

Table 1 – Acronyms and Terms

2 4 Gb/s FC I/O Module with Encryption from EMC

2.1 Product Overview

EMC Data at Rest Encryption provides hardware-based, on-array, back-end encryption for EMC storage systems, including the Symmetrix VMAX. Data at Rest Encryption protects information from unauthorized access when drives are physically removed from the system and also offers a convenient means of decommissioning all drives in the system at once.

EMC 4Gb/s Fibre Channel I/O modules implement AES-XTS 256-bit encryption on all drives in the system. These modules encrypt and decrypt data as it is being written to or read from a drive. Because the encryption happens in the I/O module, the back end drives need not be self-encrypting and all back end drive types are supported.

2.2 Cryptographic Module Specification

The module is EMC's 4 Gb/s FC I/O Module with Encryption, Part Number 303-176-100B B04. It is classified as a multi-chip embedded hardware cryptographic module, and the physical cryptographic boundary is defined as the module board, controller, flash memory, and interfaces as depicted in Figure 1 – Physical Boundary below.

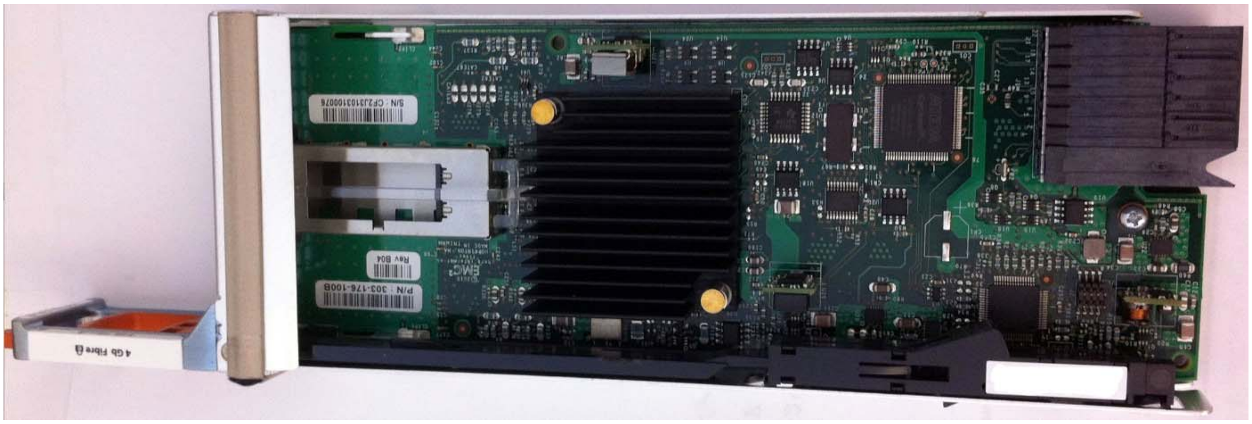

Figure 1 – Physical Boundary

No components are excluded from validation. The module encrypts and decrypts data using only a FIPS-approved mode of operation. It does not have any functional non-approved modes or bypass capability.

2.2.1 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	1

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
Electromagnetic Interference / Electromagnetic Compatibility	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 2 – Validation Level by DTR Section

The “Mitigation of Other Attacks” section is not applicable as the module does not implement any countermeasures against special attacks.

2.2.2 Approved Algorithms and Implementation Certificates

The module’s cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Symmetric Key	AES 256 in XTS mode	SP 800-38E	1638	Data encryption / decryption

Table 3 – Algorithm Certificates

2.2.3 Non-Approved Algorithms

The module implements AES key wrapping which is non-approved but allowed in FIPS mode of operation and provides 256-bits of encryption strength.

2.3 Module Interfaces

The interfaces for the cryptographic boundary include physical and logical interfaces. The physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: Data Input, Data Output, Control Input, and Status Output. The mapping of logical interfaces to module physical interfaces is provided in the following table:

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input	PCI Express QSFP
Data Output	PCI Express QSFP
Control Input	PCI Express

FIPS 140-2 Logical Interface	Module Physical Interface
Status Output	PCI Express Power / Fault LED Green indicates operational Amber indicates service action RX Loss & Link Rate LEDs Green indicates 2G FC connection at QSFP Blue indicates 4G FC connection at QSFP
Power	PCI Express

Table 4 – Logical Interface / Physical Interface Mapping

2.4 Roles, Services, and Authentication

As required by FIPS 140-2, there are two roles (a Crypto Officer role and User role) in the module that operators may assume. As allowed by Level 1, the module does not support authentication to access services.

2.4.1 Operator Services and Descriptions

The services available to the User and Crypto Officer roles in the module are as follows:

Service	Description	Service Input / Output	Interface	Key/CSP Access	Roles
Initialize	Initializes the module for FIPS mode of operation	Configuration Parameters / Module configured	PCI Express	KEK	Crypto Officer
Self Test	Performs self tests on critical functions of module (integrity and algorithm self-tests)	Initiate self tests / Self tests run	PCI Express	None	Crypto Officer
Decrypt	Decrypts data using AES	Initiate AES decryption / data decrypted	QSFP PCI Express	KEK DEK	Crypto Officer User
Encrypt	Encrypts data using AES	Initiate AES encryption/ data encrypted	QSFP PCI Express	KEK DEK	Crypto Officer User
Show Status	Shows status of the module	Show status commands / Module status	PCI Express LEDs	None	Crypto Officer
Zeroize CSPs	Clear CSPs from Flash and cache	Terminate Session / CSPs cleared	PCI Express	KEK DEK	Crypto Officer

Service	Description	Service Input / Output	Interface	Key/CSP Access	Roles
Key Unwrap	Unwrap DEK	Internally unwrap encrypted DEK / plaintext DEK. Note this is not a user-callable service.	PCI Express	KEK DEK	Crypto Officer

Table 5 – Operator Services and Descriptions

2.5 Physical Security

The module is a multiple-chip embedded module and conforms to Level 1 requirements for physical security. The cryptographic module consists of production-grade components. The physical boundary of the cryptographic module is the same as the physical boundary depicted in Figure 1 – Physical Boundary.

The module does not include a maintenance mode; therefore, the FIPS-140-2 maintenance mode requirements do not apply.

2.6 Operational Environment

The module operates in a limited operational environment and does not implement a General Purpose Operating System.

Additionally, the module meets Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part 15, Subpart B.

2.7 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

Keys and CSPs	Storage Locations	Storage Method	Input	Input Method	Output	Output Method	Generated	Zeroized	Access
KEK (AES key wrapping key)	Private NVRAM	Plaintext	Yes	Electronic, plaintext via host platform	No	NA	Generated at install time outside the module via FIPS-approved library	Yes	CO RWD User R
DEK (AES)	Cache	Plaintext	Yes	Electronic, encrypted with KEK	No	NA	Generated outside the module at time of install or replacement of disk drives outside the module via FIPS-approved library	Yes	CO RWD User RW

R = Read W = Write D = Delete

Table 6 – Module Keys/CSPs

2.8 Self-Tests

The module includes an array of self-tests that are run to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module will output an error dialog and will shutdown. When a module is in an error state, no keys, CSPs , or data will be output and the module will not perform cryptographic functions.

The module does not support a bypass function.

The following sections discuss the module's self-tests in more detail.

2.8.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and do not require operator intervention to run. If any of the tests fail, the module will not initialize. The module will enter an error state and no cryptographic functions can be accessed. The module implements the following power-on self-test:

- AES KAT (encryption and decryption)

The module performs this power-on self-test automatically during initialization, and it must pass before a User/Crypto Officer can perform cryptographic functions. The AES KAT can be run on-demand through external commands by a crypto officer when the module is idle.

The module is a hardware module and does not implement an integrity test since there is no software or firmware in the module.

2.8.2 Conditional Self-Tests

Conditional self-tests are tests that run continuously during operation of a module. The module does not perform any conditional self-tests since it does not implement any functions that require a conditional test.

The module is a hardware module and does not perform a firmware load test because there is no firmware in the module.

2.9 Mitigation of Other Attacks

The module does not mitigate other attacks.

3 Guidance and Secure Operation

This section describes how to configure the module for FIPS-approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

The Crypto Officer must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation:

- Verify that the name and part number of module is 4 Gb/s FC I/O Module with Encryption, Part Number 303-176-100B B04.
- Enable encryption on the host platform.
- Ensure that KEK and DEK are generated on the host platform via FIPS-approved module. Please note that this functionality is beyond the scope of the validation.
- Ensure that a KEK is loaded into the module.

Otherwise, no specific commands or settings are required to place the module in FIPS-approved mode of operation.

3.2 User Guidance

No additional guidance is required for Users to maintain FIPS mode of operation.

End of Document