EMC Corporation

VNX 6Gb/s SAS I/O Module with Encryption from EMC

Hardware Version: 1.1.1-303-161-103B-04 and 1.2.1-303-224-000C-03
Firmware Version: 2.09.36

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.1

Prepared for:

EMC²
where information lives®

EMC Corporation
176 South Street
Hopkinton, MA 01748
United States of America

Phone: +1 866 438 3622
http://www.emc.com

Prepared by:

Corsec

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the VNX 6Gb/s SAS I/O Module with Encryption from EMC from EMC Corporation. This Security Policy describes how the VNX 6Gb/s SAS I/O Module with Encryption from EMC meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The VNX 6Gb/s SAS I/O Module with Encryption from EMC is referred to in this document as Controller Based Encryption (CBE), crypto module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The EMC website (http://www.emc.com) contains information on the full line of products from EMC.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to EMC. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to EMC and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact EMC.

2 VNX 6Gb/s SAS I/O Module with Encryption from EMC

2.1 Overview

The EMC VNX 6Gb/s SAS I/O Module with Encryption from EMC is a SAS[1] controller executing specialized firmware that provides Data At Rest Encryption (D@RE) for EMC VNX Storage Arrays. D@RE provides data security, and offers a convenient means to decommission all drives in the system at once. Information is protected from unauthorized access even when drives are physically removed from the system.

The VNX 6Gb/s SAS I/O Module with Encryption from EMC is an optimized solution for native SAS/SATA[2] HBA[3] applications. It is the heart of any VNX storage system, providing the interface to the physical storage media. Its benefits include cost and universal drive support for SAS and SATA disks. The VNX 6Gb/s SAS I/O Module with Encryption from EMC is a high-density SAS controller solution that significantly increases total system performance, diagnostics, scalability and manageability. It provides the highest density, lowest power/port SAS controller solution available.

The EMC VNX family delivers industry-leading innovation and enterprise capabilities for file, block, and object storage in a scalable, easy-to-use solution. This next-generation storage platform combines powerful and flexible hardware with advanced efficiency, management, and protection software to meet the demanding needs of today's enterprises. All of this is available in a choice of systems ranging from affordable entry-level solutions to high-performance, petabyte-capacity configurations servicing the most demanding application requirements. The VNX family includes the VNXe series, purpose-built for the IT[4] manager in smaller environments, and the VNX series, designed to meet the high-performance, high scalability requirements of midsize and large enterprises.

The VNX 6Gb/s SAS I/O Module with Encryption from EMC implements AES[5]-XTS[6,7,8] 256-bit encryption on all SAS drives in the host array. The VNX 6Gb/s SAS I/O Module with Encryption from EMC is powered by a PMC-Sierra SAS controller, either a PM8019 or PM8009. The module encrypts and decrypts data, as it is being written to or read from a SAS drive. D@RE utilizes hardware embedded in the SAS controller for encryption.

The PM8019 is a sixteen-lane SAS controller configured to provide four quad-lane port SAS interfaces or two eight-lane SAS interfaces, and the PM8009 is an eight-lane SAS controller configured to provide two quad-lane port SAS interfaces. The module with PM8019 SAS controller is embedded in a pluggable hardware module, the UltraFlex SAS I/O Module, and the module with PM8009 SAS controller is contained within the Embedded SAS I/O Module[9] of the VNX Storage Arrays.

Figure 1 and Figure 2 below show the form factor of the Embedded SAS I/O Module (top and bottom views), while Figure 3 and Figure 4 below show the form factor of the UltraFlex SAS I/O Module (top and bottom views). In these figures "SPCv" stands for the name given by PMC-Sierra to its family of SAS controllers, which includes PM8009 and PM8019.

[1] SAS – Serial Attached SCSI (Small Computer System Interface)
[2] SATA – Serial Advanced Technology Advancement
[3] HBA – Host Bus Adapter
[4] IT – Information Technology
[5] AES – Advanced Encryption Standard
[6] XTS – XEX-based tweaked-codebook mode with ciphertext stealing
[7] XEX – XOR-Encrypt-XOR
[8] XOR – Exclusive Or
[9] The Embedded SAS I/O Module contains a SAS Expander along with a SAS Expander mounted on a Printed Circuit Board (PCB), which provides complete back-end expansion to both the internal drives and to an external Disk Array Enclosure (DAE).

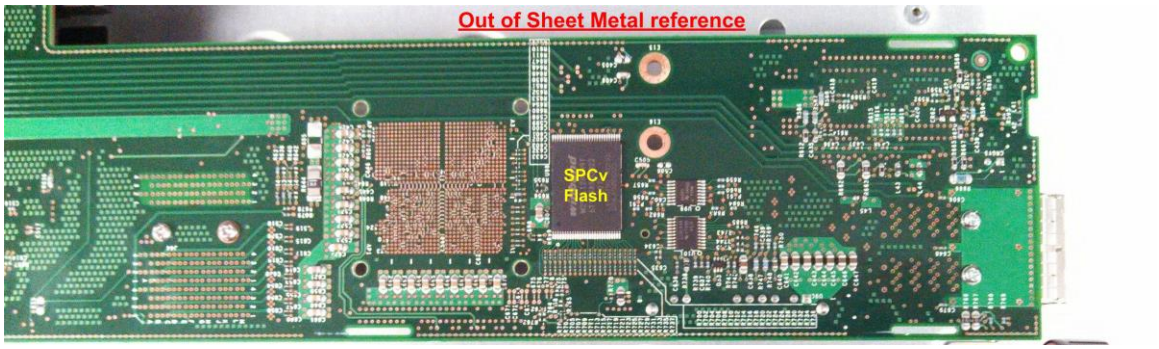

Figure 1 – Physical Embodiment of Embedded SAS I/O Module – Bottom View

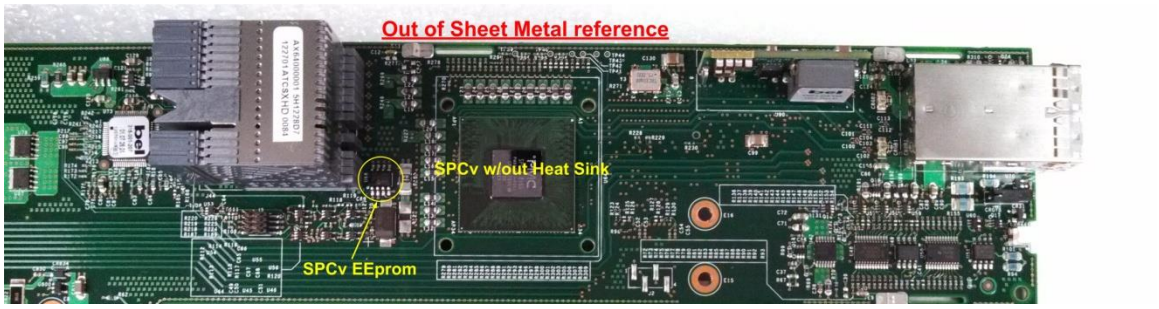

Figure 2 – Physical Embodiment of Embedded SAS I/O Module – Top View

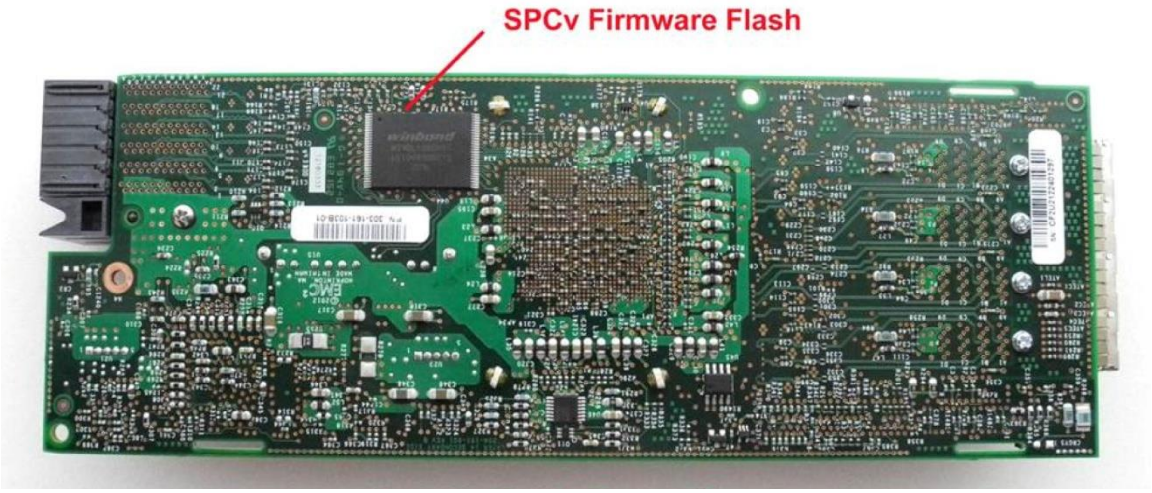

Figure 3 – Physical Embodiment of UltraFlex SAS I/O Module – Bottom View

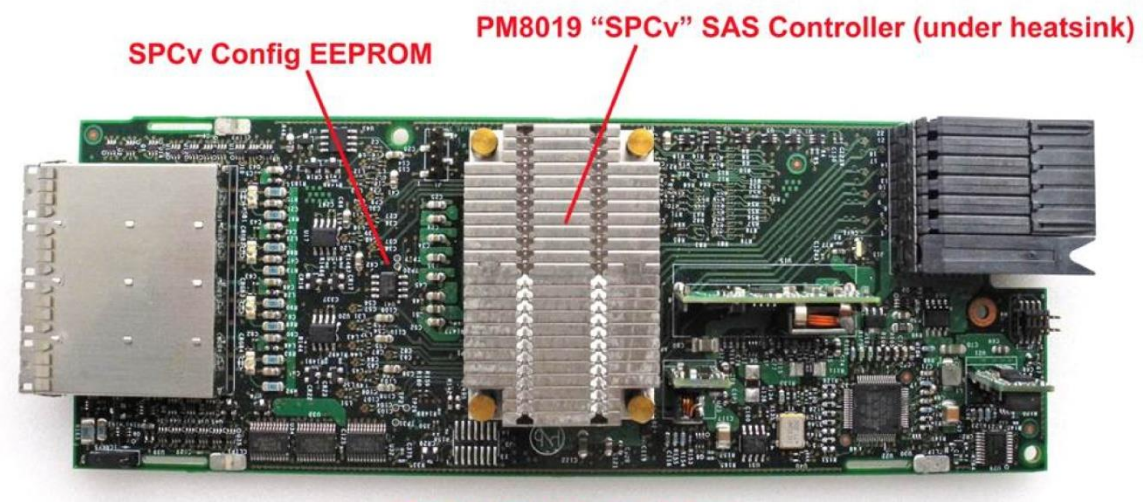

Figure 4 – Physical Embodiment of UltraFlex SAS I/O Module – Top View

The VNX 6Gb/s SAS I/O Module with Encryption from EMC is validated at the FIPS 140-2 Section levels shown in Table 1:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A[10]
7	Cryptographic Key Management	1
8	EMI/EMC[11]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The VNX 6Gb/s SAS I/O Module with Encryption from EMC is a hardware module with a multiple-chip embedded embodiment. The overall security level of the module is 1.

The cryptographic boundary of the VNX 6Gb/s SAS I/O Module with Encryption from EMC includes the following components:

- SAS controller (either PM8019 or PM8009)
  - PM8019: Sixteen-lane SAS controller configured to provide four quad-lane port SAS interfaces, and incorporates four AES-XTS encryption engines.

[10] N/A – Not Applicable
[11] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

  - PM8009: Eight-lane SAS controller configured to provide two quad-lane port SAS interfaces, and incorporates four AES-XTS encryption engines.
- Flash Memory
- SEEPROM[12]
- Reference clock

The cryptographic module with PM8019 is embedded within the SAS UltraFlex I/O Module, while the module with PM8009 is embedded within the SAS I/O Module of the host server appliance. The module includes 64MB[13] of Flash memory for firmware storage and error logging; and 32KB[14] SEEPROM for boot block, errata storage and initialization of the module. The module also includes an on-board 75 MHz reference clock. The module uses SAS ports to interface with the attached storage; and PCIe to interface with the host server. Figure 5 below presents the block diagram of the module.

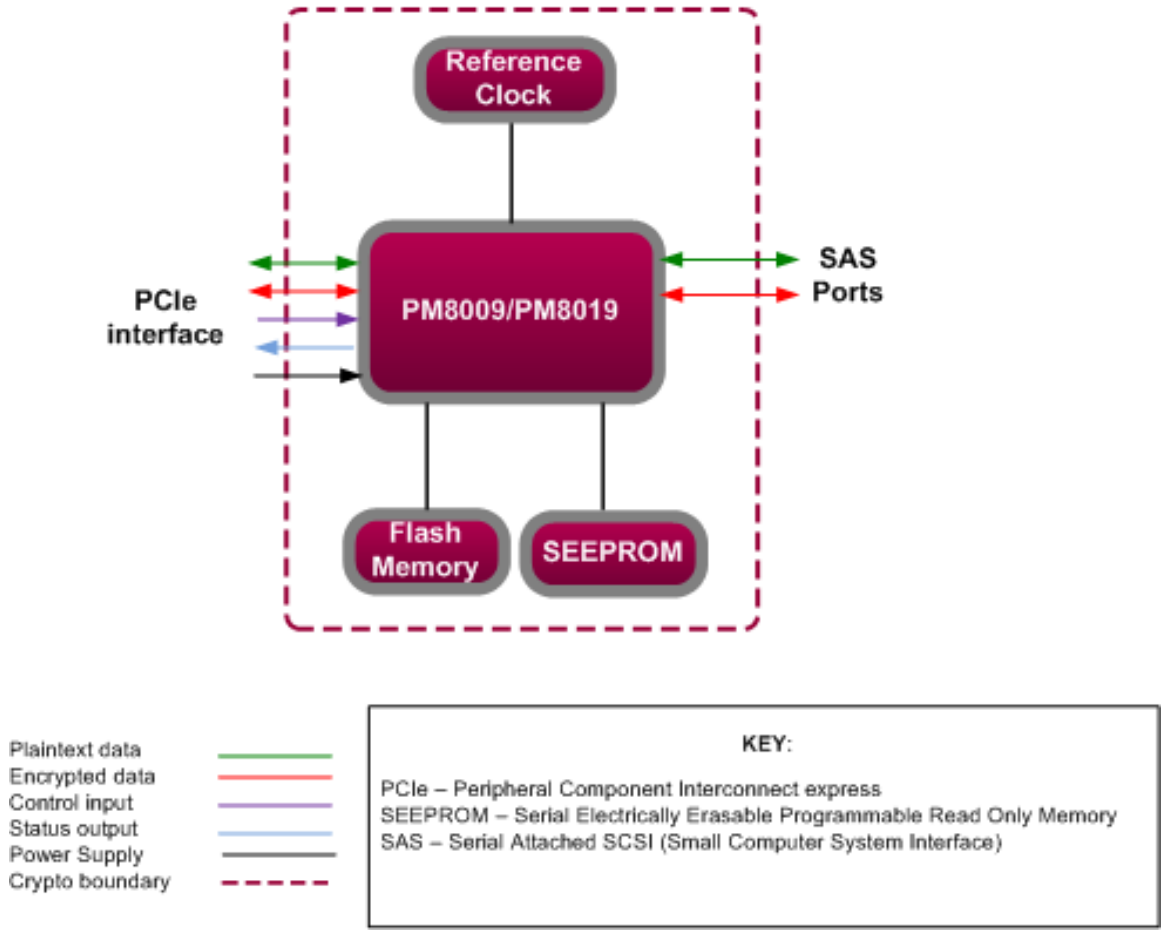

Figure 5 – VNX 6Gb/s SAS I/O Module with Encryption from EMC Block Diagram

[12] SEEPROM – Serial Electrically Erasable Programmable Read Only Encryption
[13] MB – Megabyte
[14] KB – Kilobyte

The module implements the FIPS-Approved algorithms listed in Table 2 below.

Table 2 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number (PN8009)	Certificate Number (PM8019)
AES-ECB[15] encryption/decryption with 256-bit keys	3502	3512
AES Key Wrap (unwrap only)	3502	3512
XTS[16,17,18]-AES encryption/decryption with XTS_256-bit keys	3502	3512

2.3 Module Interfaces

The module's design separates the physical ports into four logically distinct and isolated categories. They are:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

In addition, the module supports a Power Input interface.

Physical interfaces for the VNX 6Gb/s SAS I/O Module with Encryption from EMC are described in Table 3 below.

Table 3 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity	FIPS 140-2 Interface
PCIe interface	1	Data Input Data Output Control Input Status Output Power Input
SAS port(s)	PM8019: 4 x 4 (16 x 6G) ports PM8009: 2 x 4 (8 x 6G) ports	Data Input Data Output

2.4 Roles and Services

There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto-Officer (CO) role and a User role. Roles are assumed implicitly based on the service accessed.

[15] ECB – Electronic Code Book
[16] XTS - XEX-based tweaked-codebook mode with ciphertext stealing
[17] XEX – XOR-Encrypt-XOR
[18] XOR – Exclusive Or

Descriptions of the services available to a CO and a User are described below in Table 4. Please note that the keys and Critical Security Parameters (CSPs) listed in the Table 4 indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 4 – Crypto-Officer and User Services

Service	Operator		Description	Input	Output	CSP and Type of Access/Algorithm
	CO	User				
Configure encryption control parameters	✓	-	Initialize the module by configuring module's encryption control parameters. KEK-KEK entry must be performed at the factory by the manufacturer.	Command	Status output	None
Show Status	-	✓	Show module's status	Command	Status output	None
Manage KEK[19]	-	✓	Update/invalidate KEK	Command	Status output	KEK – RW (XTS-AES encryption/decryption with 256-bit keys)
Manage DEK[20]	-	✓	Update/invalidate DEK	Command	Status output	DEK – RW (XTS-AES encryption/decryption with 256-bit keys
Rekey	-	✓	Change the DEK for all or a subset of drives	Command	Status output	DEK – RW (XTS-AES encryption/decryption with 256-bit keys)
Encryption/ Decryption I/Os[21]	-	✓	Perform encryption/decryption I/Os when the host server initiates an SSP[22] I/O operation with an optional DIF[23] and/or encryption function.	Command	Status output	DEK – X KEK – X (XTS-AES encryption/decryption with 256-bit keys)
Power down	✓	✓	Power down the module using command	Command	Status output	KEK – W DEK – W (XTS-AES encryption/decryption with 256-bit keys)

[19] KEK – Key Encryption Key
[20] DEK – Data Encryption Key
[21] I/Os – Input/Outputs
[22] SSP – Serial SCSI Protocol
[23] DIF – Data Integrity Function

Service	Operator		Description	Input	Output	CSP and Type of Access/Algorithm
	CO	User				
Perform self-tests	✓	✓	Invoke self-tests via a reboot, or power-cycling	Reboot, or power-cycling	Status output	None
Decommission	✓	✓	Zeroize DEK, KEK and KEK-KEK	Command	Command response	DEK – W KEK – W KEK-KEK – W (XTS-AES encryption/decryption with 256-bit keys)
Remove RAID group	✓	✓	Zeroize DEK	Command	Command response	DEK – W (XTS-AES encryption/decryption with 256-bit keys)
Remove physical drive	✓	✓	Zeroize DEK	Command	Command response	DEK – W (XTS-AES encryption/decryption with 256-bit keys)

2.5 Physical Security

The VNX 6Gb/s SAS I/O Module with Encryption from EMC is a multiple-chip embedded cryptographic module. The module consists of production-grade[24] components that include standard passivation techniques.

2.6 Operational Environment

The cryptographic module employs a non-modifiable operating environment. The cryptographic module does not provide a general-purpose Operating System (OS) to the operator. The operational environment of the cryptographic module consists of the module's firmware v2.09.36. Only the FIPS-validated firmware verified by the module using its 32-bit CRC[25] verification method can be executed.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 5 below.

[24] Production grade is robust/rugged metal and plastic designed for intensive computing environments (i.e., server rooms) with standard passivation applied to the metal, designed to meet requirements for power, temperature, reliability, shock, and vibrations.

[25] CRC – Cyclic Redundancy Check

Table 5 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Input	Output	Storage	Zeroization	Use
DEK	AES-256	Entered electronically in ciphertext	Never exits the module	Stored in plaintext in RAM[26] [27]	Power cycling, RAID group removal, physical drive removal, decommission procedure	Encryption and decryption of volumes
KEK (AES Key Wrapping Key)	AES-256	Entered electronically in ciphertext	Never exits the module	Stored in plaintext in RAM	Power cycling or decommission procedure	Decryption of DEK
KEK-KEK (AES Key Wrapping Key)	AES-256	Preloaded	Never exits the module	Stored in plaintext In Flash	Decommission procedure	Decryption of KEK

The KEK-KEK is generated by a FIPS validated module and is loaded during manufacturing.

The KEK is wrapped outside the module boundary on the host platform with the KEK-KEK. The KEK is entered encrypted electronically from the host platform of the module. The module uses its internally stored copy of the preloaded KEK-KEK to decrypt (unwrap) the KEK using AES (Cert. #3502 or #3512) in KW mode.

The DEK is wrapped outside the module boundary on the host platform with the KEK. The DEK is entered encrypted electronically from the host platform of the module. The module then uses the KEK which was previously unwrapped to decrypt (unwrap) the DEK using AES (Cert. #3502 or #3512) in KW mode.

This functionality has been tested and the KW mode has been found compliant to SP 800-38F "Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping" and is denoted on the module certificate as KTS (AES Certs. #3502 and #3512)."

[26] RAM – Random Access Memory
[27] RAM here refers to any PM8019/PM8009 internal memory such as registers, or GSM (Global Shared Memory)

2.8 EMI/EMC

VNX 6Gb/s SAS I/O Module with Encryption from EMC was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.9 Self-Tests

Cryptographic self-tests are performed by the module when the module is first powered up and loaded into memory, or on-demand by rebooting or power cycling the module. The following sections list the self-tests performed by the module, their expected error status, and error resolutions.

2.9.1 Power-Up Self-Tests

The VNX 6Gb/s SAS I/O Module with Encryption from EMC performs the following self-tests at power-up:

- Firmware integrity test – a 32-bit CRC
- Known Answer Tests (KATs)
    - AES-ECB encrypt KAT
    - AES-ECB decrypt KAT
    - AES-XTS encrypt KAT
    - AES-XTS decrypt KAT

Self-tests are automatically invoked during power-up. If the module fails a power-up self-test, integrity test on Image Loader Agent (ILA) firmware, or main firmware then a critical error occurs and the error is reported in the registers Scratchpad Register 1 and Scratchpad Register 3. When the module enters critical error state, no cryptographic processing takes place and all data output is inhibited.

2.9.2 Conditional Self-Tests

The module does not perform any conditional self-tests.

2.9.3 Critical Functions Self-Tests

The VNX 6Gb/s SAS I/O Module with Encryption from EMC performs the following critical functional self-tests:

- AES key wrap KAT
- AES key unwrap KAT

If the module fails either of the critical functional tests then the module enters a critical error state. When in the critical error state, no cryptographic processing takes place and all data output is inhibited.

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The VNX 6Gb/s SAS I/O Module with Encryption from EMC meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Crypto-Officer Guidance

The sections below provide guidance for the CO for initial setup and secure management of the module.

3.1.1 Initial Setup

The module is available pre-installed on an EMC VNX array. The module is delivered in a non-operational factory state. The CO is responsible for initialization, configuration and management activities of the module.

The modules can be managed through the following underlying host server's interfaces

- Unisphere Command Line Interface (CLI)
- Unisphere Graphical User Interface (GUI)

The commands and buttons used in these interfaces translate to commands that enter the modules over the PCIe bus.

The CO must perform the following steps in order to put the module in FIPS mode of operation. Note: The KEK-KEK entry and activation operations must be performed at the factory prior to customer deployment.

- The CO should verify the part number of the hardware that the module is embedded into with the following part numbers:
  - PM8019, P/N 362-000-313 (found within the SAS UltraFlex I/O Module, PN: 303-161-103B-04)
  - PM8009, P/N 362-000-312 (found within the Embedded SAS I/O Module, PN: 303-224-000C-03)
  - SEEPROM, P/N 363-000-084
  - Flash, P/N 363-000-071
  - Oscillator, P/N 364-000-063
- The CO should verify that the version of the EMC firmware running on the module is version v2.18 which corresponds to v2.09.36 of the PMC firmware.
- The CO must install the CBE Enabler/License feature on the host array.
- Once the license is committed the CO should enable the encryption using "activate" operation. The CO can use the *"securedata-feature-activate"* command via Unisphere CLI or *"Activate Controller Based Encryption"* button via Unisphere GUI for enabling encryption.

At this stage, the module is in the FIPS-approved mode of operation. Access to the module via the JTAG[28] and UART[29] headers is prohibited in the FIPS mode of operation.

3.1.2 Secure Management

The CO is responsible for ensuring that the modules are operating in their FIPS-approved mode of operation.

3.1.2.1 Management

When configured according to the CO guidance in this Security Policy, the module only runs in an Approved mode of operation. The CO shall manage the module via the host server interfaces Unisphere CLI, and

[28] JTAG – Joint Test Action Group
[29] UART – Universal Asynchronous Receiver/Transmitter

Unisphere GUI. Once the module is in FIPS-approved mode of operation, for any data in place conversion operations, the CO will ensure that the host array has no network connectivity until all the existing data on the host array is encrypted. For recommendations on data in place conversion operations refer to *EMC Security Configuration Guide for VNX*.

3.1.2.2 Monitoring Status

The CO should monitor the module status regularly for FIPS-approved mode of operation. When configured according to the CO's guidance, the module only operates in the FIPS-approved mode. Thus, the current status of the modules when operational is always in the FIPS-approved mode.

The PCIe interface indicates the current status of the module via the Unisphere CLI and Unisphere GUI interfaces. The encryption mode of the array (on/off)[30] is also reported on the Unisphere CLI and Unisphere GUI host interfaces.

Detailed instructions to monitor and troubleshoot the systems are provided in the *EMC Unisphere Online Help.*

3.1.2.3 Zeroization

The DEK, KEK, and KEK-KEK can be zeroized via the decommission procedure. Additionally, KEKs and DEKs may also be zeroized on power down of the module. DEKs may be zeroized through the RAID group removal procedure, as well as when a physical drive is removed from the array. The commands processed during these operations are detailed in Table 6 below.

Table 6 – Zeroization Commands

CSP	Operator		Command	Input
	CO	User		
DEK	✓	✓	DEK_MANAGEMENT	Initiated via System Operation (RAID group removal, physical drive removal, decommission procedure, power down)
KEK	✓	✓	KEK_MANAGEMENT	Initiated via System Operation (Decommission procedure, power down)
KEK-KEK	✓	✓	KEK_MANAGEMENT	Initiated via System Operation (Decommission procedure)

3.2 User Guidance

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

3.3 Non-Approved Mode of Operation

When configured according to the Crypto Officer guidance in this Security Policy, the modules do not support a non-Approved mode of operation.

[30] In the FIPS-approved mode of operation, encryption mode of the array is always on.

4 Acronyms

Table 7 provides definitions for the acronyms used in this document.

Table 7 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CBE	Controller Based Encryption
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRC	Cyclic Redundancy Check
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DAE	Disk Array Enclosure
D@RE	Data At Rest Encryption
DEK	Data Encryption Key
DIF	Data Integrity Function
ECB	Electronic Code Book
EEPROM	Electrically Erasable Programmable Read Only Encryption
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HBA	Host Bus Adapter
ILA	Image Loader Agent
IT	Information Technology
I/O	Input/Output
JTAG	Joint Test Action Group
KAT	Known Answer Test
KEK	Key Encryption Key
KEK-KEK	Key Encryption Key-Key Encryption Key
NIST	National Institute of Standards and Technology
N/A	Not Applicable
OS	Operating System
PCB	Printed Circuit Board

Acronym	Definition
PCIe	Peripheral Component Interconnect Express
RAM	Random Access Memory
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SEEPROM	Serial Electrically Erasable Programmable Read Only Encryption
SHA	Secure Hash Algorithm
SSP	Serial SCSI Protocol
UART	Universal Asynchronous Receiver/Transmitter
XEX	XOR-Encrypt-XOR
XOR	Exclusive Or
XTS	XEX-Based Tweaked-Codebook Mode with Ciphertext Stealing

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com