Dell EMC

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

Hardware Versions: 1.1.1-303-161-103B-04 and 1.2.1-303-224-000C-03
Firmware Version: 2.13.46

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.8

Prepared for:

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

Phone: +1 806 438 3622
www.dellemc.com

Prepared by:

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

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

Table of Contents

1. Introduction 4
1.1 Purpose 4
1.2 References 4
1.3 Document Organization 4
2. VNX 6 Gb/s SAS I/O Module with Encryption 5
2.1 Overview 5
2.2 Module Specification 7
2.3 Module Interfaces 9
2.4 Roles and Services 10
2.5 Physical Security 11
2.6 Operational Environment 12
2.7 Cryptographic Key Management 12
2.8 EMI / EMC 13
2.9 Self-Tests 13
2.9.1 Power-Up Self-Tests 13
2.9.2 Conditional Self-Tests 13
2.9.3 Critical Functions Self-Tests 13
2.10 Mitigation of Other Attacks 14
3. Secure Operation 15
3.1 Initial Setup 15
3.2 Secure Management 16
3.2.1 Management 16
3.2.2 Monitoring Status 16
3.2.3 Zeroization 16
3.3 User Guidance 17
3.4 Non-FIPS-Approved Mode 17
4. Acronyms 18

List of Tables

Table 1 – Security Level per FIPS 140-2 Sections 7
Table 2 – Algorithm Certificate Numbers 9
Table 3 – FIPS 140-2 Logical Interface Mappings 9
Table 4 – CO and User Services 10
Table 5 – Services Not Requiring Role Assumption 11
Table 6 – Cryptographic Keys, Cryptographic Key Components, and CSPs 12
Table 7 – Zeroization Commands 16
Table 8 – Acronyms 18

List of Figures

Figure 1 – UltraFlex Form Factor (Top View)....5
Figure 2 – UltraFlex Form Factor (Bottom View)....6
Figure 3 – Base Module Form Factor (Top View)....6
Figure 4 – Base Module Form Factor (Bottom View)....7
Figure 5 – VNX 6 Gb/s SAS I/O Module with Encryption Block Diagram....8

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for Dell EMC's VNX 6 Gb/s[1] SAS[2,3] I/O[4] Module with Encryption (firmware version: 2.13.46). This Security Policy describes how the VNX 6 Gb/s SAS I/O Module with Encryption meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the United States (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 Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at https://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to operate 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. In this document, the VNX 6 Gb/s SAS I/O Module with Encryption is also referred to as the module.

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Dell EMC.

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 Dell EMC website (www.dellemc.com) contains information on the full line of products from Dell EMC.
- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

1.3 Document Organization

The Security Policy document is organized into two (2) primary sections. Section 2 provides an overview of the validated module. This includes a general description of the capabilities and the use of cryptography, as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the module meets FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions and management methods and policies.

[1] Gb/s – Gigabit per second
[2] SAS – Serial Attached SCSI
[3] SCSI – Small Computer System Interface
[4] I/O – Input/Output

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

2.1 Overview

The Dell EMC VNX 6 Gb/s SAS I/O Module with Encryption is a high-density SAS controller executing specialized firmware that provides Data At Rest Encryption (D@RE) for Dell 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 6 Gb/s SAS I/O Module with Encryption is an optimized solution for native SAS/SATA[5] HBA[6] applications.

The VNX 6 Gb/s SAS I/O Module with Encryption implements 256-bit XTS[7,8,9]-AES[10] encryption on all SAS drives in the host array. The module, powered by a Microchip SAS controller (PM8009 or PM8019), 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 module is currently deployed in two form factors:

- The first form factor includes the PM8019 SAS controller variant (version 1.1.1-303-161-103B-04), and is embedded in a pluggable hardware module, the UltraFlex SAS I/O Module. The PM8019 is a sixteen-lane SAS controller configured to provide four quad-lane SAS interfaces or two eight-lane SAS interfaces. Figure 1 and Figure 2 below provide top and bottom views of the UltraFlex form factor.

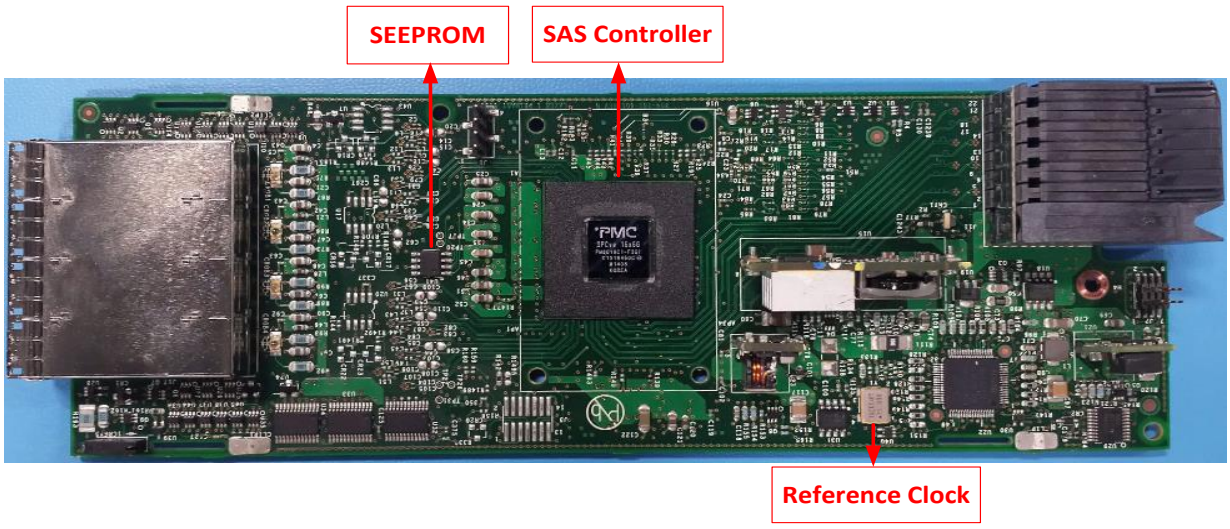

Figure 1 – UltraFlex Form Factor (Top View)

[5] SATA – Serial Advanced Technology Advancement
[6] HBA – Host Bus Adapter
[7] XTS – XEX-based tweaked-codebook mode with ciphertext stealing
[8] XEX – XOR-Encrypt-XOR
[9] XOR – Exclusive Or
[10] AES – Advanced Encryption Standard

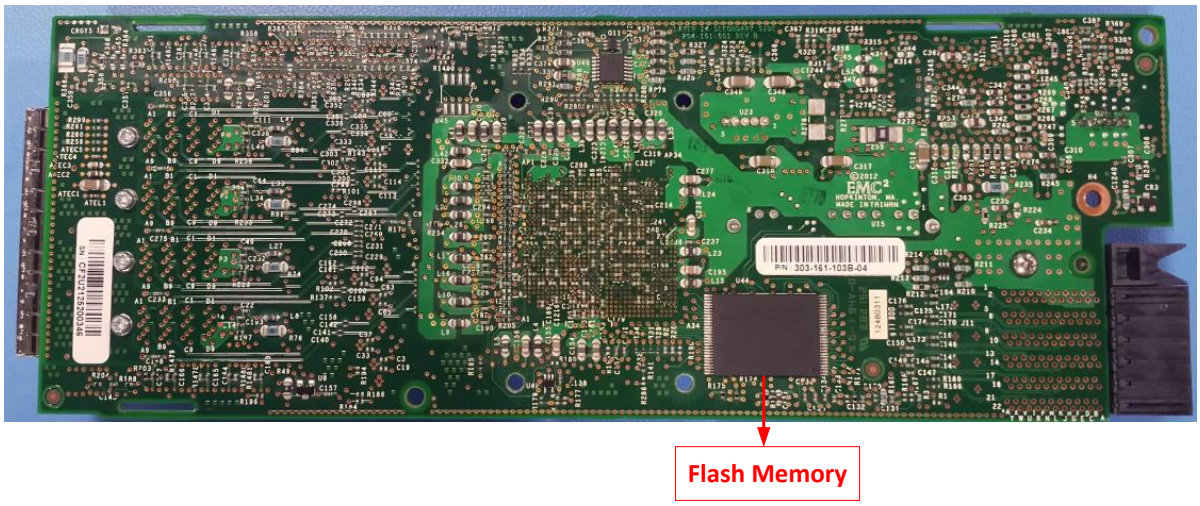

Figure 2 – UltraFlex Form Factor (Bottom View)

- The second form factor includes the PM8009 SAS controller variant (version 1.2.1-303-224-000C-03) and is embedded within the Base Module of a storage processor of the VNX Storage Arrays. The PM8009 is an eight-lane SAS controller configured to provide two quad-lane SAS interfaces. Figure 3 and Figure 4 below provide top and bottom views of the Base Module form factor.

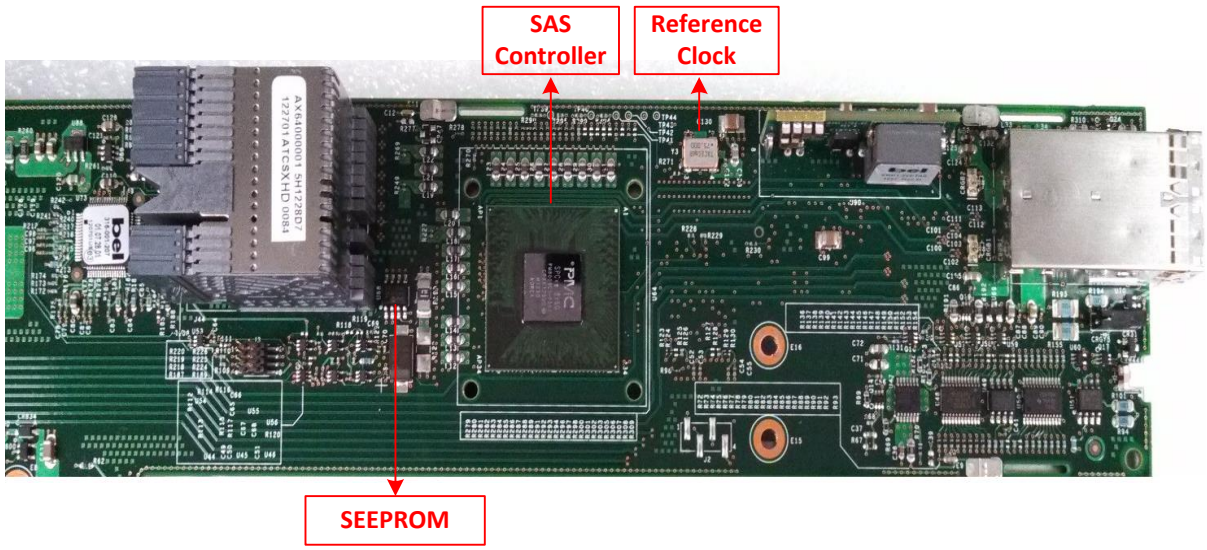

Figure 3 – Base Module Form Factor (Top View)

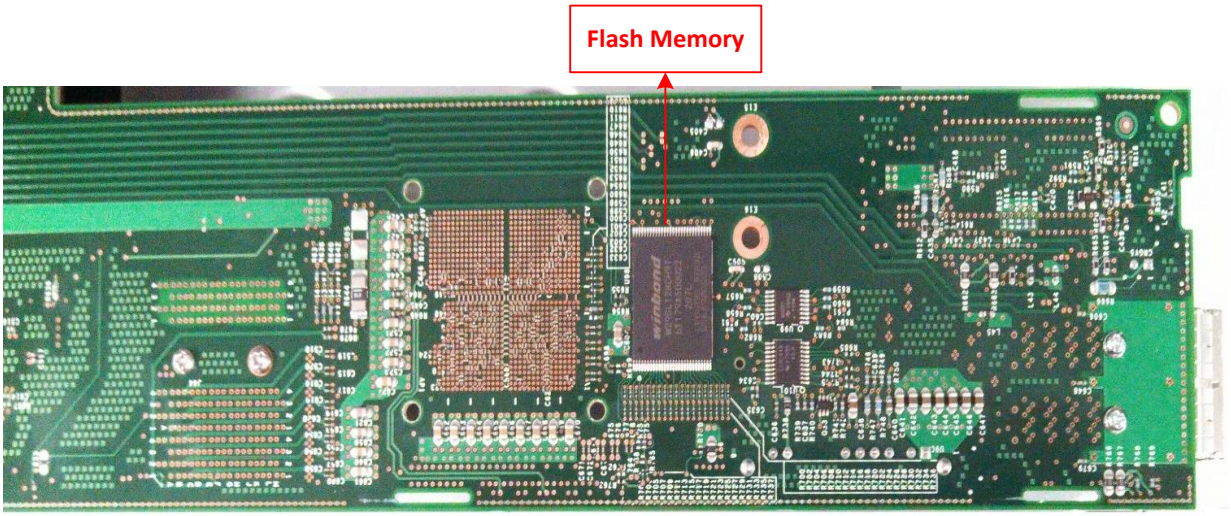

Figure 4 – Base Module Form Factor (Bottom View)

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

Table 1 – Security Level per FIPS 140-2 Sections

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[11]
7	Cryptographic Key Management	1
8	EMI/EMC[12]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

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

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

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

- SAS Controller (either PM8009 or PM8019)
- Flash Memory
- SEEPROM[13]
- Reference Clock

The cryptographic module includes 64 MB[14] of Flash memory for firmware storage and error logging and 32 KB[15] SEEPROM for boot block, errata storage, and initialization of the module. The module also includes an on-board 75 MHz[16] reference clock. The module uses SAS ports to interface with the attached storage, and PCIe[17] to interface with the host server. Figure 5 below presents the block diagram of the module.

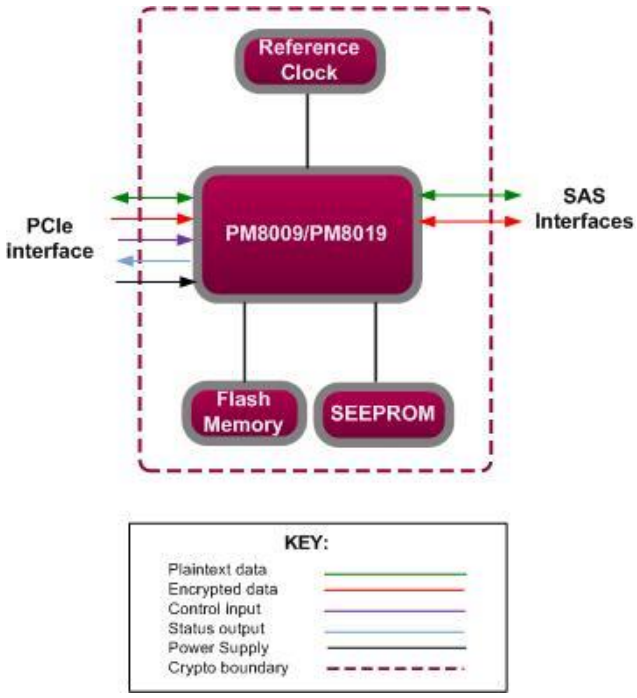

Figure 5 – VNX 6 Gb/s SAS I/O Module with Encryption Block Diagram

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

[13] SEEPROM – Serial Electrically Erasable Programmable Read Only Memory
[14] MB – Megabyte
[15] KB – Kilobyte
[16] MHz – Megahertz
[17] PCIe – Peripheral Component Interconnect Express

Table 2 – Algorithm Certificate Numbers

Certificate Number		Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
PM8009	PM8019					
3502	3512	AES	FIPS PUB[18] 197	ECB[19]	256	encryption/decryption
			FIPS PUB 197 NIST SP 800-38E	XTS	256	encryption/decryption
			FIPS PUB 197 NIST SP[20] 800-38F	KW[21]	256	key unwrapping

***Note**: XTS-AES is only approved for storage applications.*

2.3 Module Interfaces

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

- 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 6 Gb/s SAS I/O Module with Encryption 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 interface	PM8009: 2 x 4 (8 x 6G) ports	• Data input • Data output
	PM8019: 4 x 4 (16 x 6G) ports	• Data input • Data output

[18] PUB – Publication
[19] ECB – Electronic Code Book
[20] SP – Special Publication
[21] KW – Key Wrap

2.4 Roles and Services

There are two roles in the module that operators may assume: Crypto Officer (CO) role and User role. Roles are assumed implicitly based on the service accessed.

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 – CO and User Services

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Configure encryption control parameters	✓		Initialize the module by configuring module's encryption control parameters	Command	Status output	None
Show Status	✓		Show module's status	Command	Status output	None
Perform self-tests	✓		Invoke self-tests	Reboot or power-cycling	Status output	None
Manage KEK[22]		✓	Deliver the wrapped KEK to the module to update or invalidate (zeroize)	Command	Status output	KEK-KEK[23] – RX KEK – W
Manage DEK[24]		✓	Update or invalidate (zeroize) DEK	Command	Status output	DEK – W
Rekey		✓	Change the DEK for all or a subset of drives	Command	Status output	DEK – RW

[22] KEK – Key Encryption Key
[23] KEK-KEK – Key Encryption Key-Key Encryption Key
[24] DEK – Data Encryption Key

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Perform Encryption and Decryption I/Os[25]		✓	Perform encryption/ decryption I/Os when the host server initiates an SSP[26] I/O operation with an optional DIF[27] and/or encryption function	Command	Status output	KEK – RX DEK – WRX

The module also offers services that do not require the assumption of an authorized role. While several of these services do access CSPs, that access is limited to zeroization, which is allowed to be performed without requiring assumption of an authorized role (per the "Additional Comments" section in FIPS Implementation Guidance item 3.1).

Services that do not require role assumption are shown in Table 5 below.

Table 5 – Services Not Requiring Role Assumption

Service	Description	Input	Output	CSP and Type of Access
Power down	Power down the module using command	Command	Status output	KEK – W DEK – W
Decommission	Zeroize DEK, KEK, and KEK-KEK	Command	Command response	DEK – W KEK – W KEK-KEK – W
Remove RAID[28] group	Zeroize DEK	Command	Command response	DEK – W
Remove physical drive	Zeroize DEK	Command	Command response	DEK – W

2.5 Physical Security

The VNX 6 Gb/s SAS I/O Module with Encryption is a multiple-chip embedded cryptographic module. The module consists of production-grade[29] components that include standard passivation techniques.

[25] The wrapped DEK is imported to the module, unwrapped using the KEK, and stored within the controller as part of the encryption/decryption I/O command if the DEK does not already exist within the controller.
[26] SSP – Serial SCSI Protocol
[27] DIF – Data Integrity Function
[28] RAID – Redundant Array of Independent Disks
[29] Production grade is robust/rugged metal and plastic designed for intensive computing environments (i.e., server rooms) with standard passivation applied to the metal that is designed to meet requirements for power, temperature, reliability, shock, and vibrations.

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. The module only loads and executes the FIPS-validated firmware that successfully passes the 32-bit CRC[30] verification method.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 6 below.

Table 6 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
DEK	256-bit XTS-AES key	Generated externally and entered electronically in ciphertext	Never exits the module	Stored in plaintext in RAM[31] [32]	Power-cycling, RAID group removal, physical drive removal, or decommission procedure	Encryption and decryption of volumes
KEK	256-bit AES-ECB key	Generated externally and entered electronically in ciphertext	Never exits the module	Stored in plaintext in RAM	Power-cycling or decommission procedure	Unwrapping of DEK
KEK-KEK	256-bit AES-ECB key	Preloaded OR Generated externally and entered electronically in plaintext	Never exits the module	Stored in plaintext in Flash memory	Decommission procedure	Unwrapping of KEK

The KEK-KEK is generated externally and loaded into the module when encryption is activated during the module's initial configuration into the Approved mode. The KEK-KEK is loaded into the module in plaintext form from the direct-attached host device over the PCIe connection. Activation of encryption can be performed prior to delivery or by the CO upon receipt of the module.

The KEK is generated outside the module on the host platform, wrapped with the KEK-KEK, then entered electronically from the host platform of the module. The module uses the KEK-KEK to unwrap the KEK using AES in KW mode (Cert. #3502 or #3512).

[30] CRC – Cyclic Redundancy Check
[31] RAM – Random Access Memory
[32] RAM here refers to any PM8009/PM8019 internal memory such as registers, or GSM (Global Shared Memory)

The DEK is generated outside the module on the host platform, wrapped with the KEK, then entered electronically from the host platform of the module. The module then uses the KEK to unwrap the DEK using AES in KW mode (Cert. #3502 or #3512).

2.8 EMI / EMC

The VNX 6 Gb/s SAS I/O Module with Encryption 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. These power-up self-tests can be initiated on-demand at any time by rebooting or power-cycling the module. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

2.9.1 Power-Up Self-Tests

Once the module is initialized, self-tests are automatically invoked during power-up. When the power-up self-tests complete successfully, the module is in a fully operational state. The VNX 6 Gb/s SAS I/O Module with Encryption performs the following self-tests:

- Firmware Integrity Test on the Image Loader Agent firmware using an Error Detection Code (32-bit CRC)
- Firmware Integrity Test on the module's operational firmware using an Error Detection Code (32-bit CRC)
- Known Answer Tests (KATs)
    - AES-ECB Encrypt KAT
    - AES-ECB Decrypt KAT
    - XTS-AES Encrypt KAT
    - XTS-AES Decrypt KAT

If the module fails a power-up self-test, then a critical error occurs. The error is logged in 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.

To clear the critical error state, the module must be power-cycled or rebooted. If the condition persists, the module must be serviced by Dell EMC.

2.9.2 Conditional Self-Tests

The module does not perform any FIPS-required conditional self-tests.

2.9.3 Critical Functions Self-Tests

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

- AES Key Unwrap KAT
- XTS-AES Duplicate Key Test

The VNX 6 Gb/s SAS I/O Module with Encryption performs the AES Key Unwrap KAT at power-up or reboot. The XTS-AES Duplicate Key Test is performed conditionally, when the DEK is imported into the module during the encryption/decryption I/O service. If the XTS-AES Duplicate Key Test fails, the module enters a soft-error state, generating an error and outputting the failure via the status output interface. Once the status is output, the error state is automatically cleared, and the module transitions back to normal operations.

If the module fails the AES Key Unwrap KAT, then the module enters a critical error state. The error is logged in a register internally and output from the module over the PCIe interface. Once the module has entered the critical error state, all cryptographic processing and data output is inhibited.

To clear the critical error state, the module must be power cycled or rebooted. If the condition persists, the module must be serviced by Dell EMC.

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 6 Gb/s SAS I/O Module with Encryption meets Level 1 requirements for FIPS 140-2. The sections below describe how to operate the module in the FIPS-Approved mode of operation.

3.1 Initial Setup

The module is available pre-installed on a Dell EMC VNX2 array. The CO is responsible for performing all initialization, configuration, and encryption state verification activities necessary to place the module in its FIPS-Approved mode of operation.

The module can be managed through the following host server 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 module over the control input interface (PCIe bus).

During initial setup, the CO must perform the following steps to determine if the module is configured for its FIPS-Approved mode of operation:

1. The CO shall verify the part number of the module hardware with the following part numbers:
    - 1.1.1-303-161-103B-04 (for the PM8019 variant)
    - 1.2.1-303-224-000C-03 (for the PM8009 variant)

2. The CO shall verify the version of the Dell EMC firmware running on the module using the `naviseccli getresume -io` command:
    - The Dell EMC firmware v2.40 corresponds to v2.13.46 of the Microchip firmware.

3. The CO shall determine if encryption is activated. The CO shall determine if the encryption mode is set to "Controller Based Encryption" by using the *securedata -feature -info* command via the Unisphere CLI or navigating to **System -> System Properties -> Encryption** via the Unisphere GUI.

    If the CO determines that the module's encryption mode is not set, then the CO shall install and activate the "Data at Rest Encryption Enabler/License" feature on the host array. Once the license is committed, the CO shall enable encryption using the "activate" operation. The CO can use the *securedata -feature -activate* command via the Unisphere CLI or the "Data at Rest Encryption Activation Wizard" via the Unisphere GUI for activating encryption. Once these steps are completed, the CO shall verify that the encryption mode is updated to "Controller Based Encryption" to ensure that encryption has been properly activated.

For more information on activating encryption and verifying the encryption mode, refer to the *EMC VNX2: Data at Rest Encryption* white paper.

Upon successful verification, the module can be confirmed to be running in its FIPS-Approved mode of operation. If any of the verification steps fails, the CO shall contact Dell EMC Customer Support for assistance. Access to the module via the JTAG[33] and UART[34] headers is prohibited in the FIPS-Approved mode of operation.

3.2 Secure Management

The CO is responsible for ensuring that the module is operating in its FIPS-Approved mode of operation.

3.2.1 Management

When configured according to the CO guidance in this Security Policy, the module only runs in a FIPS-Approved mode of operation. The CO shall manage the module via the host server's Unisphere CLI and Unisphere GUI interfaces. Once the module is in the FIPS-Approved mode of operation, for any data-at-rest 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-at-rest conversion operations, refer to the *Security Configuration Guide for VNX.*

3.2.2 Monitoring Status

The CO should monitor the module status regularly for the FIPS-Approved mode of operation. When configured correctly, the module only operates in the FIPS-Approved mode. Thus, when operational, the current status is always in the FIPS-Approved mode.

The module indicates the current status of the module via the Unisphere CLI and Unisphere GUI interfaces. The encryption mode of the array (N/A, Unencrypted, or Controller Based Encryption)[35] is also reported on the Unisphere CLI and Unisphere GUI host interfaces.

Detailed instructions for monitoring and troubleshooting the systems are provided in the *Unisphere Online Help.*

3.2.3 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 7 below.

Table 7 – Zeroization Commands

CSP	Command	Input
DEK	DEK_MANAGEMENT	Initiated via System Operation (RAID group removal, physical drive removal, decommission procedure, power down)

[33] JTAG – Joint Test Action Group
[34] UART – Universal Asynchronous Receiver/Transmitter
[35] In the FIPS-Approved mode of operation, encryption mode of the array is always set to "Controller Based Encryption".

CSP	Command	Input
KEK	KEK_MANAGEMENT	Initiated via System Operation (Decommission procedure, power down)
KEK-KEK	KEK_MANAGEMENT	Initiated via System Operation (Decommission procedure)

3.3 User Guidance

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

3.4 Non-FIPS-Approved Mode

When initialized and configured as documented this Security Policy, the module does not support a non-FIPS-Approved mode of operation.

4. Acronyms

Table 8 below provides definitions for the acronyms used in this document.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CCCS	Canadian Centre for Cyber Security
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
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
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
Gb/s	Gigabit per second
GUI	Graphical User Interface
HBA	Host Bus Adapter
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
KB	Kilobyte
KTS	Key Transport Scheme
KW	Key Wrap
MB	Megabyte
MHz	Megahertz
N/A	Not Applicable
NIST	National Institute of Standards and Technology

Acronym	Definition
OS	Operating System
PCIe	Peripheral Component Interconnect Express
P/N	Part Number
PUB	Publication
RAID	Redundant Array of Independent Disks
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
SP	Special Publication
SSP	Serial SCSI Protocol
UART	Universal Asynchronous Receiver/Transmitter
U.S.	United States
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