



FIPS 140-2 Non-Proprietary Security Policy

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

Document Version 1.0

November 10, 2016

Prepared For:



Dell EMC
176 South Street
Hopkinton, MA 01748
www.dell EMC.com

Prepared By:



SafeLogic Inc.
459 Hamilton Ave, Suite 306
Palo Alto, CA 94301
www.safelogic.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the VMAX 6 Gb/s SAS I/O Module with Encryption.

Table of Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 4 |
| 1.1 | <i>About FIPS 140</i> | <i>4</i> |
| 1.2 | <i>About this Document.....</i> | <i>4</i> |
| 1.3 | <i>External Resources</i> | <i>4</i> |
| 1.4 | <i>Notices.....</i> | <i>4</i> |
| 1.5 | <i>Acronyms.....</i> | <i>4</i> |
| 2 | VMAX 6 Gb/s SAS I/O Module with Encryption | 6 |
| 2.1 | <i>Product Overview</i> | <i>6</i> |
| 2.2 | <i>Cryptographic Module Specification</i> | <i>6</i> |
| 2.2.1 | <i>Validation Level Detail</i> | <i>8</i> |
| 2.2.2 | <i>Approved Algorithms and Implementation Certificates.....</i> | <i>9</i> |
| 2.3 | <i>Module Interfaces</i> | <i>9</i> |
| 2.4 | <i>Roles, Services, and Authentication</i> | <i>10</i> |
| 2.4.1 | <i>Operator Services and Descriptions.....</i> | <i>10</i> |
| 2.5 | <i>Physical Security.....</i> | <i>11</i> |
| 2.6 | <i>Operational Environment.....</i> | <i>11</i> |
| 2.7 | <i>Cryptographic Key Management</i> | <i>11</i> |
| 2.8 | <i>Self-Tests</i> | <i>12</i> |
| 2.8.1 | <i>Power-On Self-Tests.....</i> | <i>12</i> |
| 2.8.2 | <i>Conditional Self-Tests</i> | <i>13</i> |
| 2.9 | <i>Mitigation of Other Attacks</i> | <i>13</i> |
| 3 | Guidance and Secure Operation | 14 |
| 3.1 | <i>Crypto Officer Guidance</i> | <i>14</i> |
| 3.2 | <i>User Guidance</i> | <i>14</i> |

List of Tables

| | |
|--|----|
| Table 1 – Acronyms and Terms..... | 5 |
| Table 2 – Validation Level by DTR Section | 8 |
| Table 3 – Algorithm Certificates | 9 |
| Table 4 – Logical Interface / Physical Interface Mapping | 9 |
| Table 5 – Operator Services and Descriptions | 11 |
| Table 6 – Module Keys/CSP | 12 |

List of Figures

| | |
|---|---|
| Figure 1 – Physical Boundary (Top) | 6 |
| Figure 2 – Physical Boundary (Bottom) | 7 |
| Figure 3 – Block Diagram | 8 |

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic module to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) runs the FIPS 140 program. The CMVP accredits independent testing labs to perform FIPS 140 testing; the CMVP also validates test reports for all modules pursuing FIPS 140 validation. *Validation* is the term given to a module 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 VMAX 6 Gb/s SAS I/O Module with Encryption solution from Dell 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.

Dell EMC's VMAX 6 Gb/s SAS I/O Module with Encryption line card may also be referred to as the "module" in this document.

1.3 External Resources

The Dell EMC website (<http://www.dell.com>) contains information on the full line of products from Dell EMC, including a detailed overview of the VMAX 6 Gb/s SAS I/O Module with Encryption solution. The Cryptographic Module Validation Program website contains links to the FIPS 140-2 certificate and Dell 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 |
| CSE | Communications Security Establishment |
| CSP | Critical Security Parameter |
| DEK | Data Encryption Key |
| DTR | Derived Testing Requirement |
| FIPS | Federal Information Processing Standard |
| GPC | General Purpose Computer |
| GPOS | General Purpose Operating System |
| I/O | Input/Output |
| KAT | Known Answer Test |
| KEK | Key Encryption Key |
| NIST | National Institute of Standards and Technology |
| NVRAM | Non-Volatile Random Access Memory |
| OSC | Oscillator |
| SAS | Serial Attached SCSI |
| SCSI | Small Computer System Interface |
| XTS | Xor-Encrypt-Xor-based Tweaked CodeBook with CipherText Stealing |

Table 1 – Acronyms and Terms

2 VMAX 6 Gb/s SAS I/O Module with Encryption

2.1 Product Overview

Dell EMC Data at Rest Encryption provides hardware-based, on-array, back-end encryption for Dell 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.

Dell EMC 6Gb/s SAS 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 Dell EMC's VMAX 6 Gb/s SAS I/O Module with Encryption, Part Number 303-161-101B-05 running firmware version 2.13.39.00 or 2.13.43.00. 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 2 – Physical Boundary below.



Figure 1 – Physical Boundary (Top)



Figure 2 – Physical Boundary (Bottom)

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.

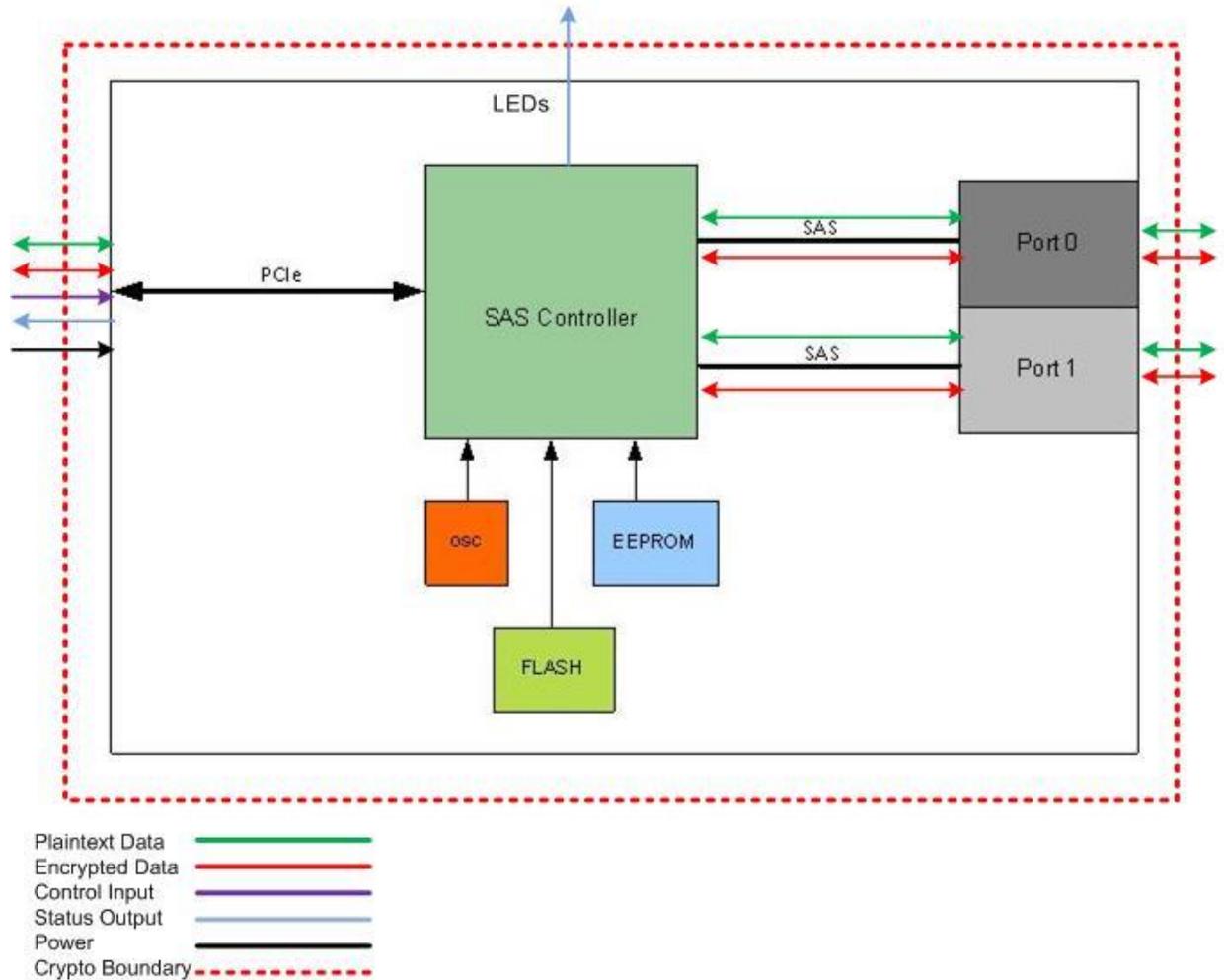


Figure 3 – Block Diagram

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 |
| 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 | CAVP Certificate |
|----------------|---|------------------|
| Symmetric Key | AES 256-bit in XTS mode AES 256-bit key wrap (unwrap only) | 3255 |
| Keyed Hash | HMAC-SHA512 | 2053 |
| Message Digest | SHA-512 | 2692 |

Table 3 – Algorithm Certificates

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 Mini-SAS HD |
| Data Output | PCI Express Mini-SAS HD |
| Control Input | PCI Express |
| Status Output | PCI Express Power / Service LED (1 per module) Green: indicates operational Amber: marking indicator; turns Green when booted with host SAS Link LEDs (1 per port, 2 per module) Green: indicates 1.5G or 3G active connection Blue: indicates 6G active connection Blue blinking: port marking – port needs service |
| 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 DEK | 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 | Mini-SAS HD PCI Express | KEK | Crypto Officer User |
| Encrypt | Encrypts data using AES | Initiate AES encryption/ data encrypted | Mini-SAS HD PCI Express | DEK | Crypto Officer User |
| Keyed Hash (HMAC) | Firmware authentication / integrity | On load / pass/fail | PCI Express | HMAC Key | Crypto Officer User |
| Message digest (SHS) | Message digest functions / support firmware integrity | Initiate message digest / data hashed | PCI Express | None | 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 |
| Decommission | Revert configuration to default | Run decommission / 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. Note that even though no claim is made for the module to meet the FIPS 140-2 Level 2 for this section, the cryptographic module consists of production-grade components¹ in a strong metal cover protected with tamper evidence labels installed at time of manufacture. The physical boundary of the cryptographic module is the same as the physical boundary depicted in Figure 2 – 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 Location / Method | Use | Input Method / Output | Generated | Zeroized | Access |
|----------------------------|---------------------------|---------------------------|--|--|------------------|------------------------|
| KEK (AES key wrapping key) | Flash in Plaintext | 256-bit key to unwrap DEK | Electronic, plaintext via host platform / No | Generated at host platform install time outside the module via FIPS-approved library | Yes Decommission | CO RWD User R |

¹ 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.

| Keys and CSPs | Storage Location / Method | Use | Input Method / Output | Generated | Zeroized | Access |
|---------------|---------------------------|---|--|--|---|--------------------------|
| DEK (AES) | DRAM in Plaintext | 256-bit key to data Encryption / Decryption | Electronic, encrypted with KEK / No | Generated outside the module at time of install or replacement of disk drives outside the module via FIPS-approved library | Yes Power Off Reset Decommission | CO RWD User RW |
| HMAC Key | EEPROM in Plaintext | 512-bit key used in firmware integrity test | Electronic, plaintext via host platform / No | Generated at host platform install time outside the module via FIPS-approved library | No | CO RW User None |

R = Read W = Write D = Delete

Table 6 – Module Keys/CSP

The DEK is entered encrypted electronically from the host platform into the module. The DEK is wrapped with the KEK. The module then uses its internally stored copy of the host platform-generated KEK to decrypt the DEK using AES (Cert. #3255) in KW mode. This functionality has been tested and 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 #3255).

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. Upon failure of the self-tests the module will halt and become inoperable.

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 XTS Encrypt KAT
- AES XTS Decrypt KAT

- AES Key Unwrap KAT
- HMAC-SHA512 KAT
- SHA512 KAT
- Firmware integrity via CRC-32 and HMAC-SHA512

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 power-up self-tests can also be performed by power-cycling 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.

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 VMAX 6 Gb/s SAS I/O Module with Encryption, Part Number 303-161-101B-05.
- Verify that the firmware version is 2.13.39.00 or 2.13.43.00
- 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.

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
