EMC Corporation

Unity 12 Gb/s SAS I/O Module with Encryption

Firmware Version: 03.90

Hardware Version:

Storage Processor SAS Module with P/N 362-000-332, P/N 363-000-071, P/N 363-000-084, and P/N 364-000-096.

Pluggable I/O SAS Module with P/N 362-000-333, P/N 363-000-071, P/N 363-000-084, and P/N 364-000-063.

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.8

Prepared for:

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

Phone: +1 806 438 3622
www.emc.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

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Unity 12 Gb/s SAS[1,2] I/O[3] Module with Encryption from EMC Corporation. This Security Policy describes how the EMC Unity 12 Gb/s SAS I/O Module with Encryption meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.[4] 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 (CSE) Cryptographic Module Validation Program (CMVP) website at http://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. The EMC Unity 12 Gb/s SAS I/O Module with Encryption is also referred to in this document as 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 (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

[1] SAS – Serial Attached SCSI
[2] SCSI – Small Computer System Interface
[3] I/O – Input/Output
[4] U.S. – United States of America

Package is proprietary to EMC and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact EMC.

2. Unity 12 Gb/s SAS I/O Module with Encryption

2.1 Overview

The EMC Unity 12 Gb/s SAS I/O Module with Encryption is a high-density SAS controller chipset executing specialized firmware that provides Data At Rest Encryption (D@RE) for EMC Unity 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 EMC Unity 12 Gb/s SAS I/O Module with Encryption is an optimized solution for native SAS HBA[5] applications.

The Unity 12 Gb/s SAS I/O Module with Encryption implements 256-bit AES[6]-XTS[7,8,9] encryption/decryption to encrypt and decrypt data as it is being written to or read from a SAS drive.

The module is available in two variants. The Storage Processor SAS Module variant is embedded on the printed circuit board (PCB) of the Storage Processor (SP). The Storage Processor SAS Module consists of:

- SAS Controller (P/N 362-000-332)
- Flash Memory (P/N 363-000-071)
- Serial EEPROM[10] (P/N 363-000-084)
- 75 MHz Clock (P/N 364-000-096)

The Pluggable I/O SAS Module variant is embedded on the PCB of a pluggable I/O Module. The Pluggable I/O SAS Module consists of:

- SAS Controller (P/N 362-000-333)
- Flash Memory (P/N 363-000-071)
- Serial EEPROM (P/N 363-000-084)
- 75 MHz Clock (P/N 364-000-063)

The EMC Unity 12 Gb/s SAS I/O Module with Encryption is validated at the FIPS 140-2 Section levels shown in Table I below.

[5] HBA – Host Bus Adapter
[6] AES – Advanced Encryption Standard
[7] XTS – XEX-Based Tweaked-Codebook Mode with Ciphertext Stealing
[8] XEX – XOR-Encrypt-XOR
[9] XOR – Exclusive OR
[10] EEPROM – Electrically Erasable Programmable Read-Only Memory

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 Unity 12 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.

The cryptographic boundary of the EMC Unity 12 Gb/s SAS I/O Module with Encryption includes the following components:

- SAS controller:
  - Within Storage Processor SAS Module – P/N 362-000-332 Eight-lane SAS controller that is configured to provide two quad-lane SAS interfaces. It incorporates FIPS 197 validated, IEEE[13] 1619-compliant XTS-AES encryption engines.
  - Within Pluggable I/O SAS Module – P/N 362-000-333 Sixteen-lane SAS controller that can be configured to provide four quad-lane SAS interfaces or two eight-lane SAS interfaces. It incorporates FIPS 197 validated, IEEE 1619-compliant XTS-AES encryption engines.
- Flash Memory (P/N 363-000-071)
- Serial EEPROM (P/N 363-000-084)
- 75 MHz reference clock:
  - Within Storage Processor SAS Module – P/N 364-000-096
  - Within Pluggable I/O SAS Module – P/N 364-000-063

[11] N/A – Not Applicable
[12] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[13] IEEE – Institute of Electrical and Electronics Engineers

The cryptographic module includes 16MB[14] of Flash memory for firmware storage and error logging and 4KB[15] SEEPROM[16] 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[17] to interface with the host device. Figure 1 below presents the block diagram of the module.

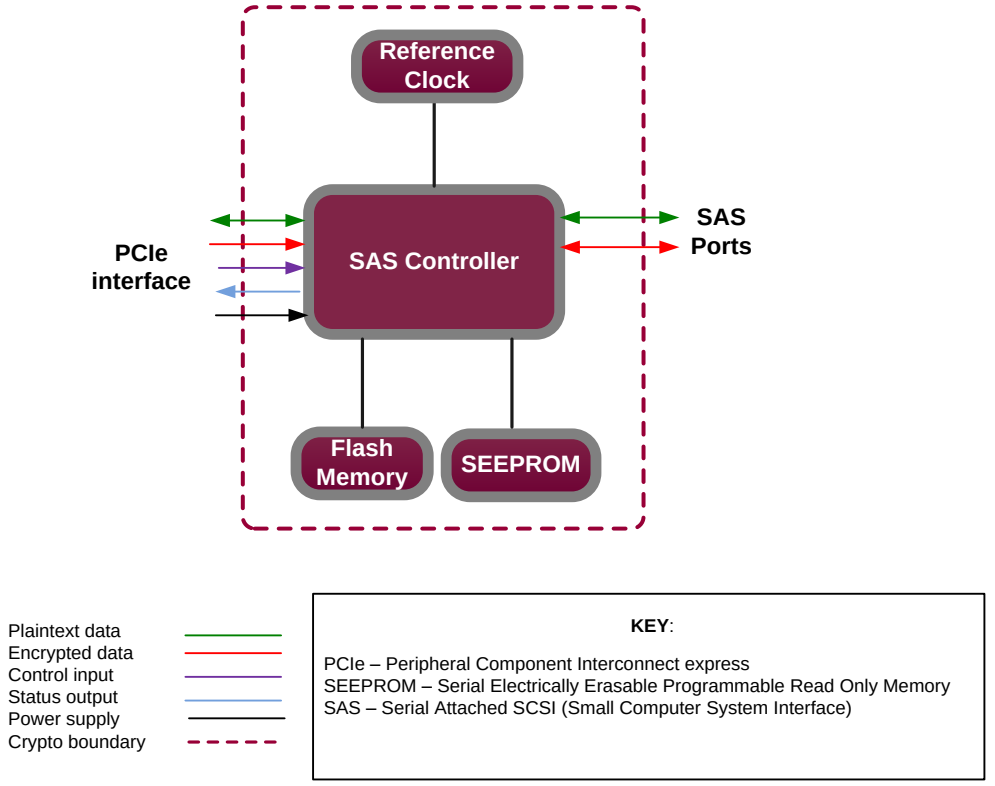

Figure 1 – Unity 12 Gb/s SAS I/O Module with Encryption Block Diagram

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

Table 2 – FIPS-Approved algorithm implementations

Algorithm	Certificate Number
256-bit AES ECB[18] encryption/decryption	3586
256-bit AES-XTS encryption/decryption[19]	3598

[14] MB – Megabyte
[15] KB – Kilobyte
[16] SEEPROM – Serial Electrically Erasable Programmable Read Only Memory
[17] PCIe – Peripheral Component Interconnect Express
[18] ECB – Electronic Code Book
[19] In compliance with IG A.9, the module performs the check of Key 1 ≠ Key 2 prior to using keys for AES-XTS encryption/decryption.

Algorithm	Certificate Number
256-bit AES Key Wrap[20]	3598
HMAC[21] with SHA[22]-512[23]	2296[24]
SHA 512[23]	2961[25]

2.3 Module Interfaces

The module's design separates the physical connections 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 EMC Unity 12 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	Storage Processor SAS Module: 1 Pluggable I/O SAS Module: 1	Data Input Data Output Control Input Status Output Power Input
SAS interface	Storage Processor SAS Module: 2 x 4 (8 x 12G[26]) ports Pluggable I/O SAS Module: 4 x 4 (16 x 12G) ports or 2 x 8 (16 x 12G) ports	Data Input Data Output

[20] 256-bit AES Key Wrap is used to unwrap the KEK and DEK when each key enters the module.
[21] HMAC – (Keyed) Hash Messaged Authentication Code
[22] SHA – Secure Hash Algorithm
[23] The module uses HMAC SHA 512 only to perform the integrity test during power-up. The HMAC and SHA algorithms are not available once the module is operational.
[24] Please note that HMAC SHA-1, HMAC SHA-224, HMAC SHA-256 and HMAC SHA-384 listed on certificate #2296 are not accessible.
[25] Please note that SHA-1, SHA-224, SHA-256 and SHA-384 listed on certificate #2961 are not accessible.
[26] G – Gigabit

2.4 Roles and Services

There are two roles in the module that operators may assume: a Crypto Officer (CO) role and a 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 – Crypto Officer and User Services

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Configure parameters	✓	-	Configuring the module's configuration parameters	Command	Status output	None
Show Status	-	✓	Show the module's status	Command	Status output	None
Load KEK[27]	✓	-	Load KEK	Command	Status output	KEK – W KEK-KEK[28] – R/X
Zeroize KEK	✓	-	Zeroize KEK Zeroize KEK-KEK	Command	Status output	KEK – W KEK-KEK – W
Load DEK[29]	✓	-	Load DEK	Command	Status output	DEK – W KEK – R/X
Zeroize DEK	✓	-	Zeroize DEK	Command	Status output	DEK – W
Encryption/ Decryption I/Os	-	✓	Perform encryption/decryption of I/Os over SAS interface	Command	Status output	DEK – R/X
Power down	✓	-	Power down the module. KEK and DEK are zeroized as part of the power down process.	Command	Status output	KEK – W DEK – W

[27] KEK – Key Encryption Key
[28] KEK-KEK – Key Encryption Key-Key Encryption Key
[29] DEK – Data Encryption Key

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Perform self-tests	✓	-	Invoke self-tests via a reboot or power cycling	Reboot or power cycling	Status output	None

2.5 Physical Security

The EMC Unity 12 Gb/s SAS I/O Module with Encryption is a multiple-chip embedded cryptographic module. The module consists of production-grade components that include standard passivation techniques. Figure 2 and Figure 3 below identifies all components within the cryptographic boundary along with module interfaces of the Pluggable I/O SAS Module. Figure 4 identifies all components within the cryptographic boundary along with module interfaces of the Storage Processor SAS Module.

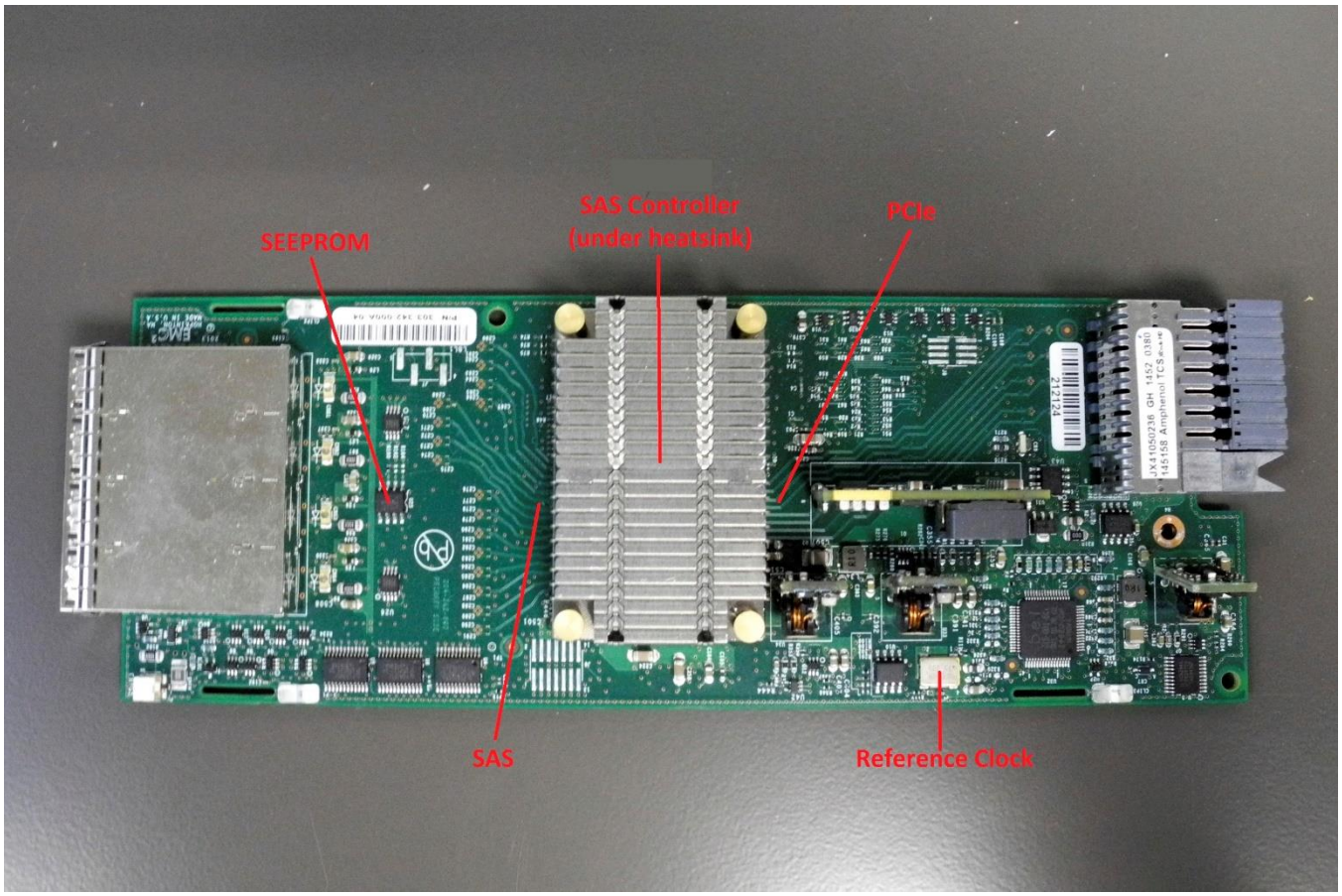

Figure 2 – Top view of Pluggable I/O SAS Module

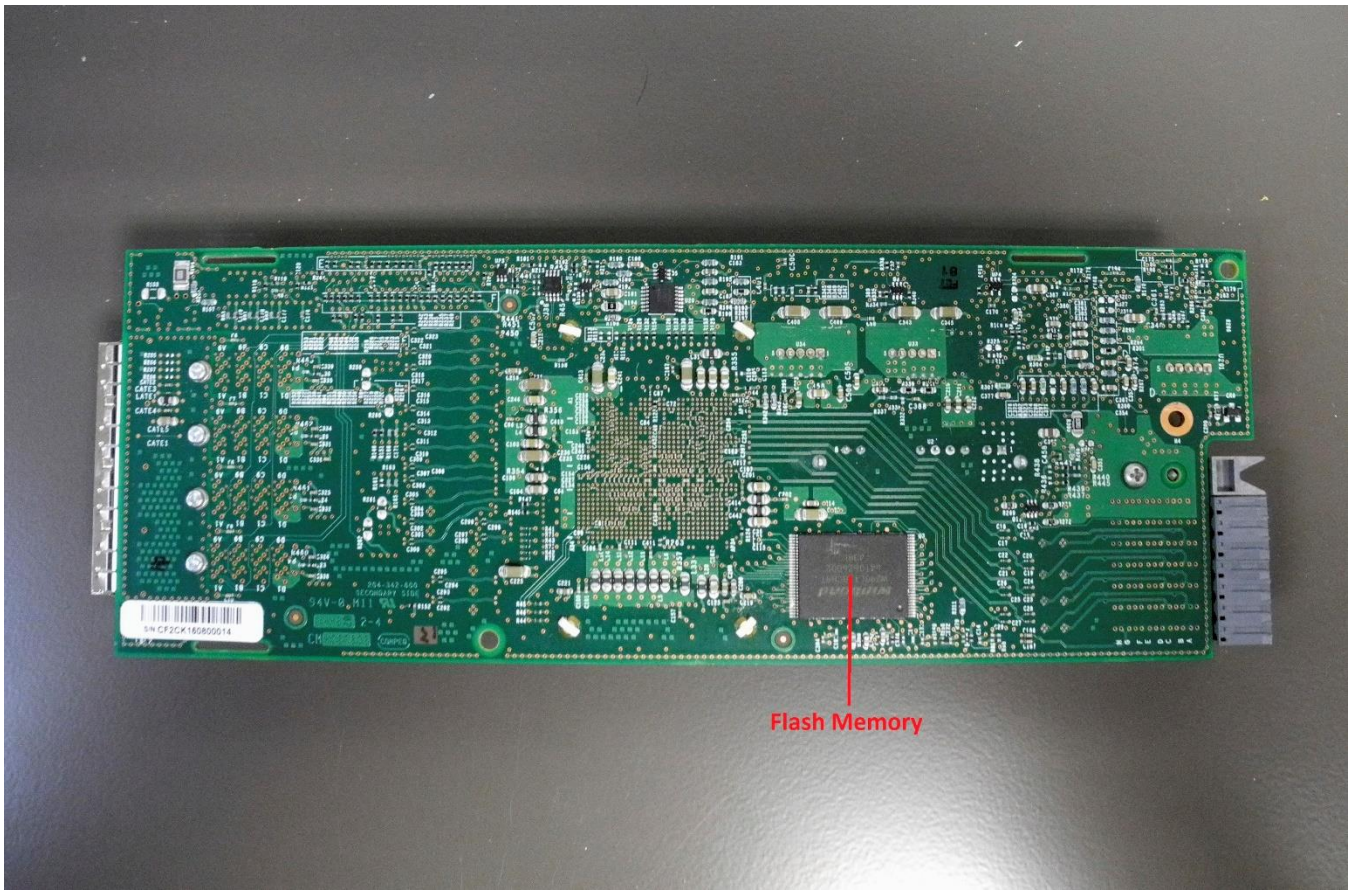

Figure 3 – Bottom view of Pluggable I/O SAS Module

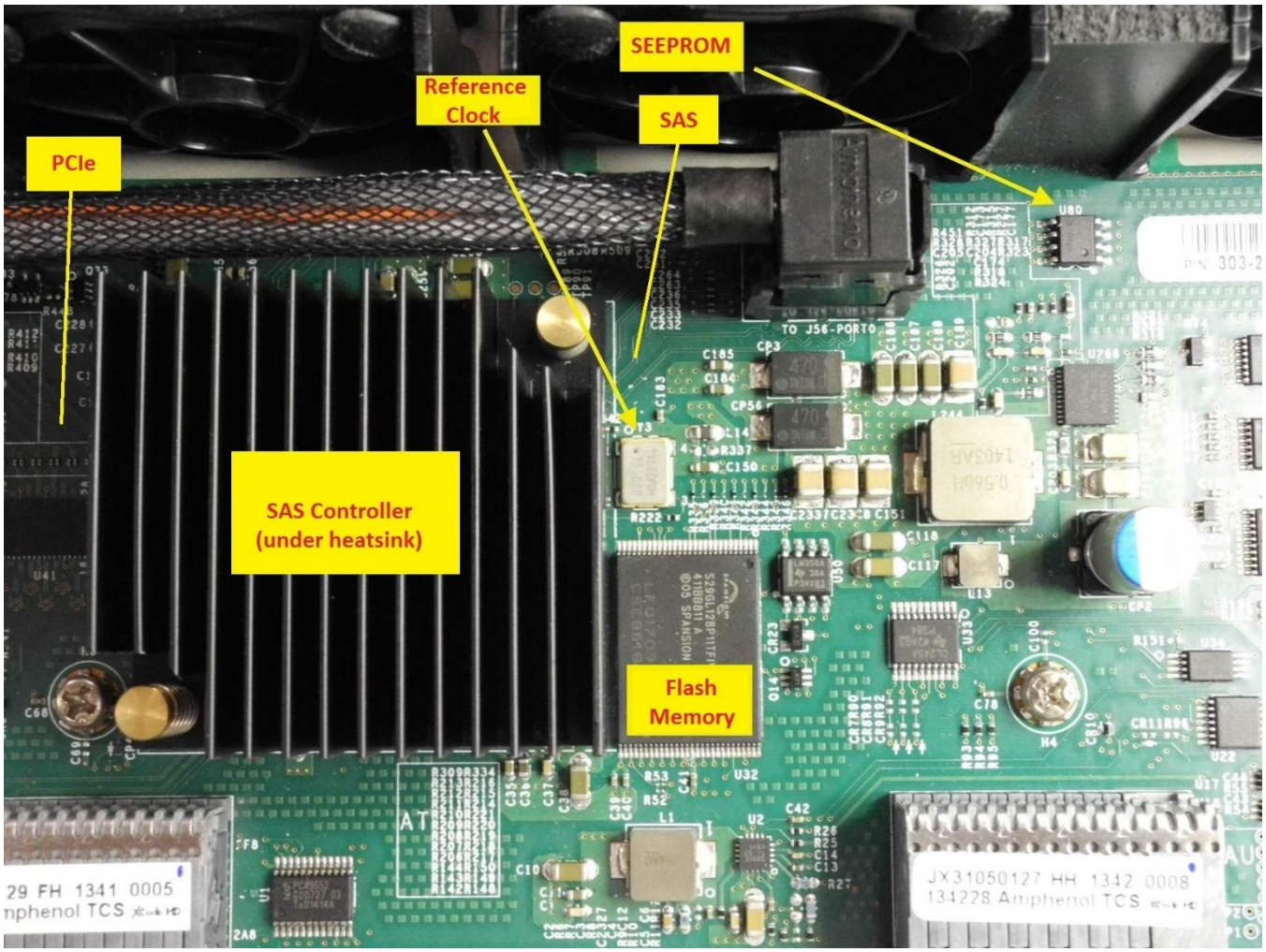

Figure 4 – Top view of Storage Processor SAS Module

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 v03.90. The module only loads and executes firmware that successfully passes the HMAC SHA-512 verification method.

2.7 Cryptographic Key Management

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

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

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
DEK	256-bit AES-XTS	Entered electronically in ciphertext	Never exits the module	Stored in plaintext within the SAS controller	Zeroize DEK service and Power down service	Encryption and Decryption of data
KEK	256-bit AES ECB Unwrap Key	Entered electronically in ciphertext	Never exits the module	Stored in plaintext within the SAS controller	Zeroize KEK service and Power down service	Decryption of DEK
KEK-KEK	256-bit AES ECB Unwrap Key	Loaded electronically in plaintext as part of module initial configuration.	Never exits the module	Stored in plaintext in flash memory	Zeroize KEK service	Decryption of KEK

The KEK-KEK is generated outside the module and automatically loaded into the module in plaintext form during initial configuration of the module into the approved mode. Configuring the module for FIPS-approved mode is detailed in Section 3.

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 KEK-KEK to decrypt (unwrap) the KEK using an AES (Cert. #3598) key unwrapping algorithm.

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 an AES (Cert. #3598) key unwrapping algorithm.

2.8 EMI / EMC

EMC Unity 12 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. These power-up self-tests can be initiated on-demand at any time by rebooting or power cycling the module. The following sections list self-tests performed by the module, their expected error status, and error resolutions.

2.9.1 Power-Up Self-Tests

During power-up, once the module is initialized, EMC Unity 12 Gb/s SAS I/O Module with Encryption performs the following power-on self-tests:

- Main module firmware integrity test – HMAC SHA-512[30]
- Known Answer Tests (KATs)
  - AES-ECB encrypt KAT
  - AES-ECB decrypt KAT
  - AES-XTS encrypt KAT
  - AES-XTS decrypt KAT

After powering–on the module, the power-up self-tests will execute automatically with no intervention from the operator. While the module is executing the self-tests all data output interfaces are inhibited. When the power-up self-tests complete successfully, then the module is in a fully operational state. If the module fails an integrity test on main firmware, or any power-up self-test, then a critical error occurs. The error is logged in a register internally and outputted 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 EMC.

2.9.2 Conditional Self-Tests

The module does not perform any conditional self-tests.

2.9.3 Critical Functions Self-Tests

The EMC Unity 12 Gb/s SAS I/O Module with Encryption performs the following critical functional self-tests at power-on or reboot of the module:

[30] HMAC SHA-512 is used by the module only to perform the main firmware integrity test and ILA integrity test. These functions are not available for any other use. The module's integrity check using HMAC-SHA-512 also serves as the known answer test for the HMAC algorithm.

- ILA[31] integrity test – HMAC SHA-512
- AES key unwrap KAT

While the module is executing the self-tests all data output interfaces are inhibited. When the critical functions self-tests complete successfully, then the module is in a fully operational state. If the module fails either of the critical functions tests, 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 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.

[31] ILA – Image Loader Agent

3. Secure Operation

The Unity 12 Gb/s SAS I/O Module with Encryption meets Level 1 requirements for FIPS 140-2. The sections below describe how to place the module in the FIPS-approved mode of operation.

3.1 Initial Setup

The module is available pre-installed on an EMC Unity 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 module can be managed through the following underlying host device'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 module over the PCIe bus.

During initial setup, the CO must perform the following steps to configure the module:

- The CO shall validate the module firmware version number 03.90 by executing the following service command: `svc_diag --state spinfo`. For more information, please refer to the *Unity Family Service Commands Technical Notes*[32] document.
- The CO shall install the Unity license file that includes the Data at Rest Encryption feature on the host device. This process will configure the KEK-KEK. For more information, please refer to the *Unity Family Security Configuration Guide*[32] and *Unity: Data at Rest Encryption White Paper*[32].
- The CO shall verify that the Encryption mode has changed from "Unencrypted" to "Controller Based Encryption" via Unisphere GUI or Unisphere CLI. To view the status via Unisphere GUI, navigate to **Settings** > **Management** > **Encryption**. To view the status via Unisphere CLI, use `/prot/encrypt show -detail` command and for more information please refer to the *Unity Family Unisphere CLI User Guide*[32].
- The CO shall reboot the system. Once the module is powered on and all power-up self-tests have completed successfully, the module is operating in FIPS-Approved mode.

Once all steps are completed, the module is initialized.

3.2 Secure Management

The CO is responsible for ensuring that the module is operating correctly.

[32] This document is available via EMC Support website

3.2.1 Management

When configured according to the guidance stated in this Security Policy, the module runs in a FIPS-Approved mode of operation. The CO shall manage the module via the host device interfaces, Unisphere CLI and Unisphere GUI.

3.2.2 Monitoring Status

The CO should monitor the module status regularly. The CO can verify that the module is operating in the approved mode by ensuring that the Encryption mode reports “Controller Based Encryption”. Please refer to Section 3.1 for the details to verify the Encryption mode. When configured according to the guidance stated in this Security Policy, the module operates in the FIPS-Approved mode. The module when operational is always in the FIPS-Approved mode.

The current status of the module which is output over the PCIe interface can be monitored via the Unisphere CLI and Unisphere GUI interfaces. The encryption mode of the array is also reported on the Unisphere CLI and Unisphere GUI host device interfaces.

Detailed instructions to monitor and troubleshoot the systems are provided via EMC Support at www.emc.com[33].

3.2.3 Zeroization

A CO can perform the Zeroize DEK service or Power down service to zeroize the DEK. The KEK is zeroized when a CO performs the Zeroize KEK service or Power down service. CO zeroizes the KEK-KEK by performing the Zeroize KEK service. Once keys are zeroized they are no longer available to the module.

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 according to the instructions in this Security Policy, the module does not support a non-FIPS-Approved mode of operation.

[33] A username and password are required to access EMC support information.

4. Acronyms

Table 6 below provides definitions for the acronyms used in this document.

Table 6 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSE	Communications Security Establishment
CSP	Critical Security Parameter
D@RE	Data At Rest Encryption
DEK	Data Encryption Key
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
HMAC	(Keyed) Hash Messaged Authentication Code
ILA	Image Loader Agent
I/O	Input/Output
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
KAT	Known Answer Test
KEK	Key Encryption Key
KEK-KEK	Key Encryption Key-Key Encryption Key
MA	Massachusetts
KB	Kilobyte
MB	Megabyte
MHz	Megahertz
N/A	Not Applicable

Acronym	Definition
NIST	National Institute of Standards and Technology
OS	Operating System
PCB	Printed Circuit Board
PCIe	Peripheral Component Interconnect Express
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SEEPROM	Serial Electrically Erasable Programmable Read Only Encryption
SSP	Serial SCSI Protocol
VA	Virginia
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