

**Mercury Systems *ASURRE-Stor*[™] SSD
Non-Proprietary FIPS 140-2 Security Policy**

Mercury Systems ASURRE-Stor[™] SSD

ASD256/512, and ADR256/512

Solid State Self-Encrypting Drives

Non-Proprietary FIPS 140-2 Security Policy

(Firmware 1.5.0 and Hardware Revision 3.0)

Document Revision: 1.5.0.00

Date: February 16, 2017

Table of Contents

References	4
1 Overview	6
1.1 Product Description	6
1.2 Versions, Configurations and FIPS 140-2 Modes of Operation	8
1.3 Cryptographic Physical Boundary and Module Ports	11
2 Cryptographic Functionality	13
2.1 Critical Security Parameters	14
3 Roles, Authentication, and Services	15
3.1 Roles	15
3.2 Authentication	16
3.3 Services	18
4 Self-test	21
5 Physical Security	22
6 Electromagnetic Interference and Compatibility (EMI/EMC)	22
7 Mitigation of Other Attacks Policy	22
8 Security Guidance	23
9 Change log	25

List of Figures

Figure 1: Views of the Module	6
Figure 2: ATA Password Functionality (Refer to page 22 of the ATA7 Specification)	9
Figure 3: Ports on the Module	11
Figure 4: Module Block Diagram	12
Figure 5: Screw Head in Daylight	23
Figure 6: Screw Head in UV Light	23
Figure 7: After Strong UV Exposure	23
Figure 8: Holographic Label	24
Figure 9: Text on Holographic Label	24

List of Tables

Table 1: References	4
Table 2: Proprietary Configuration, Setup, and Reference, Documents Available to Customers	4
Table 3: Acronyms and Definitions	5
Table 4: Hardware Part Number and Version Summary	7
Table 5: Security Level of Security Requirements	7
Table 6: Non-Approved Modes of Operation.....	8
Table 7: FIPS 140-2 Approved Modes of Operation and Authentication Source.....	8
Table 8: Module Port Summary	11
Table 9: LED Indicator Port.....	12
Table 10: Approved Cryptographic Functions	13
Table 11: Non-Approved but Allowed Cryptographic Function	13
Table 12: Private CSP Values.....	14
Table 13: Public Key Value	14
Table 14: Authentication Strengths for User Role in all Six (6) FIPS modes.....	17
Table 15: Authentication Strengths for Crypto Officer Role.....	17
Table 16: Services and Authentication by Approved Mode and Role.....	19
Table 17: CSP and Public Key Access within Services.....	20
Table 18: Self-tests (NA = Not applicable, VA = Vendor Affirmed).....	21
Table 19: Conditional Tests	21
Table 20: Password Strengths in Bits.....	23

References

Acronym	Full Specification Name
[FIPS140-2]	NIST, <i>Security Requirements for Cryptographic Modules</i> , May 25, 2001
[SP800-131A]	<i>Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths</i> , January 2011
[FIPS197]	NIST, <i>Advanced Encryption Standard (AES)</i> , FIPS Publication 197, November 26, 2001
[FIPS 186-4]	NIST, <i>Digital Signature Standard (DSS)</i> , FIPS Publication 186-4, July 2013
[FIPS 180-4]	NIST, <i>Secure Hash Standard</i> , FIPS Publication 180-4, March 2012
[SP 800-38E]	NIST Special Publication 800-38E, <i>Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices</i> , January 2010
[SP 800-90A]	NIST Special Publication 800-90A, <i>Recommendation for Random Number Generation Using Deterministic Random Bit Generators</i> , January 2012
[IG]	NIST, Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, last updated 25 July 2013
ATA Specification ATA7 Specification	This specification defines industry standard storage commands used by the module. The document is available on the T13.org website. D1532v1r4b-AT_Attachment_with_Packet_Interface_-_7_Volume_1.pdf

Table 1: References

Document name	Description
MDU User's Guide (mduUsersGuide.pdf)	This manual describes the MDU utility. Chapters in the document include screen shots and simple to follow step-by-step instructions to guide the Crypto Officer through the process of performing the initial secure configuration of the module.
Programmer's Guide or SSD Programmer's Guide (ssdProgrammersGuide.pdf)	This document provides detailed register-level information describing how to use commands supported by the module that allow filling of keys and configuring security features. Designers intending to create their own version of the Mercury Systems MDU utility would use this document as a reference manual.
SSD User's Hardware Setup Guide (ssdUsersHardwareSetupGuide.pdf)	This document is intended for the novice user of secure SSDs in defense applications. It describes how to connect the module to a host system and how to connect external switches to the SATA Power Segment Port to add external Secure Erase Trigger capability. The document also contains basic information describing some of the key management features of the module.

Table 2: Proprietary Configuration, Setup, and Reference, Documents Available to Customers

Acronym	Definition
AES	Advanced Encryption Standard Algorithm (FIPS 197. Also refer to NIST SP 800-38A and SP 800-38E.
Armor™ Processor	This is the Mercury Systems marketing name for the combination of the module firmware and module hardware.
ATA Specification ATA7 Specification	An industry standard for ATA based storage devices. The document defines the functional behavior, commands, and software interface for devices that implement the ATA interface. The specification is available on the T13.org website.
ATA commands SATA commands	Storage commands defined by the industry ATA standard. Volume 1 of the specification has the command descriptions. D1532v1r4b-AT_Attachment_with_Packet_Interface_-_7_Volume_1.pdf
CSP	Critical Security Parameter, see [FIPS 140-2]
CMVP	Cryptographic Module Validation Program
COMSEC	Abbreviation for Communications Security. The methods and disciplines needed to ensure communications security.
DRBG	Deterministic Random Bit Generator (SP800-90A)
ECDSA	Elliptic Curve Digital Signature Algorithm; specified in ANS X9.62. FIPS PUB 186-4
Fast Clear	For Defense SSDs, Fast Clear is an operation that erases the NAND media using the NAND manufacturers ERASE operation. In addition, the encryption key and potentially other CSP are destroyed. Which CSP is destroyed varies by manufacturer.
HMAC	Keyed-Hash Message Authentication Code
IDENTIFY DEVICE COMMAND	IDENTIFY DEVICE is an industry standard ATA command used by host systems to determine features supported by an attached storage device. Products must support this command to be compatible with the ATA specification. Refer to the IDENTIFY DEVICE command and Table 16 of volume 1 of the ATA specification pages 115-122.
LBA	Logical Block Address. Unit of storage on a hard drive. Typically 512 bytes. Same as a sector.
LED	Light Emitting Diode
LVTTL	3.3 V Low Voltage Transistor-Transistor Logic.
Master ATA Password	Password defined by the ATA specification for use by an Administrator or Crypto Officer. The ATA specification supports a Security Mode Feature Set of two passwords, a Master ATA Password and a User ATA Password. The passwords restrict access to data stored on the device. Refer to the ATA7 specification V1 page 22.
MDU MDU Utility	Mercury Systems Drive Utility. MDU is a Windows GUI utility that allows a Crypto Officer to quickly and easily perform the initial secure configuration of the Mercury Systems FIPS 140-2 secure storage module.
Non-Volatile memory, NVM, NVRAM	Non-Volatile Memory is a memory technology that retains data across power cycles. (e.g., EEPROM, NAND Flash)
PBKDF	Password Based Key Derivation Function (SP 800-132)
RBG or RNG or NDRBG	Random Bit generator, Random Noise generator Non-Deterministic Random Noise generator.
SANITIZE or SANITIZE PROTOCOL (in reference to defense SSDs)	Sanitize is an operation that runs repeated erase and pattern over-write operations of the storage media. In addition, the encryption key and other CSP (if any) are destroyed. Exactly which CSP is destroyed varies by manufacturer.
SATA	Serial ATA. A bus interface between a host computer and a mass storage device using a serial version of the ATA specification. The specification is available from the Serial ATA International Organization.
SECTOR	Unit of storage on a hard drive. Typically 512 bytes. Same as an LBA.
SECURE ERASE or ZEROIZE	Secure Erase and Zeroize and many trademarked variations imply some sort of erase operation that destroys/erases the storage media and potentially CSP as well. Exactly what is destroyed, storage media, keys, passwords, KEKs, etc. varies greatly from one manufacturer to another.
SHA, SHS	Secure Hash Algorithm (FIPS 180-4), Secure Hash Standard
SED	Self-Encrypting Drive.
SMART or S.M.A.R.T.	SMART stands for Self-Monitoring, Analysis and Reporting Technology. As part of the ATA specification, SMART commands provide a way for vendors to implement custom commands that enhance functionality of products by allowing entry of security parameters and reporting of health parameters such as, operation logs, temperature, and errors.
SSD	Solid State Hard Drive. An SSD is a 100% solid state version of a standard mechanical hard drive. SSDs use NAND flash devices as the storage media. Standard mechanical hard drives use a rotating magnetic platter for the storage media.
SFF-8201	Specification for 2.5" Form Factor Drive Dimensions developed by the SFF Committee
TRRUST-Purge™	TRRUST-Purge™ is a Mercury Systems trademarked name for an operation that destroys the encryption key in Mercury Systems SSDs by over-writing the key value with zeros.
User ATA Password	Password defined by the ATA specification for use by a user of a storage device. See Master ATA Password above and refer to the ATA specification (ATA7) volume 1 page 22 for additional details.

Table 3: Acronyms and Definitions

1 Overview

This document defines the Non-Proprietary Security Policy for the Mercury Systems **ASURRE-Stor™** cryptographic SSD, hereafter also denoted as the *module*. The module, validated to FIPS 140-2 overall Level 2, is a multi-chip embedded module packaged in the industry standard SFF-8201 2.5" form factor. The module uses a SATA interface protocol and conforms to the ATA7 specification. The cryptographic boundary is the module enclosure.

The module is a limited operational environment under the FIPS 140-2 definitions. The module includes an authenticated signature validation function (ECDSA) to support firmware updates.

The quality of the Integrated Circuits (IC) in the module is standard, production-quality, industrial temperature range, ICs, and passive components. The components meet or exceed commercial and industrial specifications for Power, Temperature, Reliability, Shock, and Vibration. An eight (8) hour final test production screen over the -40 °C to +85 °C temperature range assures consistent product quality across production lots.

Unlike most other secure SSD products, the Mercury Systems **ASURRE-Stor™** module does not depend on a TPM device, TCG, or OPAL to implement security. Instead the **ASURRE-Stor™** module implements security using AES-256 XTS encryption and several key management techniques that are compatible with the ATA specification. These techniques provide superior and flexible solutions for mission critical defense applications and have no requirements for unencrypted shadow MBR sectors or 3rd party OPAL software.

1.1 Product Description

The Mercury Systems **ASURRE-Stor™** SSD module is a secure solid state hard drive (SSD). A hard drive is a storage device that is commonly used in computers as the primary booting device to load the Operating System or to store large amounts of data. In the simplest terms, the **ASURRE-Stor™** module is a highly secure version of an industry standard 2.5" SATA hard drive.

Four (4) capacity levels are available differentiated by model number. The cryptographic security subsystem implemented in each of the four models is identical.

The following components are non-security relevant and excluded from the requirements of FIPS 140-2:

- Enclosure Grounding Resistor
- Standard SATA connector
- Hypertronics Rugged SATA connector
- Amphenol Rugged SATA connector

The Mercury Systems **ASURRE-Stor™** SSD module implements encryption with a built-in hardware based AES-256 XTS encryption engine using a 256-bit AES key and a different 256-bit XTS key. The module supports user filled keys as well as the ability to self-generate keys. The ATA Specification limits the maximum length of Data units to 2^{16} blocks, which limits the implementation of the module XTS-AES to a maximum of 2^{16} blocks. This meets the XTS-AES Data unit limit of 2^{20} blocks per NIST SP 800-38E.

Views of the ASD512AM2R-000IF model appear below in Figure 1.



Figure 1: Views of the Module

FIPS 140-2 approved hardware part numbers and hardware versions are shown below in Table 4.

HW Part Number	Hardware Part Number Suffix Description	HW Version
ASD256AM2R-0yzIF	<p style="text-align: center;">Option fields y and z</p> <p>Option Field y: 0 = Standard product. 1 = Enclosure isolated from ground.</p> <p>Option Field z: 0= Standard Product 2 = Hypertronics Rugged SATA connector 8 = Amphenol Rugged SATA Connector</p>	3.0
ASD512AM2R-0yzIF	Same options as ASD256AM2R-0yzIF	3.0
ADR256AM2R-0yzIF	Same options as ASD256AM2R-0yzIF (This model has reduced overprovisioning)	3.0
ADR512AM2R-0yzIF	Same options as ASD256AM2R-0yzIF (This model has reduced overprovisioning)	3.0

Table 4: Hardware Part Number and Version Summary

The FIPS 140-2 security levels for the module are as follows:

Area	Description	Level
1	Module Specification	3
2	Ports and Interfaces	2
3	Roles and Services	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	3
9	Self-test	2
10	Design Assurance (Development)	3
11	Mitigation of Other Attacks	N/A
Overall		2

Table 5: Security Level of Security Requirements

1.2 Versions, Configurations and FIPS 140-2 Modes of Operation

Hardware PCB revision number:	3.0 (Accessible using the ATA IDENTIFY DEVICE command, word 134)
FIPS 140-2 approved firmware revision:	1.5.0
Number of FIPS 140-2 approved modes:	6
Number of FIPS 140-2 non-approved modes:	3
FIP 140-2 approved mode Indicator:	Accessible using the IDENTIFY DEVICE command word 135
FIPS 140-2 approved part numbers:	Refer to Table 4

FIPS 140-2 Non-Approved Modes

Table 6 lists the FIPS non-approved modes. Permanent key modes with no ATA password are non-approved because there is no authentication. The Factory Mode is a FIPS 140-2 non-approved mode and is not intended for use by customers.

FIPS 140-2 Non-Approved Modes of Operation	Authentication
Permanent Self-generated key with no ATA Password.	None
Permanent User filled key with no ATA Password.	None
Factory Mode (not intended for use by customers)	32-byte password

Table 6: Non-Approved Modes of Operation

The FIPS 140-2 Approved-Mode-Indicator

The module provides a FIPS 140-2 approved mode Indicator. The indicator is evaluated using the industry standard ATA IDENTIFY DEVICE command or with the MDU utility. In response to the IDENTIFY DEVICE command, the module returns 256 words (512 bytes) of data. The FIPS approved mode indicator is located in the Vendor Specific area at word 135. A non-zero value indicates that the module is operating in a FIPS 140-2 approved mode. A value of 0 indicates that the module is operating in a non-approved mode. Refer to the Programmer’s Guide (available from Mercury Systems) and the ATA7 specification, section 6.17.8, Table 16, pages 115-121 for specific details on the operation of the IDENTIFY DEVICE command.

The module defines multiple approved modes as a way to characterize the different authentication and key management schemes the module provides. All algorithms are tested during power-up self-test regardless of the “mode” and all algorithms may be used in the process of changing modes.

FIPS 140-2 Approved Modes

Table 7 lists the FIPS 140-2 approved modes and the source of authentication.

FIPS Mode Number	FIPS 140-2 Approved Mode Name	Authentication
1	Self-generated Permanent key with ATA Password.	Correct host system supplied password entered by User Role ^{1,2}
2	Permanent key with ATA Password.	Correct host system supplied password entered by User Role ^{1,2}
3	Session key	Correct Session key consisting of a 256-bit AES key and a 256-bit XTS key.
4	Session key with ATA Password	Correct host supplied password entered by User Role ^{1,2} and the correct Session key consisting of a 256-bit AES and a 256-bit XTS key.
5	KEK with BLACK key	Correct wrapped BLACK key consisting of a 256-bit AES key and a 256-bit XTS key
6	KEK with BLACK key and ATA Password	Correct host supplied password entered by User Role ^{1,2} and wrapped BLACK key consisting of a 256-bit AES key and a 256-bit XTS key.

Table 7: FIPS 140-2 Approved Modes of Operation and Authentication Source.

Note 1: BIOS firmware on host systems may not accept User ATA Passwords with unprintable characters and may limit password length to 8 characters.

Note 2: The module supports User ATA password lengths of up to 64 bytes.

FIPS Modes 1, 2: Self-generated Permanent or Permanent key with ATA Password.

The Self-generated Permanent and Permanent key mode with ATA Password use the User ATA Password as the authentication factor. A diagram of ATA password functionality is shown in Figure 2. Refer to the ATA7 specification for more details.

The Crypto Officer is responsible for installing the initial User ATA Password, ATA Master Password, enforcing a minimum password length as well as configuring the Authentication Penalty count. For the Permanent key with ATA Password, the Crypto Officer must configure and fill the Permanent 256-bit AES key and 256-bit XTS key values.

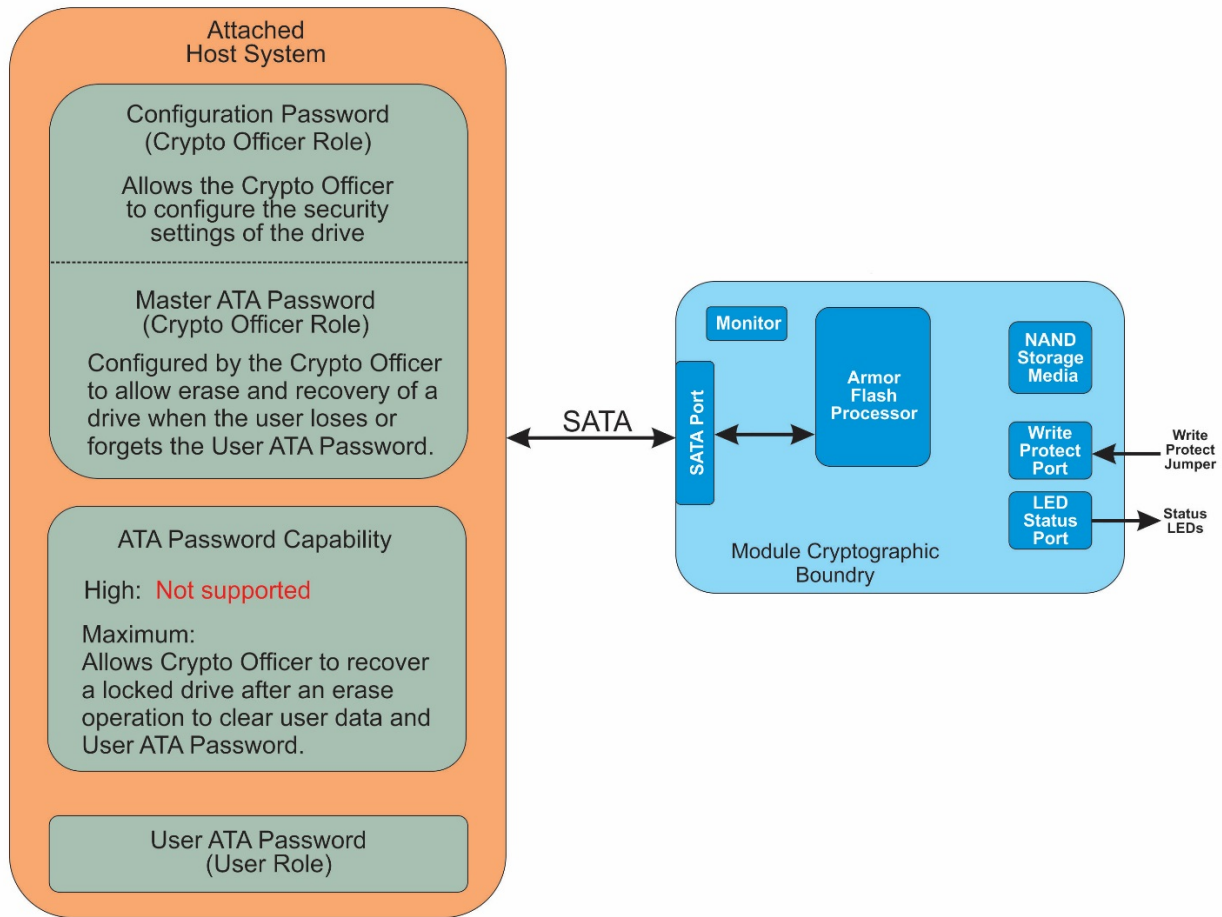


Figure 2: ATA Password Functionality (Refer to page 22 of the ATA7 Specification)

FIPS Modes 3, 4: Session key and Session key with ATA Password

The Session key mode uses a 256-bit AES key and 256-bit XTS key as the authentication factor. The Session key must be entered at each successive power-on cycle and must match the value of the Session key first entered during module configuration by the Crypto Officer. The Session key with ATA Password is identical to the Session key mode except that the module remains locked until the correct User ATA Password is entered.

FIPS Modes 5, 6: KEK with BLACK key, and KEK with BLACK key and ATA Password

The KEK with BLACK key mode uses an AES wrapped (AES-KW-256, SP 800-38F) BLACK key consisting of a 256-bit AES key and a different 256-bit XTS key as the authentication factor. The KEK with BLACK key and ATA Password mode is identical to the KEK with BLACK key mode except that the host system must supply the correct ATA Password and then the correct BLACK key value. The Crypto Officer is responsible for creating the initial ATA Password, KEK, and BLACK key values as well as installing the KEK in the module.

Module state when shipped from the factory

For simplicity of initial setup, modules ship from Mercury Systems in a Self-generated Permanent key mode with no ATA passwords. Without an ATA Password, there is no authentication, and therefore, the mode is non-approved. The Crypto Officer taking possession of factory delivered module(s) performs an initial secure configuration of the module. The initial secure configuration defines the FIPS approved mode, sets passwords, and selects other features as required by the specific end application of the module.

Using MDU to performing the initial Secure Configuration of the module

The initial secure configuration of the module is preferably accomplished by connecting the module to a PC computer using standard SATA/Power cables, launching the Mercury Systems MDU utility, and beginning configuration.

The process to complete the initial secure configuration is greatly simplified by referring to the MDU User's Guide. The MDU User's Guide provides simple, step-by-step, screen shots taken directly from the MDU utility. The document visually guides the Crypto Officer through the entire configuration process with examples of selecting the FIPS mode, setting the Configuration Password, User ATA Password, Master ATA password, zeroization features, external trigger options, failed authentication attempts penalty etc.

Using a custom program to perform the initial Secure Configuration of the module

The initial secure configuration of the module can also be accomplished by creating a custom program that interfaces with the module using standard ATA commands. The Mercury Systems SSD Programmer's Guide provides a register level description of supported commands and is invaluable in understanding how to configure options, features, key filling, FIPS modes, passwords, and Secure Erase options.

Factory Mode (non-approved mode of operation)

The module includes a Factory Mode that Mercury Systems uses during automated production assembly to set module attributes that are unknown until manufacture time, for example the model number and LBA count.

Entry to the Factory Mode is protected through use of a 256-bit password. The Factory Mode has no access to CSPs or the NAND storage media. The module does not store the Factory Password internally. Instead the module stores a hash of the Factory Password.

The Factory Mode is not intended for use by customers. Operation in the Factory Mode is a FIPS 140-2 non-approved mode of operation. Mercury Systems does not supply the Factory Password to customers.

1.3 Cryptographic Physical Boundary and Module Ports

The module conforms to the industry standard 2.5" 9.5mm thick hard drive form factor (SFF-8201). The cryptographic boundary is the entire module enclosure. Module ports include a Write Protect port, a LED Indicator port, a SATA Power Segment port and a SATA Signal Segment port as shown in Figure 3.

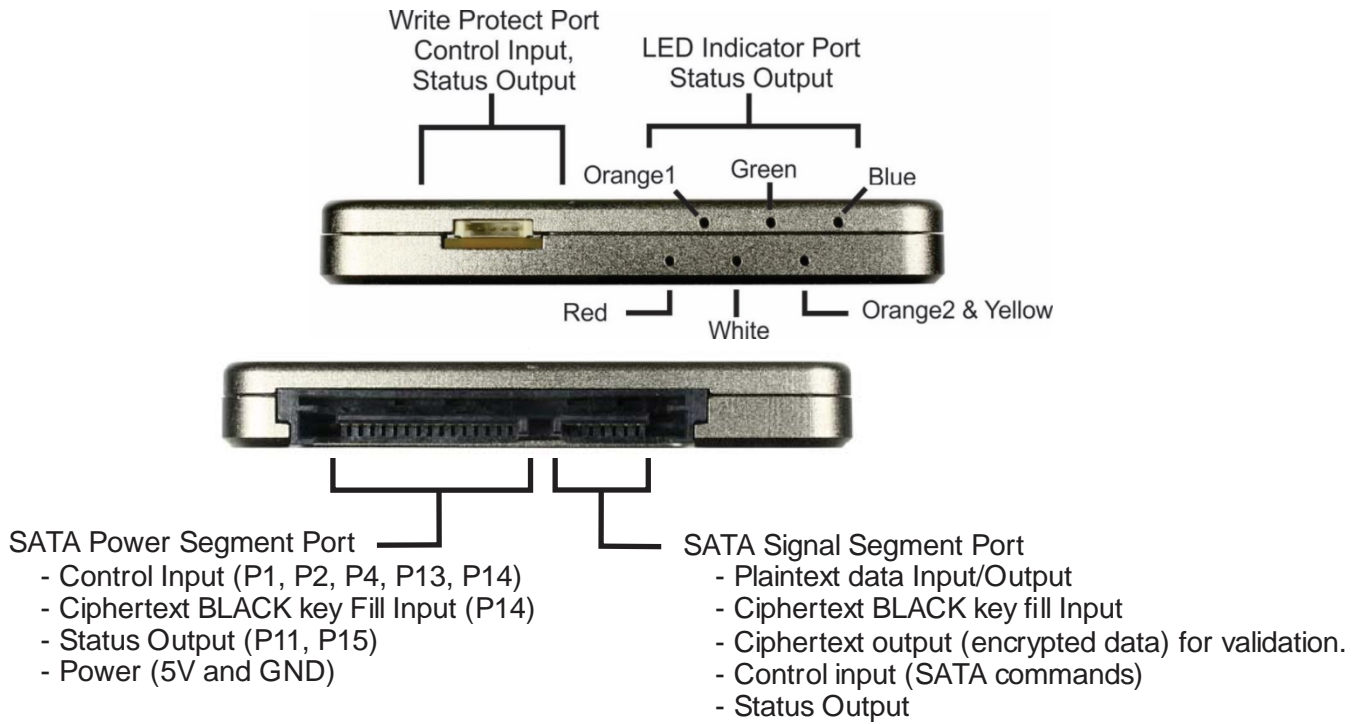


Figure 3: Ports on the Module

The module instantiates the physical SATA interface using an industry standard SATA connector. The SATA connector has two (2) segments, a SATA Signal Segment and a SATA Power Segment. The SATA Signal Segment provides Status Output, Control Input, Plaintext data Input/Output and Ciphertext Output. The Ciphertext Output capability allows validation of encrypted data in the NAND media. In the KEK/BLACK key mode, the SATA Signal Segment port allows filling of the BLACK key.

Table 8 summarizes the ports present on the module.

Module Ports	FIPS 140 Interface Type
SATA signal segment	Data Input
SATA signal segment	Data Output
SATA signal segment	Control Input
SATA signal segment	Status Output
SATA power segment	Control Input
SATA power segment	Data Input
SATA power segment	Status Output
SATA power segment, 5V and GND pins	Power
LED indicator Port	Status Output
Write Protect Connector port	Control Input and Status output

Table 8: Module Port Summary

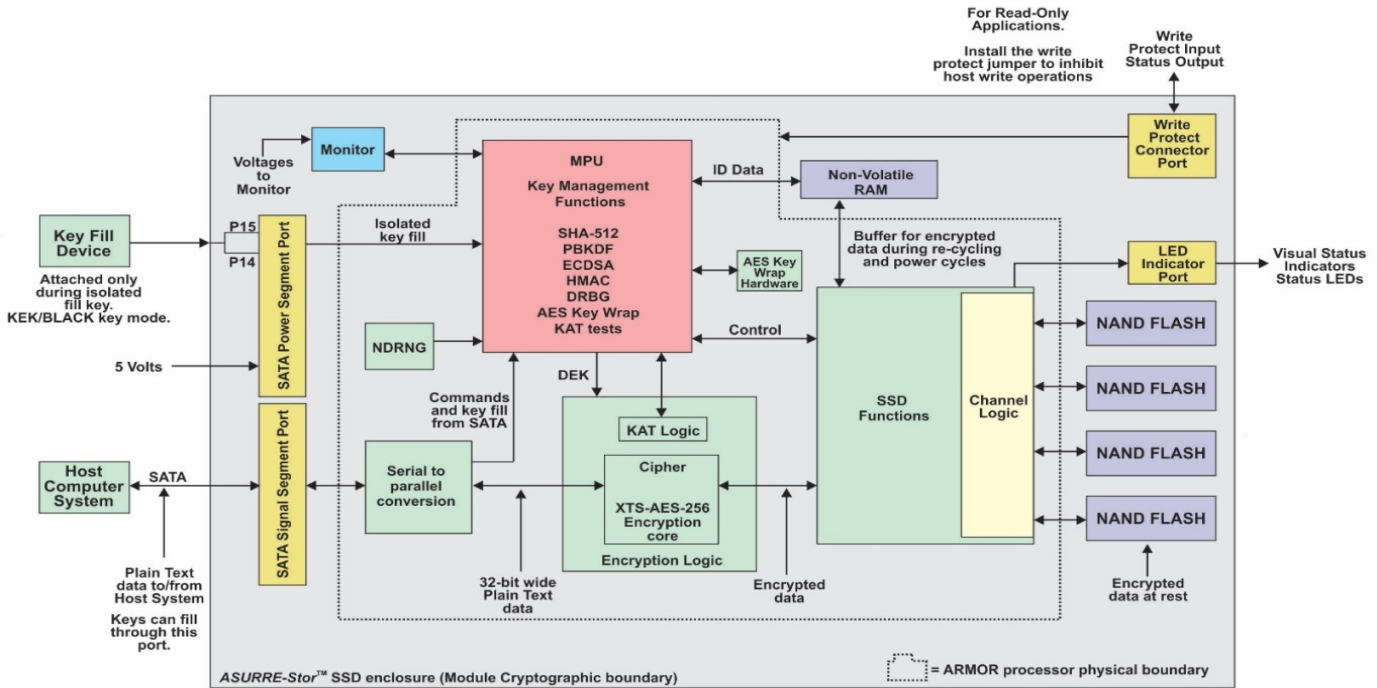


Figure 4: Module Block Diagram

As indicated in the block diagram of Figure 4, a host system interfaces with the module using the SATA Signal Segment port. The SATA Signal Segment port forms a bi-directional serial interface that implements the industry standard Serial ATA (SATA) protocol.

The Serial-to-Parallel-Conversion logic and the MPU block separates host Plaintext data from Control and Status information according to the ATA and SATA specifications. Plaintext data supplied by the attached host system flows into the Encryption Logic block and is encrypted according to the AES-256 XTS specification. During power-on cycles (and on demand using the ATA SMART_OFF_LINE_IMMEDIATE command), the MPU inhibits normal operation and runs a Known Answer Test (KAT) to validate that the hardware AES XTS encryption logic is operating properly.

The SATA Power Segment port provides 5V power, Ground and Input/Outputs. The Monitor, MPU, and SSD Functions block, control the operation of the module. Pins P14 and P15 of the SATA Power Segment port implement a two (2) wire isolated 3.3V LVTTTL (Low Voltage Transistor- Transistor Logic) serial key fill interface. The interface supports key filling from RS-232 in a Simple Key fill mode, or a DS-101 protocol as defined by COMSEC controlled key fill devices. A Write Protect Connector port provides control input to implement a Write Protect feature for the module. The write protect port also provides Voltage, Temperature, and drive state status output. A LED Indicator port includes LEDs that visibly indicate status information about the module as defined in Table 9.

LED Color	LED purpose
Blue and Green	The LEDs provide immediate visual feedback for the Crypto Officer during module configuration.
	Crypto Officer Role active – Blue LED blinks once per second. Green LED is on.
	User Role active – Green LED on continuously. Blue LED is off.
	Initializing – Blue LED blinks four (4) times per second. Green LED is off.
	Secure Erasing – Green LED blinks four (4) times per second. Blue LED is off.
	Failure – Blue LED is on continuously. Green LED is off.
	Other LED patterns – Reserved.
RED	Solid or flashing indicates module is waiting for an encryption key fill operation.
White	Indicates that the SATA interface is operating at 1.5Gb/s.
Yellow	Reserved for factory use.
Orange1	Indicates SATA activity in the module.
Orange 2	Flashes to indicate that the module is waiting for entry of a User ATA password.

Table 9: LED Indicator Port

2 Cryptographic Functionality

The module implements several approved cryptographic functions as listed in Table 10. A non-Approved but allowed cryptographic function is listed in Table 11.

Approved Cryptographic Functions (used in all modes)					
CAVP Certificate	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
2802 (as Microsemi)	AES	FIPS 197 SP 800-38A SP 800-38E	ECB, XTS	256	Data Encryption / Decryption for the NAND media
3986	AES	FIPS 197 SP 800-38A	ECB	256	Prerequisite AES ECB algorithm for AES key Wrap
3987	AES	FIPS 197 SP 800-38F	KW	256	Key Wrapping / Unwrapping
1179	DRBG	SP 800-90A	HASH SHA-512		Deterministic Random Bit Generation
883	ECDSA	FIPS 186-4		P-521	Digital Signature verification for firmware updates
2602	HMAC	FIPS 198-1	HMAC-SHA-512	512	Message authentication for the Session, key, BLACK key, and all passwords.
Vendor Affirmation	PBKDF	SP 800-132	HMAC-SHA-512 Option 2a		Keys derived from passwords, as shown in SP 800-132, may only be used in storage applications. Deriving key to wrap the Permanent and Self-generated Permanent key.
3291	SHS	FIPS 180-4	SHA-512		Message Digests

Table 10: Approved Cryptographic Functions

A hardware based non-deterministic bit generator provides the required seeding for the DRBG.

Non-Approved but Allowed Cryptographic Function	
Algorithm	Use
NDRNG Entropy Noise Source	Hardware based Random Bit Generator noise source. The noise source is used for seeding the DRBG.

Table 11: Non-Approved but Allowed Cryptographic Function

2.1 Critical Security Parameters

Module private and public CSP values are listed and described in Tables 12. Table 13 lists Public key values. Refer to Table 17 for a cross-reference of which services use individual CSP values.

CSP Name	Description
ATA Password	Up to 64-byte password passed to the module by the host. Mode 1,2: Input to PBKDF to derive the DKEK. Mode 3: Not used. Mode 4: Input to PBKDF which is compared to previously saved value for user authentication. Mode 5: Not used. Mode 6: Input to PBKDF to derive the IKEK. The ATA Password is destroyed, not retained, when power is removed.
Configuration Password	32-byte password passed to the module by the host. This password authenticates the Crypto Officer Role. Used in all modes.
DEK ³	512-bit AES-XTS-256 Data Encryption Key (DEK) used to encrypt and decrypt user data. Used in all modes. In modes 1 and 2 it is also referred to as the Permanent key. In modes 3 and 4 it is referred to as the Session Key. In modes 5 and 6 when wrapped with the DKEK it is referred to as the BLACK Key.
DKEK	256-bit AES DEK Key Encryption Key (KEK) used to Wrap/Unwrap the DEK using SP800-38F compliant KW. Modes 1, 2: Derived from the ATA Password using PBKDF. Modes 3, 4: Not used. Modes 5, 6: Entered by the user. Wraps/unwraps the DEK.
DRBG	SP 800-90A Hash_DRBG seed material (collected from the hardware based NDRNG) and state (Key and V). The module zeroizes all DRBG state information and seed material after each use.
IKEK	256-bit AES Intermediate Key Encryption Key (KEK) used to Wrap/Unwrap the DKEK using SP800-38F compliant KW. Mode 1, 2, 3, 4: Not used. Mode 5, 6: Derived from PBKDF.

Table 12: Private CSP Values

Key Name	Description
Public Key	All modes: ECDSA public key value used to validate signed firmware updates.

Table 13: Public Key Value

Note 3: Key values consist of a 256-bit AES key and a 256-bit XTS key. FIPS requires that the AES and XTS key values are different. The module (and the MDU Utility) performs a check to verify that the keys are different. The module will reject a key fill operation if the AES and XTS key values are identical.

3 Roles, Authentication, and Services

3.1 Roles

The module supports role based authentication for two separate roles.

Crypto Officer Role – This role allows the Crypto Officer to configure the module.

User Role – This role is the normal operating mode of the module after configuration.

The module does not support multiple concurrent roles. When changing from one role to another, the characteristics and capabilities of the new role replace the characteristics and capabilities of the previous role.

Crypto Officer Role

The module supports a Crypto Officer Role. The Crypto Officer is responsible for taking possession of new modules delivered by Mercury Systems, and for performing the initial secure configuration of the module.

The Crypto Officer role is authenticated using the Configuration Password and the Crypto Officer is responsible for installing the initial Configuration Password. The module supports a limited feature set for the Crypto Officer Role. The features available to the Crypto Officer role are limited to Configuration operations.

User Role

The module supports a User Role for a single User. The module enters a fully functional User Role only after completing a successful authentication.

After successful authentication in the User Role, the module accepts plaintext data, encrypts it, and moves the encrypted result to the NAND media. The User Role, after successful authentication, can access previously encrypted data stored in the NAND media. Prior to authentication, the User Role cannot write data or read previously stored data.

3.2 Authentication

The type of authentication differs depending on the FIPS 140-2 mode. Refer to Table 7 for a list of FIPS modes and the type of authentication required in each mode. Table 14 has a summary of the authentication strength for each FIPS approved mode under the User Role.

FIPS 140-2 mode	Authentication Parameter	Strength of Authentication
Self-generated Permanent key (FIPS Mode 1) or User filled Permanent key (FIPS Mode 2) with ATA Password	Up to 64 byte User ATA Password supplied by the attached host system. Minimum 8 character ATA Password	The probability of a random attempt for an eight (8) character field using 94 characters (all printable characters excluding space) is $1/(94^8) = 1.7E-16 < 1/1,000,000$. When configured according to the security guidance, the Authentication Penalty (maximum failed authentications) is 15. Power cycles do not reset the count. The probability of a successful random attempt during a one-minute period of time is $15/(94^8) = 2.5E-15 < 1/100,000$. When configured according to security guidance, after Authentication Penalty number of sequential failed authentication attempts, the module erases keys and storage media.
Session key (FIPS Mode 3)	Session key: 256-bit AES value 256-bit XTS value	The Session key consists of a 256-bit AES key value and a different 256-bit XTS key value. The probability of randomly authenticating with the module is then: $1/(2^{512}) = 7.5E-155 < 1/1,000,000$. When configured according to the security guidance the Authentication Penalty (maximum failed authentications) is 15. Power cycles do not reset the count. The probability of a successful random attempt during a one-minute period of time is $15/(2^{512}) = 1.1E-153 < 1/100,000$ requirement. When configured according to security guidance, after Authentication Penalty number of sequential failed authentication attempts, the module erases keys and storage media.
Session key with ATA Password (FIPS Mode 4)	Up to 64 byte User ATA Password supplied by the attached host system. Minimum 8 character ATA Password and Session key: 256-bit AES value 256-bit XTS value	The probability of a random attempt for an eight (8) character field using 94 characters (all printable characters excluding space) is $1/(94^8) = 1.7E-16 < 1/1,000,000$. When configured according to the security guidance, the Authentication Penalty (maximum failed authentications) is 15. Power cycles do not reset the count. The probability of a successful random attempt during a one-minute period of time is $15/(94^8) = 2.5E-15 < 1/100,000$. When configured according to security guidance, after Authentication Penalty number of sequential failed authentication attempts, the module erases keys and storage media. ***** After entering the correct ATA Password, the correct Session key is required. The Session key consists of a 256-bit AES key value and a different 256-bit XTS key value. The probability of randomly authenticating with the module is then: $1/(2^{512}) = 7.5E-155 < 1/1,000,000$. When configured according to the security guidance the Authentication Penalty (maximum failed authentications) is 15. Power cycles do not reset the count. The probability of a successful random attempt during a one-minute period of time is $15/(2^{512}) = 1.1E-153 < 1/100,000$ requirement. When configured according to security guidance, after Authentication Penalty number of sequential failed authentication attempts, the module erases keys and storage media.

<p>KEK and BLACK Key (FIPS Mode 5)</p>	<p>BLACK key value</p>	<p>The BLACK key is consists of a 256-bit AES key value and a different 256-bit XTS key value.</p> <p>The probability of randomly authenticating with the module is then: $1/(2^{512}) = 7.5E-155 < 1/1,000,000$.</p> <p>When configured according to the security guidance, the Authentication Penalty (maximum failed authentications) is 15. Power cycles do not reset the count. The probability of a successful random attempt during a one-minute period of time is $15/(2^{512}) = 1.1E-153 < 1/100,000$ requirement.</p> <p>When configured according to security guidance, after Authentication Penalty number of sequential failed authentication attempts, the module erases keys and storage media.</p>
<p>KEK with BLACK key with ATA Password (FIPS Mode 6)</p>	<p>Up to 64 byte User ATA Password supplied by the attached host system.</p> <p>Minimum 8 character ATA Password.</p> <p>and</p> <p>BLACK key value</p>	<p>The probability of a random attempt for an eight (8) character field using 94 characters (all printable characters excluding space) is $1/(94^8) = 1.7E-16 < 1/1,000,000$.</p> <p>When configured according to the security guidance, the Authentication Penalty (maximum failed authentications) is 15. Power cycles do not reset the count. The probability of a successful random attempt during a one-minute period of time is $15/(94^8) = 2.5E-15 < 1/100,000$.</p> <p>When configured according to security guidance, after Authentication Penalty number of sequential failed authentication attempts, the module erases keys and storage media.</p> <p>*****</p> <p>After the ATA Password is entered, the correct BLACK key value is required.</p> <p>The BLACK key is consists of a 256-bit AES key value and a different 256-bit XTS key value. The probability of randomly authenticating with the module is then: $1/(2^{512}) = 7.5E-155 < 1/1,000,000$.</p> <p>When configured according to the security guidance, the Authentication Penalty (maximum failed authentications) is 15. Power cycles do not reset the count. The probability of a successful random attempt during a one-minute period of time is $15/(2^{512}) = 1.1E-153 < 1/100,000$ requirement.</p> <p>When configured according to security guidance, after Authentication Penalty number of sequential failed authentication attempts, the module erases keys and storage media.</p>

Table 14: Authentication Strengths for User Role in all Six (6) FIPS modes

Table 15 has a summary of the authentication strength for authenticating the Crypto Officer Role.

Role	Authentication Parameter	Strength of Authentication
<p>Crypto Officer Role</p>	<p>Configuration Password</p> <p>32 byte Configuration Password</p> <p>Minimum 12 character Configuration Password.</p>	<p>The probability of a random attempt for an 12 character field using 94 characters (all printable characters excluding space) is $1/(94^{12}) = 2.10E-24 < 1/1,000,000$.</p> <p>When configured according to the security guidance, the Authentication Penalty (maximum failed authentications) is 15. Power cycles do not reset the count. The probability of a successful random attempt during a one-minute period of time is $15/(94^{12}) = 3.15E-23 < 1/100,000$.</p> <p>When configured according to security guidance, after Authentication Penalty number of sequential failed authentication attempts, the module erases keys and storage media.</p>

Table 15: Authentication Strengths for Crypto Officer Role

3.3 Services

The module supports required ATA7 services (commands) as well as Mercury Systems defined key filling services. All of the services are accessed using commands specified by the ATA7 specification. The ATA7 specification is available at the T13.org website. Volume 1 of the specification contains command descriptions.

Refer to ATA document *D1532v1r4b-AT_Attachment_with_Packet_Interface_-_7_Volume_1.pdf*

Certain standard ATA commands/services are required by the ATA specification to function without authentication. These services do not return stored user data; instead they return module information and attributes that the attached host system requires to effectively communicate with the module. Table 16 depicts what services are available to each role and which FIPS modes need authentication to access types of services.

In FIPS modes that utilize the ATA password, the drive is in a password “Locked” condition until the User ATA Password is entered by the User Role. When “Locked”, the module will only respond to informational services, for example the IDENTIFY DEVICE COMMAND. Refer to the ATA7 specification, V1, pages 27-28 for a list of how each specific ATA commands/services respond in the ATA password locked state. Table 17 lists services supported by the module and the CSP accessed by the service.

Service (or ATA command group)	User Role	Crypto Officer Role	Approved mode 1,2 Permanent and Self-Generated Permanent key with ATA Password	Approved mode 3 Session Key	Approved mode 4 Session Key with ATA Password	Approved mode 5 KEK/BLACK key	Approved mode 6 KEK/BLACK key with ATA Password
SATA Identify Device Command	Yes	Yes	NA	NA	NA	NA	NA
Execute Device Diagnostic	Yes	Yes	NA	NA	NA	NA	NA
SMART Off-line immediate	Yes	Yes	NA	NA	NA	NA	NA
Read Logical Sectors	Yes	Yes Always returns 0xFF data	A	A	A	A	A
Write Logical Sectors	Yes	–	A	A	A	A	A
Read Physical Sectors (after an erase/sanitize)	Yes	Yes	A	NA	A	NA	A
Write Physical Sectors (after an erase/sanitize)	Yes	Yes	A	NA	A	NA	A
Read MSD Configuration	Yes	Yes	A	NA	A	NA	A
Write MSD Configuration	–	Yes	A(Crypto Officer)	A(Crypto Officer)	A(Crypto Officer)	A(Crypto Officer)	A(Crypto Officer)
Read MSD Settings	Yes	Yes	A	NA	A	NA	A
Write MSD Settings	Yes	–	A(User)	NA	A(User)	NA	A(User)
Isolated Key Fill port	Yes*	–	A(User)	NA	A(User)	NA	A(User)
SMART Read Data	Yes	Yes	NA	NA	NA	NA	NA
Secure Firmware Update	Yes*	Yes	A(User)	A(User)	A(User)	A(User)	A(User)
Security Erase Prepare Security Erase Unit (from SATA)	Yes	Yes	A	NA	A	NA	A
External Trigger input (Zeroize/Secure Erase from trigger input pins)	Yes*	Yes*	NA*	NA*	NA*	NA*	NA*
Security Set Password Security Unlock	Yes	Yes	A	NA	A	NA	A
Password Clearing Procedure	Yes*	Yes*	NA	NA	NA	NA	NA

Table 16: Services and Authentication by Approved Mode and Role

- Yes = The role can access this service. Refer to the approved FIPS modes columns to determine if authentication is required.
- NA = Service is available with No Authentication. The service may be required by the SATA specification for compatibility.
- A = Authentication required to access service. ATA password modes require password entry prior to using certain services.
- () = Service available only to the role listed in parentheses
- = Service is not available to this role or to this role in the specific approved FIPS mode.
- * = Service may not be available dependent on options selected by the Crypto Officer during the initial secure configuration.

Service	ATA Password	Configuration Password	DEK	DKEK	IKEK	DRBG	Public Key
SATA Identify Device Command	-	-	-	-	-	-	-
Execute Device Diagnostic	-	-	-	-	-	-	-
SMART Off-line immediate	-	-	-	-	-	-	-
Read logical sectors	I,U*	-	U*	U*	U*	-	-
Write logical sectors	I,U*	-	U*	U*	U*	-	-
Read physical sectors	I,U*	-	-	-	-	-	-
Write physical sectors	I,U*	-	-	-	-	-	-
Read MSD Configuration	I,U*	-	-	-	-	-	-
Write MSD Configuration	I,U*	I,U,W, Z	Z,G,W,U*	Z*	U*	U,Z	-
Read MSD Settings	I,U*	-	-	-	-	-	-
Write MSD Settings	I,U*	-	I,W,U	I,W,U	G,U*	-	-
Isolated Key Fill*	U*	-	I,W,U	I,W,U	G*,U*	-	-
SMART Read Data	-	-	-	-	-	-	-
Secure Firmware update* (Update zeroes the drive)	I,U,Z*	Z	Z,G,W	Z	-	U,Z	I,U
Security Erase Prepare Security Erase Unit (from SATA)	I,U,Z*	-	Z,G,W, U	Z	Z	U,Z	-
External Trigger input (Zeroize/Secure Erase from trigger input pins)	Z*	-	Z,G,W,U*	Z*	Z*	U,Z	-
Security Set Password Security Unlock (From SATA)	I,U,W	-	-	-	G,U	U,Z	-
Password Clearing Procedure *	Z	Z	Z,U,G,W*	Z	-	U,Z	-

Table 17: CSP and Public Key Access within Services

- = No Access: The service does not access the CSP
- G = Generate/Derive: The module Generates/Derives the CSP.
- I = Input: Input the CSP.
- U = Use: The module uses the CSP.
- W = Write: The module writes the CSP into memory in the module. The CSP value written may be zeros.
- Z = Zeroize:
 - a. Module zeroizes the CSP during Erase/Sanitize/Fast Clear or operations.
 - b. The module zeroizes CSP during mode change operations.
 - c. The Crypto Officer may choose options to preserve the ATA Password after Secure Erase, Sanitize/Fast Clear operations.
 - d. DRBG state information is zeroized immediately after each use of the DRBG.
- * = Access may only apply to certain modes. See mode descriptions in Section 1.2.

4 Self-test

The module enters a Failure State when an error is detected. In the Failure State, the module continuously illuminates the blue LED. During the Failure State, the module aborts all write services and returns 0xFF values for read services.

How to execute self-tests

The User or Crypto Officer Roles can run self-tests on demand by cycling power or by executing the ATA EXECUTE DEVICE DIAGNOSTIC and the SMART OFF-LINE-IMMEDIATE services from the attached host system. The tests complete in less than 2 seconds. The blue LED will illuminate continuously if an error is detected. If the blue LED does not illuminate, the self-test passed. The SMART READ DATA service provides information about the cause of a failure. Refer to the product Programmer's Guide for more details. Table 18 lists self-test operations and Table 19 lists conditional self-tests. Neither is dependent on the mode of operation.

Test Target	CAVP Certificate	Description	When	Condition on Failure
Firmware Integrity test	NA	Armor™ Processor CRC (32-bit polynomial CRC IEEE 802 standard), MONITOR Firmware Checksum, NVRAM test, and Media test.	Power-on	Failure mode
AES-256 XTS Encrypt	2802	Performs an encryption KAT	Power-on and on demand	Failure mode.
AES-256 XTS Decrypt	2802	Performs an decryption KAT	Power-on and on demand	Failure mode.
SHA-2	3291	Performs a SHA-512 KAT	Power-on and on demand	Failure mode.
HMAC	2602	Performs HMAC SHA-512 KAT.	Power-on and on demand	Failure mode.
AES Key Wrap	3986,3987	Performs an encryption KAT and separate decryption KAT.	Power-on and on demand	Failure mode.
PBKDF	VA	Performs a KAT using a known password value and compares for an expected MK value.	Power-on and on demand	Failure mode.
DRBG	1179	Performs a HASH DRBG KAT using SHA-512.	Power-on, on demand, and prior to DRBG use	Failure mode.
ECDSA	883	Performs a signature verification KAT	Power-on, on demand, and prior to accepting a firmware update.	Failure mode.
NDRNG Entropy Source	NA	Runs a health check test.	On demand, and continuous for creation of a self-generated random key value	Failure mode.
Temperature, Power, and firmware	NA	Constant monitoring of temperature, input and internal supply voltages and out of range firmware variables.	Continuously running	Failure mode.

Table 18: Self-tests (NA = Not applicable, VA = Vendor Affirmed)

The module performs the conditional tests listed in Table 19. Performed when needed and on a continual basis.

Test Target	CAVP Certificate	Description
NDRNG (entropy source)	NA	Test performed continuous for random values requested by the DRBG.
DRBG	1179	Health check performed per SP 800-90A Section 11.3.
ECDSA Firmware Update	883	Prior to accepting a new firmware update, an ECDSA signature verification KAT is performed. The new firmware is accepted only if the KAT passes and the signature of new firmware validates. The ECDSA KAT also runs on every power-on cycle.

Table 19: Conditional Tests

5 Physical Security

The module meets the physical security requirements for FIPS 140-2 level 2. Physical security features of the module include:

- The module enclosure consists of an opaque two (2) piece structure held together with several screws.
- The heads of two exposed enclosure corner screws are filled with a proprietary orange colored material that obscures a custom screw head pattern. The custom screw head pattern design is unique to Mercury Systems.
- All components in the module use production grade materials. The printed circuit board is conformal-coated and all BGA devices are under-filled with a hard opaque epoxy to prevent easy probing of individual signals.
- All probable openings in the module enclosure include a 90 degree angle to prevent easy probe access.
- The module includes a difficult to duplicate holographic label located in the center of the front side main product label. The holographic label is not a tamper seal. Mercury Systems uses the custom label as an aid to help identify potential counterfeit units in the field.

6 Electromagnetic Interference and Compatibility (EMI/EMC)

The module successfully completed EMI/EMC testing and conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

7 Mitigation of Other Attacks Policy

The module does not mitigate any other attacks.

8 Security Guidance

The following security guidance must be followed when implementing applications using the module:

- The Crypto Officer shall inspect each module carefully for any signs of tampering during shipment from Mercury Systems. Any module that shows signs of tampering should be returned to Mercury Systems.
- The Crypto Officer shall perform the initial secure configuration of the module. Mercury Systems recommends following the FIPS configuration procedure described in the MDU User’s Guide.
- The Crypto Officer shall make no assumptions as to default values for any configurable module parameter.
- The Crypto Officer shall configure the initial Configuration Password (Crypto Officer Password) with a minimum Configuration Password length of 12 characters and preferably 32, 8-bit bytes.
- The Crypto Officer shall enforce the use of eight (8) character minimum password lengths for the User ATA Password, Master ATA Password. The security strength of passwords is directly proportional to the length of the password and the number of possible symbols per character as shown in Table 20.

Password Length	Password bit strength using all printable characters except the space. (6.555-bits entropy per symbol)	Password bit strength with all possible 8-bit values. (8-bits entropy per symbol)
8	52	64
12	78	96
16	104	128
24	157	192
32	209	256
64	419	512

Table 20: Password Strengths in Bits

- The Crypto Officer shall enable and configure the Authentication Penalty count to a value of 5, 10, or 15 attempts and inform users that the module allows a specific number of failed authentication attempts before executing a penalty to clear CSP and all data in the module. The failed attempt count increments for invalid ATA and Configuration Passwords, key values, and for invalid digital signatures during firmware updates.
- The Crypto Officer shall setup a security inspection policy to inspect the module for evidence of enclosure tampering a minimum of once per year. Tamper evidence appears as enclosure dents, marring, or scratches caused by prying, milling or drilling. It may also appear as missing screws, scratched screw heads, damaged screw heads or missing orange colored material (see Figures 5 through 7 below) covering two (2) enclosure corner screw heads. Since the screws are small, it may be necessary to inspect the orange material under magnification. The surface of the orange material should be intact, shiny, and smooth. The orange colored material is slightly UV reactive and will glow yellow/orange under UV LED light. After brief exposure to bright UV LED light, the orange colored material turns a brown/black color for several seconds before returning to an orange color. Recommended examination lamp is the NiteCore TUBE-UV or similar.



Figure 5: Screw Head in Daylight



Figure 6: Screw Head in UV Light



Figure 7: After Strong UV Exposure

- The Crypto Officer shall setup a security inspection policy to inspect the holographic label for signs of removal at least once per year. While not intended as a tamper seal, the label can be difficult to remove and will show signs of damage such as tearing or discoloration if improperly handled during a tamper event.



Figure 8: Holographic Label



Figure 9: Text on Holographic Label

- The Crypto Officer shall enable and configure the initial User ATA Password and Master ATA Password in FIPS modes that utilize the ATA Passwords.
- The Crypto Officer shall select the option to disable Firmware Updates. This option prevents the User Role from changing to a different FIPS firmware version in the field.
- The Crypto Officer Role or User Role can command the module to perform power-on self-test suite by cycling power or using the ATA EXECUTE DEVICE DIAGNOSTIC and the SMART OFF-LINE-IMMEDIATE commands.
- The Crypto Officer shall change all passwords when switching between an approved and non-approved FIPS mode of operation.
- The Crypto Officer shall command the module to perform power-on self-test by cycling power when switching between an approved and non-approved FIPS mode of operation.
- The module, by design, does not output CSPs under any conditions.

9 Change log

Revision	By	Description
Rev. 1.5.0.00	Bob Laz.	Final release