Mercury Systems ASURRE-Stor®

ASD256/512 and ADR256/512

Solid State Self-Encrypting Drives

Non-Proprietary Administrative Guidance

(Firmware revision 1.5.1 and Hardware revision 3.0)

Date: February 4, 2020

Document revision 1.5.1

Table of Contents

List of Tables

List of Figures

Reference documentation

Acronym	Full Specification Name
ATA Specification ATA7 Specification	The ATA specification defines industry standard storage commands used by the TOE. The document is available on the T13.org website. D1532v1r4b-AT_Attachment_with_Packet_Interface_-_7_Volume_1.pdf
cPP	Collaborative Protection Profile for Full Drive Encryption - Encryption Engine v2.0 January 2, 2019. Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition v2.0, January 2, 2019. Filenames: CPP_FDE_EE_V2.0E.pdf, CPP_FDE_AA_V2.0E.pdf
FIPS140-2	NIST, *Security Requirements for Cryptographic TOEs*, May 25, 2001
ST	Security Target for Mercury Systems ASURRE-Stor® Solid State Self-Encrypting Drives
NIST 800-38F	NIST Special Publication: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping

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 TOE. *Please note that use of the MDU utility is optional and not part of the evaluation.*
Programmer's Guide or SSD Programmer's Guide *(ssdProgrammersGuide.pdf)*	This document provides detailed register-level information describing how to use commands/services supported by the TOE that allow filling of keys and configuring security features. Designers intending to create their own version of the Mercury Systems MDU utility use this document as a reference manual. *Please note that use of this document is optional and not part of the evaluation.*
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 TOE 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 TOE. *Please note that use of this document is optional and not part of the evaluation.*
SSD Secure Configuration Programmer's Guide (*ssdSecureConfigurationProgrammersGuide.pdf*)	This document is intended for users desiring to implement their own *ASURRE-Stor*® configuration tools using standard SATA commands. The document provides the low level details required to perform configuration operations replicated in the MDU utility. This document is part of the evaluated administrative guidance for the TOE, and is available directly from Mercury.

Table 2: Additional support documentation available from Mercury Systems

Acronym	Definition
Armor™ Processor	This is the Mercury Systems marketing name for the combination of the TOE firmware and TOE hardware.
ATA Specification ATA7 Specification	The ATA specification defines the operation of 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
BEV	Border Encryption Value. In this document, the BEV and KEK (Key Encryption Key) are used interchangeably.
BLACK DEK	An encrypted version of the media DEK (Data Encryption Key)
BLACK KEK	An encrypted version of the KEK (Key Encryption Key). The KEK is used to decrypt the BLACK DEK.
CC	Common Criteria
CC cPP	Common Criteria collaborative Protection Profile
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.
DEK	Data Encryption Key. The key used to encrypt or decrypt user data.
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.
FIPS	Federal Information Processing Standards
FDE	Full Drive Encryption
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.
KEK	Key Encryption Key. A key used to wrap (AES key wrap, SP 800-38F) or un wrap (AES key wrap, SP 800-38F) the DEK.
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. ATA also defines two capability levels, High and Maximum, which determine how the TOE behaves when the Master Password issued to unlock 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 Asurre-Stor® SSD. *Please note that use of the MDU utility is optional and not part of the evaluation.*
Non-Volatile memory (NVM)	Non-Volatile Memory is a memory technology that retains data across power cycles. (e.g., EEPROM, NAND Flash)
OPAL	A security specification defined by the Trusted Computer group that utilizes a TPM in a computer host.
RBG or RNG or NDRBG or NDRNG	Random Bit Generator, Random Noise Generator, Non-deterministic Random Bit Generator, Non-deterministic Random Number 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 or LBA	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 from one manufacturer to another.
SHA	Secure Hash Algorithm (FIPS 180-4)
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 vs a rotating magnetic platter for the storage media.
SFF-8201	Specification for 2.5" Form Factor Drive Dimensions developed by the SFF Committee
ST	Security Target
TOE	Target Of Evaluation
TCG and TPM	Trusted Computer Group and Trusted Platform Module
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.
XTS	AES encryption utilizes block cipher modes. XTS is the block cipher mode most commonly used in secure storage.

Table 3: Acronyms and Definitions

1 Introduction

This document provides administrative guidance for the ***ASURRE*-Stor**® 2.5" Solid State encrypting hard drive, hereafter denoted TOE *or* ***ASURRE*-Stor**® SSD. The document describes how to identify the product, install it in a typical host system, and describes the steps necessary to begin the initial secure configuration of the TOE. The document is intended for use by the Administrator or Crypto Officer responsible for configuring the product prior to field deployment.

The reader may notice that the document refers to a value called the BEV. The BEV is a term that originated in the FDE Collaborative Protection Profile and stands for Border Encryption Value. The BEV performs the same function in the ***ASURRE*-Stor**® SSD as a KEK (Key Encryption Key) and is used to decrypt the media DEK (Data Encryption Key). The document uses the terms BEV and KEK interchangeably.

2 Product Description

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

Unlike most other secure solid state drive products, the Mercury Systems ***ASURRE*-Stor**® SSD does not depend on a TPM module, TCG, or OPAL to implement security. Instead the ***ASURRE*-Stor**® SSD implements security using hardware-based AES-256 XTS encryption and key management techniques that are compatible with the industry standard 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.
The ***ASURRE*-Stor**® SSD was evaluated against the Common Criteria Collaborative Protection Profile for Full Drive Encryption - Encryption Engine, v2.0 dated January 2, 2019 and the Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v2.0 dated January 2, 2019.

3 Product Configuration and Deployment

The Mercury Systems ***ASURRE*-Stor**® SSD is shipped with the optional MDU configuration utility. While the MDU provides an easier-to-use method of performing some of the required administrative configuration functions, the MDU is a utility provided by Mercury that is not part of the evaluated configuration and this should be taken into account by users of the system. The use of this utility was not evaluated. Therefore, the interfaces used as part of the evaluation are the direct SATA interfaces.

The programmer's guide and security configuration programmer's guide describe the administrative interface that is used in the evaluated configuration that was tested. The configuration instructions for activities mandated by the ST are provided in this document; locations of the instructions are given by reference to the programmer's guides, and for convenience some references using the MDU visual interface are given as well.

4 Deployed TOE usage scenario:

The TOE usage scenario is a re-occurring mission model. The TOE supports two CC compliant modes of operation:

1. ATA password with Self-generated Permanent key (Mode 1)
2. ATA Password with KEK and BLACK key (Mode 6)

Mode 1: ATA password with Self-generated Permanent key

This scenario begins with the Crypto Officer (CO) configuring the TOE in a secure location using MDU or a similar custom utility program. The CO configures the TOE to operate in Mode 1. The TOE uses a hardware based NDRNG and a DRBG algorithm to self-generate a random DEK. The DEK consists of a 256-bit AES key and a different 256-bit XTS key. The CO enters a password of up to 64 characters. The TOE conditions the password with PBKDF (Password Based Key Derivation Function SP 800-132) to create a derived 256-bit key (BEV/KEK) that the TOE uses to AES key wrap (AES-KW-

256, SP 800-38F) the DEK. The TOE then overwrites the password that was entered by the CO and the derived key (BEV/KEK) resulting from the PBKDF function and saves the wrapped DEK in NVRAM. After configuration completes, the CO exits the Crypto Officer role. At this point the TOE is operational and ready to accept mission data in a User Role. Mission personnel load mission data into the TOE then turn off TOE power. Removing power purges the DEK from the TOE. In the powered-off state the TOE contains only the wrapped DEK located in NVRAM.

The TOE is transported to the mission vehicle and installed. The mission vehicle host system provides the password. The TOE conditions the password with PBKDF to create a derived key (BEV/KEK) that is then used to un-wrap (AES-KW-256, SP 800-38F) the DEK. If the unwrap operation completes successfully and the resulting DEK is the correct DEK, the TOE enters a normal operating mode which allows the mission to begin. When the mission completes, TOE data, if applicable, is retrieved.

The TOE retains the AES wrapped DEK across power cycles in NVRAM, however; the password must fill on each power cycle to complete the key chain.

Mode 6: ATA password with KEK and BLACK key

Pre-configuration operations, separate from the TOE, are described below.

In Mode 6, the Crypto Officer (CO) begins by creating three keys, a 256-bit BEV(KEK), a 512-bit DEK, and a 576-bit BLACK key. The DEK consists of a 256-bit AES key and a different 256-bit XTS key. The CO uses the BEV(KEK) and AES key wrap (AES-KW-256, SP 800-38F) to wrap the DEK. The resulting wrapped DEK is referred to as the BLACK key. The CO and mission personnel must retain the BLACK key for filling the TOE at each mission power-on cycle.

TOE configuration operations (performed on the TOE):

The CO configures the TOE using MDU or a similar custom utility program to operate in Mode 6. The CO fills the BEV(KEK) and enters a password of up to 64 characters. The TOE conditions the password with PBKDF (Password Based Key Derivation Function SP 800-132) to create a derived 256-bit key that the TOE uses to AES key wrap (AES-KW-256, SP 800-38F) the BEV(KEK). The TOE saves the wrapped BEV(KEK) in NVRAM. The CO then cycles TOE power off then on again.

Next, the CO fills the TOE with the password followed by the BLACK key. The TOE conditions the password using PBKDF (Password Based Key Derivation Function SP 800-132) to create a derived intermediate key and uses it to AES unwrap (AES-KW-256, SP 800-38F) the BEV(KEK). The TOE then uses the BEV(KEK) to unwrap the BLACK key re-creating the DEK and completing the key chain. The TOE overwrites the password and derived key. The CO exits the Crypto Officer role.

At this point the TOE is operational and ready to accept mission data in a User Role. Mission personnel load mission data into the TOE then turn off TOE power. Removing power purges the DEK and unwrapped BEV from the TOE RAM. In the powered off state, the TOE contains only the wrapped BEV(KEK) in NVRAM.

The TOE is transported to the mission vehicle and installed. The mission vehicle host system provides the password and the BLACK key. The TOE conditions the password with PBKDF to create a derived intermediate key that the TOE uses to unwrap the BEV(KEK) previously saved in NVRAM. If the unwrap operation succeeds, the TOE uses the BEV(KEK) to unwrap the BLACK key. If the unwrap operation succeeds and the resulting DEK is the correct DEK, the TOE enters a normal operating mode which allows the mission to begin.

When the mission completes, TOE data, if applicable, is retrieved.

The TOE retains the AES wrapped BEV(KEK) in NVRAM across power cycles. The password and BLACK key must fill on each power cycle to complete the key chain.

5 Failed attempts penalty

The TOE supports a feature to limit the number of sequential failed attempts to enter correct passwords, key values, and correct digital signature during firmware updates. When the maximum number of failed attempts count is

exceeded, the TOE performs a zeroize/clear operation that erases the wrapped DEK (mode 1) and wrapped BEV(KEK) (Mode 6), as well as all of the NAND media. As part of the Administrative Guidance, the CO is instructed to enable this feature and use a failed attempts count of 1, 5, 10 or 15.

6 TOE operation prior BLACK key fill

The key chain for the TOE is not complete until the password (mode 1 and 6) and BLACK key (mode 6) fill. After the CO completes the initial secure configuration, and prior to password and/or BLACK key fill, the TOE responds to informational ATA commands as required by the ATA specification. In response to these commands the TOE returns information and attributes about the TOE that the attached host system requires to properly communicate with the TOE. The TOE returns values of all 0xFF for read user data commands and a failure for any attempt to write user data.

7 Power States

The TOE automatically enforces operation in ACPI device power states D0 and D3. Specifically, D0 and D3 (cold). D0 is defined as the fully on, active state, and D3 (cold) is the state where the device is fully powered off. The TOE supports other power saving states as required by the ATA specification; however, as part of the Administrative Guidance, the CO is instructed to disable other power states and force the TOE to only support D0 and D3 (cold).

To authenticate and enter power state D0 from a power-on cycle, the TOE requires an ATA password in Modes 1 and 6. Additionally, the correct BLACK key is required in Mode 6. Access to plain text is only allowed when authentication completes successfully. When power is removed from the TOE, the TOE enters power state D3 (cold), a fully powered-off condition. Only power state D0 allows access to plain text data. Since SSDs never receive warning of imminent power loss, the design of the TOE assures that there are no scenarios where an unexpected power loss can result in the TOE entering a non-compliant power state.

8 Immediate Key destruction

The TOE never uses the NAND storage media to hold encryption keys, passwords, or any intermediate security related variables. Instead, the DEK resides in the NAND controller's RAM and wrapped keys reside in a separate NVRAM. This architectural model allows the TOE to immediately destroy key information regardless of ongoing operations in NAND such as garbage collection, wear-leveling, Block Retirement, or any SATA operations including TRIM.

9 Key Recovery

The TOE contains no mechanism to allow export or recovery of encryption keys or wrapped keys.

10 Product Identification

As with any secure product, it is important to verify that the product received from Mercury Systems has not been tampered with or replaced with a similar but non-compliant product during shipment. For an additional fee, Mercury Systems can ship the product using FedEx Custom Critical services. Refer to the FedEx website to determine what FedEx services match required security needs.

The Administrator or CO responsible for configuring the product prior to field deployment is encouraged to consider the guidelines below to ensure the authenticity and integrity of the received TOE.

- The main label of the TOE contains the product part number. Referring to the part number section of this document, verify that the part number on the main label matches one of the part numbers in Table 4 and also matches what was ordered from Mercury Systems.
- The TOE includes a difficult to duplicate holographic label shown in Figure 1. The label isn't intended to be a tamper seal, however the label can be difficult to remove and will show signs of tearing or discoloration if improperly handled during a tamper event.

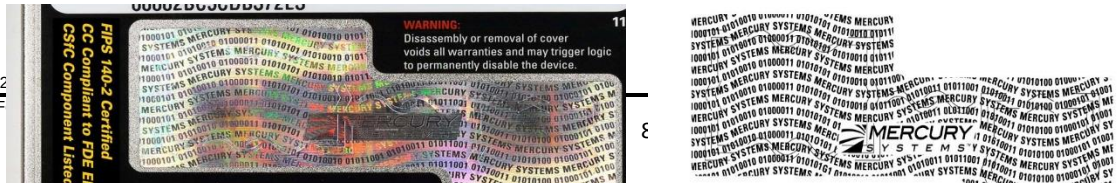

Figure 1: View of the holographic label located in the center of the main label.

- Verify that the Firmware version (FW) and Hardware revision (HW) printed on the main label matches the following: "FW 1.5.1 HW 3.0"
- The main label contains a Common Criteria validation report number. Verify that the validation report number (VR#) matches the number listed on the CC certificate on the NIAP website.
- The heads of two exposed enclosure corner screws are filled with an orange material that obscures a custom screw head pattern. Inspect the two corner screws for evidence of tampering. Since the screws are very small, inspection with magnification is recommended.
- Use the SATA command described in SSD Secure Configuration Programmer's Guide, section 2.2, to verify that the TOE reports Firmware revision number 1.5.1. Alternatively, the MDU utility can be used (Refer to MDU section) to verify that the TOE reports Firmware revision number 1.5.1.
- Images of the *ASURRE-Stor*® SSD appear in Figure 2. Inspect the TOE to verify that the product received matches the images of Figure 1 and 2.

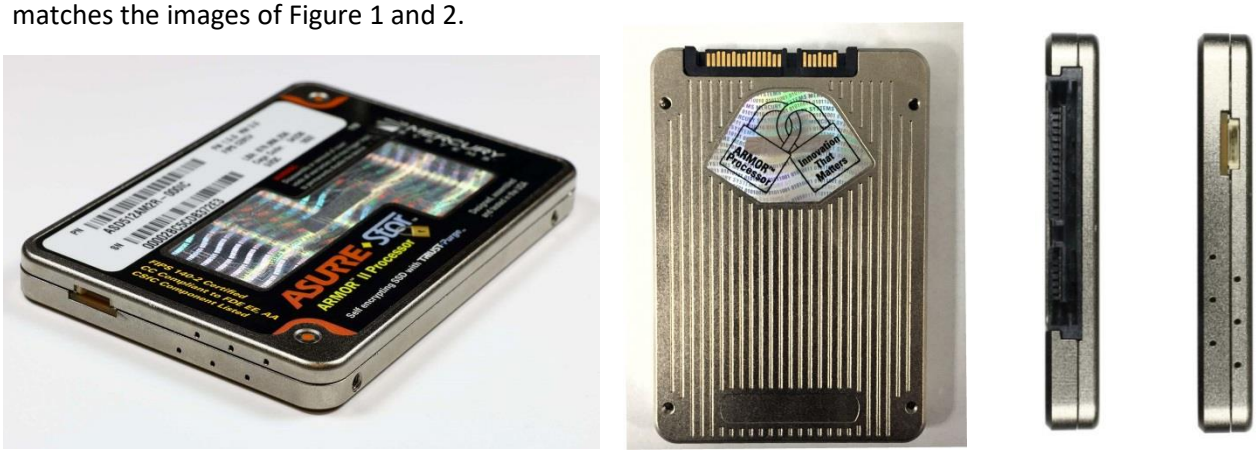

Figure 2: Images of the *ASURRE-Stor*® SSD

11 Evaluated Configuration

The TOE evaluation covers the following hardware models with Firmware 1.5.1 and Hardware revision 3.0.

ASD256AM2R, ASD512AM2R, ADR256AM2R, ADR512AM2R

The physical boundary of the TOE is the drive enclosure.
The TOE can be configured to operate in one of several modes of operation. The modes of operation differ in how the DEK is established and stored. Two modes are CC compliant and are covered by this evaluation.

- ATA password with Self-generated Permanent key
- ATA password with KEK with BLACK Key

12 Part numbers

The CC compliant part numbers are shown below in Table 4.

Part number	Part number suffix description
ASD256AM2R-xyzIC	Option Field x: 0 = Standard product. 1 = Omit the LED Indicator Port and the Write Protect Port. Option Field y: 0 = Standard product. 1 = Electrically isolate enclosure. 2 = Erase pin 1 option. Trigger an erase/sanitize operation from SATA pin P1. Option Field z: 0 = Standard product. 1 = Legacy erase option. Same as field y Option 2 except from SATA pin P13. 2 = Hypertronics Rugged connector 3 = Option 1 and 2 4 = Erase pin low option. Same as field y Option 2 except from SATA pin P4 low. 5 = NA 6 = Option 2 and 4 8 = Amphenol Rugged Connector 9 = Option 8 and 1 C= Option 8 and 4
ASD512AM2R-xyzIC	Same options as ASD256AM2R-xyzIC
ADR256AM2R-xyzIC	Same options as ASD256AM2R-xyzIC (This model has reduced overprovisioning)
ADR512AM2R-xyzIC	Same options as ASD256AM2R-xyzIC (This model has reduced overprovisioning)

Table 4: Part number summary

13 Scope of evaluation

The ***ASURRE-Stor***® SSD was evaluated to the security functional requirements specified in the document "Security Target for Mercury Systems ASURRE-Stor® Solid State Self-Encrypting Drives".

The TOE does not depend on a TPM (Trusted Platform Module) or OPAL (a security specification) to provide security. Instead the TOE supports 6 FIPS 140-2 approved modes, of which, two modes satisfy the requirements of the Collaborative Protection Profile for Full Drive Encryption - Encryption Engine, v2.0 dated January 2, 2019 and the Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v2.0 dated January 2, 2019.

To provide consistency to the FIPS Security Policy documentation, the CC documentation for the ***ASURRE-Stor***® SSD uses the same numbering for the key management modes as the FIPS 140-2 Security Policy. Using the FIPS mode numbering scheme, the TOE supports CC compliant modes of Mode 1 and Mode 6. No other key management modes were evaluated during the course of the CC-Evaluation.

Mode #	Mode name	Key Chain
1	Self-generated random Permanent key with ATA Password	During configuration: The TOE self-generates a random 256-bit AES key and different 256-bit XTS key for use as the media DEK. A password is filled and is conditioned by PBKDF(SP 800-132) to create an intermediate derived key that is used to AES key wrap (AES-KW-256, SP 800-38F) the DEK. The wrapped DEK is saved in NVRAM. During normal operation: On each power cycle, the password must fill. The TOE conditions the password with PBKDF to create an intermediate derived key (BEV/KEK) that is then used to un-wrap (AES-KW-256, SP 800-38F) the DEK previously saved in NVRAM.
6	ATA password with KEK and BLACK key	Pre-configuration: The CO creates two keys, a 256-bit BEV(KEK) and a 512-bit DEK. The DEK consists of a 256-bit AES key and a different 256-bit XTS key. The CO creates a password of up to 64 characters. The CO conditions the password using PBKDF (SP 800-132) to create a derived 256-bit key used to AES key wrap (AES-KW-256, SP 800-38F) the DEK to create the BLACK key. During Configuration: The CO fills the BEV(KEK) and password into the TOE. The TOE conditions the password with PBKDF (SP 800-132) creating a derived 256-bit key used to AES key wrap (AES-KW-256, SP 800-38F) the BEV(KEK). The TOE saves the wrapped BEV(KEK) in NVRAM. During normal operation: On each power cycle, the user enters the password and BLACK key. The password is conditioned with PBKDF creating a derived 256-bit key used to un-wrap the BEV/KEK previously saved in NVRAM. The un-wrapped BEV/KEK is used to un-wrap the BLACK key to re-create the DEK.

Table 5: CC Compliant modes

14 Operating Environment

The ***ASURRE-Stor***® SSD is compliant and compatible with the industry standard SATA specification and conforms to the ATA7 specification and command set. The ***ASURRE-Stor***® SSD will function correctly in all products that include a standard SATA interface and are compliant to the SATA and ATA7 specification.

15 Operating environment assumptions and requirements

The guidance for the ***ASURRE*-Stor**® SSD makes the following assumptions:

- The TOE encrypts all data with AES-256 XTS. There are no configuration options or support for different key sizes.
- The TOE is not dependent on the operational environment to perform DEK purging or memory clear operations. All operations that perform clear and purge operations, once triggered, operate indecently of the host SATA interface.
- The ***ASURRE*-Stor**® SSD does not support TCG or require a trusted platform module for secure operation.
- The ***ASURRE*-Stor**® SSD is located in a secure environment during the initial secure configuration.
- The Administrator or Crypto Officer connects the ***ASURRE*-Stor**® SSD to a host system that includes the electrical and software interface support necessary to implement an industry standard SATA interface as defined by the Serial ATA specification, revision 2.6.
- When configuring the TOE using a custom designed utility, the Administrator shall verify that the custom utility configures the TOE to the same configuration described by the SSD Secure Configuration Programmer's Guide configuration procedure.
- Administrators preferably fill the password, BLACK key, and BEV(KEK) over the standard SATA interface using the MDU utility. The BLACK key and BEV(KEK) can also fill from a 2-pin serial interface located on pins P14 and P15 of the SATA connector. This interface is only used when filling with COMSEC controlled DS-101 key fill devices. When utilizing COMSEC key fill devices, P14 acts as a 3.3 V, RS-232 Rx signal and Pin P15 acts as a 3.3 V, RS-232 Tx signal. The protocol settings for the key fill device should be set to 2400 baud, 8 data bits, 1 stop bit, and no parity. Mercury Systems provides technical support to help interface with COMSEC key fill devices and can provide the technical details needed to create custom key fill cables and any needed voltage translation.
- The Administrator and/or system designers shall implement application techniques, safeguards, and/or procedures to assure that power is removed from the TOE, state D3 (cold), when the host system is left unattended. On removal of power, the TOE purges the DEK key and enters a full-off state in less than 20 milliseconds.
- The Administrator shall verify that TOE users are trained on how to power-off the host system and TOE.
- The ***ASURRE*-Stor**® SSD accepts passwords lengths of up to 64, 8-bit bytes. Administrators and Crypto Officers shall enforce password lengths and complexity to provide suitable security strength.
- After completing the secure configuration of the TOE, the Administrator or Crypto Officer will verify that the TOE is operating in a CC compliant configuration. Use the SSD Secure Configuration Programmer's Guide to determine the SATA commands required to verify this information.
- The TOE product is compliant to the EE and AA protection profiles. It is assumed that the external interface providing the password to the AA portion of the TOE, is in close enough proximity to the TOE during operation that a threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.
- The Administrator understands that Mercury Systems supplies the TOE in an erased state. The TOE contains no data when delivered by Mercury systems. The Administrator shall not store information on the TOE until after completing the initial secure configuration procedure.
- The Administrator shall implement methods and procedures to assure that the host system is free of malware that could interfere with the correct operation and power-off procedures of the host system connected to the TOE.
- The Administrator is responsible for completing the initial secure configuration of the TOE and for generating password, BEV(KEK), and BLACK key values that meet the requirements of the EE and AA protection profiles for both strength and entropy.
- The Administrator shall train any users involved in the provisioning of the TOE in the methods and procedures to properly handle, store, and secure the password, BEV(KEK) and BLACK key values. For example, the password and BLACK key values should be stored separately from the host system and the TOE.

16 Unattended operation

The TOE is compliant to the Serial ATA specification. The SATA specification defines a set of commands the host system uses to write/read data to/from the TOE. Since the TOE cannot independently initiate communication with the host, the TOE has no mechanism to determine when a host system is unattended, or for example, in a lock-screen or sleep state. For this reason, the Administrator and system designers must implement host system application techniques, safeguards, and/or procedures that remove power from the TOE whenever the host platform is left unattended. Upon removal of power, the TOE purges the DEK and moves to a complete power-off state in less than 20 milliseconds.

17 TOE state when shipped from Mercury Systems

For simplicity of initial setup at the customer site, ***ASURRE-Stor***® SSDs ship from Mercury Systems fully erased and in a non-compliant mode. The Administrator or Crypto Officer taking possession of factory delivered ***ASURRE-Stor***® SSDs must perform an initial secure configuration of each TOE to place the TOE into a CC compliant operating mode prior to deployment.

18 Secure Configuration

Prior to configuration, the Administrator must determine the appropriate key management mode for operation. Selecting the mode impacts how the host system interacts with the TOE. In both CC compliant modes, the host system must supply authentication that allows the TOE to complete the key chain. The required authentication is a password in Mode 1 or a password and a BLACK key in Mode 6. Block diagrams of the two CC compliant modes are shown in Figure 3 and Figure 4.

In Mode 1, the TOE self generates the media DEK. The ATA Password conditioned by PBKDF (SP 800-132) creates an intermediate derived key that is used to AES key wrap (AES-KW-256, SP 800-38F) the DEK. The wrapped DEK is saved in NVRAM. The ATA Password must be entered on every power-on cycle. The ATA Password is conditioned by PBKDF (SP 800-132) to create a derived key used to un-wrap DEK and allow normal operation.

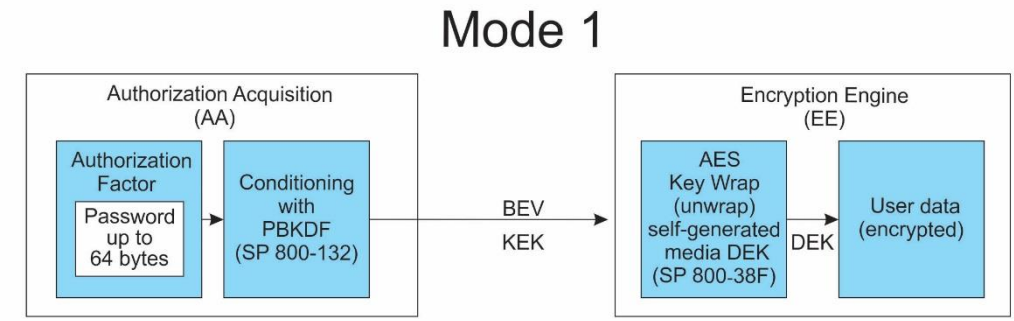

Figure 3: Diagram of operation in Mode 1, ATA Password with self-generated Permanent key

In Mode 6, the TOE accepts a plain-text BEV(KEK). The TOE uses the ATA password, conditioned by PBKDF (SP 800-132), to create an intermediate derived key used to AES key wrap (AES-KW-256, SP 800-38F) the BEV(KEK) The wrapped BEV(KEK) is saved in NVRAM. During normal operation, the user must enter the password and a BLACK key on every power-on cycle. The Password is conditioned by PBKDF (SP 800-132) to create a derived key used to un-wrap BEV(KEK) which is them used to unwrap the BLACK key value to re-create the DEK and allow normal operation.

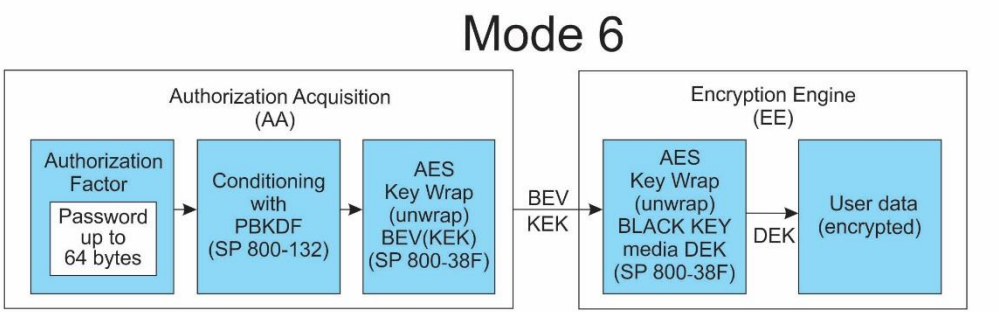

Figure 4: Diagram of operation in Mode 6, ATA Password with KEK and BLACK key

Direct Configuration

The initial secure configuration of the TOE can be accomplished using standard SATA commands and referencing register level descriptions defined in the SSD Programmer's Guide and the SSD Secure Configuration Programmer's Guide.

During the secure configuration procedure, specific configuration parameters are configured to CC compliant values. The TOE parameters that do not affect CC compliance are allowed but were not evaluated. Examples of parameters required for CC compliance are listed below.

a. "KEK and BLACK DEK" mode must be set to "KEK and BLACK DEK".
b. The "Key Source" selection is determined by the CO as required by the fielded application.
c. "Require the ATA user password…" (enables the KEK with BLACK key and ATA Password mode). Set the "ATA Password Length" to 64 bytes.
d. Enable the "Secure Erase Trigger" option.
e. Select a "Default Secure Erase Operation". All erase operations erase the key and are CC compliant.
f. Enable the "Authentication Penalty" by selecting a value of 1, 5, 10, or 15.
g. To prevent the user from changing the firmware after configuration completes, select "Disable" for the "Firmware Updates" option.
h. Disable the "Password Recovery" feature.
i. Verify that the "MSD Settings Log" is set to a value of "Version 3".
j. Disable the "Intermediate Power Save Mode" option.
k. Define the Configuration Password.
l. Issue the "Execute Security Command" and define a User ATA password.
m. Define and install the BEV(KEK) and BLACK key values.
n. Cycle TOE power, and then verify the TOE is in a (CSfC) CC compliant mode.

The detailed commands to perform these steps are found (in sequential order, with all implementation details referenced) in section 2 of the SSD Secure Configuration Programmer's Guide.

19 The Mercury Systems MDU Utility

The initial secure configuration of the TOE can be accomplished using the Mercury Systems MDU Utility, though this is not evaluated functionality. When using MDU for configuration, connect the ***ASURRE-Stor***® SSD to a PC computer using standard SATA/Power cables, launching the Mercury Systems MDU utility, then beginning configuration.

The MDU utility runs on Windows XP, Windows 7 and Windows 10. After MDU opens, it may be necessary to press the "Scan for Hardware Changes" button to scan for Mercury ***ASURRE-Stor***® SSDs, however, MDU generally auto-detects them. In the "Mercury Drives:" window in the upper left corner, MDU lists all the Mercury Systems ***ASURRE-Stor***® SSDs detected. Use the cursor to select to a specific TOE and press the "Get drive information" button. This causes MDU to read the TOE configuration and display it as shown in the screen shot of Figure 5 below.

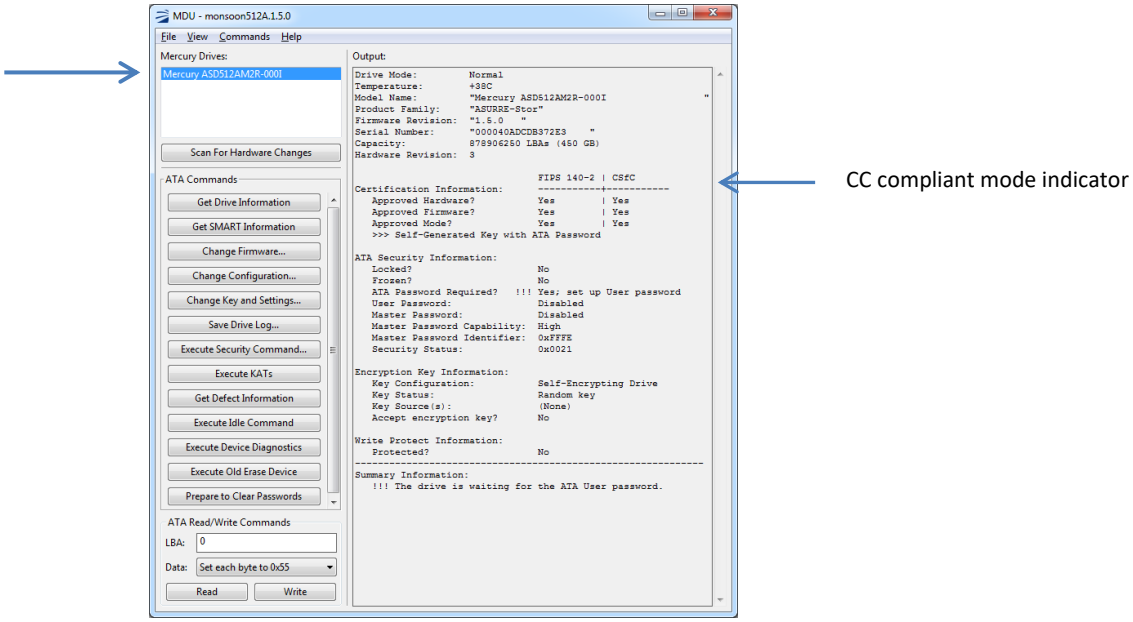

Figure 5: MDU utility top level screen

During the secure configuration procedure, specific configuration parameters are configured to CC compliant values. The TOE parameters that do not affect CC compliance are allowed but were not evaluated. Examples of parameters required for CC compliance are listed below.

a. "KEK and BLACK DEK" mode must be set to "KEK and BLACK DEK".
b. The "Key Source" selection is determined by the CO as required by the fielded application.
c. "Require the ATA user password…" (enables the KEK with BLACK key and ATA Password mode). Set the "ATA Password Length" to 64 bytes.
d. Enable the "Secure Erase Trigger" option.
e. Select a "Default Secure Erase Operation". All erase operations erase the key and are CC compliant.
f. Enable the "Authentication Penalty" by selecting a value of 1, 5, 10, or 15.
g. To prevent the user from changing the firmware after configuration completes, select "Disable" for the "Firmware Updates" option.
h. Disable the "Password Recovery" feature.
i. Verify that the "MSD Settings Log" is set to a value of "Version 3".
j. Disable the "Intermediate Power Save Mode" option.
k. Define the Configuration Password. Press the "Set Password" button and follow instructions.
l. Use the "Execute Security Command" button and define a User ATA password.
m. From the "Change key and Settings…" window, define and install the BEV(KEK) and BLACK key values.
n. Cycle TOE power, and then use the MDU "Get Drive Information" button to verify the TOE is in a (CSfC) CC compliant mode.

The process to complete the initial secure configuration using MDU is greatly simplified by referring to the MDU User's Guide. The MDU User's Guide provides simple, step-by-step instructions with screen shots taken directly from the MDU utility. The document guides Administrators and Crypto Officers through the entire secure configuration process. Refer to section 3 of the MDU User's Guide for the full configuration procedure.

20 Changing the BEV (KEK) and BLACK key after the TOE is configured

The TOE verifies that the BLACK key that fills on each power cycle is identical to the BLACK key filled during the initial secure configuration procedure. This is done both for authentication and to prevent TOE data corruption. In order to change to a different BLACK key or BEV(KEK) an erase operation is required. The erase operation outlined below erases the existing BLACK key DEK, BEV(KEK), User ATA Password and the NAND media. The operation also causes the TOE to prepare to accept new BEV(KEK) and BLACK key values.

A summary of the steps needed to change the key values appears below.

1. Obtain the current TOE configuration Log, and modify the "Default Secure Erase" parameter to "Fast Clear."
2. Unlock the TOE by entering the correct User ATA Password by sending the "Execute Security Command" command.
3. Send the "Erase the drive" command. The drive green LED on the LED indicator port will flash until the erase operation completes. This will take less than 8 seconds for the Fast Clear protocol. At this point the drive has no key values, no ATA Password, and the NAND media is clear. Drive data is forensically unrecoverable.
4. Read the TOE configuration file and modify it to include the new BEV(KEK) value and send the configuration to the TOE
5. Repeat for the BLACK key value.
6. Repeat for the ATA password.
7. Cycle TOE power, enter the ATA password, and issue the "Get Drive Information" command and verify that the TOE is in a CC compliant mode.

21 Changing the User or Master ATA Password after the TOE is configured

The TOE supports changing the User ATA password after initial configuration. The host system must unlock the TOE by entering the correct User ATA password, then once unlocked, the host system can change the User ATA password. The host system can use ATA commands defined in the SSD Programmer's Guide or the host can use MDU to simplify this process. The TOE uses the PBKDF-conditioned User ATA password to unwrap the encryption key, then conditions the new User ATA password with PBDKF to wrap the encryption key. The TOE overwrites all old information in the keychain with information based on the new User ATA password.

The TOE supports changing the Master ATA Password, but only when no master password exists. The host must use ATA commands (or MDU) to disable the Master ATA password prior to specifying a new Master password.

22 Ports on the *ASURRE-Stor*® SSD

The ***ASURRE-Stor***® SSD conforms to the industry standard 2.5" 9.5mm thick hard drive form factor (SFF-8201). Photos in Figure 6 show views of TOE ports that may be useful during configuration. Table 6 and 7 briefly describe each port. The TOE contains a Write Protect port, a LED Indicator port, a SATA Power Segment port and a SATA Signal Segment port. To operate the TOE in Read-Only applications, install a write protect jumper (available from Mercury) into the Write Protect port connector.

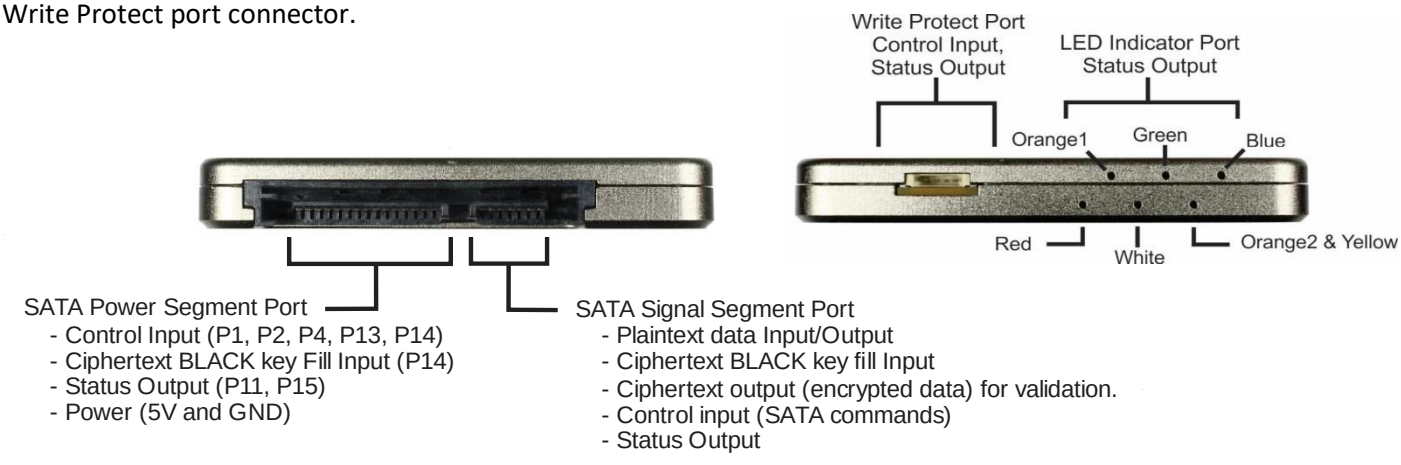

Figure 6: Ports on the TOE

TOE 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 6: TOE Port Summary

LED Color	LED purpose
Blue and Green	The LEDs provide immediate visual feedback for the Crypto Officer during TOE 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 4 times per second. Green LED is off. Secure Erasing – Green LED blinks 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 TOE is waiting for an encryption key fill operation.
White	Indicates that the SATA interface is operating at 1.5Gb/s when illuminated.
Yellow	Reserved for factory use.
Orange1	Indicates SATA activity in the TOE.
Orange 2	Flashes to indicate that the TOE is waiting for entry of a User ATA Password.

Table 7: LED Indicator Port

23 Installing the TOE into a host system

ESD

The *ASURRE*-Stor® SSD utilizes both active and passive techniques to mitigate damage caused by severe electro-static discharge. Mercury Systems recommends following industry standard ESD precautions and procedures when handling *ASURRE*-Stor® SSDs. It is important to note that the enclosure is tied to DC power ground. This provides the most reliable operation should ESD events occur during normal operation. As an ordering option, the TOE is available with the enclosure isolated from DC ground.

Installing the TOE in a host computer system

The TOE has 4 mounting screw locations on the bottom side and 2 mounting locations along each of the 100.4 mm edges. Mercury Systems includes four M3 mm screws in the packaging with each TOE. To avoid damaging the enclosure and internal electronics, do not attempt to use longer screws unless a maximum insertion depth of 3 mm is maintained from the outside edge of the enclosure. Connect the SATA signal and SATA power cables from the host to the corresponding connectors on the *ASURRE*-Stor® SSD. The TOE is now ready for operation.

Using the TOE with commercial SATA and power cables

Industry standard SATA connectors have two segments that separate data and power signals from each other. Some host systems include a single cable that runs from the host computer to the SATA drive, integrating both the power and data segments into a single cable. Other host systems use separate cables and connectors for the power and data segments. Mercury Systems *ASURRE*-Stor® SSDs use the “MIL” pin out on the SATA connector power segment. The “MIL” pin out re-targets the 3.3 V and 12 V pins (P1, P2, P3, P13, P14, and P15) on the SATA Power Segment to External

Secure Erase triggers, COMSEC key fill, and other operations common to the defense industry. The *ASURRE*-Stor® SSD data sheet contains a pinout table and a description of the MIL pinout supported by the *ASURRE*-Stor® SSD.

SATA Connector Warning

The power segments of most commercial SATA connectors have every three pins shorted. Refer to images in Figure 7.

- P1, P2, and P3 (3.3V) shorted
- P4, P5, and P6 (GND) shorted
- P7, P8, and P9 (5V) shorted
- P10, P11, and P12 (GND) shorted
- P13, P14 and P15 (12 V) shorted

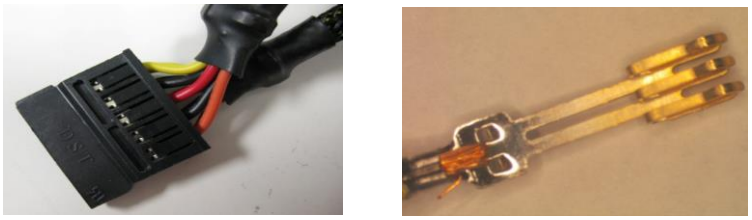

Figure 7: SATA power connector with 12 V pin (P13, P14, P15) removed to show pin shorts

When possible, Mercury Systems recommends the use of connectors with individualized pins for each of the 15 pins in the power segment or an interface board that separates individual pins in the power segment. Figure 8 shows examples of SATA connectors with individualized pins.

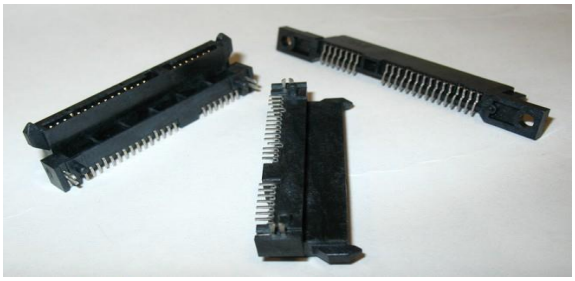

Figure 8: SATA connectors with separate pins

24 Roles

The TOE supports role based authentication for a Crypto Officer and a single user. The TOE does not support multiple concurrent roles. When changing from one role to another, the characteristics and capabilities of the new role replace the capabilities of the previous role.

Crypto Officer Role
The TOE supports a Crypto Officer Role. The Crypto Officer role is the role used during the initial secure configuration of the TOE. The Crypto Officer role is authenticated using a Configuration Password. For simplicity of initial configuration, Mercury Systems ships *ASURRE*-Stor® SSDs with no Configuration Password. The Crypto Officer is responsible for installing the initial Configuration Password during the initial secure configuration procedure.

User Role
The TOE supports a User Role for a single user. The TOE enters a fully functional User Role from power-on only after completing a successful authentication. User authentication consists of supplying the correct password in Mode 1 or a password and a BLACK key in Mode 6.

After successful authentication in the User Role, the TOE 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.

25 Product Updates

The *ASURRE*-Stor® SSD supports a service to update the internal firmware after an authentication to verify the digital signature of the new firmware. The signature validation process verifies that the new firmware was signed by and originated from Mercury Systems. The process uses ECDSA, (Elliptical Curve Digital Signature Algorithm) with a P521 prime curve. The TOE performs signature verification before accepting new firmware. As an extra security precaution, the TOE erases all user data as part of the firmware update process.

Firmware updates are released by Mercury Systems in the following forms:

(a) MDU Utility
The new firmware is embedded into the MDU utility itself. Updating the TOE firmware is simple; from the MDU main screen, press the “Change Firmware…” button and follow the onscreen instructions.

(b) Firmware File
The firmware file is provided to update the firmware via the ATA DOWNLOAD MICROCODE command. The host executes a series of ATA DOWNLOAD MICROCODE commands to update the TOE firmware; the ATA-7 specification defines the ATA DOWNLOAD MICROCODE command.

Mercury Systems makes firmware updates available to customers using a secure FTP login with a unique user name and password. The FTP site is managed by Mercury Systems. Contact your Mercury Systems sales representative to have a FTP login name and password generated.

26 Physical Security

The ***ASURRE*-Stor®** SSD includes physical security features that meet the physical security requirements of FIPS 140-2 level 2. Physical security features of the TOE include:

- The TOE enclosure consists of an opaque 2 piece structure held together with several screws.
- The heads of two exposed enclosure corner screws are filled an custom orange material that obscures a custom screw head pattern. Tamper evidence consists of damaged/removed orange material covering the 2 exposed corner screws, exposed screw heads, damage to the enclosure screws or damage to the enclosure.
- All components in the TOE 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 TOE enclosure include a 90 degree angle to prevent easy probe access.
- The TOE includes a difficult to duplicate holographic label located in the center of the front side main product label. While not intended as a tamper seal, the holographic label can be difficult to remove and will show signs of tearing or discoloration if improperly handled during a tamper event. Mercury Systems uses the custom label as an aid to help identify potential counterfeit units in the field.

27 Electromagnetic Interference and Compatibility (EMI/EMC)

The TOE 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.

28 Mitigation of Other Attacks Policy

The TOE does not mitigate any other attacks.

29 Security Guidance Summary

The following security guidance may be useful when using the ***ASURRE-Stor***® SSD in mission critical applications:

- The TOE can be configured to operate in one of several modes of operation. The modes of operation differ in how the TOE DEK is established and stored. Only 2 modes are CC compliant and covered by the CC evaluation.
    a) Self-generated random Permanent key with ATA Password (Mode 1).
    b) KEK with BLACK key and ATA Password (Mode 6).

  Administrators and Crypto Officers performing the initial secure configuration must configure the TOE into one of these two modes to ensure that the TOE is CC compliant.
- The Crypto Officer **shall** inspect each TOE carefully for any signs of tampering that may have occurred during shipment from Mercury Systems. Any TOE that shows signs of tampering should be returned to Mercury Systems.
- The Crypto Officer **shall** perform the initial secure configuration of the TOE prior to deploying the unit to the field.
- The Crypto Officer **shall** make no assumptions as to default values for any configurable TOE 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 to 64, 8-bit bytes.
- The Crypto Officer **shall** select the option to disable Firmware Updates. This option prevents an attacker from attempting to change to a different firmware version in the field.
- The Crypto Officer **shall** enforce the use of 8 character minimum password lengths for the User ATA Password, Master ATA Password. Be aware that the security strength of passwords is directly proportional to the length of the password and the number of bits per character as shown in Table 8.

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 8: Password strength in bits

- The Crypto Officer **shall** enable and configure the Authentication Penalty Count to a value of 1, 5, 10 or 15 and inform users that the TOE allows a limited number of failed authentication attempts before executing a penalty to clear keys, and all user data in the TOE. The failed attempts counter increments for invalid ATA Passwords, Configuration Passwords, key values, and invalid signatures during firmware updates.
- The Crypto Officer **shall** enable and configure the initial User ATA Password and Master ATA Password in both CC compliant modes.
- The Crypto Officer **shall** disable intermediate power-savings modes in both CC compliant modes. This option prevents the TOE from entering into a power state other than D0 or D3.
- The Crypto Officer **shall** setup a security inspection policy to inspect the TOE for evidence of enclosure tampering a minimum of once per year. Tamper evidence appears as enclosure dents, marring, 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 (Figure 9, 10, 11) covering 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 shiny and smooth. The orange colored material is slightly UV reactive and will glow yellow/orange under UV LED light. After a 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 9: Screw head in daylight

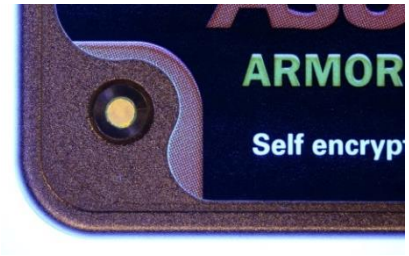

Figure 11: Screw head in UV light

Figure 10: 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 can show signs of damage such as tearing, discoloration or other damage if improperly handled during a tamper event. Refer to the label image in Figure 1.
- The Crypto Officer Role or User Role can command the TOE to perform power-on self-test suite by cycling power or using the ATA EXECUTE DEVICE DIAGNOSTIC and the SMART OFF-LINE-IMMEDIATE commands. Refer to the ATA7 specification for more details.
- The TOE, by design, does not output key values or passwords under any conditions.
- The Crypto Officer should ensure the host system does not include firmware that captures and stores the ATA User and Master password information external to the TOE. For lost password recovery, some BIOS manufacturer's save the ATA password information, which creates a backdoor to the password and breaks the security of the system.

30 Change log

Revision	By	Description
Rev. 1.5.0.00	Bob Laz.	11/21/2016 Numerous changes to support operation with an AA profile. Changes are highlighted in yellow. 06/26/2017 Very minor change, fixed spelling error in Section 3. (TEO should have been TOE). Changed document data on cover pager to 6/26/2017 Changed footer to reflect new date 6/26/2017 8/16/2017 Added references to the SSD Secure Configuration Programmer's Guide in section 16 and in the reference documents list, Table 2. Changed dates in Footer to August 2017 and cover sheet to August 16, 2017. 8/23/17 Modified per Evaluation findings.
Rev. 1.5.1	Bob Laz. Sabrina Piña	8/21/2019 Updates for re-certification. Document Dates, footers, and cPP versions updated. 11/25/2019 Updated Mercury logo, document dates, TOC, header, and footer. Updated sections 7, 18, and 29 to describe the management of power-saving states. Improved section 29 to better identify the secure configuration steps as requirements by bolding the shall text. Added section 20 to describe how to change the User or Master ATA password after initial TOE configuration. 12/30/2019 Updated section 25 to describe changing firmware using a file provided by Mercury Systems and the ATA DOWNLOAD MICROCODE command. 2/4/2020 Updated document dates and copyright on cover page and footer. Updated section 29 to warn Crypto Officers about BIOS manufacturer's that capture and store ATA password information for lost password recovery. Improved the description of Mode 6 set up on page 7 to add clarity on how the BEV(KEK) is created and used.