National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Mercury Systems, Inc.

ASURRE-Stor™ Solid State Self-Encrypting Drive Hardware revision 3.0, Firmware revision 1.5.0

Report Number: CCEVS-VR-10783-2017
Dated: **25 August 2017**
Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Panel

James J Donndelinger

Kenneth B Elliott III

Herbert J Ellis

The Aerospace Corporation, Columbia, MD

Common Criteria Testing Laboratory

Kenji Yoshino

Ryan Day

UL Verification Services Inc.

San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the Mercury Systems, Inc. ASURRE-Stor™ Solid State Self-Encrypting Drive Hardware revision 3.0, Firmware revision 1.5.0.

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The TOE functions as a standard 2.5" SATA self-encrypting solid state hard drive. The TOE is a solid state device that stores all user data in encrypted form. This provides secure storage of data and facilitates rapid cryptographic erasure via sanitization of the encryption key. The TOE incorporates functionality to perform both acquisition of the authorization information (a password, or a password and a black key) as well as data encryption.

This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
Host System	Serial ATA revision 2.6 compatible host.
Admin Utility / Host Interface Software	Configuration and Operational SW that sends the correct ATA commands to the TOE. Mercury provides the Mercury Drive Utility (MDU) that can be used for configuration, but is not considered part of the TOE.
Serial Key Loader	(optional) Key load device for loading keys over the serial port.

Table 1: Operational Environment Components

2 Identification of the TOE

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE), the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	ASURRE-StorTM Solid State Self-Encrypting Drive Hardware revision 3.0, Firmware revision 1.5.0
Protection Profile	collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 1.0, dated January 26, 2015 collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 1.0, January 26, 2015
Security Target	Security Target for Mercury Systems ASURRE-Stor™ Solid State Self-Encrypting Drives, Version 1.0, August 21, 2017
Dates of Evaluation	July 2016 – August 2017
Conformance Result	Pass
Common Criteria Version	3.1 Revision 4
Common Evaluation Methodology (CEM) Version	CCMB-2012-09-004
Evaluation Technical Report (ETR)	17-3660-R-0007 V1.2
Sponsor/Developer	Mercury Systems, Inc.
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc.
CCTL Evaluators	Kenji Yoshino, Ryan Day
CCEVS Validators	James J Donndelinger, Kenneth B Elliott, Herbert J Ellis

Table 2: Product Identification

3 Technical Decisions

All technical decisions issued by the Full Disk Encryption Interpretations Team (FIT) at the time of the issuance of the certificate were applied. These were captured in FDE Interpretations #201701

(describes evaluation activities necessary for FCS_CKM.4 for the EE cPP), #201702 (allows hardcoded (in addition to the existing configurable) number of failed BEV validation attempts before key zeroization), and #201703 (allows selection of any of the P-256, P-384, or P-521 curves instead of requiring P-256 and P-384).

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

- Cryptographic Support
- User Data Protection
- Security Management
- Protection of the TSF

4.1 Cryptographic Support

The TOE utilizes the following cryptographic algorithms:

- AES-XTS-256 – Encryption/decryption of stored data.
- DRBG – Generation of cryptographic keys.
- AES Key Wrap – Encryption/decryption of cryptographic keys.
- SHA-512 – DRBG, HMAC, and ECDSA primitive.
- PBKDF – Derivation of a key from a user provided password.
- ECDSA – Verification of firmware updates.

All algorithms, except for PBKDF, were validated by the CAVP.

4.2 User Data Protection

The TOE uses the XTS-AES-256 algorithm to encrypt all user data on the drive. The TOE does not write any plaintext user data to persistent storage.

4.3 Security Management

The TOE allows authorized users to change the data encryption key (DEK), cryptographically erase the DEK, initiate firmware updates, import wrapped DEK, change passwords, and configure cryptographic functionality. This is accomplished by commands made available at the device's SATA interface. The user has to either provide a means to send those commands to the interface, or use the vendor's Mercury Systems Drive Utility (MDU) Windows-based GUI to issue the commands to the interface.

4.4 Protection of the TSF

The TOE protects itself by running a suite of self-tests at power-up, authenticating firmware and by not providing any mechanism to export any key values. The customer is encouraged to externally fill keys so that an unpowered module contains no CSP information that would lead to

compromise of the encrypted data at rest. Beyond self-tests and crypto KATs, the module has numerous continuously running checks built into the C code and the VHDL code. Whenever an error is detected, (corruption, impossible states, out of range values, extra bytes in queues, etc.) that might compromise the security of the module, the module sets a flag and resets. This eliminates any CSP values in FPGA RAM and renews/reloads logic in the FPGA.

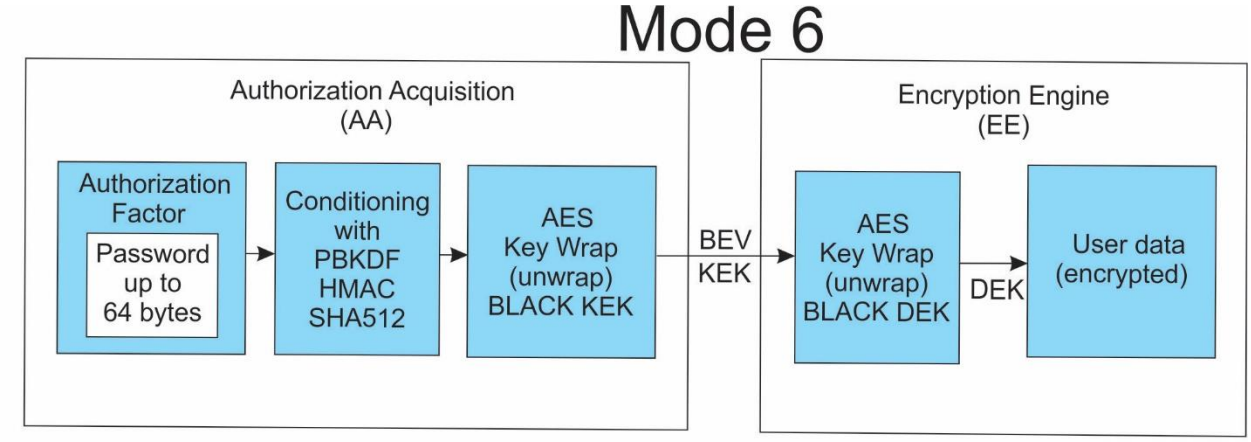
5 Architectural Information

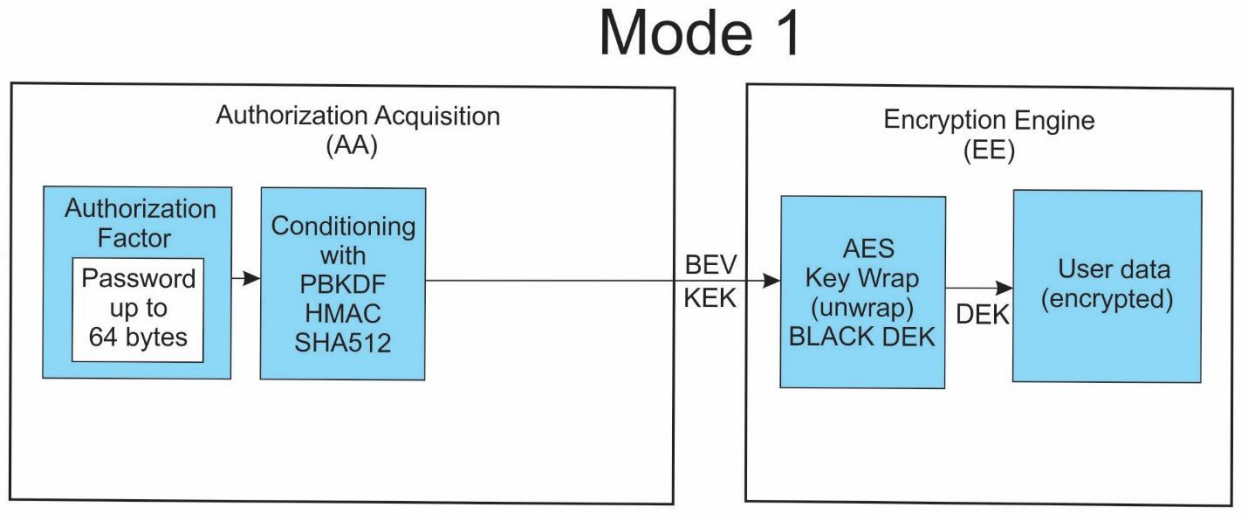
The TOE consists of firmware revision 1.5.0 and hardware revision 3.0 of the following models:

- ASD256AM2R
- ASD512AM2R
- ADR256AM2R
- ADR512AM2R

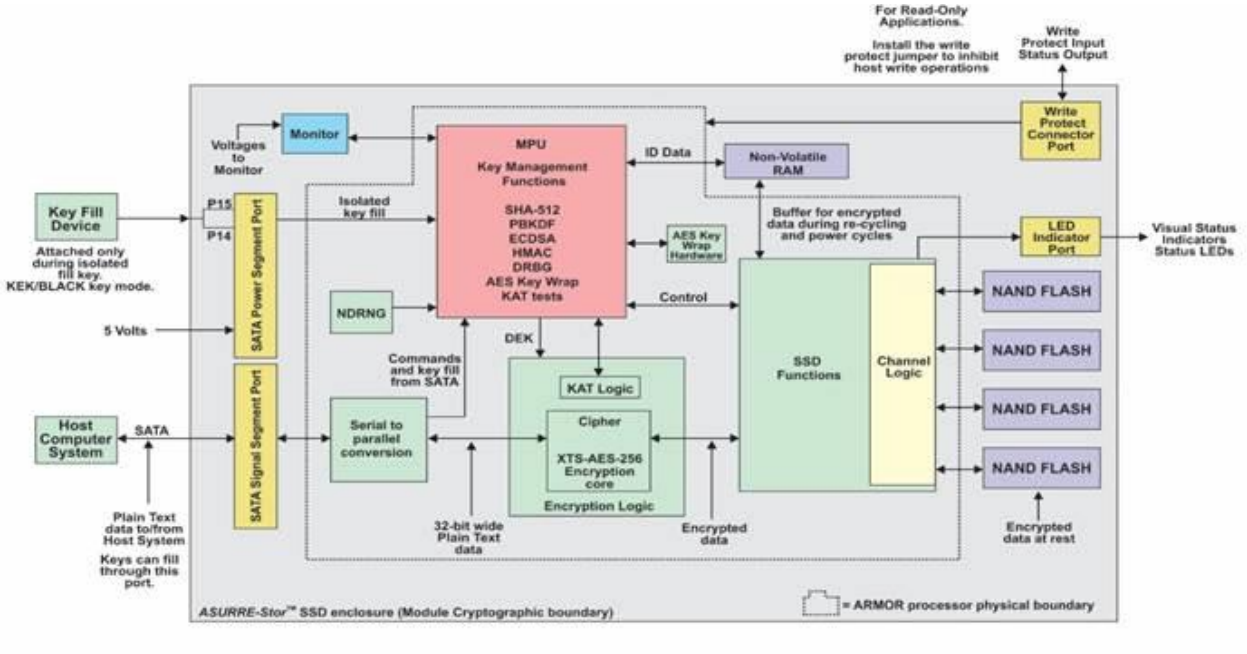
The TOE is a solid state SATA (revision 2.6) hard drive whose interface conforms to the ATA7 specification. There is no external software or firmware that runs on a host that is part of the TOE; the interface presented by the TOE is the SATA interface.

The TOE can be operated (in the evaluated configuration) in one of two modes: Mode 1 requiring a password, and Mode 6 requiring a password and Black KEK. The operations in these modes are depicted below:





The internal architecture of the device is depicted below, showing the SATA interface, internal computational components, and notional data flow internal to the TOE:



6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the ASURRE-Stor™ Solid State Self-Encrypting Drive. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.

The vendor documents that apply to the CC evaluation are identified below:

6.1 Design Documentation

Document	Revision	Date
Mercury Systems ASURRE-Stor™ ASD256/512, and ADR256/512 Solid State Self-Encrypting Drives Entropy Assessment	1.5.0.00	February 1, 2017
ASURRE-Stor™ ASD256-512 and ADR256/512 Solid State Self-Encrypting Drives Key Management Description (KMD)	1.5.0.00	June 26, 2017

6.2 Guidance Documentation

Document	Revision	Date
Mercury Systems ASURRE-Stor™ SSD Non—Non-Proprietary Administrative Guidance	1.5.0.00	August 23, 2017
SSD Secure Configuration Programmer's Guide	1.5.0.00	August 17, 2017

6.3 Security Target

Document	Revision	Date
Security Target for Mercury Systems ASURRE-Stor™ Solid State Self-Encrypting Drives	1.0	August 21, 2017

7 IT Product Testing

This section describes the testing efforts of the Evaluation Team.

7.1 Evaluation Team Independent Testing

The evaluation team performed the test assurance activities specified in the collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 1.0, January 26, 2015 and collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 1.0, January 26, 2015. The evaluation team verified that the TOE passed each test.

Because of the nature of the TOE, the test setup was very straightforward, and consisted of a Windows 7 Enterprise host that connected to the TOE through a standard SATA cable. All testing was performed on the ASD512AM2R, except for FPT_DSK_EXT.1. The different models only differ in capacity and ratio of overprovisioning. Installation, confirmation, firmware update, authentication, entropy, and encryption are the same across all models. The evaluators performed FDP_DSK_EXT.1 testing on all four models, because the test is related to storage and requires data to be written to the highest logical address (which is different for each model).

Testing was performed using a combination of the vendor-provided MDU configuration utility and specialized test scripts that were written at the level of the SATA interface. The evaluators verified that the MDU configuration utility properly invoked the TOE (SATA) interface in performing the tests required by the cPPs.

7.2 Vulnerability Analysis

A public domain (cvedetails.com) search for potential vulnerabilities was performed using the following search terms:

- Altera Nios II Processor

- Asurre-Stor
- Mercury Systems, Inc.
- Microsemi
- ARMOR processor

No potential vulnerabilities were identified that might apply to the TOE.

8 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in both the AA and EE collaborative Protection Profiles. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation against the CEM are recorded in the Evaluation Technical Report (ETR), which is controlled by the UL CCTL. The security assurance requirements are listed in the following table.

Assurance Component ID	**Assurance Component Name**
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, the appropriate CEM work units, and correctly verified that the product meets the claims in the ST.

9 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation.

Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and firmware versions identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
5. The following specific product capabilities are excluded from use in the evaluated configuration:
    a. Non-FIPS 140-2 mode of operation—this mode of operation allows cryptographic operations that are not FIPS-approved
    b. Encryption Modes other than 1 and 6—the device has the capability for several operational modes; however, only modes 1 and 6 were evaluated.
6. The TOE administrative interface is the SATA interface and what was evaluated against the administrative-related requirements (e.g., FMT_SMF). No software or tools (e.g., the MDU configuration utility) that were used during testing are part of the TOE.

10 Validator Comments/Recommendations

While the TOE is a SED that can be used in a variety of situations, one key use case is as a SED for a mission system, where the device is configured using one host system (not the mission system), and then installed in the mission system where different host hardware and software are used to communicate with the TOE. While the vendor provides a utility (the MDU configuration tool) that can be used to perform some of the configuration functions that are described in the ST, the actual TOE administrative interface is at the SATA level. The MDU is not part of the TOE, so it was not comprehensively evaluated against the applicable requirements of the AA cPP. It was used in testing however, and the evaluators did provide analysis to demonstrate that it was invoking the TOE administrative interface appropriately, and that the TOE correctly implemented the administrative functions specified in the ST.

While the public-facing admin guide gives a good overview of the functions that need to be performed in order to accomplish the required configuration actions, in some cases specific pointers to the Secure Configuration Programmer's Guide are not present. The procedures are contained in the Secure Configuration Guide, however, and were exercised during the evaluation.

11 Terms

11.1 Acronyms

CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MDU	Mercury Drive Utility
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SED	Self-Encrypting Drive
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

12 Bibliography

The following lists the applicable documentation in addition to that specified in Section 6.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, Version 3.1 Revision 4, CCMB-2012-09-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, September 2012, Version 3.1, Revision 4, CCMB-2012-09-004.

[5] collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 1.0, January 26, 2015.

[6] Supporting Document Mandatory Technical Document Full Drive Encryption: Encryption Engine, Version 1.0, February 2015.

[7] collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 1.0, January 26, 2015.

[8] Supporting Document Mandatory Technical Document Full Drive Encryption: Authorization Acquisition, Version 1.0, February 2015.