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 1.5.1

Report Number: CCEVS-VR-11041-2020
Dated: **03/06/2020**
Version: **1.2**

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

John Butterworth

The MITRE Corporation

David Challener

John Hopkins Applied Physics Laboratory

Richard George

John Hopkins Applied Physics Laboratory

Jerome Myers

The Aerospace Corporation

Common Criteria Testing Laboratory

Gerrit Kruitbosch

Oleg Andrianov

Lucas Shaffer

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 1.5.1.

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.

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	Configuration SW that sends the correct ATA commands to the TOE. Mercury provides the Mercury Drive Utility (MDU) that can be used.
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-Stor™ Solid State Self-Encrypting Drive Hardware revision 3.0, Firmware revision 1.5.1
Protection Profile	collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019
Security Target	Security Target for Mercury Systems ASURRE-Stor™ Solid State Self-Encrypting Drive, Version 1.1, February 6, 2020
Dates of Evaluation	July 2019 – March 2020
Conformance Result	Pass
Common Criteria Version	3.1 Revision 5
Common Evaluation Methodology (CEM) Version	CCMB-2017-04-004
Evaluation Technical Report (ETR)	20-3516-R-0002 V1.1
Sponsor/Developer	Mercury Systems, Inc.
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc.
CCTL Evaluators	Oleg Andrianov, Gerrit Kruitbosch, Lucas Shaffer
CCEVS Validators	John Butterworth, David Challener, Richard George, Jerome Myers

Table 2: Product Identification

3 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

3.1 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.

3.2 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.

3.3 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.

3.4 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 a 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.

4 Assumptions, Threats, Clarification of scope

4.1 Secure Usage Assumptions and Threats

The Security Problem Definition, including the assumptions and threats, may be found in the following documents:

- collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019
- collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019

4.2 Organizational Security Policies

The TOE does not enforce any OSPs.

4.3 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in Protection Profile(s) and performed by the Evaluation team).
- 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.
- The TOE consist of hardware and firmware and do not rely on the operational environment for any supporting security functionality.
- 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.
- The TOE must be installed, configured and managed as described in the documentation referenced in Section 7.2 of this Validation Report.

5 Architectural Information

The TOE is classified as Self-Encrypting Drive (SED) for Common Criteria purposes. The TOE is made up of hardware and firmware components.

The TOE functions as a standard 2.5” SATA self-encrypting solid state hard drive. The physical embodiment conforms to the EIA SFF-8201 specification. The electrical and software interface is the Serial ATA revision 2.6 specification.

The TOE consists of firmware revision 1.5.1 and hardware revision 3.0 of the following models:

- ASD256AM2R
- ASD512AM2R
- ADR256AM2R
- ADR512AM2R

6 Evaluated configuration

The evaluated configuration consists of TOE when installed and configured in accordance with the documents listed in Section 7.2 in bold type. Note that only the procedures described in the Non-proprietary Admin Guide are required to put the TOE in the evaluated configuration; the proprietary Programmer's Guide is not required.

7 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.

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

7.1 Design Documentation

Document	Revision	Date
ASURRE-Stor™ ASD256/512 and ADR256/512 Solid State Self-Encrypting Drives Key Management Description (KMD)	1.5.1.00	December 18, 2019
Entropy Analysis Report	1.2	September 30, 2019
Mercury Systems ASURRE-StorTM SSD Non-Proprietary Addendum to Entropy Report	N/A	October 17, 2019

7.2 Guidance Documentation

The guidance documentation examined during the evaluation and delivered with the TOE and considered part of the TOE as follows. Note that even though the Programmer's guide is delivered with the TOE, it is a proprietary document and is not required to install, administer, or use the TOE in its evaluated configuration.

Document	Revision	Date
Mercury Systems ASURRE-Stor® ASD256/512 and ADR256/512 Solid State Self-Encrypting Drives Non-Proprietary Administrative Guidance	**1.5.1**	**February 4, 2020**

Document	Revision	Date
SSD Secure Configuration Programmer's Guide ASURRE-Stor™ FIPS 140-2, CC (CSfC) 256 GB and 512 GB Solid State Drives	**1.5.1.00**	**November 21, 2019**

Documentation, that are available to the customers, but not required for TOE secure configuration and operation and were not part of evaluation are as follows:

Document	Revision	Date
MDU User's Guide	1.5.1.0	November 21, 2019
SSD Programmer's Guide	1.5.1.0	February 06, 2020
SSD User's Hardware Setup Guide	1.5.1.0	December 12, 2016

This evaluation provides no assurance of any additional documentation provided with the product, or which may be available online, that was not included in the scope of the evaluation. Only the documentation that was part of the evaluation may be trusted for the purpose of installing, administering, or using the product in its evaluated configuration.

7.3 Security Target

Document	Revision	Date
Security Target for Mercury Systems ASURRE-Stor™ Solid State Self-Encrypting Drive	1.1	February 6, 2020

8 IT Product Testing

This section describes the testing efforts of the Evaluation Team. No evidence of developer testing is required in the Assurance Activities for this product.

8.1 Evaluation Team Independent Testing

The evaluation team in conjunction with the developer performed the test assurance activities specified in the collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190102, February 1, 2019 and collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019. The evaluation team verified that the TOE passed each test. A description of the test configuration, test tools and test assurance activities can be found in the Assurance Activity Report.

8.2 Vulnerability Analysis

A public domain search for potential vulnerabilities was performed as prescribed by [6] and [8]. The terms used for the search were as follows: Assure-stor, Mercury, Armor, ASD512AM2R, NIOS, Altera, Drive encryption, Disk encryption, key destruction, key sanitization, SED, Self-encrypting, OPAL. No potential vulnerabilities were identified that apply to the TOE. A description of this assurance activity and a listing of the CVE identifiers for the specific vulnerabilities considered can be found in Section 3.5 of the Assurance Activity Report.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.

UL has determined that the TOE meets the security criteria in the Security Target, which specifies an assurance level of “PP Compliant”. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in January 2020.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR’s within the Security Target was evaluated. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The validators also recommend that users be aware that, despite the TOE itself being capable of accepting any 8-bit byte as a character in a password or passphrase, an external interface collecting this input may accept only a reduced subset of the 8-bit range, thus reducing the potential complexity of the input.

11 Security Target

Security Target for Mercury Systems ASURRE-Stor™ Solid State Self-Encrypting Drives, Version 1.1, February 6, 2020.

12 Terms

12.1 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

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, Version 3.1 Revision 5, CCMB-2017-04-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, April 2017, Version 3.1, Revision 5, CCMB-2017-04-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, April 2017, Version 3.1, Revision 5, CCMB-2017-04-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.

[5] collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019.

[6] Supporting Document Mandatory Technical Document Full Drive Encryption: Encryption Engine, Version 2.0 + Errata 20190201, February 2019.

[7] collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019.

[8] Supporting Document Mandatory Technical Document Full Drive Encryption: Authorization Acquisition, Version 2.0 + Errata 20190201, February 2019.