National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 1.0, January 26, 2015

Report Number:	**CCEVS-VR-PP-0038**
Dated:	**5 September 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

Common Criteria Testing Laboratory

Base and Additional Requirements
UL Verification Services Inc.
709 Fiero Lane, Suite 25
San Luis Obispo, CA 93401

Table of Contents

Table of Tables

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Security Requirements for the collaborative Protection Profile for Full Drive Encryption - Encryption Engine (version 1.0), also referred to ascPPFDEEE10. It presents a summary of the cPPFDEEE10 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the cPPFDEEE10 was performed concurrent with the first product evaluation against the cPP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Full Drive Encryption - Encryption Engine. The evaluation was performed by UL Verification Services, Inc. Common Criteria Testing Laboratory (CCTL) in San Luis Obispo, California, United States of America, and was completed in August 2017. This evaluation addressed the base requirements of the cPPFDEEE10, as well as additional requirements contained in the appendices.

Additional review of the cPP to confirm that it meets the claimed APE assurance requirements was performed independently by the VR author as part of the completion of this VR.

The evaluation determined that the cPPFDEEE10 is both Common Criteria Part 2 Extended and Part 3 Conformant. The cPP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). Because the ST contains material drawn directly from the cPPFDEEE10, performance of the majority of ASE work units serves to satisfy the APE work units as well.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the cPPFDEEE10 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the assurance activity report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTL). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the cPP.

In order to promote thoroughness and efficiency, the evaluation of the cPPFDEEE10 was performed concurrent with the first product evaluation against the cPP. In this case the TOE for this first product was the Full Drive Encryption - Encryption Engine. The evaluation was performed by UL Verification Services, Inc. in San Luis Obispo, California, United States of America, and was completed in August 2017.

The cPPFDEEE10 contains a set of "base" requirements that all conformant STs must include, and in addition, contains "Optional" and "Selection-based" requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in the base requirements and the capabilities of the TOE.

Because these discretionary requirements may not be included in a particular ST, the initial use of the cPP will address (in terms of the cPP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the cPPFDEEE10 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the cPP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this cPP, as well as subsequent evaluations that address additional optional requirements in the cPPFDEEE10.

Protection Profile	*collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 1.0, 26 January 2015*
ST (Base)	*Security Target for Mercury Systems* *ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target, Version 1.0, August 21, 2017*
Assurance Activity Report (Base)	*Assurance Activity Report VID 10783 17-3660-R-0008, Version 1.2, August 24, 2017*
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTL	UL Verification Services, San Luis Obispo, CA
CCEVS Validators	James J. Donndelinger, The Aerospace Corporation Kenneth B. Elliot, The Aerospace Corporation Herbert J. Ellis, The Aerospace Corporation

3 cPPFDEEE10 Description

The cPPFDEEE10 is a cPP that describes security requirements for the Full Drive Encryption - Encryption Engine. The TOE is the Encryption Engine or a combined evaluation of both Authorization Acquisition and Encryption Engine. The Encryption Engine manages both the encryption and decryption of data on a storage device. Compliant TOEs will manage the encryption and decryption of data on a storage device, provide key management, conduct authorization checks and policy enforcement, and erase cryptographic data. This is ultimately used to handle the cryptographic aspects of self-encrypting hard disk drives.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
A.TRUSTED_CHANNEL	Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure. In cases in which a single product fulfils both cPPs, then the communication between the components does not extend beyond the boundary of the TOE (e.g., communication path is within the TOE boundary). In cases in which independent products satisfy the requirements of the AA and EE, the physically close proximity of the two products during their operation means that the threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.
A.INITIAL_DRIVE_STATE	Users enable Full Drive Encryption on a newly provisioned storage device free of protected data in areas not targeted for encryption. It is also assumed that data intended for protection should not be on the targeted storage media until after provisioning. The cPP does not intend to include requirements to find all the areas on storage devices that potentially contain protected data. In some cases, it may not be possible - for example, data contained in "bad" sectors. While inadvertent exposure to data contained in bad sectors or un-partitioned space is unlikely, one may use forensics tools to recover data from such areas of the storage device. Consequently, the cPP assumes bad sectors, unpartitioned space, and areas that must contain unencrypted code (e.g., MBR and AA/EE pre-authentication software) contain no protected data.
A.TRAINED_USER	Users follow the provided guidance for securing the TOE and authorization factors. This includes conformance with authorization factor strength, using external token authentication factors for no other purpose and ensuring external token authorization factors are securely stored separately from the storage device and/or platform. The user should also be trained on how to power off their system.
A.PLATFORM_STATE	The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.
A.POWER_DOWN	The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off. This properly clears memories and locks down the device, so memory remnant attacks are infeasible. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile

Assumption Name	Assumption Definition
	storage (e.g., Lockscreen or sleep state). Users power the platform and/or storage device down or place it into a power managed state, such as a “hibernation mode”.
A.STRONG_CRYPTO	All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG.

4.2 Threats

The threats listed below are addressed by the cPPFDEEE10.

Table 2: Threats

Threat Name	Threat Definition
T.UNAUTHORIZED_DATA_ACCESS	The cPP addresses the primary threat of unauthorized disclosure of protected data stored on a storage device. If an adversary obtains a lost or stolen storage device (e.g., a storage device contained in a laptop or a portable external storage device), they may attempt to connect a targeted storage device to a host of which they have complete control and have raw access to the storage device (e.g., to specified disk sectors, to specified blocks).
T.KEYING_MATERIAL_COMPROMISE	Possession of any of the keys, authorization factors, submasks, and random numbers or any other values that contribute to the creation of keys or authorization factors could allow an unauthorized user to defeat the encryption. The cPP considers possession of keying material of equal importance to the data itself. Threat agents may look for keying material in unencrypted sectors of the storage device and on other peripherals in the operating environment (OE), e.g. BIOS configuration, SPI flash, or TPMs.
T.AUTHORIZATION_GUESSING	Threat agents may exercise host software to repeatedly guess authorization factors, such as passwords and PINs. Successful guessing of the authorization factors may cause the TOE to release DEKs or otherwise put it in a state in which it discloses protected data to unauthorized users.
T.KEYSPACE_EXHAUST	Threat agents may perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms and/or parameters allow attackers to exhaust the key space through brute force and give them unauthorized access to the data.
T.KNOWN_PLAINTEXT	Threat agents know plaintext in regions of storage devices, especially in uninitialized regions (all zeroes) as well as regions that contain well known software such as operating systems. A poor choice of encryption algorithms, encryption modes, and initialization vectors along with known plaintext could allow an attacker to recover the effective DEK, thus providing unauthorized access to the previously unknown plaintext on the storage device.
T.CHOSEN_PLAINTEXT	Threat agents may trick authorized users into storing chosen plaintext on the encrypted storage device in the form of an image, document, or some other file. A poor choice of encryption algorithms, encryption modes, and initialization

Threat Name	Threat Definition
	vectors along with the chosen plaintext could allow attackers to recover the effective DEK, thus providing unauthorized access to the previously unknown plaintext on the storage device.
T.UNAUTHORIZED_UPDATE	Threat agents may attempt to perform an update of the product which compromises the security features of the TOE. Poorly chosen update protocols, signature generation and verification algorithms, and parameters may allow attackers to install software that bypasses the intended security features and provides them unauthorized access to data.

4.3 Organizational Security Policies

No organizational policies have been identified that are specific to the TOE described by this cPP.

4.4 Security Objectives

The following table contains objectives for the Operational Environment.

Table 3: Security Objectives for the Operational Environment

Environmental Security Obj.	Environmental Security Objective Definition
OE.TRUSTED_CHANNEL	Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure.
OE.INITIAL_DRIVE_STATE	The OE provides a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption.
OE.PASSPHRASE_STRENGTH	An authorized administrator will be responsible for ensuring that the passphrase authorization factor conforms to guidance from the Enterprise using the TOE.
OE.POWER_DOWN	Volatile memory is cleared after entering a Compliant power saving state or turned off so memory remnant attacks are infeasible.
OE.SINGLE_USE_ET	External tokens that contain authorization factors will be used for no other purpose than to store the external token authorization factor.
OE.STRONG_ENVIRONMENT_CRYPTO	The Operating Environment will provide a cryptographic function capability that is commensurate with the requirements and capabilities of the TOE and Appendix A.
OE.TRAINED_USERS	Authorized users will be properly trained and follow all guidance for securing the TOE and authorization factors.

5 Requirements

As indicated above, requirements in the cPPFDEEE10 are comprised of the “**Base**” requirements and additional requirements that are conditionally optional. The following are table contains the “base” requirements that were validated as part of the Full Drive Encryption – Encryption Engine evaluation activity referenced above.

Table 4: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM.1 Cryptographic Key Generation (Data Encryption Key)	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FCS_CKM_EXT.4 Cryptographic Key and Key Material Destruction	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FCS_CKM.4 Cryptographic Key Destruction	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FCS_KYC_EXT.2 Key Chaining	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FCS_SMV_EXT.1 Validation	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
FDP: User Data Protection	FDP_DSK_EXT.1 Protection of Data on Disk	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
FMT: Security Management	FMT_SMF.1 Specification of Management Functions	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
FPT: Protection of the TSF	FPT_KYP_EXT.1 Protection of Key and Key Material	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FPT_TST_EXT.1 TSF Testing	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FPT_TUD_EXT.1 Trusted Update	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Table 5: Optional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_KDF_EXT.1 Cryptographic Key Derivation	
	FCS_CKM.1(b) Cryptographic Key Generation (Asymmetric Keys)	
	FCS_COP.1(a) Cryptographic Operation (Signature Verification)	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FCS_COP.1(c) Cryptographic Operation (Keyed Hash Algorithm)	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FCS_COP.1(e) Cryptographic Operation (Key Transport)	
	FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption)	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FCS_COP.1(g) Cryptographic Operation (Key Encryption)	
	FCS_SMC_EXT.1 Submask Combining	

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Table 6: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	FCS_COP.1(d) Cryptographic Operation (Key Wrapping)	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target

There are no "**Objective**" requirements defined for this cPP.

6 Assurance Requirements

The following are the assurance requirements contained in the cPPFDEEE10:

Table 7: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	ASE_ECD.1: Extended Components Definition	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	ASE_INT.1: ST Introduction	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	ASE_OBJ.1: Security Objectives for the Operational Environment	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	ASE_REQ.1: Stated Security Requirements	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	ASE_SPD.1: Security Problem Definition	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	ASE_TSS.1: TOE Summary Specification	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
ADV: Development	ADV_FSP.1 Basic Functional Specification	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	AGD_PRE.1: Preparative Procedures	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
	ALC_CMS.1: TOE CM Coverage	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
ATE: Tests	ATE_IND.1: Independent Testing - Sample	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target

7 Results of the Evaluation

Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

Table 8: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
APE_ECD.1	Pass	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
APE_INT.1	Pass	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
APE_OBJ.1	Pass	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target
APE_REQ.1	Pass	ASURRE-Stor^{TM} Solid State Self-Encrypting Drives Security Target

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the cPPFDEEE10 Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 4, dated: September 2012.

[5] UL Verification Services Inc., *Assurance Activity Report VID 10783 17-3660-R-0008*, Version 1.2, 24 August 2017.

[6] UL Verification Services Inc., *Security Target for Mercury Systems ASURRE-Stor^{TM} Solid State Self-Encrypting Drives*, Version 1.0, 21 August 2017.

[7] *Full Drive Encryption – Encryption Engine Protection Profile*, Version 1.0, 26 January 2015

[8] *Full Drive Encryption: Encryption Engine Supporting Document*, Version 1.0, January 2015