National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

collaborative Protection Profile for Full Drive Encryption – Encryption Engine

Version 2.0+Errata 20190201

26 April 2019

Report Number: **CCEVS-VR-PP-0048**
Dated: **26 April 2019**
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
Leidos, Inc. Common Criteria Testing Laboratory
Columbia, Maryland

Additional Requirements
Gossamer Security Solutions Common Criteria Testing Laboratory
Catonsville, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0, (FDEEEcPP), It presents a summary of the FDEEEcPP and the evaluation results.

The evaluation of the FDEEEcPP was performed concurrent with the first two product evaluations against the cPP's requirements. In this case the Target of Evaluations (TOEs) were the:

1. Seagate Secure TCG SSC Self-Encrypting Drives, performed by Leidos Inc. in Columbia, MD, United States of America.
2. Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer, performed by Gossamer Security Solutions in Catonsville, Maryland, United States of America.

These evaluations addressed the base requirements of the FDEEEcPP, and most of the additional requirements contained in Appendices A and B.

An additional review of the cPP was performed independently by the Validation Report (VR) author as part of the completion of this VR, to confirm that it meets the claimed APE assurance requirements.

The evaluation determined that the FDEEEcPP is both Common Criteria Part 2 Extended and Part 3 Conformant. The cPP identified in this VR has been evaluated at NIAP approved CCTLs using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). Because the ST contains only material drawn directly from the FDEEEcPP, the majority of the ASE work units served to satisfy the APE work units as well.

The initial results by the validation team found that the evaluation showed that the FDEEEcPP did not meet the requirements of the APE components. These findings were confirmed by the VR author and NIAP. NIAP notified the Full Disk Encryption international Technical Community (FDE iTC) of all noted deficiencies. The FDE iTC updated the cPP and determined the impact of the changes were typographical errors related to the conventions for indicating assignments and selections and did not affect the security functionality of the PP. Subsequently, the FDE iTC corrected all deficiencies, incorporated all technical decisions, and published the FDEEEcPP 2.0 + Errata 20190201. NIAP reviewed the Errata and confirmed all changes were made. As a result, the validation team found that the evaluation confirmed that the FDEEEcPP 2.0 + Errata 20190201 meets the requirements of the APE components.

NIAP also reviewed each previously evaluated product and confirmed the changes did not impact the security functionality of the products. Therefore, the evaluated products also comply with the FDEEEcPP 2.0 + Erratta 20190201. Note that this is true despite the fact that the FDEEEcPP 2.0 + Errata 20190201 conforms to Common Criteria v3.1, Release 5, while the previous FDEEEcPP 2.0 conformed to Release 4; the changes between releases did not impact the relevant evaluations.

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 CCTLs. CCTLs evaluate products against cPPs that contain 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 FDEEEcPP was performed concurrent with the first two product evaluation against the cPP's requirements. In this case the Target of Evaluations (TOEs) were the:

1. Seagate Secure TCG SSC Self-Encrypting Drives, performed by Leidos Inc. in Columbia, MD, United States of America;
2. Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer, performed by Gossamer Security Solutions in Catonsville, Maryland, United States of America.

These evaluations addressed the base requirements of the FDEEEcPP, and most of the additional requirements contained in Appendices A and B.

The FDEEEcPP contains a set of "base" requirements that all conformant STs must include, and additionally 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 FDEEEcPP 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 when that occurs.

The following identifies the cPP subject of the evaluation/validation, as well as the supporting information from the evaluation performed against this cPP and any subsequent evaluations that address additional optional and/or selection-based requirements in the FDEEEcPP.

Protection Profiles	collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0, 09 September 2016 collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, 01 February 2019

ST (Base)	Seagate Secure TCG SSC Self-Encrypting Drives Security Target, Version 1.0, 04 April 2018. Curtis-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer (FDEEEcPP20/FDEAAcPP20) Security Target, Version 0.7, 14 August 2018
Assurance Activity Report (Base)	Seagate Secure TCG SSC Self-Encrypting Drives Assurance Activity Report, Version 1.2, 04 April 2018. Assurance Activity Report (FDEEEcPP20/FDEAAcPP20) for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer, Version .3, 14 August 2018.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTLs	Leidos, Inc., Columbia, MD, USA Gossamer Security Solutions, Catonsville, MD, USA

3 FDEEEcPP Description

The FDEEEcPP specifies information security requirements for full drive encryption engines, as well as the assumptions, threats, organizational security policies, objectives, and requirements of a compliant TOE.

A full drive encryption engine in the context of the cPP is a device composed of software and/or hardware that provides requirements for Data-at-Rest protection for a lost device that contains storage. The form factor for a storage device may vary, but could include: system hard drives/solid state drives in servers, workstations, laptops, mobile devices, tablets, and external media. A hardware solution could be a Self-Encrypting Drive or other hardware-based solutions; the interface (USB, SATA, etc.) used to connect the storage device to the host machine is outside the scope. The requirements for the Encryption Engine includes encryption/decryption of the data by the DEK, proper handling of cryptographic keys, updates performed in a trusted manner, audit and self-tests.

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, un-partitioned 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 the device is in a Compliant power saving state or has fully powered off. This properly clears memories and locks down the device. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen 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.

A.PHYSICAL	The platform is assumed to be physically protected in its Operational Environment and not subject to physical attacks that compromise the security and/or interfere with the platform's correct operation.

4.2 Threats

The following table contains applicable threats.

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 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.
T.UNAUTHORIZED_FIRMWARE_UPDATE	An attacker attempts to replace the 24 firmware on the SED via a command from the AA or from the host platform with a malicious 25 firmware update that may compromise the security features of the TOE.
T.UNAUTHORIZED_FIRMWARE_MODIFY	An attacker attempts to modify the firmware in the SED via a command from the AA or from the host platform that may compromise the security features of the TOE.

4.3 Organizational Security Policies

The following table contains applicable organizational security policies.

Table 3: Organizational Security Policies

Threat Name	Threat Definition
There are no organizational security policies addressed by this cPP.	

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
There are no listed security objectives for the TOE.	

The following table contains security objectives for the Operational Environment.

Table 5: 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.TRAINED_USERS	Authorized users will be properly trained and follow all guidance for securing the TOE and authorization factors.
OE.PHYSICAL	The Operational Environment will provide a secure physical computing space such that an adversary is not able to make modifications to the environment or to the TOE itself.

5 Requirements

As indicated above, requirements in the FDEEEcPP are comprised of the "base" requirements and additional requirements that are conditionally optional. The following table contains the "base" requirements that were validated as part of the Seagate and Curtis-Wright evaluation activities referenced above.

Table 6: Base Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM.1(c): Cryptographic Key Generation (Data Encryption Key)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_CKM.4(a): Cryptographic Key Destruction (Power Management)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_CKM_EXT.4(a): Cryptographic Key and Key Material Destruction (Destruction Timing)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_CKM_EXT.4(b): Cryptographic Key and Key Material Destruction (Power Management)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_CKM_EXT.6: Cryptographic Key Destruction Types	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_KYC_EXT.2: Key Chaining (Recipient)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_SNI_EXT.1: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_VAL_EXT.1: Validation	Seagate Secure TCG SSC Self-Encrypting Drives
FDP: User Data Protection	FDP_DSK_EXT.1: Protection of Data on Disk	Seagate Secure TCG SSC Self-Encrypting Drives
FMT: Security Management	FMT_SMF.1: Specification of Management Functions	Seagate Secure TCG SSC Self-Encrypting Drives
FPT: Protection of the TSF	FPT_KYP_EXT.1: Protection of Key and Key Material	Seagate Secure TCG SSC Self-Encrypting Drives
	FPT_PWR_EXT.1: Power Saving States	Seagate Secure TCG SSC Self-Encrypting Drives
	FPT_PWR_EXT.2: Timing of Power Saving States	Seagate Secure TCG SSC Self-Encrypting Drives

	FPT_TST_EXT.1: TSF Testing	Seagate Secure TCG SSC Self-Encrypting Drives
	FPT_TUD_EXT.1: Trusted Update	Seagate Secure TCG SSC Self-Encrypting Drives

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 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
FPT: Protection of the TSF	FPT_FAC_EXT.1: Firmware Access Control	Seagate Secure TCG SSC Self-Encrypting Drives
	FPT_RBP_EXT.1: Rollback Protection	Seagate Secure TCG SSC Self-Encrypting Drives
FCS: Cryptographic Support	FCS_CKM.4(e): Cryptographic Key Destruction (Key Cryptographic Erase)	Seagate Secure TCG SSC Self-Encrypting Drives

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 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM.1(a): Cryptographic Key Generation (Asymmetric Keys)	PP Evaluation
	FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_CKM.4(b): Cryptographic Key Destruction (TOE-Controlled Hardware)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_CKM.4(c): Cryptographic Key Destruction (General Hardware)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_CKM.4(d): Cryptographic Key Destruction (Software TOE, 3rd Party Storage)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_COP.1(a): Cryptographic Operation (Signature Verification)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_COP.1(b): Cryptographic Operation (Hash Algorithm)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_COP.1(c): Cryptographic Operation (Message Authentication)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_COP.1(d): Cryptographic Operation (Key Wrapping)	Seagate Secure TCG SSC Self-Encrypting Drives

	FCS_COP.1(e): Cryptographic Operation (Key Transport)	PP Evaluation
	FCS_COP.1(f): Cryptographic Operation (AES Data Encryption/Decryption)	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_COP.1(g): Cryptographic Operation (Key Encryption)	Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer
	FCS_KDF_EXT.1: Cryptographic Key Derivation	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_RBG_EXT.1: Random Bit Generation	Seagate Secure TCG SSC Self-Encrypting Drives
	FCS_SMC_EXT.1: Submask Combining	PP Evaluation
FPT: Protection of the TSF	FPT_FUA_EXT.1: Firmware Update Authentication	Seagate Secure TCG SSC Self-Encrypting Drives

6 Assurance Requirements

The following are the assurance requirements contained in the FDEEEcPP.

Table 9: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	Seagate Secure TCG SSC Self-Encrypting Drives
	ASE_ECD.1: Extended Components Definition	Seagate Secure TCG SSC Self-Encrypting Drives
	ASE_INT.1: ST Introduction	Seagate Secure TCG SSC Self-Encrypting Drives
	ASE_OBJ.1: Security Objectives for the Operational Environment	Seagate Secure TCG SSC Self-Encrypting Drives
	ASE_REQ.1: Stated Security Requirements	Seagate Secure TCG SSC Self-Encrypting Drives
	ASE_SPD.1: Security Problem Definition	Seagate Secure TCG SSC Self-Encrypting Drives
	ASE_TSS.1: TOE Summary Specification	Seagate Secure TCG SSC Self-Encrypting Drives
ADV: Development	ADV_FSP.1 Basic Functional Specification	Seagate Secure TCG SSC Self-Encrypting Drives
AGD: Guidance Documents	AGD_OPE.1: Operational User Guidance	Seagate Secure TCG SSC Self-Encrypting Drives
	AGD_PRE.1: Preparative Procedures	Seagate Secure TCG SSC Self-Encrypting Drives
ALC: Life-cycle Support	ALC_CMC.1: Labeling of the TOE	Seagate Secure TCG SSC Self-Encrypting Drives
	ALC_CMS.1: TOE CM Coverage	Seagate Secure TCG SSC Self-Encrypting Drives
ATE: Tests	ATE_IND.1: Independent Testing - Sample	Seagate Secure TCG SSC Self-Encrypting Drives

AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	Seagate Secure TCG SSC Self-Encrypting Drives

7 Results of the Evaluation

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

Table 10: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	Seagate Secure TCG SSC Self-Encrypting Drives; PP evaluation
APE_ECD.1	Pass	Seagate Secure TCG SSC Self-Encrypting Drives; PP evaluation
APE_INT.1	Pass	Seagate Secure TCG SSC Self-Encrypting Drives; PP evaluation
APE_OBJ.1	Pass	Seagate Secure TCG SSC Self-Encrypting Drives; PP evaluation
APE_REQ.1	Pass	Seagate Secure TCG SSC Self-Encrypting Drives; PP evaluation
APE_SPD.1	Pass	Seagate Secure TCG SSC Self-Encrypting Drives; PP evaluation

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 FDEEEcPP 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.
- **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 VR:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] Seagate Secure TCG SSC Self-Encrypting Drives Security Target (cppfdeee20), Version 1.0, 04 April 2018.

[7] Seagate Secure TCG SSC Self-Encrypting Drives Assurance Activity Report (cppfdeee20), Version 1.2, 04 April 2018.

[8] *collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0, 09 September 2016.

[9] *collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata 20190201, 01 February 2019.

[10] Curtis-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer (FDEEEcPP20/FDEAAcPP20) Security Target, Version 0.6, 18 October 2018.

[11] Assurance Activity Report (FDEEEcPP20/FDEAAcPP20) for Curtiss-Wright Defense Solutions Data Transport System 1-Slot Software Encryption Layer, Version 0.3, 18 October 2018.