National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Protection Profile for Software Full Disk Encryption, Version 1.1

Report Number: CCEVS-VR-PP-0003
Dated: 7 April 2014
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 Requirements
Leidos (formerly SAIC)
Columbia, 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 Protection Profile for Software Full Disk Encryption, Version 1.1 (SWFDEPP). It presents a summary of the SWFDEPP and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the SWFDEPP was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Microsoft Windows 8, Microsoft Windows Server 2012 capability (provided primarily by BitLocker). The evaluation was performed by the Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in April 2014. This evaluation addressed the base requirements as well as additional requirements in Appendix C of the SWFDEPP.

The information in this report is largely derived from the Evaluation Technical Report (ETR), written by the CCTL listed above.

The evaluation determined that the SWFDE is both **Common Criteria Part 2 Extended and Part 3 Conformant**. The PP 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 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 3). Because the ST contains only material drawn directly from the SWFDEPP, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme 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 SWFDEPP meets the requirements of the APE components. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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 (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the SWFDEPP was performed concurrent with the first product evaluation against the PP. In this case the TOE

for this first product was the Microsoft Windows 8, Microsoft Windows Server 2012 capability (provided primarily by BitLocker). The evaluation was performed by the Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in April 2014.

The SWFDEPP contains a set of "base" requirements that all conformant STs must include, and in addition contain a set of "optional" requirements that may be included based on the selections made in the base requirements and the capabilities of the TOE. Because the optional requirements do not have to be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any optional requirements that are incorporated into the that initial ST. Subsequently, TOEs that are evaluated against the SWFDEPP that incorporate optional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and the appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP; it will be amended as subsequent evaluations address additional optional requirements in the SWFDEPP.

Protection Profile	*Protection Profile for Software Full Disk Encryption, Version 1.1, 07 April 2014*
ST (Base)	Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption Security Target, Version 1.0, April 3, 2014
Evaluation Technical Report (Base)	Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption Security Target, Version 1.0, 29 July 2013
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL (Base and Additional)	Leidos (formerly SAIC), Columbia, MD
CCEVS Validators	Ken Elliott, The Aerospace Corporation

3 SWFDE Description

The SWFDE PP addresses the threat that an adversary will obtain a lost or stolen hard disk (e.g., a disk contained in a laptop or a portable external hard disk drive) containing sensitive data. The Target of Evaluation (TOE) defined in the Protection Profile (PP) is for a software full disk encryption product that encrypts the data on the hard disk device. As defined in NIST SP 800-111: "*Full Disk Encryption (FDE)*, also known as whole disk encryption, is the process of encrypting all the data on the hard drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication to the FDE product." Note that software encryption products will leave a portion of the drive unencrypted for the Master Boot Record (MBR) and the initial

bootable partition. For this Protection Profile, the term “disk encryption” will be interpreted as per the NIST definition of full disk encryption modified to allow software disk encryption products to leave a portion of the drive unencrypted for the MBR and bootable partition so long as no information is written there that could contain user data.

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: TOE Assumptions

Assumption	Description of Assumption
A.AUTHORIZED_USER	Authorized users will follow all provided user guidance, including keeping passphrases and external tokens secure and stored separately from the disk.
A.ET_AUTH_USE_ONLY	External tokens that contain authorization factors will be used for no other purpose than to store the external token authorization factor.
A.PASSPHRASE_BASED_ AUTH_FACTOR	An authorized administrator will be responsible for ensuring that the passphrase authorization factor has sufficient strength and entropy to reflect the sensitivity of the data being protected.
A.PLATFORM_I&A	The TOE will be installed on a platform that supports individual user identification and authentication. This I&A functionality shall remain unaffected by the TOE.
A.PROTECT_INTEGRITY	The user will exercise due diligence in physically protecting the TOE, and ensuring the IT environment will sufficiently protect against logical attacks.
A.SHUTDOWN	An authorized user will not leave the machine in a mode where sensitive information persists in non-volatile storage (e.g., power it down or enter a power managed state, such as a “hibernation mode”).
A.TRAINED_ ADMINISTRATORS	Authorized administrators are appropriately trained and follow all administrator guidance.

4.2 Threats

A threat consists of a threat agent, an asset and an adverse action of that threat agent on that asset.

The threat agents are the entities that put the assets at risk if an adversary obtains a lost or stolen hard disk. For instance, a threat in the chart below is T.UNAUTHORIZED_DISK_ACCESS. The threat agent is the possessor (unauthorized user) of a lost or stolen hard disk. The asset is the data on the storage device, while the adverse action is to attempt to obtain those data from the hard disk. This threat drives the functional requirements for the disk encryptor (TOE) to authorize who can use the TOE to access the hard disk and encrypt/decrypt the data. Since possession of the KEK, DEK, intermediate 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, keying material is considered equivalent to the data in importance and is the other asset addressed in the threat table.

It is important to reemphasize at this point that the product (TOE) is not expected in general to defend against the possessor of the lost or stolen hard disk who can introduce malicious code or exploitable hardware components into the Target of Evaluation (TOE) or the Operational Environment. It is assumed that the user will ensure the TOE is physically protected and that the Operational Environment provides sufficient protection against logical attacks. One specific area where some protection is offered by conformant TOEs is in providing updates to the TOE; other than this area, though, no countermeasures are mandated by this PP. Similarly, these requirements do not address the "lost and found" hard disk problem, where an adversary may have taken the hard disk, compromised the unencrypted portions of the boot device (e.g., MBR, boot partition), and then made it available to be recovered by the original user so that they would execute the compromised code.

Table 2: Threats

Threat	Description of Threat
T.KEYING_MATERIAL_ COMPROMISE	An attacker can obtain unencrypted key material (the KEK, the DEK, authorization factors, submasks, and random numbers or any other values from which a key is derived) that the TOE has written to persistent memory and use these values to gain access to user data.
T.PERSISTENT_INFORMATION	The TOE and/or the Operational Environment can go into a power saving mode so that the data or keying material are left unencrypted in persistent memory.
T.KEYSPACE_EXHAUST	An unauthorized user may attempt a brute force attack to determine cryptographic keys or authorization factors to gain unauthorized access to data or TOE resources.

T.TSF_ COMPROMISE	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted) to gain access to key material or user data.
T.UNAUTHORIZED_DISK_ACCESS	An unauthorized user that has access to the lost hard disk may gain access to data for which they are not authorized according to the TOE security policy.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.UNSAFE_AUTHFACTOR_VERIFICATION	An attacker can take advantage of an unsafe method for performing verification of an authorization factor, resulting in exposure of the KEK, DEK, or user data.

4.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. There are no organizational security policies for the SWFDEPP.

4.4 Security Objectives for the TOE

Table 4: Security Objectives for the TOE

Objective	Objective Description
O.AUTHORIZATION	The TOE must obtain the authorization factor(s) from a user to be able to decrypt the data on the hard disk.
O.CORRECT_TSF_OPERATION	The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF in its operational environment.
O.ENCRYPT_ALL	The TOE will encrypt all data that are stored on a hard drive. (Note that this may exclude the MBR and the bootable partition that it points to.)
O.DEK_SECURITY	The TOE will mask the DEK using a key encryption key (KEK) created from one or more submasks (which in turn are derived from the authorization

	factors) so that a threat agent who does not have authorization factor(s) will be unable to gain access to the user data by obtaining the DEK.
O.KEY_MATERIAL_COMPROMISE	The TOE will zeroize key material as soon as it is no longer needed to decrease the chance that such material could be used to discover a KEK or DEK.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.OWNERSHIP	The TOE shall ensure that ownership is taken (that is, a DEK is created, authorization factors are established, any default authorization factors are changed, a KEK is formed from the derived submasks, and the DEK is associated with the KEK) prior to any user data being accessible while the TOE is in operation.
O. SAFE_AUTHFACTOR_ VERIFICATION	The TOE shall perform verification of the authorization factors in such a way that the KEK, DEK, or user data are not inadvertently exposed.
O.TRUSTED_UPDATE	The TOE shall provide administrators the capability to update the TOE firmware/software, and verify that updates to the product are received from the intended source.

The following table contains objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

Objective	Objective Description
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.PLATFORM_I&A	The Operational Environment will provide individual user identification and authentication mechanisms that operate independently of the authorization factors used by the TOE.
OE.POWER_SAVE[1]	The Operational environment must be configurable so that there exists at least one mechanism that will cause the system to power down after a period of time in the same fashion as the user electing to shutdown the system. Any such mechanism (e.g., sleep, hibernate) that does not conform to this requirement must be capable of being disabled by the administrator.

[1] If the TOE encompasses the platform and there is no "operational environment", then the ST author renames this objective "O.POWER_SAVE" and modifies the description to begin "The TOE must be configurable so that there…" The rationale will also need to be updated.

OE.RESTRICTED_FUNCTIONS	Management functions will be limited to an authorized administrator.
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.

5 Requirements

As indicated above, requirements in the SWFDEPP are comprised of the "base" requirements (appearing in Section 4.1) and additional requirements appearing in Appendix C of the SWFDEPP. The following are table contains the "base" requirements that were validated as part of the Microsoft Windows evaluation activity referenced above.

Requirement Class	Requirement Component
FCS: Cryptographic support	FCS_CKM.1(1): Cryptographic Key Generation (DEK)
	FCS_CKM.1(2): Cryptographic Key Generation (KEK)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
FDP: User data protection	FDP_DSK_EXT.1: Extended: Protection of Data on Disk
FIA: Identification and authentication	FIA_AUT_EXT.1: Extended: FDE User Authorization
FMT: Security management	FMT_SMF.1: Specification of Management Functions
FPT: Protection of the TSF	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Extended: Trusted Update

The following table contains the "optional" requirements contained in Appendix C, 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.

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic support	FCS_COP.1(1): Cryptographic Operation (Disk Encryption)	Microsoft Windows 8 and Server 2012, 03 April 2014
	FCS_COP.1(2): Cryptographic Operation (Signature Verification)	Microsoft Windows 8 and Server 2012, 03 April 2014
	FCS_COP.1(3): Cryptographic Operation (Cryptographic Hashing)	Microsoft Windows 8 and Server 2012, 03 April 2014
	FCS_COP.1(4): Cryptographic Operation (Key Masking)	Microsoft Windows 8 and Server 2012, 03 April 2014
	FCS_RBG_EXT.1: Extended:	Microsoft Windows 8 and

Requirement Class	Requirement Component	Verified By
	Cryptographic Operation (Random Bit Generation)	Server 2012, 03 April 2014
	FCS_COP.1: Cryptographic Operation (Keyed Cryptographic Hashing)	
	FCS_CKM.1(Y): Cryptographic Key Generation (Passphrase formation and conditioning)	Microsoft Windows 8 and Server 2012, 03 April 2014
	FCS_CKM.1(Y): Cryptographic Key Generation (External token authorization factor generation)	Microsoft Windows 8 and Server 2012, 03 April 2014
FDP: User Data Protection	FDP_PM_EXT.1: Extended: Protection of Data in Power Managed States	Microsoft Windows 8 and Server 2012, 03 April 2014
FIA: User Authentication	FIA_UID.2: User identification before any action	
	FIA_UAU.2: User authentication before any action	

6 Assurance Requirements

The following are the assurance requirements contained in the SWFDEPP:

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. 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.

APE Requirement	Evaluation Verdict

APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.2	Pass

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 SWFDEPP 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 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Science Applications International Corporation. *Evaluation Technical Report for Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption Part 2 (Proprietary)*, Version 1.0. 29 July 2013.

[7] Microsoft Corporation. *Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption Security Target*, Version 1.0, April 3, 2014

[8] *Protection Profile for Software Full Disk Encryption*, Version 1.1, 31 March 2014