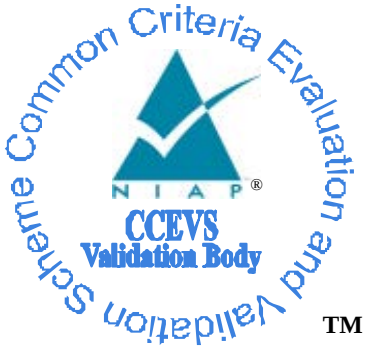
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



TM

Validation Report

Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption

Report Number: CCEVS-VR-VID10540-2014
Dated: 07 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

Validation Team

Members from

The Aerospace Corporation,
National Security Agency

Common Criteria Testing Laboratory

Leidos (formerly SAIC, Inc.)
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the Microsoft Windows 8 and Microsoft Windows Server 2012 Full Disk Encryption product was performed by 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 evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 and assurance activities specified in the Protection Profile for Software Full Disk Encryption, Version 1.1, 31 March 2014. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the product is conformant to the Protection Profile for Software Full Disk Encryption, Version 1.1, 31 March 2014. The information in this Validation Report is largely derived from the Assurance Activities Report, the Evaluation Technical Report (ETR), and associated test reports produced by the Leidos evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The focus of this evaluation is on BitLocker, which is part of the Windows 8 and Server 2012 operating systems. BitLocker encrypts fixed and removable disk volumes, including volumes that contain the operating system and user data. Access to the encrypted volume is protected by one or more protectors, also known as authorization factors, which are specified by the administrator for the computer.

Bitlocker offers a rich set of authorization factors, some of which were not covered by this evaluation. The following table presents the set of Bitlocker authorization factors supported for Windows 8 and Server 2012, and whether there use is covered by the evaluation in the evaluated configuration.

Protector	Input into the TOE by	Unlocks	Part of evaluated configuration?
TPM	TPM	Operating System Drive	No
TPM + PIN	TPM + keyboard	Operating System Drive	No
TPM + Start-up Key	TPM + USB	Operating System Drive	Yes
TPM + PIN + Start-up Key	TPM + keyboard + USB	Operating System Drive	Yes
TPM + Enhanced PIN	TPM + keyboard	Operating System Drive	No
TPM + Enhanced PIN + USB [Start-up Key]	TPM + keyboard + USB	Operating System Drive	Yes
External Key[1]	USB	Operating System Drive and Data Volume	Yes
Recovery Password	Keyboard	Operating System Drive and Data Volume	No
Clear Key	See Security Target	Operating System Drive	No
Passphrase	Keyboard	Data Volumes (and	Yes

[1] This can be startup key or a recovery key.

		Windows To Go) and Operating System Drive	
Public Key (RSA and ECDH)	Smart card	Data Volume	No

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption Security Target (ST).

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	Windows 8, Windows Server 2012
Sponsor:	Microsoft Corporation
Developer:	Microsoft Corporation
CCTL:	Leidos (formerly SAIC) 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	03 June 2013
Completion Date:	07 April 2014
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 4, September 2012.
Evaluation Class:	None
Description:	The TOE provides capabilities for encryption and decryption operating system storage volumes and data storage volumes using a variety of authorization factors.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

PP:	Protection Profile for Software Full Disk Encryption, Version 1.1, 31 March 2014
Evaluation Personnel:	Leidos (formerly SAIC): Anthony J. Apted Gary Grainger Pascal Patin Chris Keenan Jose Bell
Validation Body:	National Information Assurance Partnership, CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An attacker can obtain unencrypted key material (a Key Encrypting Key (KEK), the Disk Encryption Key (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.
- 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.
- 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.
- 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.
- 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.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- 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.

2 Identification

The evaluated product is **Microsoft Windows 8 and Microsoft Windows Server 2012**, with focus on **Bitlocker** that is part of these Windows operating systems.

3 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: *Much of the description of the security policy has been derived from the Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption Security Target and Final ETR.*

3.1 Cryptographic Protection

Windows provides FIPS-140-2 validated cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, cryptographic key agreement (which is not studied in this evaluation), and random number generation. The TOE additionally provides support for public keys, credential management and certificate validation functions and provides support for the National Security Agency's Suite B cryptographic algorithms. Windows also provides extensive auditing support of cryptographic operations, the ability to replace cryptographic functions and random number generators with alternative implementations,[2] and a key isolation service designed to limit the potential exposure of secret and private keys. In addition to supporting its own security functions with cryptographic support, the TOE offers access to the cryptographic support functions for user application programs. Public key certificates generated and used by the TOE authenticate users and machines as well as protect user and system data at rest.

- **Software-based disk encryption:** Windows implements BitLocker to provide encrypted data storage for fixed and removable volumes and protects the disk volume's encryption key with one or more intermediate keys and authorization factors.

3.2 User Data Protection

In the context of this evaluation, Windows provides encryption of fixed and removable volumes.

3.3 Identification & Authentication

In the context of this evaluation, Windows provides the ability to generate, store, and protect authorization factors which provide access to data on the encrypted fixed and removable volumes.

3.4 Security Management

Windows includes several functions to manage local and group security policies. Policy management is controlled through a combination of access control, membership in administrator groups, and privileges.

3.5 Protection of the TOE's Security Functions

Windows provides a number of features to ensure the protection of TOE security functions. Windows ensures process isolation security for all processes through private virtual address spaces, execution context, and security context. The Windows data structures defining process address space, execution context, memory protection, and security context are stored in protected kernel-mode memory. Windows 8 and Windows Server 2012 Windows includes self-testing features that ensure the integrity of executable TSF images and Windows cryptographic functions. Finally, Windows provides a trusted update mechanism to update Windows binaries itself.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- Authorized users will follow all provided user guidance, including keeping passphrases and external tokens secure and stored separately from the disk.

[2] This option is not included in the Windows Common Criteria evaluation.

- External tokens that contain authorization factors will be used for no other purpose than to store the external token authorization 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.
- 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.
- The user will exercise due diligence in physically protecting the TOE, and ensuring the IT environment will sufficiently protect against logical attacks.
- 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").
- Authorized administrators are appropriately trained and follow all administrator guidance.
- Authorization factors stored on a TPM device must be protected by a PIN, and the TPM device must implement an anti-hammer capability to prevent brute-force guessing attacks.

4.1 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 Protection Profile for Software Full Disk Encryption and performed by the evaluation team).
2. This evaluation covers only the specific product version identified in this document, and not any earlier or later versions released or in process.
3. 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 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target and guidance documentation.

The logical boundary of the TOE includes:

- The **Boot Manager**, which is invoked by the computer's bootstrapping code.
- The **Windows Loader** which loads the operating system into the computer's memory.
- **Windows OS Resume** which reloads an image of the executing operating system from a hibernation file as part of resuming from a hibernated state.
- The **Windows Kernel** which contains device drivers for the Windows NT File System, full volume encryption, the crash dump filter, and the kernel-mode cryptographic library.
- The **Cryptographic Services** module which confirms the signatures of Windows program files.

- **Windows Explorer** which can be used to manage BitLocker and check the integrity of Windows files and updates.
- The **manage-bde** console application to manage BitLocker.
- The **Get-AuthenticodeSignature PowerShell Cmdlet** which can be used to confirm the signatures of Windows program files.
- **PowerShell Cmdlets** to manage BitLocker:
    - **Add-BitLockerKeyProtector**
    - **Backup-BitLockerKeyProtector**
    - **Clear-BitLockerAutoUnlock**
    - **Disable-BitLocker**
    - **Disable-BitLockerAutoUnlock**
    - **Enable-BitLocker**
    - **Enable-BitLockerAutoUnlock**
    - **Get-BitLockerVolume**
    - **Lock-BitLocker**
    - **Remove-BitLockerKeyProtector**
    - **Resume-BitLocker**
    - **Suspend-BitLocker**
    - **Unlock-BitLocker**
- **Local and Group policies** to manage BitLocker
- The **Windows Trusted Installer which installs updates to the Windows operating system.**

Physically, each TOE tablet, workstation, or server consists of an x86 or x64 computer. The TOE executes on processors from Intel (x86 and x64), AMD (x86 and x64). The specific devices listed in the ST are:

- Microsoft Surface Pro, Intel Core i5, 64-bit
- Dell Optiplex 755, 3.0 GHz Intel Core 2 Duo E8400, 64-bit
- Dell Precision 690, 1.995 GHz Xeon Family 6 Model 15 Stepping 6, 64-bit

A set of devices may be attached as part of the TOE:

- Display Monitors
- Fixed Disk Drives (including disk drives and solid state drives)
- Removable Disk Drives (including USB storage)
- Network Adaptor
- Keyboard
- Mouse
- Printer
- Audio Adaptor
- CD-ROM Drive

- Smart Card Reader
- Trusted Platform Module (TPM) version 1.2 or 2.0.

While this set of devices is larger than is needed to evaluate BitLocker, it is the same set of devices as the General Purpose Operating System Protection Profile evaluation. By using the same set of devices for both evaluations, consumers can gain assurance by using both core OS capabilities and BitLocker in combination.

The TOE does not include any network infrastructure components.

6 Documentation

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- Microsoft Windows 8, Microsoft Windows Server 2012 Common Criteria Supplemental Admin Guidance for Software Full Disk Encryption
- On-line documentation referenced by the Supplemental Admin Guidance

7 Product Testing

This section describes the testing efforts of the Evaluation Team. It is derived from information contained in the Microsoft Windows 8 and Windows Server 2012 Software Full Disk Encryption Test Report and associated test script and test result documentation.

Evaluation team testing was conducted at the Leidos (formerly SAIC) CCTL in Columbia, MD.

7.1 Developer Testing

The assurance activities in the Protection Profile for Software Full Disk Encryption do not specify any requirement for developer testing of the TOE.

7.2 Evaluation Team Independent Testing

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the Protection Profile for Software Full Disk Encryption. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the Microsoft Windows 8 and Windows Server 2012 Software Full Disk Encryption Test Report. Tests were executed on all platforms claimed in the ST, with the exception of Windows Server 2012 Datacenter Edition, for which an equivalence argument to the Windows Server 2012 Standard Edition was provided. The tested platforms consisted of 7 combinations of the OS and hardware. While each test case was not executed on each test system, the evaluation team documented the subset of tests that ran on each system and justified the testing approach to the satisfaction of the validation team.

The testing demonstrated the TOE satisfies the security functional requirements specified in the Protection Profile for Software Full Disk Encryption.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any vulnerability applicable specifically to the TOE in its evaluated configuration.

The survey identified two vulnerabilities that potentially apply to full disk encryption products in general. The team determined the general potential vulnerabilities do not apply to the TOE in the operational environment specified in the ST.

8 Evaluated Configuration

The evaluated version of the TOE consists of the following:

The following Windows Operating Systems (OS):

- Microsoft Windows 8 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 8 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2012 Standard Edition
- Microsoft Windows Server 2012 Datacenter Edition

The following security updates and patches must be applied to the above Windows 8 products:

- All critical security updates published as of June 2013.

The following security updates must be applied to the above Windows Server 2012 products:

- All critical security updates published as of June 2013.

TOE Hardware Identification: The following real and virtualized hardware platforms and components are included in the evaluated configuration: \

- Microsoft Surface Pro, Intel Core i5, 64-bit
- Dell Optiplex 755, 3.0 GHz Intel Core 2 Duo E8400, 64-bit
- Dell Precision 690, 1.995 GHz Xeon Family 6 Model 15 Stepping 6, 64-bit

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the Protection Profile for Software Full Disk Encryption, in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

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 Protection Profile for Software Full Disk Encryption, and correctly verified that the product meets the claims in the ST.

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

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification

Assurance Component ID	Assurance Component Name
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

10 Validator Comments/Recommendations

The Protection Profile for Software Full Disk Encryption does not specify requirements for (nor call for an assessment of) any key escrow capability provided by compliant TOEs. The only capability specified and tested for compliant TOEs is the ability to configure the TOE such that any key escrow capability that happens to be provided can be "turned off."

The evaluated TOE allows recovery keys, which may appear to be a key escrow mechanism. However, as configured according to the administrative guidance and as described in the ST, such keys are only allowed if they are stored on a medium under the sole control of the user; in other words, they cannot be used as a "third-party escrow" capability, but rather as a recovery device for an individual user. Use as a third-party escrow mechanism (e.g., when they are stored in Active Directory) was not examined as part of this evaluation.

As indicated in the executive summary, several authorization factors are not covered by the evaluation. It is important to note that this limitation is imposed by the Protection Profile, and does not necessarily imply that there are issues with the authorization factors that are not supported in the evaluated configuration. Should an end user wish to use such authorization factors in their deployment, we recommend additional testing to ensure that their use and the protection they afford is commensurate with what is required in the end-user's environment.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption Security Target, Version 1.0, April 03, 2014.

13 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003.

4. Common Methodology for Information Technology Security: Evaluation Methodology, Version 3.1, Revision 4, September 2012, CCMB-2012-09-004.
5. Protection Profile for Software Full Disk Encryption, Version 1.1, 31 March 2014.
6. Microsoft Windows 8, Microsoft Windows Server 2012 Full Disk Encryption Security Target, Version 1.0, April 03, 2014.