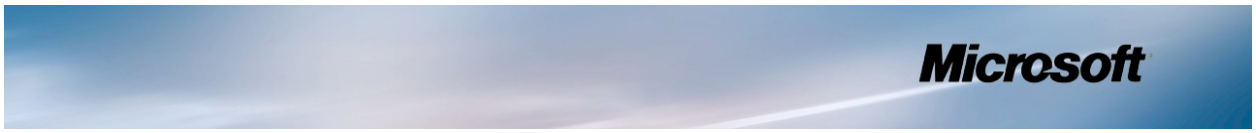


Non-proprietary Security Policy for FIPS 140-2 Validation

BitLocker® Dump Filter (dumpfve.sys) in Microsoft Windows 10 Pro Windows 10 Enterprise Windows 10 Mobile Windows 10 for Surface Hub

DOCUMENT INFORMATION

Version Number	1.5
Updated On	August 16, 2016

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

CHANGE HISTORY

Date	Version	Updated By	Change
26 OCT 2015	1.0	Tim Myers	First release to validators
11 MAR 2016	1.1	Tim Myers	Updates in response to comments
30 MAR 2016	1.2	Tim Myers	Updates in response to comments
30 APR 2016	1.3	Tim Myers	Updates in response to comments
6 MAY 2016	1.4	Tim Myers	Updates in response to comments
16 AUG 2016	1.5	Tim Myers	Added Windows 10 November 2015 Update and new platforms to OE

TABLE OF CONTENTS

1 Introduction

BitLocker® Drive Encryption is a data protection feature. BitLocker is Microsoft's response to one of our top customer requests: address the very real threats of data theft or exposure from lost, stolen or inappropriately decommissioned computer hardware with a tightly integrated solution in the Windows Operating System.

The Operational Environments (OEs) are:

- Windows 10 Enterprise (x64) running on a **Microsoft Surface Pro** with AES-NI
- Windows 10 Enterprise (x64) running on a **Microsoft Surface Pro 2** with AES-NI
- Windows 10 Enterprise (x64) running on a **Microsoft Surface Pro 3** with AES-NI
- Windows 10 Pro (x64) running on a **Microsoft Surface Pro** with AES-NI
- Windows 10 Pro (x64) running on a **Microsoft Surface Pro 2** with AES-NI
- Windows 10 Pro (x64) running on a **Microsoft Surface Pro 3** with AES-NI
- Windows 10 Enterprise (x64) running on a **Microsoft Surface 3** with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Enterprise (x86) running on a Dell Inspiron 660s without AES-NI or PCLMULQDQ or SSSE 3
- Windows 10 Pro (x86) running on a Dell Inspiron 660s without AES-NI or PCLMULQDQ or SSSE 3
- Windows 10 Enterprise (x64) running on a HP Compaq Pro 6305 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Pro (x64) running on a HP Compaq Pro 6305 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Mobile (ARMv7) running on a **Microsoft Lumia 950**
- Windows 10 Mobile (ARMv7) running on a **Microsoft Lumia 635**
- Windows 10 Enterprise (x64) running on a **Microsoft Surface Book** with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Pro (x64) running on a **Microsoft Surface Book** with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Enterprise (x64) running on a **Microsoft Surface Pro 4** with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Pro November 2015 Update (x64) running on a **Microsoft Surface Pro 4** with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 for Surface Hub (x64) running on a **Microsoft Surface Hub 84"** with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 for Surface Hub (x64) running on a **Microsoft Surface Hub 55"** with AES-NI and PCLMULQDQ and SSSE 3

herein referred to as Windows 10 OEs.

BitLocker prevents an attacker who boots another operating system or runs a software hacking tool from breaking Windows file and system protections or performing offline viewing of the files stored on the protected drive. This protection is achieved by encrypting the entire Windows volume. With BitLocker all user and system files are encrypted including the swap and hibernation files.

BitLocker ideally uses a Trusted Platform Module (TPM 1.2 or 2.0) to protect user data and to ensure that a computer running Windows 10 OEs has not been tampered with while the system was offline.

BitLocker provides its users enhanced data protection should their systems be lost or stolen, and more secure data deletion when it comes time to decommission those assets. BitLocker enhances data protection by bringing together two major sub-functions: full drive encryption and the integrity checking of early boot components.

Integrity checking the early boot components helps to ensure that data decryption is performed only if those components appear unmolested and that the encrypted drive is located in the original computer.

BitLocker offers the option to lock the normal boot process until the user supplies a PIN, much like an ATM card PIN, or inserts a USB flash drive that contains keying material. These additional security measures provide multi-factor authentication and assurance that the computer will not boot or resume from hibernation until the correct PIN or USB flash drive is presented.

This security policy document describes the BitLocker Dump Filter cryptographic module which protects hibernation files and crash dump files on BitLocker encrypted volumes. For BitLocker security policy details related to boot components, see the security policy documents for Boot Manager, Windows OS Loader, and Windows OS Resume.

1.1 List of Cryptographic Module Binary Executables

DUMPFVE.SYS – Version 10.0.10586 for Windows 10 OEs

1.2 Brief Module Description

The BitLocker Dump Filter is the full volume encryption (FVE) filter that sits in the system dump stack. Whenever the dump stack is called (in the event of a crash or for hibernation), this filter ensures that all data is encrypted before it gets written to the disk as a dump file or hibernation file. Figure 1 gives a visual representation of how this particular module fits into the overall BitLocker architecture and its connections to other related modules.

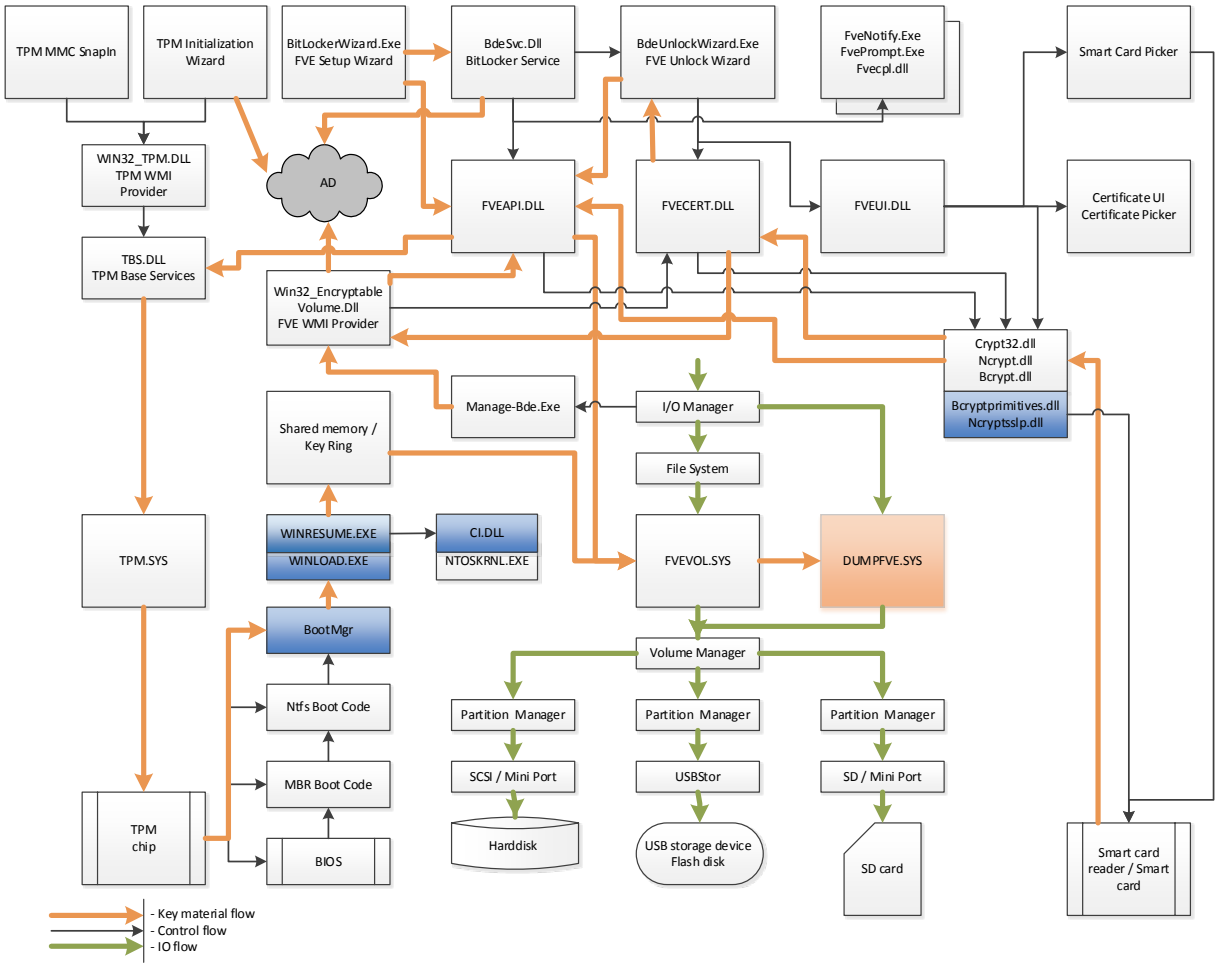


Figure 1 - Logical Operation of Module
(This module is orange; other related modules are blue.)

1.3 Validated Platforms

The BitLocker Dump Filter component listed in Section 1.1 was validated using the following machine configurations:

- Windows 10 Enterprise (x64) - **Microsoft Surface Pro** - Intel x64 Processor with AES-NI
- Windows 10 Enterprise (x64) - **Microsoft Surface Pro 2** - Intel Core i5 with AES-NI
- Windows 10 Enterprise (x64) - **Microsoft Surface Pro 3** - Intel Core i7 with AES-NI
- Windows 10 Pro (x64) - **Microsoft Surface Pro** - Intel x64 Processor with AES-NI
- Windows 10 Pro (x64) - **Microsoft Surface Pro 2** - Intel Core i5 with AES-NI
- Windows 10 Pro (x64) - **Microsoft Surface Pro 3** - Intel Core i7 with AES-NI
- Windows 10 Enterprise (x64) - **Microsoft Surface 3** - Intel Atom x7 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Enterprise (x86) - Dell Inspiron 660s - Intel Core i3 without AES-NI or PCLMULQDQ or SSSE 3
- Windows 10 Pro (x86) - Dell Inspiron 660s - Intel Core i3 without AES-NI or PCLMULQDQ or SSSE 3
- Windows 10 Enterprise (x64) - HP Compaq Pro 6305 - AMD A4 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Pro (x64) - HP Compaq Pro 6305 - AMD A4 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Mobile (ARMv7) - **Microsoft Lumia 950** - Qualcomm Snapdragon 808 (A57, A53)
- Windows 10 Mobile (ARMv7) - **Microsoft Lumia 635** - Qualcomm Snapdragon 400 (A7)
- Windows 10 Enterprise (x64) - **Microsoft Surface Book** - Intel Core i7 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Pro (x64) - **Microsoft Surface Book** - Intel Core i7 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Enterprise (x64) - **Microsoft Surface Pro 4** - Intel Core i5 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Pro (x64) - **Microsoft Surface Pro 4** - Intel Core i5 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 for Surface Hub (x64) - **Microsoft Surface Hub 84"** - Intel Core i7 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 for Surface Hub (x64) - **Microsoft Surface Hub 55"** - Intel Core i5 with AES-NI and PCLMULQDQ and SSSE 3

1.4 Cryptographic Boundary

The Windows 10 OEs BitLocker® Dump Filter cryptographic boundary consists solely of the BitLocker Dump Filter component, DUMPFVE.SYS. The physical configuration of the BitLocker Dump Filter, as defined in FIPS-140-2, is multi-chip standalone.

2 Security Policy

BitLocker Dump Filter operates under several rules that encapsulate its security policy.

- BitLocker Dump Filter is validated on Windows 10 OEs.

- Windows 10 OEs are operating systems supporting a “single user” mode where there is only one interactive user during a logon session.
- BitLocker Dump Filter is only in its Approved mode of operation when Windows is booted normally, meaning Debug mode is disabled and Driver Signing enforcement is enabled.
- The Debug mode status and Driver Signing enforcement status can be viewed by using the bcdedit tool.
- BitLocker Dump Filter is only in its Approved mode of operation when the “System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing” policy setting is enabled.
- BitLocker Dump Filter will only operate in compliance once BitLocker volume conversion (encryption) has completed and the volume is fully encrypted.
- BitLocker Dump Filter operates in FIPS mode of operation only when used with the FIPS 140-2 validated version of Windows 10 OEs Code Integrity (ci.dll) Cert. # 2604 operating in FIPS mode.

2.1 FIPS 140-2 Approved Algorithms

BitLocker Dump Filter implements the following FIPS 140-2 Approved algorithms.

- AES CBC 128 and 256, AES XTS[1] 128 and 256; AES CCM 256 (Cert. # 3629 and Cert. # 3653)

Note that not all of the algorithms and modes verified through the CAVP certificates listed are implemented by this module.

2.2 Cryptographic Bypass

Cryptographic bypass is not supported by BitLocker® Dump Filter.

2.3 Machine Configurations

BitLocker Dump Filter was tested using the machine configurations listed in Section 1.3 - Validated Platforms.

3 Operational Environment

The operational environment for BitLocker Dump Filter (DUMPFVE.SYS) is the Windows 10 OEs running on the software and hardware configurations listed in Section 1.3 - Validated Platforms.

4 Integrity Chain of Trust

Boot Manager is the start of the chain of trust for the collection of cryptographic modules that cooperate to provide the Windows feature called BitLocker®. Boot Manager cryptographically checks its own integrity during its startup. It then cryptographically checks the integrity of the Windows OS Loader or Windows OS Resume (if resuming from hibernation) before starting it. The Windows OS Loader or Windows OS Resume module then checks the integrity of the Code Integrity crypto module, the operating system kernel, and other boot stage binary images. Finally, the Code Integrity crypto module checks the integrity of the BitLocker Dump Filter.

[1] For XTS-AES the length of the data unit does not exceed 2^20 blocks. XTS-AES mode is only used by the module for the cryptographic protection of data on storage devices.

Code Integrity verifies the integrity of the BitLocker Dump Filter using the following FIPS-140-2 Approved algorithms.

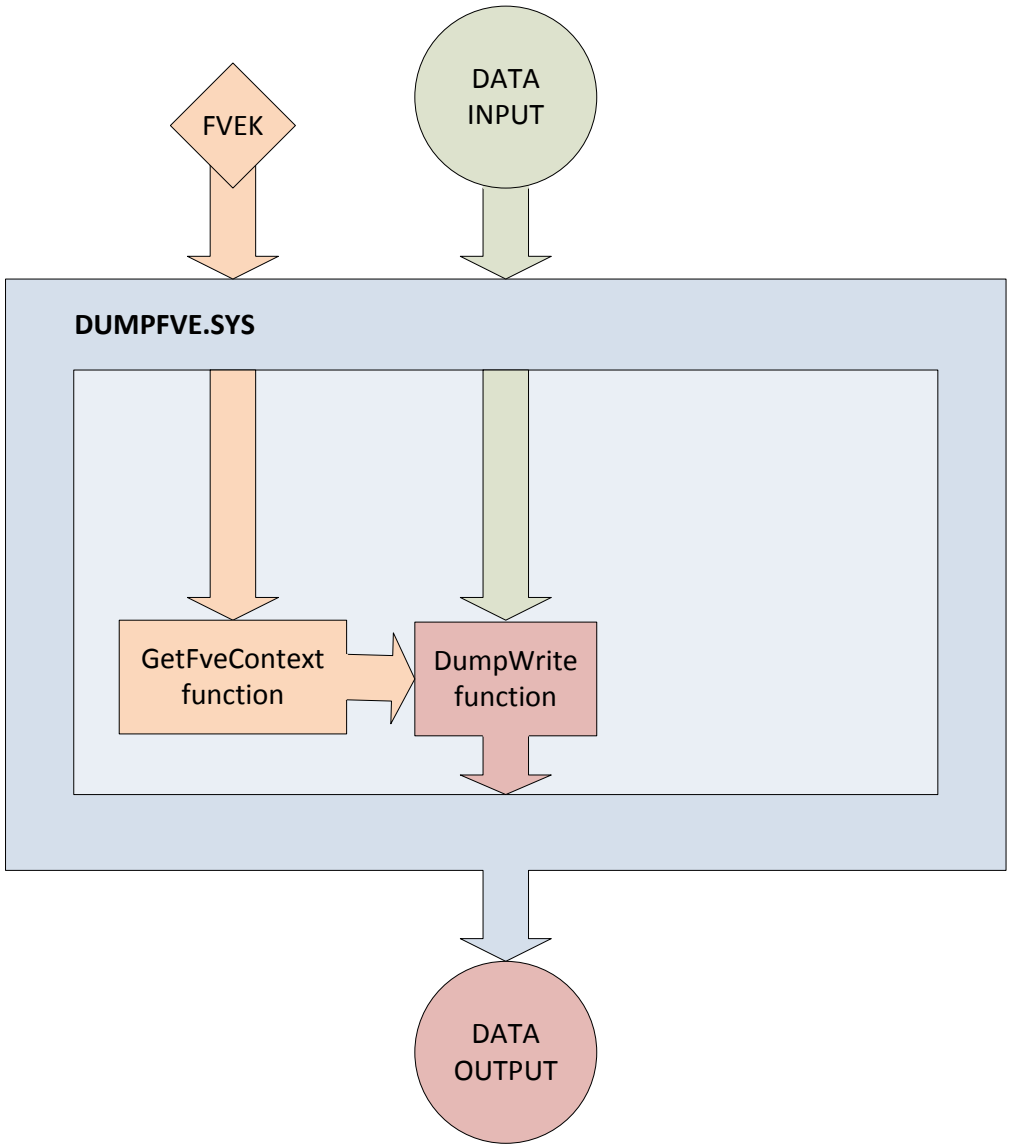
- RSA PKCS#1 (v1.5) verify with public key
- SHA-256 hash

BitLocker Dump Filter ensures that Windows 10 OEs crash dump files and/or hibernation files are encrypted on shutdown, thus ensuring the contents can only be accessed through the integrity chain of trust above.

5 Ports and Interfaces

The following block diagram show the interfaces and internal functions of the BitLocker Dump Filter (DUMPFVE.SYS) component. A Full Volume Encryption Key (FVEK) is one of the required inputs.

Figure 2 – BitLocker Dump Filter Block Diagram



5.1 Control Input Interface

The BitLocker Dump Filter module's control input interface consists of parameter interfaces for the GetFveContext and DumpWrite functions. These interfaces are not exported, but rather, are internal to the cryptographic module.

5.1.1 GetFveContext

```
NTSTATUS  GetFveContext(
        __in PFILTER_EXTENSION Context,
        __in ULONG MaxPagesPerWrite,
        __inout_xcount(FveContext->StructureSize) PFVE_CONTEXT FveContext
        )
```

This function gets the FVEK for the volume. The Context parameter supplies the dump stack filter context. The FveContext parameter supplies the internal FVE context, which includes the FVE status and FVEK in this context so it can be used later when writing data to the volume.

5.1.2 DumpWrite

```
NTSTATUS  DumpWrite(
            PFILTER_EXTENSION Context,
            PLARGE_INTEGER DiskByteOffset,
            PMDL Mdl
            )
```

This function uses the FVEK from the Context parameter that is provided by the GetFveContext interface. The DiskByteOffset parameter is used to specify the location on the volume to receive the encrypted output data. The Mdl parameter points to the input data to be encrypted.

5.2 Status Output Interface

The BitLocker Dump Filter status output is a return value of type NTSTATUS that indicates whether the function completed successfully or not.

The BitLocker Dump Filter has no status output interface for self-test errors. If the self-tests pass, the module is loaded. If not, the dump filter securely zeroes out memory for any keys handed to it and unloads itself.

5.3 Data Output Interface

The Data Output Interface is the data returned from the DumpWrite function.

This function is responsible for providing the encrypted content for the crash dump file or hibernate file. Data exits the module in the form of encrypted blocks that may be written to a crash dump file or a hibernation file on an encrypted volume.

5.4 Data Input Interface

The Data Input Interface includes the GetFveContext function and DumpWrite function. GetFveContext is responsible for reading the FVEK. DumpWrite accepts the memory blocks to encrypt with the FVEK and the target disk locations for the blocks as input.

6 Specification of Roles

BitLocker Dump Filter provides two different, implicitly assumed roles and a set of services (see Section 7 Services) particular to each of the roles. As a FIPS 140-2 level 1 validated product, BitLocker Dump Filter itself does not provide any authentication.

6.1 Maintenance Roles

Maintenance roles are not supported.

6.2 Multiple Concurrent Interactive Operators

There is only one interactive operator in Single User Mode. When run in this configuration, multiple concurrent interactive operators are not supported.

7 Services

Services are described below. This module does not export any cryptographic functions. The services are listed in the following table along with their associated cryptographic algorithms, critical security parameters (CSPs), and invocations.

Table 1

Service	Algorithms	CSPs	Invocation
Write encrypted crash dump file to an encrypted volume	AES CBC 128 and 256; AES XTS 128 and 256; AES CCM 256	Full Volume Encryption Key (FVEK)	This service is fully automatic. The User / Cryptographic Officer does not take any actions to explicitly start this service. This service is executed whenever the system crashes and must write the crash dump file to an encrypted volume.
Write encrypted hibernation file to an encrypted volume	AES CBC 128 and 256; AES XTS 128 and 256; AES CCM 256	Full Volume Encryption Key (FVEK)	This service is fully automatic. The User / Cryptographic Officer does not take any actions to explicitly start this service. This service is executed whenever the system crashes and must write the hibernation file to an encrypted volume.
Show Status	None	None	This service is fully automatic. The User / Cryptographic Officer does not take any actions to explicitly start this service. This service is executed upon completion of the Control Input Interfaces.
Self-Tests	AES-CBC - Encrypt/Decrypt KATs AES-CCM - Encrypt/Decrypt KATs Software Integrity Test (2048-bit RSA w/ SHA-256)	None	This service is fully automatic. The User / Cryptographic Officer does not take any actions to explicitly start this service. This service is executed upon startup of this module.
Zeroization	None	None	This service is fully automatic. The

(see Section 9)			User / Cryptographic Officer does not take any actions to explicitly start this service. This service is executed as part of the module shutdown.

Table 2

Service	Internal Functions
Write encrypted crash dump file to an encrypted volume	GetFveContext DumpWrite
Write encrypted hibernation file to an encrypted volume	GetFveContext DumpWrite
Show Status	GetFveContext DumpWrite
Self-Tests	Module startup
Zeroization (see Section 9)	Module shutdown

7.1 Show Status Services

The status information is returned to the caller as the return value from the function. The User / Cryptographic Officer does not have any direct access to the return value.

7.2 Self-Test Services

BitLocker Dump Filter automatically executes Self-Tests upon being loaded, which provides the User / Cryptographic Officer assurance that the module is operating properly. Upon failing a Self-Test, this module will fail to load. The Self-Test functionality is described in Section 10 Self-Tests.

7.3 Service Inputs / Outputs

The User / Cryptographic Officer does not have access to the service inputs and outputs that are specified in Section 5 Ports and Interfaces.

8 Authentication

The module does not provide authentication. Roles are implicitly assumed based on the services that are executed.

9 Cryptographic Key Management

BitLocker encrypts disk sectors with a Full Volume Encryption Key (FVEK). This module receives the FVEK from Windows 10 OEs and uses it to encrypt crash dump files and hibernation files.

9.1 Cryptographic Keys

The BitLocker Dump Filter uses only the Full Volume Encryption Key it receives, and does not generate any cryptographic keys. It receives the necessary full volume encryption key for encrypting dump files

and hibernation files from the Cryptographic Operator by way of the running system booted through the Integrity Chain of Trust. On shutdown, the FVEK is zeroized in memory (by overwriting once with 0s).

9.2 Critical Security Parameters

The BitLocker Dump Filter cryptographic module has the following Critical Security Parameter (CSP):

Table 3

Critical Security Parameter	Description
Full Volume Encryption Key (FVEK)	A 128/256 bit AES key that is input into the crypto module as plaintext and is used for encryption of crash dump files and hibernation files

9.3 Access Control Policy

The BitLocker Dump Filter crypto module does not allow read or write access to the cryptographic keys contained within it. Neither role (Crypto Officer or User) sees the key within the module. Nevertheless, both roles have execute access to the FVEK. Due to the simplicity of this policy, an access control policy table is not included in this document. BitLocker Dump Filter simply automatically uses the FVEK to write crash dump and hibernation files, for the role of the User (or Crypto Officer if that applies). Since the module has to operate under an assumed role, the operator must have the FVEK in order to encrypt data to the drive.

10 Self-Tests

10.1 Power-On Self-Tests

The BitLocker Dump Filter implements Known Answer Test (KAT) functions each time the module is loaded. The module performs the following KATs:

- AES-CBC - Encrypt/Decrypt KATs
- AES-CCM - Encrypt/Decrypt KATs
- Software Integrity Test (2048-bit RSA w/ SHA-256)

  Note: the Software Integrity Test is performed by the Code Integrity (CI.dll) cryptographic module.

If the self-test fails, the module will not load and status will be returned. If the status is STATUS_FAIL_CHECK, then that is the indicator a self-test failed.

11 Design Assurance

The secure installation, generation, and startup procedures of this cryptographic module are part of the overall operating system secure installation, configuration, and startup procedures for the Windows 10 OEs. The various methods of delivery and installation for each product are listed in the following table.

Table 4

Product	Delivery and Installation Method
Windows 10 Pro, Windows 10 Enterprise	• Pre-installed on the computer by OEM • Download that updates to Windows 10
Surface Book, Surface Pro 4, Surface Pro 3, Surface 3, Surface Pro 2, Surface Pro, Surface Hub 84”, Surface Hub 55”, Lumia 950, Lumia 635	• Pre-installed by the OEM (Microsoft)

After the operating system has been installed, it must be configured by enabling the "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" policy setting followed by restarting the system. This procedure is all the crypto officer and user behavior necessary for the secure operation of this cryptographic module.

An inspection of authenticity of the physical medium can be made by following the guidance at this Microsoft web site: https://www.microsoft.com/en-us/howtotell/default.aspx

The installed version of Windows 10 OEs must be verified to match the version that was validated. See Appendix A for details on how to do this.

For Windows Updates, the client only accepts binaries signed by Microsoft certificates. The Windows Update client only accepts content whose SHA-2 hash matches the SHA-2 hash specified in the metadata. All metadata communication is done over a Secure Sockets Layer (SSL) port. Using SSL ensures that the client is communicating with the real server and so prevents a spoof server from sending the client harmful requests. The version and digital signature of new cryptographic module releases must be verified to match the version that was validated. See Appendix A for details on how to do this.

12 Mitigation of Other Attacks

The following table lists the mitigations of other attacks for this cryptographic module:

Table 5

Algorithm	Protected Against	Mitigation	Comments
AES	Timing Analysis Attack	Constant Time Implementation	
	Cache Attack	Memory Access pattern is independent of any confidential data	Protected Against Cache attacks only when used with AES NI

13 Security Levels

The security level for each FIPS 140-2 security requirement is given in the following table.

Table 6

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	NA
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	2
Mitigation of Other Attacks	1

14 Additional Details

For the latest information on Microsoft Windows, check out the Microsoft web site at:

http://windows.microsoft.com

For more information about FIPS 140 validations of Microsoft products, please see:

http://technet.microsoft.com/en-us/library/cc750357.aspx

15 Appendix A – How to Verify Windows Versions and Digital Signatures

15.1 How to Verify Windows Versions

The installed version of Windows 10 OEs must be verified to match the version that was validated using the following method:

1. In the Search box type "cmd" and open the Command Prompt desktop app.
2. The command window will open.
3. At the prompt, enter "ver".
4. The version information will be displayed in a format like this:
   `Microsoft Windows [Version 10.0.xxxxx]`

If the version number reported by the utility matches the expected output, then the installed version has been validated to be correct.

15.2 How to Verify Windows Digital Signatures

After performing a Windows Update that includes changes to a cryptographic module, the digital signature and file version of the binary executable file must be verified. This is done like so:

1. Open a new window in Windows Explorer.
2. Type "C:\Windows\" in the file path field at the top of the window.
3. Type the cryptographic module binary executable file name (for example, "CNG.SYS") in the search field at the top right of the window, then press the Enter key.
4. The file will appear in the window.
5. Right click on the file's icon.
6. Select Properties from the menu and the Properties window opens.
7. Select the Details tab.
8. Note the File version Property and its value, which has a number in this format: xx.x.xxxxx.xxxx.
9. If the file version number matches one of the version numbers that appear at the start of this security policy document, then the version number has been verified.
10. Select the Digital Signatures tab.
11. In the Signature list, select the Microsoft Windows signer.
12. Click the Details button.
13. Under the Digital Signature Information, you should see: "This digital signature is OK." If that condition is true, then the digital signature has been verified.