



Security Policy

for FIPS 140-2 Validation

Microsoft Windows 8

Microsoft Windows Server 2012

Microsoft Windows RT

Microsoft Surface Windows RT

Microsoft Surface Windows 8 Pro

Microsoft Windows Phone 8

BitLocker® Dump Filter (DUMPFVE.SYS)

DOCUMENT INFORMATION

Version Number	1.1
Updated On	July 17, 2013

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.

Complying with all applicable copyright laws is the responsibility of the user. This work is licensed under the Creative Commons Attribution-NoDerivs-NonCommercial License (which allows redistribution of the work). To view a copy of this license, visit <http://creativecommons.org/licenses/by-nd-nc/1.0/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2013 Microsoft Corporation. All rights reserved.

Microsoft, Windows, the Windows logo, Windows Server, and BitLocker are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

TABLE OF CONTENTS

<u>1</u>	<u>INTRODUCTION</u>	<u>5</u>
1.1	LIST OF CRYPTOGRAPHIC MODULE BINARY EXECUTABLES.....	5
1.2	BRIEF MODULE DESCRIPTION.....	5
1.3	VALIDATED PLATFORMS	7
1.4	CRYPTOGRAPHIC BOUNDARY	7
<u>2</u>	<u>SECURITY POLICY</u>	<u>7</u>
2.1	FIPS 140-2 APPROVED ALGORITHMS.....	8
2.2	CRYPTOGRAPHIC BYPASS	8
2.3	MACHINE CONFIGURATIONS.....	8
<u>3</u>	<u>OPERATIONAL ENVIRONMENT.....</u>	<u>8</u>
<u>4</u>	<u>INTEGRITY CHAIN OF TRUST.....</u>	<u>8</u>
<u>5</u>	<u>PORTS AND INTERFACES</u>	<u>9</u>
5.1	CONTROL INPUT INTERFACE.....	10
5.1.1	GETFVECONTEXT	10
5.1.2	DUMPWRITE	11
5.2	STATUS OUTPUT INTERFACE	11
5.3	DATA OUTPUT INTERFACE.....	11
5.4	DATA INPUT INTERFACE.....	11
<u>6</u>	<u>SPECIFICATION OF ROLES.....</u>	<u>12</u>
6.1	MAINTENANCE ROLES	12
6.2	MULTIPLE CONCURRENT INTERACTIVE OPERATORS.....	12
6.3	SHOW STATUS SERVICES	12
6.4	SELF-TEST SERVICES.....	12
6.5	SERVICE INPUTS / OUTPUTS	12
<u>7</u>	<u>AUTHENTICATION</u>	<u>13</u>

<u>8</u>	<u>CRYPTOGRAPHIC KEY MANAGEMENT</u>	<u>13</u>
<u>8.1</u>	<u>CRYPTOGRAPHIC KEYS.....</u>	<u>13</u>
<u>8.2</u>	<u>CRITICAL SECURITY PARAMETERS.....</u>	<u>13</u>
<u>8.3</u>	<u>ACCESS CONTROL POLICY.....</u>	<u>13</u>
<u>9</u>	<u>SELF-TESTS</u>	<u>13</u>
<u>9.1</u>	<u>POWER-ON SELF-TESTS.....</u>	<u>13</u>
<u>10</u>	<u>DESIGN ASSURANCE.....</u>	<u>14</u>
<u>11</u>	<u>MITIGATION OF OTHER ATTACKS</u>	<u>15</u>
<u>12</u>	<u>ADDITIONAL DETAILS.....</u>	<u>15</u>
<u>13</u>	<u>APPENDIX A – HOW TO VERIFY WINDOWS VERSIONS AND DIGITAL SIGNATURES</u>	<u>16</u>
<u>13.1</u>	<u>HOW TO VERIFY WINDOWS VERSIONS.....</u>	<u>16</u>
<u>13.2</u>	<u>HOW TO VERIFY WINDOWS DIGITAL SIGNATURES</u>	<u>16</u>

1 Introduction

BitLocker® Drive Encryption is a data protection feature available in Windows 8, Windows RT, Windows Server 2012, and Windows Phone 8. 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.

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 8, Windows RT, Windows Server 2012, and Windows Phone 8 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 6.2.9200 for Windows 8, Windows RT, Windows Server 2012, and Windows Phone 8

1.2 Brief Module Description

The BitLocker Dump Filter is the full volume encryption 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.

BitLocker Dump Filter

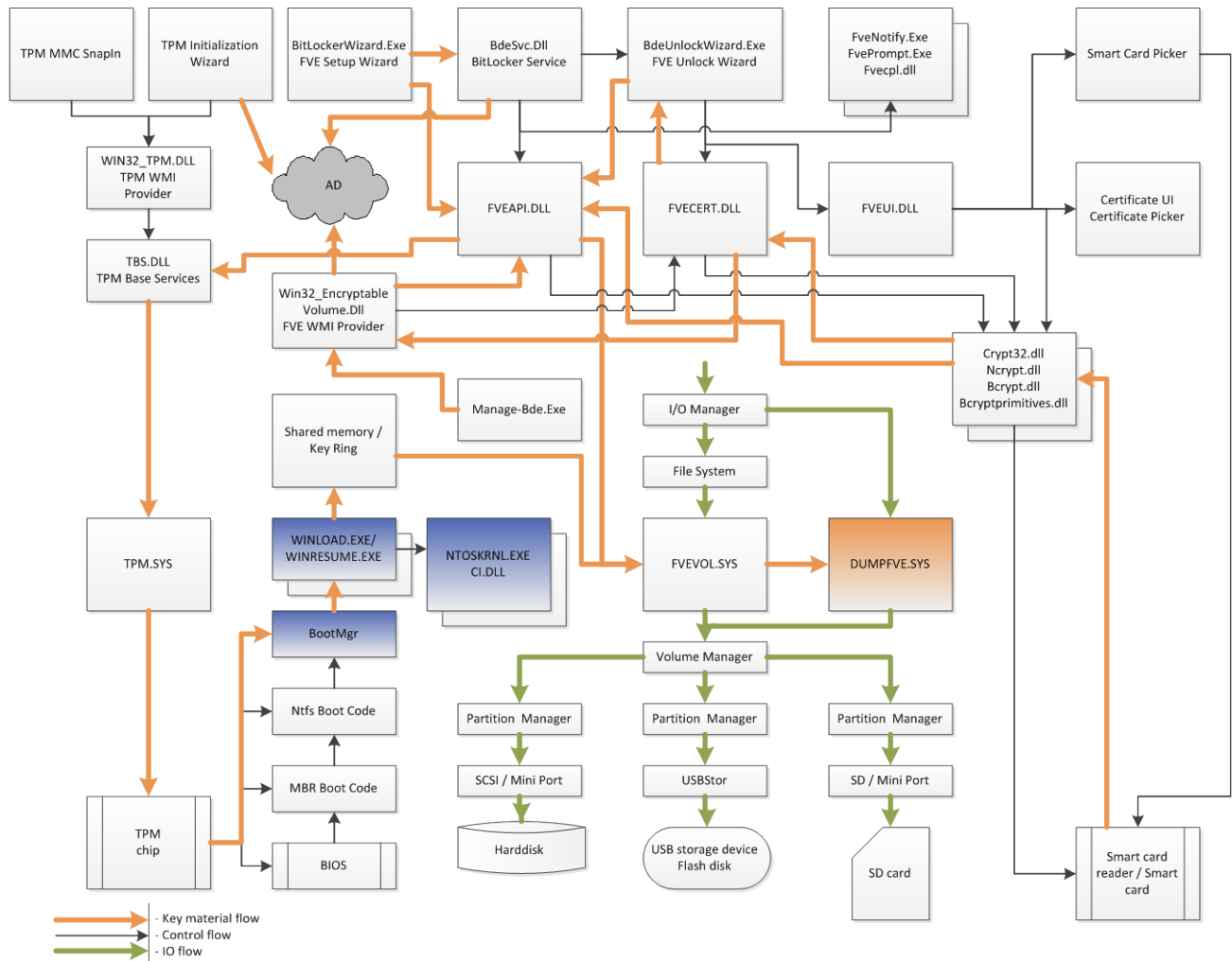


Figure 1 - Logical Operation of Module (this cryptographic module is in orange, other BitLocker-related cryptographic modules are in blue)

1.3 Validated Platforms

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

- x86 Microsoft Windows 8 Enterprise – Dell Dimension C521 (AMD Athlon 64 X2 Dual Core)
- x64 Microsoft Windows 8 Enterprise – Dell PowerEdge SC430 (Intel Pentium D without AES-NI)
- x64-AES-NI Microsoft Windows 8 Enterprise – Intel Client Desktop (Intel Core i7 with AES-NI)
- x64 Microsoft Windows Server 2012 – Dell PowerEdge SC430 (Intel Pentium D without AES-NI)
- x64-AES-NI Microsoft Windows Server 2012 – Intel Client Desktop (Intel Core i7 with AES-NI)
- ARMv7 Thumb-2 Microsoft Windows RT – NVIDIA Tegra 3 Tablet (NVIDIA Tegra 3 Quad-Core)
- ARMv7 Thumb-2 Microsoft Windows RT – Qualcomm Tablet (Qualcomm Snapdragon S4)
- ARMv7 Thumb-2 Microsoft Windows RT – Microsoft Surface Windows RT (NVIDIA Tegra 3 Quad-Core)
- x64-AES-NI Microsoft Windows 8 Pro – Microsoft Surface Windows 8 Pro (Intel x64 Processor with AES-NI)
- ARMv7 Thumb-2 Microsoft Windows Phone 8 – Windows Phone 8 (Qualcomm Snapdragon S4)

BitLocker Dump Filter maintains FIPS 140-2 validation compliance (according to FIPS 140-2 PUB Implementation Guidance G.5) on the following platforms:

- x86 Microsoft Windows 8
- x86 Microsoft Windows 8 Pro

- x64 Microsoft Windows 8
- x64 Microsoft Windows 8 Pro
- x64 Microsoft Windows Server 2012 Datacenter

- x64-AES-NI Microsoft Windows 8
- x64-AES-NI Microsoft Windows 8 Pro
- x64-AES-NI Microsoft Windows Server 2012 Datacenter

1.4 Cryptographic Boundary

The Windows 8, Windows RT, Windows Server 2012, and Windows Phone 8 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 Microsoft Windows 8 running on x86 and x64.
- BitLocker Dump Filter is validated on Microsoft Windows RT running on ARMv7 Thumb.
- BitLocker Dump Filter maintains FIPS 140-2 validation compliance on Microsoft Windows Server 2012 running on x64.

- Windows 8, Windows RT, Windows Server 2012, and Windows Phone 8 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 approved version of Windows 8, Windows RT, Windows Server 2012, and Windows Phone 8 Code Integrity (ci.dll) validated to FIPS 140-2 under Cert. #1897, respectively, operating in FIPS mode.

2.1 FIPS 140-2 Approved Algorithms

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

- AES (Certs #2196 and #2198)

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 Windows 8, Windows RT, Windows Server 2012, and Windows Phone 8 running on the hardware 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.

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-1 hash
- SHA-256 hash

BitLocker Dump Filter ensures that Windows 8, Windows RT, Windows Server 2012, and Windows Phone 8 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.

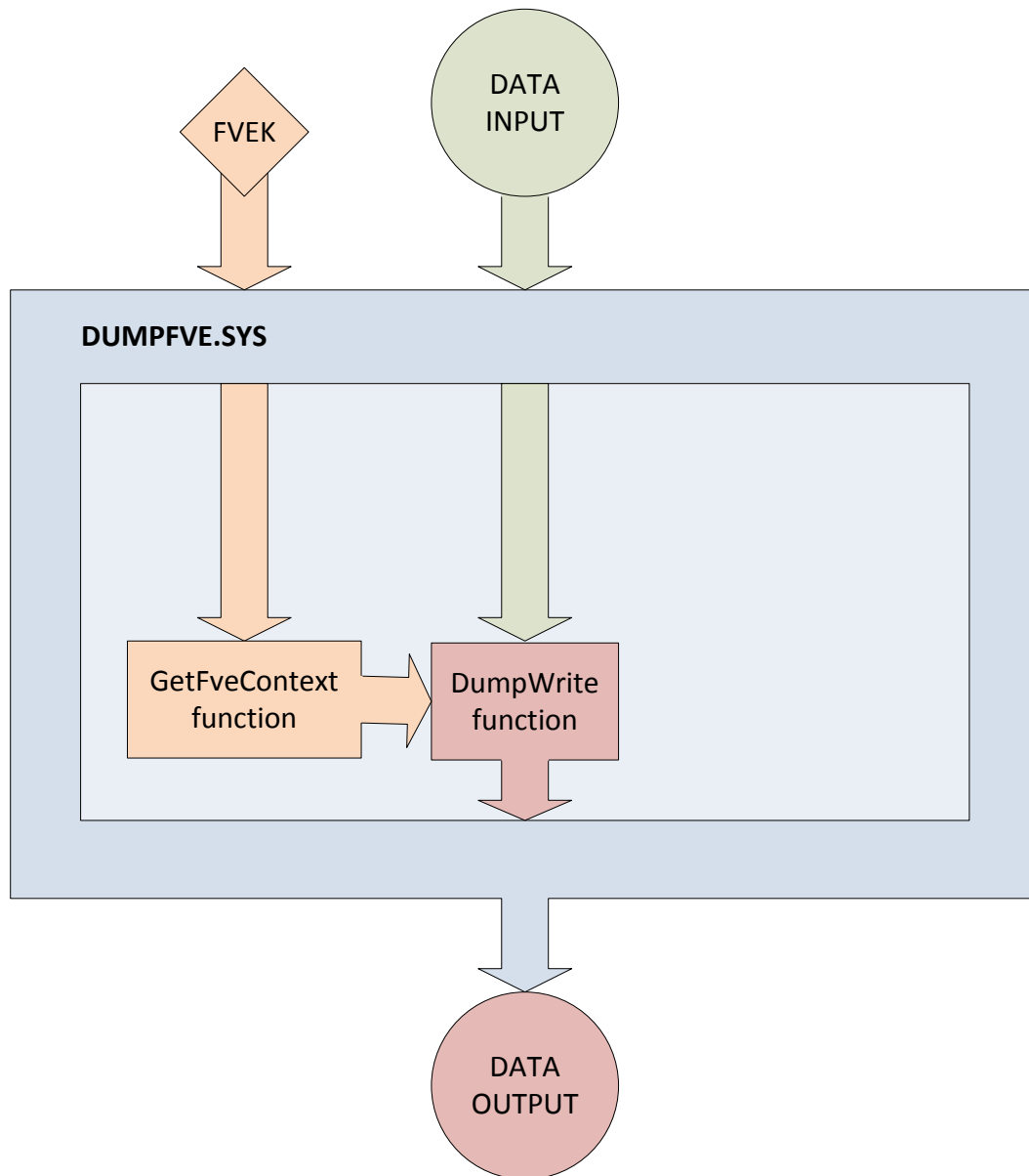


Figure 2 – BitLocker Dump Filter Block Diagram

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 Full Volume Encryption Key (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 particular to each of the roles. As a FIPS 140-2 level 1 validated product, BitLocker Dump Filter itself does not provide any authentication.

Services available to the Cryptographic Officer role:

- Configure BitLocker into FIPS mode (see section 8)
- Write encrypted crash dump file to disk
- Write encrypted hibernation file to disk

Services available to the User role:

- Write encrypted crash dump file to disk
- Write encrypted hibernation file to disk

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.

6.3 Show Status Services

The User and Cryptographic Officer roles have the same Show Status functionality, which is, for each function, the status information is returned to the caller as the return value from the function.

6.4 Self-Test Services

The User and Cryptographic Officer roles have the same Self-Test functionality, which is described in Section 9 Self-Tests.

6.5 Service Inputs / Outputs

The User and Cryptographic Officer roles have service inputs and outputs as specified in Section 5 Ports and Interfaces.

7 Authentication

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

8 Cryptographic Key Management

BitLocker encrypts disk sectors with a Full Volume Encryption Key (FVEK). This module receives the FVEK from Windows 8, Windows RT, Windows Server 2012, and Windows Phone 8 and uses it to encrypt crash dump files and hibernation files.

8.1 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).

8.2 Critical Security Parameters

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

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

8.3 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.

9 Self-Tests

9.1 Power-On Self-Tests

The BitLocker Dump Filter implements Known Answer Test (KAT) functions each time the module is loaded. The module performs KATs for AES CCM and AES CBC encrypt/decrypt. 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.

10 Design Assurance

The secure installation, generation, and startup procedures of this cryptographic module are part of the overall Windows 8, Windows RT, and Windows Server 2012 operating system secure installation, configuration, and startup procedures. 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.

Windows Phone 8 does not use the same installation, configuration, and startup procedures as the Windows operating system on a computer, but rather, is securely installed and configured by the cellular telephone carrier.

The procedures required for maintaining security while distributing and delivering versions of a cryptographic module to authorized operators are:

1. The secure distribution method is via the physical medium for product installation delivered by Microsoft Corporation, which is a DVD in the case of Windows 8 and Windows Server 2012. In the case of Windows RT, Surface Windows RT, Surface Windows 8 Pro, and Windows Phone 8, the cryptographic module is already installed at the factory and is only distributed with the hardware.
2. An inspection of authenticity of the physical medium can be made by following the guidance at this Microsoft web site: <http://www.microsoft.com/en-us/howtotell/default.aspx>
3. The installed version of Windows 8, Windows RT, and Windows Server 2012 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.

11 Mitigation of Other Attacks

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

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

12 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 evaluations of Microsoft products, please see:

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

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

13.1 How to Verify Windows Versions

The installed version of Windows 8, Windows RT, and Windows Server 2012 must be verified to match the version that was validated using one of the following methods:

1. The ver command
 - a. From Start, open the Search charm.
 - b. In the search field type "cmd" and press the Enter key.
 - c. The command window will open with a "C:\>" prompt.
 - d. At the prompt, type "ver" and press the Enter key.
 - e. You should see the answer "Microsoft Windows [Version 6.2.9200]".
2. The systeminfo command
 - a. From Start, open the Search charm.
 - b. In the search field type "cmd" and press the Enter key.
 - c. The command window will open with a "C:\>" prompt.
 - d. At the prompt, type "systeminfo" and press the Enter key.
 - e. Wait for the information to be loaded by the tool.
 - f. Near the top of the output, you should see:

OS Name:	Microsoft Windows 8 Enterprise
OS Version:	6.2.9200 N/A Build 9200
OS Manufacturer:	Microsoft Corporation

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

13.2 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: x.x.xxxx.xxxxx.
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.