Non-proprietary Security Policy for

FIPS 140-2 Validation

BitLocker® Windows Resume (winresume) in Windows 10 Enterprise LTSB

DOCUMENT INFORMATION

Version Number	1.4
Updated On	May 9,2018

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
14 OCT 2015	1.0	Tim Myers	First release to validators
20 FEB 2016	1.1	Tim Myers	Updates in response to comments
28 APR 2016	1.2	Tim Myers	Updates in response to comments
27 MAR 2018	1.3	Iffat Qamar	Update for build 10.0.10240.17643 (3SUB)
9 MAY 2018	1.4	Iffat Qamar	Updated CAVP, Bounded Module added

TABLE OF CONTENTS

1 Introduction

BitLocker ® Windows Resume, WINRESUME.EXE, is an operating system loader which loads the operating system kernel (ntoskrnl.exe) and other boot stage binary image files, as well as previous operating system state information, when Windows has been previously put into a sleep (S3) or hibernate (S4) power state. Throughout this document, BitLocker ® Windows Resume may be called Windows Resume for short.

The Operational Environments (OEs) are:

- Windows 10 Enterprise LTSB (x86) running on a Dell Inspiron without AES-NI or PCLMULQDQ or SSSE 3
- Windows 10 Enterprise LTSB (x64) running on a HP Compaq Pro 6305 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Enterprise LTSB (x64) running on a Dell XPS 8700 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Enterprise LTSB (x64) - Microsoft Surface Pro 3 - Intel Core i7 with AES-NI
- Windows 10 Enterprise LTSB (x64) - Microsoft Surface 3 - Intel Atom x7 with AES-NI
- Windows 10 Enterprise LTSB (x64) - Microsoft Surface Pro 2 - Intel Core i5 with AES-NI
- Windows 10 Enterprise LTSB (x64) - Microsoft Surface Pro - Intel x64 Processor with AES-NI

herein referred to as Windows 10 OEs.

1.1 List of Cryptographic Module Binary Executables

WINRESUME.EXE – Version 10.0.10240.17643 for Windows 10 OEs on systems using conventional BIOS.

WINRESUME.EFI – Version 10.0.10240.17643 for Windows 10 OEs on systems using UEFI firmware.

1.2 Version Info

OS Build version numbers are:

10.0.10240.17643 for Windows 10 OEs

1.3 Brief Module Description

Windows Resume is the binary executable that handles loading the Windows operating system when resuming from hibernation. At resume time, if BitLocker is enabled, the encrypted hibernation data is decrypted as it is paged back into memory.

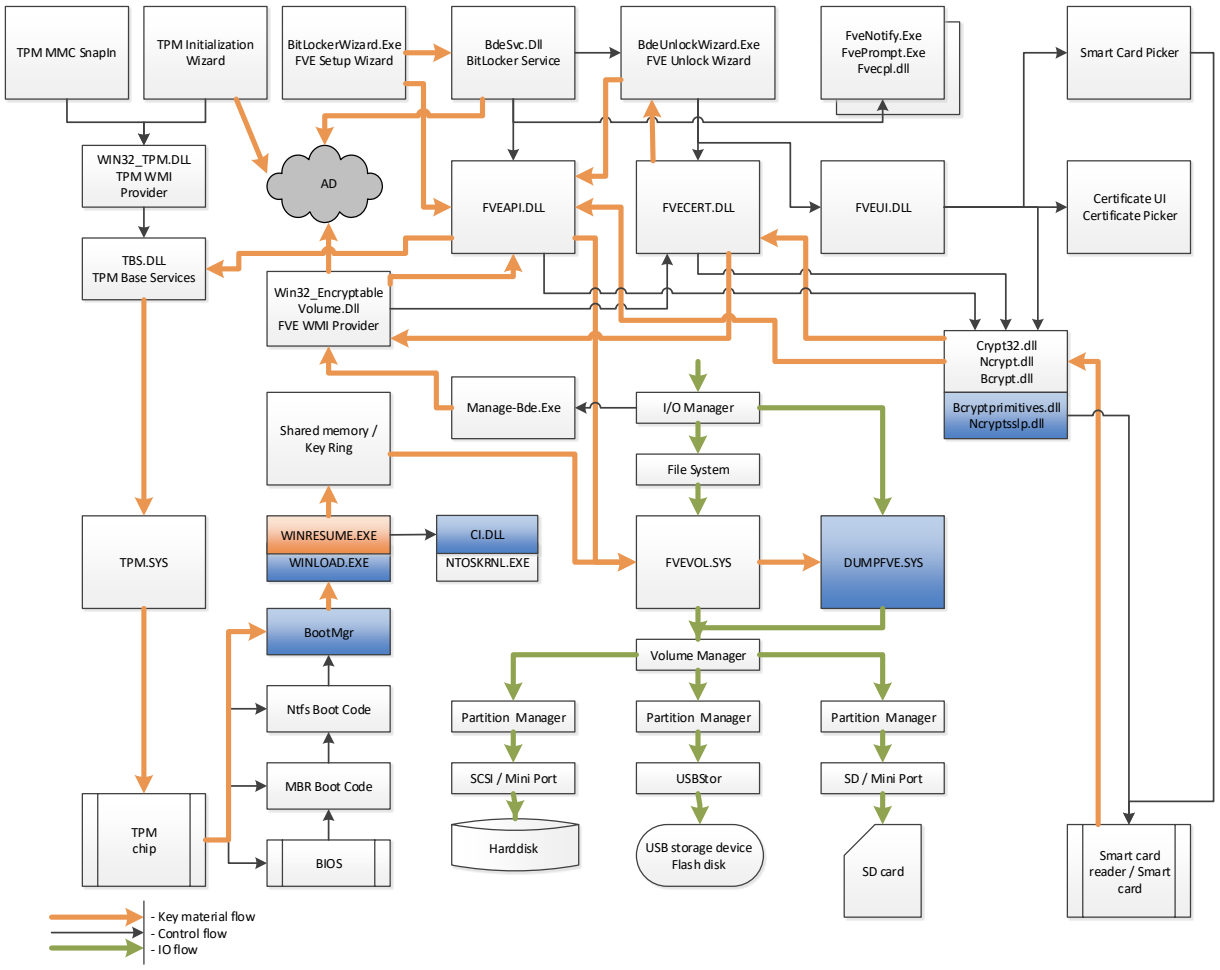


Figure 1 - Logical Operation of Module
(This module is orange; other modules are blue.)

1.4 Validated Platforms

The Windows Resume components listed in Section 1.1 were validated using the following machine configurations:

- Windows 10 Enterprise LTSB (x86) - Dell Inspiron 660s - Intel Core i3 without AES-NI or PCLMULQDQ or SSSE 3
- Windows 10 Enterprise LTSB (x64) - HP Compaq Pro 6305 - AMD A4 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Enterprise LTSB (x64) - Dell XPS 8700 - Intel Core i7 with AES-NI and PCLMULQDQ and SSSE 3
- Windows 10 Enterprise LTSB (x64) - Microsoft Surface Pro 3 - Intel Core i7 with AES-NI
- Windows 10 Enterprise LTSB (x64) - Microsoft Surface 3 - Intel Atom x7 with AES-NI
- Windows 10 Enterprise LTSB (x64) - Microsoft Surface Pro 2 - Intel Core i5 with AES-NI
- Windows 10 Enterprise LTSB (x64) - Microsoft Surface Pro - Intel x64 Processor with AES-NI

1.5 Cryptographic Boundary

The software cryptographic boundary for Windows Resume is defined as the binaries WINRESUME.EXE and WINRESUME.EFI.

2 Security Policy

Windows Resume operates under several rules that encapsulate its security policy.

- Windows Resume is validated on the Windows 10 OEs.
- Windows Resume operates in FIPS mode of operation only when used with the FIPS validated version of Windows 10 OEs Boot Manager (bootmgr) validated to FIPS 140-2 under Cert. #3415 operating in FIPS mode.
- Windows 10 OEs are operating systems supporting a “single user” mode where there is only one interactive user during a logon session.
- Windows Resume 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.

The following diagram illustrates the master components of the Windows Resume module:

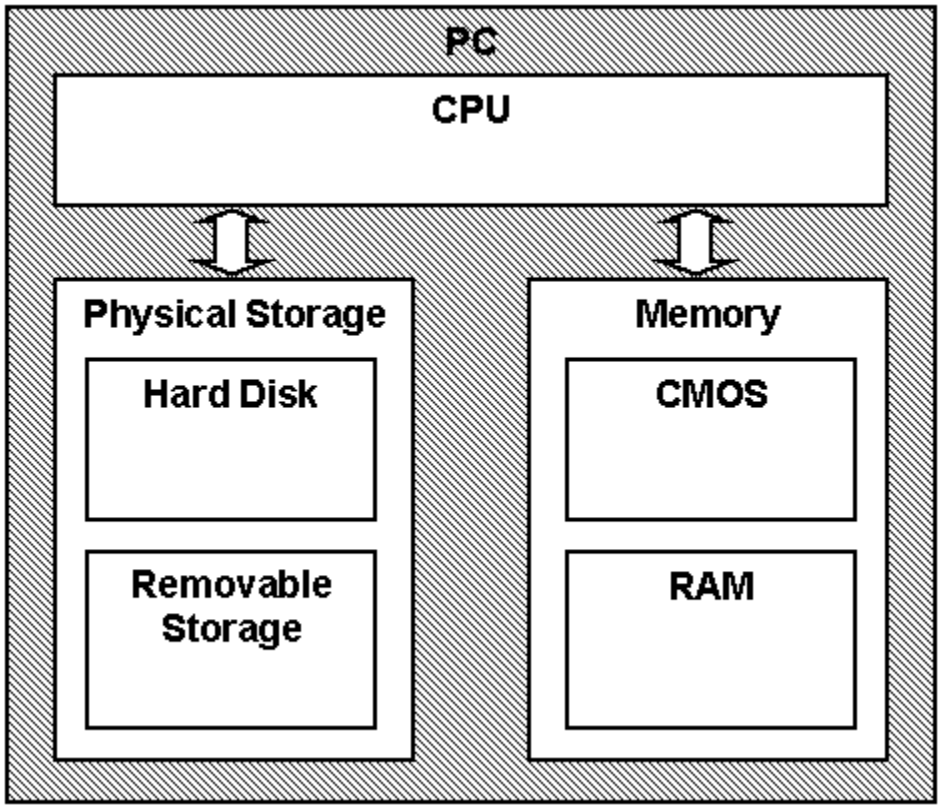
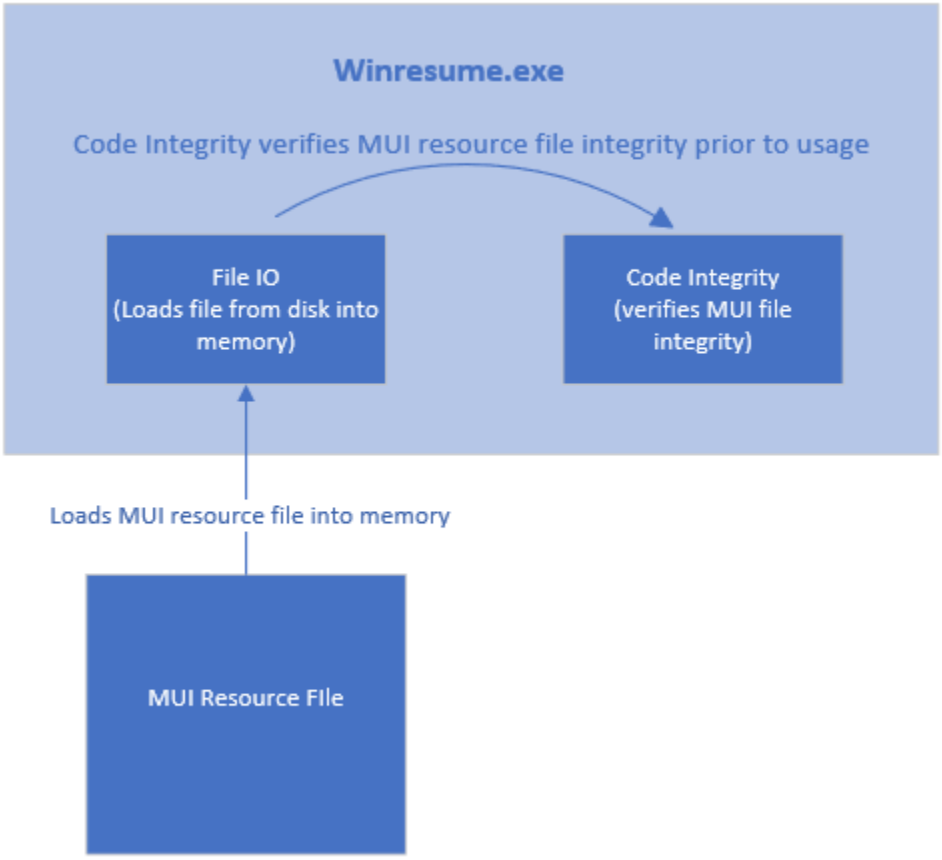


Figure 2 Master Components

The following diagram illustrates Windows Resume module interaction with other cryptographic modules:

Figure 3 Module Interaction



- Windows Resume's main service is to load the Windows 10 OEs operating system kernel (ntoskrnl.exe) and other boot stage binary image files, including Code Integrity cryptographic module (ci.dll). After the kernel and boot stage binary image files, including Code Integrity, are loaded, Windows Resume passes the execution control to the kernel and it terminates its own execution. In addition to this service, Windows Resume also provides status and self-test services. The Crypto officer and User have access to all services WINRESUME supports.
- The module provides a power-up self-tests service that is automatically executed when the module is loaded into memory. The module also provides a show status service that is automatically executed by the module to provide the status response of the module either via output to the GPC monitor or to log files.
- Windows Resume is a multi-chip standalone module that operates in FIPS-approved mode during normal operation of the computer and Windows operating system boot sequence.
- Windows Resume verifies the integrity of the non-critical Multilingual User Interface (MUI) resource file.

2.1 FIPS 140-2 Approved Algorithms

Windows Resume implements the following FIPS-140-2 Approved algorithms:

- FIPS 186-4 RSA PKCS#1 (v1.5) digital signature verification with 1024, 2048, and 3072 modulus; supporting SHA-1, SHA-256, SHA-384, and SHA-512 (Cert. # 2829)
- FIPS 180-4 SHS SHA-1, SHA-256, SHA-384, and SHA-512 (Cert. # 4249)
- FIPS 197 AES CBC 128 and 256 encryption (self-tests only) and decryption (Cert. #5291), SP800-38C AES CCM encryption (self-tests only) and decryption 256 (Cert. #5293)

Note: not all the algorithms / modes verified through the CAVP certificates listed are implemented by this module.

2.2 Non-Approved Algorithms

Windows Resume also includes a legacy implementation of MD5[1] for backwards compatibility with the verification of the certificate chain of old certificates that might have been used by certificate authorities (CAs) to sign certificates on kernel mode drivers outside of Windows. This legacy implementation of MD5 is not used for checking the integrity of this cryptographic module nor any other Windows cryptographic module.

2.3 Cryptographic Bypass

Cryptographic bypass is not supported by Windows Resume.

2.4 FIPS 140-2 Approved Algorithm from Bounded Module

A bounded module is a FIPS 140 module which provides cryptographic functionality that is relied on by a downstream module. As described in the Integrity Chain of Trust (section 4), the Windows Resume depends on the following algorithms:

Implemented in the Boot Manager (Cert. #3415):

- CAVP certificates #2829 (Windows 10 Enterprise LTSB) for FIPS 186-4 RSA PKCS#1 (v1.5 digital signature verification with 2048 modulus; supporting SHA-256
- CAVP certificate #4249 for FIPS 180-4 SHS with SHA-256

[1] MD5 is not allowed for usage in FIPS mode.

2.5 Machine Configurations

BitLocker Windows Resume was tested using the machine configurations listed in Section 1.4 - Validated Platforms.

3 Operational Environment

The operational environment for Windows Resume is Windows 10 OEs running on the software and hardware configurations listed in Section 1.4 - Validated Platforms. Windows Resume services are only available before the startup of the operating system. This is done inside the Trusted Computing Base (TCB).

4 Integrity Chain of Trust

4.1 Conventional BIOS and UEFI without Secure Boot Enabled

Boot Manager is the start of the chain of trust. It cryptographically checks its own integrity during its startup. It then cryptographically checks the integrity of Windows Resume (if resuming from hibernation) before starting it. An RSA signature with a 2048-bit key and SHA-256 message digest are used.

Windows Resume verifies the integrity of the non-critical Multilingual User Interface (MUI) resource file in the same manner as described above.

4.2 UEFI with Secure Boot Enabled

On UEFI systems with Secure Boot enabled, Boot Manager is still the OS binary from which the integrity of all other OS binaries is rooted, and it does cryptographically check its own integrity. However, Boot Manager's integrity is also checked and verified by the UEFI firmware, which is the root of trust on Secure Boot enabled systems. An RSA signature with a 2048-bit key and SHA-256 message digest are used.

5 Ports and Interfaces

5.1 Control Input Interface

The Windows Resume Control Input Interface is the set of internal functions responsible for intercepting control input. These functions are:

- BlBdInitialize – Reads the system status to determine if a boot debugger is attached.
- OslMain – This function receives and parses the Boot Application parameters, which are passed to the module when execution is passed from Boot Manager.
- BlInitializeLibrary – Performs the parsing Boot Application parameters.
- BlXmiRead – Reads the operator selection from the Windows Resume user interface.

5.2 Status Output Interface

The Status Output Interface is the BlXmiWrite function that is responsible for displaying the integrity verification errors to the screen. The Status Output Interface is also defined as the BlLogData responsible for writing the name of the corrupt driver to the bootlog.

5.3 Data Output Interface

The Data Output Interface is represented by the OslArchTransferToKernel function and the AhCreateLoadOptionsString function. OslArchTransferToKernel is responsible for transferring the execution from Winresume to the initial execution point of the Windows 10 OEs kernel. Data exits the module in the form of the initial instruction address of the Windows 10 OEs kernel.

Data exits the module from the AhCreateLoadOptionsString function in the form of boot application parameters passed to the Windows 10 OEs kernel.

5.4 Data Input Interface

The Data Input Interface is represented by the BlFileReadEx function and the BlDeviceRead function. BlFileReadEx is responsible for reading the binary data of unverified components from the computer hard drive. In addition, the BitLocker Full Volume Encryption Key (FVEK) can also be entered into the module over the module's data input interface. BlDeviceRead is responsible for reading data directly from devices.

6 Specification of Roles

Windows Resume supports both User and Cryptographic Officer roles (as defined in FIPS-140-2). Both roles have access to all services implemented in Windows Resume. The module does not implement any authentication services. Therefore, roles are assumed implicitly by booting the Windows 10 OEs operating systems.

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. Windows Resume does not export any cryptographic functions. The only service triggered by the User/Cryptographic Officer is zeroization. Everything else is started by the Boot Manager. The only service for which there is any output to the User/Cryptographic Officer is the Show Status service. The services are:

- Resume the OS from Hibernation

- Show Status
- Self-Tests
- Zeroization (see Section 8 Cryptographic Key Management)
- Legacy Certificate Chain Authentication (non-FIPS Approved service)

The following table maps the services to their corresponding algorithms and critical security parameters (CSPs).

Table 1

Service	Algorithms	CSPs	Invocation
Resume the OS from Hibernation	FIPS 186-4 RSA PKCS#1 (v1.5) verify with public key FIPS 180-4 SHS: SHA-256 hash SHA-512 hash AES CBC decryption 128 and 256 bits AES CCM decryption 256 bits	Asymmetric Public keys (to verify integrity of MUI resource files) Full Volume Encryption Key (FVEK) (to load the BitLocker encrypted data containing the OS).	This service is fully automatic. The User / Cryptographic Officer does not take any actions to start this service.
Show Status	None	None	This service is fully automatic. The User / Cryptographic Officer does not take any actions to start this service.
Self-Tests	FIPS 186-4 RSA PKCS#1 (v1.5) verify with public key KAT and signature verification KAT FIPS 180-4 SHS: SHA-1 KAT SHA-256 KAT SHA-512 KAT AES CBC KAT AES CCM KAT	None	This service is fully automatic. The User / Cryptographic Officer does not take any actions to start this service.
Zeroization	None	None	See section 8.
Legacy certificate chain authentication (non-FIPS Approved service)	MD5 (non-FIPS Approved algorithm)	Asymmetric Public keys	This service is fully automatic. The User / Cryptographic Officer does not take any actions to start this service.

7.1 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.

7.2 Self-Test Services

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

7.3 Service Inputs / Outputs

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

8 Cryptographic Key Management

Windows Resume does not store any secret or private cryptographic keys across power-cycles. However, it does use an AES key in support of the BitLocker feature. This key is:

- Full Volume Encryption Key (FVEK) - 128 or 256-bit AES key that is used to decrypt data on disk sectors of the hard drive. FVEK is in plaintext in memory.

Procedural zeroization of this ephemeral key (RAM only) for this software cryptographic module consists of rebooting the operating system.

Windows Resume also uses the Microsoft root CA public key certificate stored in plaintext on the computer hard disk to verify digital signatures using its implementation of RSA PKCS#1 (v1.5) verify. This public key is available to both roles. Procedural zeroization of persistent keys for this software cryptographic module consists of uninstallation of the cryptographic module and reformatting and overwriting, at least once, the hard drive or other permanent storage media upon which the operating system was installed.

8.1 Access Control Policy

All the keys (mentioned above) are accessed only by the Windows Resume service that loads the operating system kernel (ntoskrnl.exe) and other boot stage binary image files, including Code Integrity. This service only has execute access to the keys mentioned above. Due to such simplicity, an access control policy table is not included in this document.

9 Self-Tests

9.1 Power-On Self Tests

Windows Resume performs the following power-on (startup) self-tests:

- RSA PKCS#1 (v1.5) verify with public key Known Answer Test

    - RSA signature verification Known Answer Test with 1024-bit key and SHA-1 message digest
    - RSA signature verification Known Answer Test with 2048-bit key and SHA-256 message digest
- SHS (SHA-1) Known Answer Test
- SHS (SHA-256) Known Answer Test
- SHS (SHA-512) Known Answer Test
- AES-CBC - Encrypt/Decrypt Known Answer Tests
- AES-CCM - Encrypt/Decrypt Known Answer Tests

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

9.2 Conditional Self-Tests

Windows Resume does not perform conditional self-tests.

10 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 2

Product	Delivery and Installation Method
Windows 10 Enterprise LTSB	• Pre-installed on the computer by OEM • Download that updates to Windows 10
Surface Pro 3, Surface 3, Surface Pro 2, Surface Pro	• 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.

11 Mitigation of Other Attacks

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

Table 3

Algorithm	Protected Against	Mitigation	Comments
SHA1	Timing Analysis Attack	Constant Time Implementation	
	Cache Attack	Memory Access pattern is independent of any confidential data	
SHA2	Timing Analysis Attack	Constant Time Implementation	
	Cache Attack	Memory Access pattern is independent of any confidential data	
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 Security Levels

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

Table 4

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

13 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

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

14.1 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.

14.2 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.