Microsoft Windows

FIPS 140 Validation

Microsoft Windows 10 (May 2019 Update, November 2019 Update and May 2020 Update)

Non-Proprietary

Security Policy Document

Document Information	
Version Number	1.1
Updated On	October 12, 2022

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.

Version History

Version	Date	Summary of changes
1.0	November 4, 2020	Draft sent to NIST CMVP
1.1	October 12, 2022	Updates in response to NIST comments

TABLE OF CONTENTS

1 Introduction

Windows Resume, WINRESUME.EFI and 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 the hibernation data file which was encrypted by BitLocker Drive Encryption, when Windows has been previously put into a hibernate (S4) power state and returning to the working (S0) power state. Windows Resume is a part of BitLocker Drive Encryption, which is a data protection feature of the Windows 10 operating system which encrypts data on a storage volume.

1.1 List of Cryptographic Module Binary Executables

The Windows Resume module contains the following binaries. Each binary has a distinct implementation per build for each instruction set (x86, x64, ARM64).

- WINRESUME.EFI
- WINRESUME.EXE

The Windows builds and instruction sets covered by this validation are:

- Windows 10 version 1903, build 10.0.18362
  - x86
  - x64
- Windows 10 version 1909, build 10.0.18363
  - x86
  - x64
- Windows 10 version 2004, build 10.0.19041
  - x86
  - x64
  - ARM64

Tables 1-3 below present the matrix of hardware platforms, Windows builds, and Windows editions validated.

1.2 Validated Platforms

The Windows editions covered by this validation are:

- Microsoft Windows 10 Home Edition (32-bit version)
- Microsoft Windows 10 Pro Edition (64-bit version)
- Microsoft Windows 10 Enterprise Edition (64-bit version)
- Microsoft Windows 10 Education Edition (64-bit version)

The Windows Resume components listed in Section 1.1 were validated using the combination of computers and Windows operating system editions specified in the table below.

All the computers for Windows 10 and Windows Server listed in the table below are all 64-bit Intel architecture and implement the AES-NI instruction set but not the SHA Extensions. The exceptions are:

- Dell Inspiron 660s - Intel Core i3 without AES-NI and SHA Extensions
- HP Slimline Desktop - Intel Pentium with AES-NI and SHA Extensions
- Dell PowerEdge 7425 - AMD EPYC 7251 with AES-NI and SHA Extensions
- Microsoft Surface Pro X - Microsoft SQ1 with Arm Neon

Table 1 Validated Platforms for Windows 10 and Windows Server version 1903

Computer	Windows 10 Home	Windows 10 Pro	Windows 10 Enterprise	Windows 10 Education	Windows Server Core	Windows Serve Core Datacenter
Microsoft Surface Go - Intel Pentium		√				
Microsoft Surface Book 2 - Intel Core i7		√	√			
Microsoft Surface Pro 6 - Intel Core i5		√	√			
Microsoft Surface Laptop 2 - Intel Core i5		√	√	√		
Microsoft Surface Studio 2 - Intel Core i7			√			
Microsoft Windows Server 2019 Hyper-V[1]						
Microsoft Windows Server 2016 Hyper-V[2]						
Dell Latitude 12 Rugged Tablet - Intel Core i5		√				

[1] Hardware Platform: Dell PowerEdge R740 Server - Intel Xeon Gold

[2] Hardware Platform: Dell PowerEdge R7425 Server - AMD EPYC 7251

Dell Latitude 5290 - Intel Core i7			√			
Dell PowerEdge R740 - Intel Xeon Gold						
Dell PowerEdge R7425 - AMD EPYC 7251						
Dell Inspiron 660s [with x86 Windows] - Intel Core i3	√					
HP Slimline Desktop - Intel Pentium		√				
HP ZBook15 G5 - Intel Core i5		√				
HP EliteBook x360 830 G5 - Intel Core i5			√			
Samsung Galaxy Book 10.6” - Intel Core m3		√				
Samsung Galaxy Book 12” - Intel Core i5			√			
Panasonic Toughbook - Intel Core i5		√				

Table 2 Validated Platforms for Windows 10 and Windows Server version 1909

Computer	Windows 10 Home	Windows 10 Pro	Windows 10 Enterprise	Windows 10 Education	Windows Server Core	Windows Server Core Datacenter
Microsoft Surface Go - Intel Pentium				√		
Microsoft Surface Go LTE - Intel Pentium			√			
Microsoft Surface Book 2 - Intel Core i7			√			

Microsoft Surface Pro LTE - Intel Core i5		√				
Microsoft Surface Pro 6 - Intel Core i5			√			
Microsoft Surface Laptop 2 - Intel Core i5		√				
Microsoft Surface Studio 2 - Intel Core i7		√				
Microsoft Windows Server 2019 Hyper-V[3]						
Microsoft Windows Server 2016 Hyper-V[4]						
Dell Latitude 7200 2-in-1 - Intel Core i7		√				
Dell Latitude 5300 2-in-1 - Intel Core i7			√			
Dell PowerEdge R740 - Intel Xeon Platinum						
Dell PowerEdge R7425 - AMD EPYC 7251						
Dell Inspiron 660s [with x86 Windows] - Intel Core i3		√				
HP ProBook 650 G5 - Intel Core i7		√				
HP EliteBook x360 830 G6 - Intel Core i7			√			
HP Slimline Desktop - Intel Pentium	√					

[3] Hardware Platform: Dell PowerEdge R740 Server - Intel Xeon Platinum
[4] Hardware Platform: Dell PowerEdge R7425 Server - AMD EPYC 7251

Panasonic Toughbook CF-33 - Intel Core i5			√			
Samsung Galaxy Book 10.6" - Intel Core m3		√				
Samsung Galaxy Book 12" - Intel Core i5			√			
Microsoft Surface Pro 7 - Intel Core m3		√				
Microsoft Surface Laptop 3 - Intel Core i5			√			

Table 3 Validated Platforms for Windows 10 and Windows Server version 2004

Computer	Windows 10 Home	Windows 10 Pro	Windows 10 Enterprise	Windows 10 Education	Windows Server Core	Windows Server Core Datacenter
Microsoft Surface Pro LTE - Intel Core i5		√				
Microsoft Surface Pro 7 - Intel Core i3			√			
Microsoft Surface Pro 6 - Intel Core i7			√			
Microsoft Surface Pro X - Microsoft SQ1			√			
Microsoft Surface Go - Intel Pentium				√		
Microsoft Surface Go LTE - Intel Core i7		√				
Microsoft Surface Go 2 - Intel Core m3		√				
Microsoft Surface Go 2 LTE - Intel Pentium			√			

Microsoft Surface Laptop 2 - Intel Core i5		√				
Microsoft Surface Laptop 3 - Intel Core i5		√				
Microsoft Surface Book 2 - Intel Core i7			√			
Microsoft Surface Studio 2 - Intel Core i7		√				
Microsoft Windows Server 2019 Hyper-V[5]						
Microsoft Windows Server 2016 Hyper-V[6]						
Dell Latitude 7200 2-in-1 - Intel Core i7		√				
Dell Latitude 5300 2-in-1 - Intel Core i7			√			
Dell PowerEdge R640 - Intel Xeon Gold						
Dell PowerEdge R740 - Intel Xeon Platinum						
Dell Inspiron 660s [with x86 Windows] - Intel Core i3		√				
Dynabook TECRA-X50-F - Intel Core i7		√				
HP Slimline Desktop - Intel Pentium	√					
HP ZBook 15G6 - Intel Core i7		√				

[5] Hardware Platform: Dell Precision 5810 - Intel Xeon E5
[6] Hardware Platform: Dell PowerEdge R740 - Intel Xeon Platinum

HP EliteBook x360 830 G6 - Intel Core i7			√			
HP ProBook 650 G5 - Intel Core i7		√				
Panasonic Toughbook FZ-55 - Intel Core i5			√			
Dell PowerEdge R7515 - AMD EPYC 7702P						

2 Cryptographic Module Specification

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.

The following configurations and modes of operation will cause Windows Resume to operate in a non-approved mode of operation:

- Boot Windows in Debug mode
- Boot Windows with Driver Signing disabled

2.1 Cryptographic Boundary

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

2.2 FIPS 140-2 Approved Algorithms

Table 4 Windows Resume implements the following FIPS 140-2 Approved algorithms:[7]

Algorithm	Windows 10 version 1903	Windows 10 version 1909	Windows 10 version 2004
FIPS 186-4 RSA PKCS#1 (v1.5) digital signature verification with 1024, 2048, and 3072 moduli; supporting SHA-1, SHA-256, SHA-384, and SHA-512	#C795	#C1367	#C1947
FIPS 180-4 SHS SHA-1, SHA-256, SHA-384, and SHA-512	#C785	#C1363	#C1897
FIPS 197 AES CBC 128and 256	#C785	#C1363	#C1897
NIST SP 800-38E AES XTS 128 and 256	#C785	#C1363	#C1897

[7] This module may not use some of the capabilities described in each CAVP certificate.

NIST SP 800-38C AES CCM 256	#C798	#C1364	#C1946
NIST SP 800-38D AES-256 GCM for decryption only	#C785	#C1363	#C1897
NIST SP 800-108 Key Derivation Function (KDF) HMAC (SHA-256)	#C785	#C1363	#C1897
FIPS PUB 198-1 HMAC-SHA-256	#C785	#C1363	#C1897

2.3 Non-Approved Algorithms

Windows Resume implements the following non-approved algorithm:

- IEEE 1619-2007 AES-XTS 128 and 256, non-compliant

2.4 FIPS 140-2 Approved Algorithms from Bounded Modules

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, Windows Resume depends on the following algorithms:

The Boot Manager version 1903 (module certificate # 3923) provides:

- CAVP certificate #C 795 (Windows 10 and Windows Server) for FIPS 186-4 RSA PKCS#1 (v1.5) digital signature verification with 2048 moduli; supporting SHA-256
- CAVP certificate #C 785 (Windows 10 and Windows Server) for FIPS 180-4 SHS SHA-256

The Boot Manager version 1909 (module certificate # 3923) provides:

- CAVP certificate #C 1367 (Windows 10 and Windows Server) for FIPS 186-4 RSA PKCS#1 (v1.5) digital signature verification with 2048 moduli; supporting SHA-256
- CAVP certificate #C 1363 (Windows 10 and Windows Server) for FIPS 180-4 SHS SHA-256

The Boot Manager version 2004 (module certificate # 3923) provides:

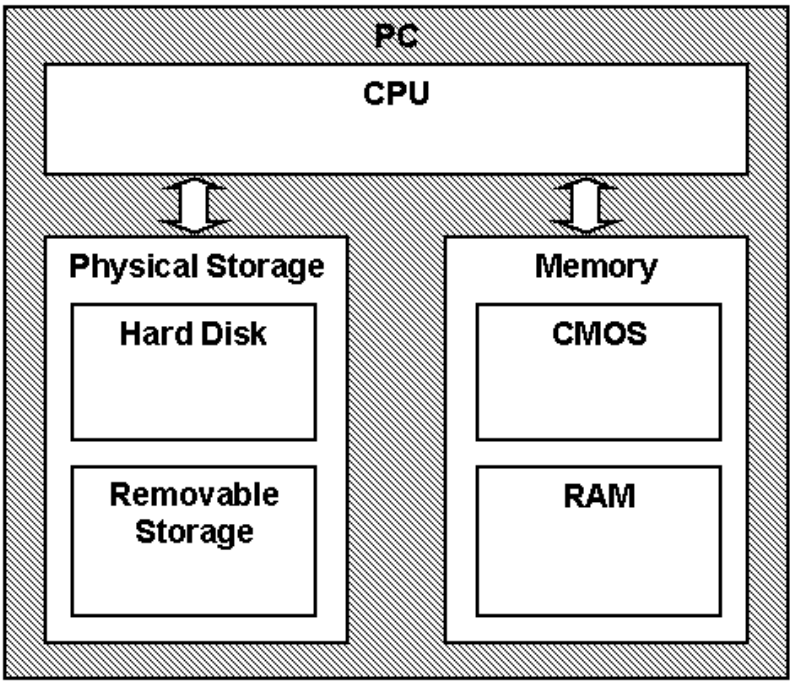
- CAVP certificate #C1947 (Windows 10 and Windows Server) for FIPS 186-4 RSA PKCS#1 (v1.5) digital signature verification with 2048 moduli; supporting SHA-256
- CAVP certificate #C1897 (Windows 10 and Windows Server) for FIPS 180-4 SHS SHA-256

2.5 Cryptographic Bypass

Cryptographic bypass is not supported by Windows Resume.

2.6 Hardware Components of the Cryptographic Module

The physical boundary of the module is the physical boundary of the computer that contains the module. The following diagram illustrates the hardware components used by the Windows Resume module:



3 Ports and Interfaces

3.1 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.

3.2 Status Output Interface

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

3.3 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 Windows Resume to the initial execution point of the Windows 10 kernel. Data exits the module in the form of the initial instruction address of the Windows 10 kernel.

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

3.4 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.

4 Roles, Services and Authentication

4.1 Roles

In Windows 10, authentication and assignment of roles happens after the OS initializes. Since Windows Resume functions only during the period between wake-from-hibernation and OS operation, the module's functions are fully automatic and not configurable. FIPS 140 validations define formal "User" and "Cryptographic Officer" roles. Both roles can use any Windows Resume service.

4.2 Services

Windows Resume services are described below. It does not export any cryptographic functions.

1. **Resuming the OS from Hibernation** – Windows Resume's main service is to load the hibernation state file (hiberfil.sys). When BitLocker is enabled on the operating system volume, Windows Resume decrypts the hiberfil.sys using the keys passed to it by Boot Manager. After loading the hibernation file, Windows Resume passes execution control to the kernel and it terminates its own execution.
2. **Show Status** – The module 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 display or to log files.
3. **Self-Tests** - The module provides a power-up self-test service that is automatically executed when the module is loaded into memory.
4. **Zeroizing Cryptographic Material** (see Cryptographic Key Management)

The following table maps the services to their corresponding algorithms and critical security parameters (CSPs) as described in Cryptographic Key Management.

Table 5 Services

Service	Algorithms	CSPs	Invocation
Resuming 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	RSA public key Full Volume Encryption Key (FVEK) (to load the BitLocker encrypted system hibernation file)	This service is fully automatic.

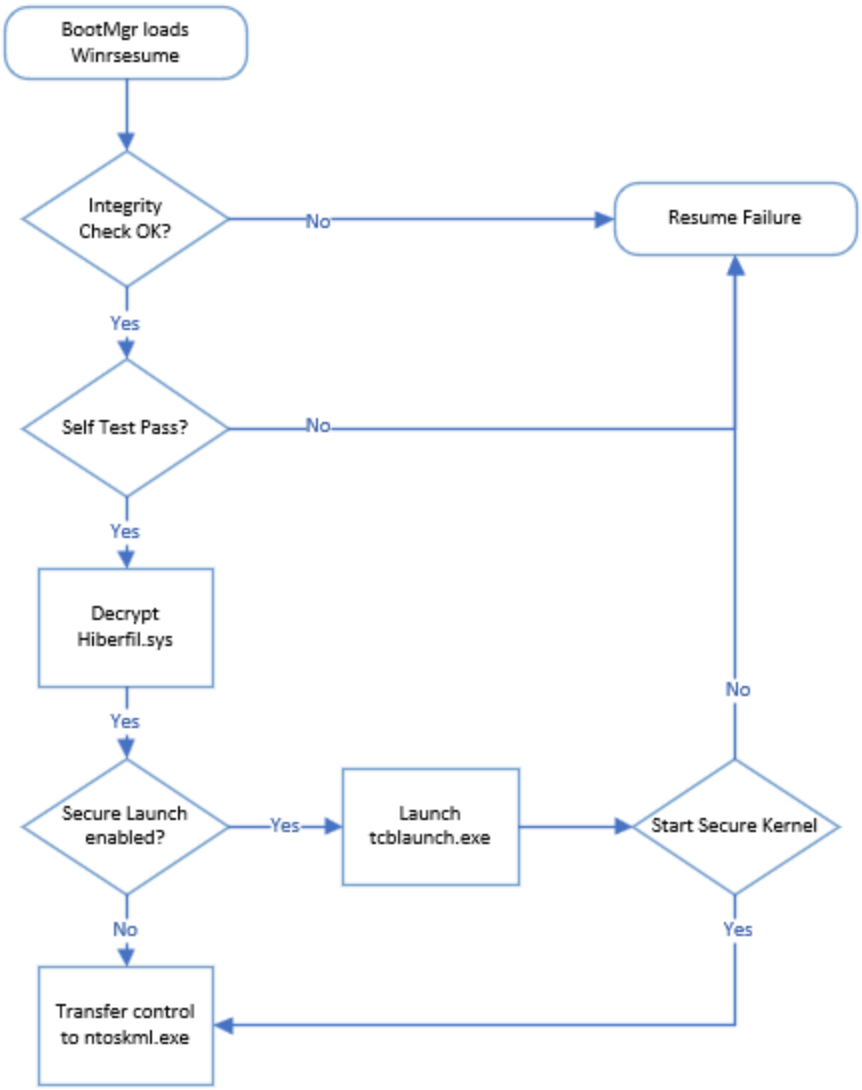
	FIPS 197 AES: AES CBC AES XTS[8] AES GCM AES CCM	VSM Key (to decrypt the encrypted data used by Virtual Secure Mode)	
Show Status	None	None	This service is fully automatic.
Self-Tests	FIPS 186-4 RSA PKCS#1 (v1.5) verify with public key KAT and signature verification KAT FIPS 180-4 SHS: SHA-1 KAT SHA-256 KAT SHA-512 KAT FIPS 197 AES: AES CBC KAT AES CCM KAT AES XTS KAT AES GCM KAT	None	This service is fully automatic.
Zeroizing Cryptographic Material	None	Full Volume Encryption Key (FVEK)	See Zeroization.

5 Finite State Model

5.1 Specification

The following diagram shows the finite state model for Windows Resume:

[8] The length of the data unit does not exceed 2^{20} AES blocks for storage applications such as BitLocker.



6 Operational Environment

The operational environment for Windows Resume is the Windows 10 operating system running on a supported hardware platform.

6.1 Single Operator

During the operating system resume process there is no logged on user, so the single operator requirement is met.

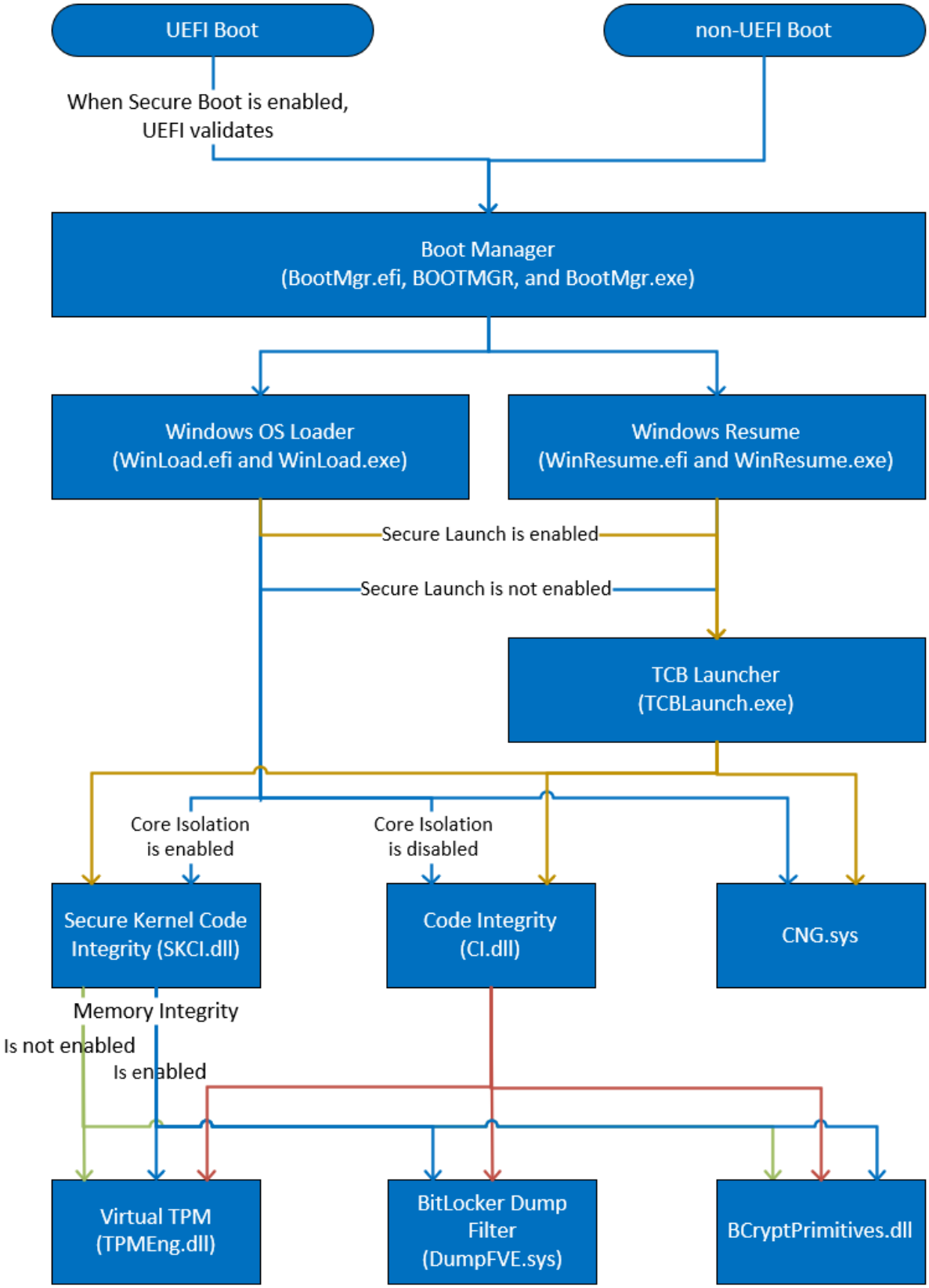
6.2 Cryptographic Isolation

While it is running, Windows Resume is the only process running on the computer.

6.3 Integrity Chain of Trust

Windows uses several mechanisms to provide integrity verification depending on the stage in the boot sequence and the hardware and configuration. The following diagram describes the Integrity Chain of trust for each supported configuration for the following versions:

- Windows 10 version 1903 and Windows Server build 10.0.18362
- Windows 10 version 1909 and Windows Server build 10.0.18363
- Windows 10 version 2004 and Windows Server build 10.0.19041



Note: TCB Launcher was not tested for Windows 10 version 1903.

The integrity of Windows Resume is checked by Boot Manager before it is loaded. This integrity check is based on the verification of an RSA signature over the binary using a 2048-bit key and a SHA-256 hash and verifying that the signing certificate is the Microsoft Code Signing Certificate.

Windows binaries include a SHA-256 hash of the binary signed with the 2048-bit Microsoft RSA code-signing key (i.e., the key associated with the Microsoft code-signing certificate). The integrity check uses the public key component of the Microsoft code signing certificate to verify the signed hash of the binary.

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

7 Cryptographic Key Management

7.1 Critical Security Parameters

When the System Volume is encrypted with BitLocker, Windows Resume uses this critical security parameter (CSP):

- Full Volume Encryption Key (FVEK) - 128 or 256-bit AES key that is used to decrypt data on disk sectors of the hard drive.
- VSM Key (VSMK) – 256-bit AES that is used to protect data used by the secure kernel during hibernation.
- Key Derivation Function Key (KDFK) - 256-bit key that is the output from the Windows Resume Internal Key Derivation Function
- RSA public key – 1024, 2048 or 3072-bit RSA public key to verify the integrity of components mentioned in **Error! Reference source not found.**

The FVEK is provided to Windows Resume by Boot Manager, and the VSMK is unsealed by the computer's TPM.

Windows Resume also uses as a CSP the public key component of the Microsoft code signing certificate as described in Integrity Chain of Trust.

7.2 Zeroization

The FVEK and VSMK are zeroized when the module is unloaded from memory after control is transferred to ntoskrnl.exe.

7.3 Access Control Policy

Windows Resume does not allow access to the cryptographic keys contained within it, so, an access control table is not included in this document. Windows Resume receives keys from outside and then

manages them appropriately once received. Windows Resume prevents access to its keys by zeroizing them.

8 Self-Tests

8.1 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-CCM Encrypt/Decrypt Known Answer Tests
- AES-CBC Encrypt/Decrypt Known Answer Tests
- XTS-AES Encrypt/Decrypt Known Answer Tests
- AES-GCM Encrypt/Decrypt Known Answer Tests
- SP 800-108 KDF Known Answer Test

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.

8.2 Conditional Self-Tests

Windows Resume does not perform conditional self-tests.

9 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 operating system.

The Windows 10 operating system must be pre-installed on a computer by an OEM, installed by the end-user, by an organization's IT administrator, or updated from a previous Windows 10 version downloaded from Windows Update.

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 must be checked 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 with Microsoft certificates. The Windows Update client only accepts content whose signed 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.

10 Mitigation of Other Attacks

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

Table 6 Mitigation of Other Attacks

Algorithm	Protected Against	Mitigation
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

11 Security Levels

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

Table 7 Security Levels

Security Requirement	Security Level
Overall	1
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

12 Additional Details

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

https://www.microsoft.com/en-us/windows

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

https://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 10 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.

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: 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.