McAfee Core Cryptographic Module (kernel)
Version 1.0 and 1.1.0.203.0

FIPS 140-2 Non-Proprietary
Security Policy

Level 1 Validation

Document revision 015, February 2017

Prepared for McAfee, Inc. by

McAfee, Inc.
2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

Rycombe Consulting Limited
http://www.rycombe.com
+44 1273 476366

Contents

Figures

1 Introduction

This section identifies the cryptographic module; describes the purpose of this document; provides external references for more information; and explains how the document is organized.

1.1 Identification

Module Name	McAfee, Inc. McAfee Core Cryptographic Module (kernel)
Module Version	1.0 and 1.1.0.203.0
Software Version	1.0 and 1.1.0.203.0

1.2 Purpose

This is the non-proprietary FIPS 140-2 Security Policy for the McAfee Core Cryptographic Module (kernel), also referred to as "the module" within this document. This Security Policy details the secure operation of McAfee Core Cryptographic Module (kernel) as required in Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

1.3 References

For more information on McAfee products please visit: http://www.mcafee.com. For more information on NIST and the Cryptographic Module Validation Program (CMVP), please visit http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.4 Document Organization

This Security Policy document is one part of the FIPS 140-2 Submission Package. This document outlines the functionality provided by the module and gives high-level details on the means by which the module satisfies FIPS 140-2 requirements. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission documentation may be McAfee, Inc. proprietary or otherwise controlled and releasable only under appropriate non-disclosure agreements. For access to these documents, please contact McAfee, Inc.

The various sections of this document map directly onto the sections of the FIPS 140-2 standard and describe how the module satisfies the requirements of that standard.

1.5 Document Terminology

TERM	DESCRIPTION
AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions. Seven instructions for accelerating different sub-steps of the AES algorithm included in some Intel and AMD microprocessors.
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameters
DLL	Dynamic Link Library
DLM	Dynamic Link Module (a type of DLL used in the Pre-boot environment)
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GUI	Graphical User Interface
IPC	Inter-process communication
MBR	Master Boot Record
McAfee ePO	McAfee ePolicy Orchestrator: A McAfee software installation to allow configuration and management of a McAfee product deployment
OS	Operating System
Pre-boot environment	The operating environment of a GPC before the operating system is loaded
SHA	Secure Hash Algorithm
SP	Security Policy
Storage Media	Any media for which Cryptographic Module protection in the form of data encryption is required. Storage Media include internal and external hard drives, memory sticks and floppy disks.
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
XML	Extensible Markup Language

Figure 1 Glossary

2 McAfee Core Cryptographic Module (kernel)

This section provides the details of how the module meets the FIPS 140-2 requirements.

2.1 Overview

The module provides AES encryption services to McAfee, Inc. products.

The module is packaged as a Mac OS or Microsoft Windows kernel mode device driver.

2.2 Module Specification

2.2.1 Hardware, Software and Firmware components

There are no specific hardware or firmware requirements for the module. The module is a software only module, which resides on a General Purpose Computer (see Figure 3).

There are three distinct, though functionally identical versions of the module, one for each of the environments indicated below:

File Name	Operating Environment	Package
MFECCF*aa*.sys	Microsoft Windows	32-bit
MFECCF*aa*.sys	Microsoft Windows	64-bit
MFECCF64*aa*.kext	Apple MacOS	64-bit

Figure 2 Module binary image

Note: On XP, a driver must have an 8.3 filename. *aa* are alphanumeric product identifiers, such as MFECCFDE.sys for Driver Encryption and MFECCFFF.sys for Files and Folders.

2.2.2 Cryptographic Boundary

The cryptographic boundary of the module is the case of the General Purpose Computer (GPC) on which it is installed. See Figure 3. The module is a software module running on a general-purpose computer. The processor of this platform executes all software. All software components of the module are persistently stored within the device and, while executing, are stored in the device local RAM.

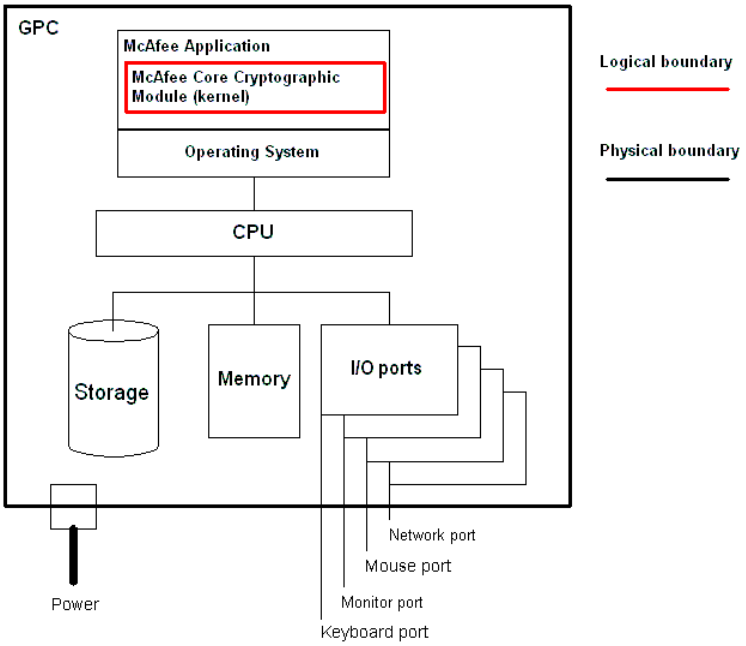

Figure 3 Block Diagram of the Cryptographic Boundary

2.2.3 Scope of Validation

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2, with Design Assurance at Level 3.

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Figure 4 Security Level specification per individual areas of FIPS 140-2

2.2.4 Cryptographic Algorithms

The module only supports an Approved mode of operation. The following approved algorithms are included within the module:

Algorithm Type	Algorithm	CAVP Certificate	Use
Hashing	SHA-256	#2287	Used in the module integrity test.
Message authentication code	HMAC	#1605	Module integrity testing.
Symmetric key	AES-256 – CBC, ECB and CFB8. Encrypt and decrypt	#2592 #2755	Service provided to encrypt and decrypt block of data.

Figure 5 Approved Algorithms

Note: The AES-256 algorithm can run on processors with or without AES-NI capability. However, it will only use AES-NI instructions if run on AES-NI enabled processors.

2.2.5 Components excluded from the security requirements of the standard

There are no components excluded from the security requirements of the standard.

2.3 Physical ports and logical interfaces

The module is classified as a multi-chip standalone module for FIPS 140-2 purposes. The module's physical boundary is that of the device on which it is installed. The device shall be running a supported operating system (OS) and supporting all standard interfaces, including keys, buttons and switches, and data ports.

The module provides all logical interfaces via Application Programming Interface (API) calls. This logical interface exposes services (described in section 2.4.2) that the User and operating system may utilize directly.

The logical interfaces provided by the module are mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, and status output as follows:

FIPS 140-2 Logical Interface	Module Mapping
Data Input	Parameters passed to the module via API calls
Data Output	Data returned from the module via API calls
Control Input	API Calls and/or parameters passed to API calls
Status Output	Information received in response to API calls
Power Interface	There is no separate power or maintenance access interface beyond the power interface provided by the GPC itself

Figure 6 Module Interfaces

2.4 Roles, Services and Authentication

2.4.1 Roles

The Cryptographic Module implements both a Crypto Officer role and a User role. Roles are assumed implicitly upon accessing the associated services. Section 2.4.2 summarizes the services available to each role.

ROLE	DESCRIPTION
Crypto Officer	The administrator of the module having full configuration and key management privileges.
User	General User of the module

Figure 7 Roles

2.4.2 Services

Most of the services provided by the module are provided via access to API calls using interfaces exposed by the module.

However, some of the services, such as power-up module integrity testing are performed automatically and so have no function API, but do provide status output.

SERVICE	API	DESCRIPTION	SERVICE INPUT	SERVICE OUTPUT
Key	epe_aesfips_init_key_context	Initialises an AES key expansion with the given key data.	Key and key context	Status, either success (zero) or failure (non-zero return code).
	epe_aesfips_reset_key_context	Resets the given key context.	Key context	Status, either success (zero) or failure (non-zero return code).
Symmetric encryption/decryption	epe_aesfips_crypt_bytes	Encrypts or decrypts some data.	Encryption: plaintext data, key context and IV. Decryption: encrypted data, key	Encryption: encrypted data. Decryption: plaintext data.

SERVICE	API	DESCRIPTION	SERVICE INPUT	SERVICE OUTPUT
			context and IV	
	epe_aesfips_crypt_blocks	Encrypts or decrypts data in blocks with the given key (context).	Encryption: plaintext data, key context and IV. Decryption: encrypted data, key context and IV	Encryption: encrypted data. Decryption: plaintext data.
	epe_aesfips_get_info	Gets the information about the algorithm.	None	Information about the encryption algorithm.
	eeff_crypt	Encrypts or decrypts some data.	Encryption: plaintext data, key context and IV. Decryption: encrypted data, key context and IV.	Encryption: encrypted data. Decryption: plaintext data.
	secure_crypt_blocks	Encrypts or decrypts data in blocks using a secured key	Encryption: plaintext data and IV. Decryption: encrypted data and IV.	Encryption: encrypted data. Decryption: plaintext data.
Self-tests	N/A	The power-up software integrity test and AES Known answer test are run	None	If integrity test passes, the module writes the string "Pass" to the module

SERVICE	API	DESCRIPTION	SERVICE INPUT	SERVICE OUTPUT
		automatically when the module is loaded and started.		IntegrityStatus registry key, otherwise writes the string “Fail” to this registry key and initiates a stop error. If the algorithm self-tests pass, the module is initialised and the entry function returns SUCCESS. If the algorithm self-tests fail, the module returns an error and is not loaded.
Show Status	N/A	Status is returned in response to individual service API calls and at the completion of the self-tests.	None	Module Status

Figure 8 User Services

SERVICE	API	DESCRIPTION	SERVICE INPUT	SERVICE OUTPUT
Installation	N/A	The module is deployed as part of a McAfee, Inc. product installation.	None	Installed module

SERVICE	API	DESCRIPTION	SERVICE INPUT	SERVICE OUTPUT
Uninstallation	N/A	The module is uninstalled during the uninstallation of the product that deployed the module.	None	Uninstalled module
Key Zeroization	N/A	Keys are zeroized using the zeroization procedure. This is described in section 2.7.4.	None	All keys zeroized.

Figure 9 Crypto Officer Services

2.4.3 Authentication

The module has been validated to FIPS 140-2 level 1 and no claims are made for authentication.

2.5 Physical Security

The Cryptographic Module is a software-only cryptographic module and therefore the physical security requirements of FIPS 140-2 do not apply.

2.6 Operational Environment

The Cryptographic Module has been tested on and found to be conformant with the requirements of FIPS 140-2 overall Level 1 on the following GPC operating systems:

Platform	CPU	RdRand[1]	AES-NI[2]	Operating System (all tested in single-user mode)	AES Register Implementation[3]
Dell E5510	Intel Core i3			Windows XP 32-bit	
Dell E5510	Intel Core i3			Windows 7 64-bit	
Lenovo Yoga	Intel Core i7	X	X	Windows 7 64-bit	
Lenovo Yoga	Intel Core i7	X	X	Windows 8 64-bit	
Dell Latitude 10	Intel Atom			Windows 8 32-bit	
MacBook	Intel Core 2 Duo			MacOS X Lion v10.7	
MacPro	Intel Xeon			MacOS X Mountain Lion v10.8	
MacBook Air	Intel Core i3	X	X	MacOS X Mountain Lion v10.8	
Mac Mini	Intel Core i5	X	X	MacOS X Lion v10.7	
MacBook Pro	Intel Core i7	X	X	MacOS X Mountain Lion v10.8	
Dell E6320	Intel Core i5		X	Windows Vista 32-bit	
Dell E6410	Intel Core i7		X	Windows Vista 64-bit	
Dell E6320	Intel Core i5		X	Windows 7 32-bit	
Lenovo W530	Intel Core i5	X	X	Windows 8 32-bit	
Lenovo W530	Intel Core i5	X	X	Windows 8 64-bit	
Intel UBHB2SISQ	Intel Core i5	X	X	Windows 8 64-bit	X
Lenovo Thinkpad 2	Intel Atom			Windows 8 32-bit	X
Intel UBHB2SISQ	Intel Core i5	X	X	Windows 8 running in 64-bit UEFI mode	X
Lenovo Thinkpad 2	Intel Atom			Windows 8 running in 32-bit UEFI mode	X

Figure 10 Operating Platforms

The module is also capable of running on the following platforms but has not been tested during this evaluation and no compliance is being claimed on these platforms:

- Windows 10 using McAfee Core Cryptographic Module version 1.1.0.203.0
- Windows Server 2008 (32-bit and 64-bit) with SP1
- Windows Server 2008 R2 (64-bit only)
- Windows 2003 Server (32-bit only) with SP2
- Windows 2003 Server R2 (32-bit only) with SP2

Note:

1. RdRand is an instruction for returning random numbers from a random number generator built into the microprocessor. However, RdRand is not used by the cryptographic module.
2. AES-NI (the Intel Advanced Encryption Standard (AES) New Instructions (AES-NI)) is an extension to the x86 instruction set architecture for microprocessors from Intel and AMD. The purpose of the instruction set is to improve the speed of applications performing encryption and decryption using AES.
3. AES Register Implementation: The module can use MSRs (model-specific registers) to store the AES System key so that it is stored within the microprocessor and not in system RAM. The decision to use the MSRs in this way is made by the application using the module and it is this application that is responsible for loading the key into the MSRs.

The cryptographic module runs in its own operating system threads. This provides it with protection from all other processes, preventing access to all keys, intermediate key generation values, and other CSPs.

The task scheduler and architecture of the operating system maintain the integrity of the cryptographic module.

The module supports only one single user and only one operator can have access to the device that contains the module at a time.

2.7 Cryptographic Key Management

2.7.1 Random Number Generators

The module does not contain any random number generators.

2.7.2 Key Generation

The module does not generate keys.

2.7.3 Key Table

The following tables list all of the keys and CSPs within the module, describe their purpose, and describe how each key is generated, entered and output, stored and destroyed.

KEY	System Key
PURPOSE	To encrypt all user data written to the module and decrypt all user data read from it.
KEY LENGTH/STRENGTH	AES 256 bit
GENERATION	N/A
STORAGE LOCATION	Not persistently stored.
ENCRYPTED/PLAINTEXT	Plaintext
ENTRY/OUTPUT	Entered into module via user service API (Key Establishment is N/A per IG 7.7). Not output.
DESTRUCTION	Zeroized using the key zeroization service.

Figure 11 Key Table

2.7.4 Key Destruction

All key material managed by the module can be zeroized using the zeroization procedure. This requires uninstallation of the cryptographic module and reformatting the hard drive on which it was installed.

The CO should uninstall the module and then reformat the hard drive on which it was installed and overwrite it at least once. The operator should remain present during this process. This process meets the requirements of IG 7.9 for key zeroization.

Reformatting the hard drive will remove any encrypted keys from the hard disk.

In this way all key material and CSPs are zeroized. There are no user-accessible plaintext keys or CSPs in the module.

2.7.5 Access to Key Material

The following table shows the access that an operator has to specific keys or other critical security parameters when performing each of the services relevant to his/her role.

Access Rights

Blank Not Applicable
R Read
W Write
U Use

SERVICE / KEY	SYSTEM KEY
User Services	
Key	W
Symmetric encryption	RWU
Self-tests	
Show Status	
Crypto Office Services	
Installation	U
Uninstallation	U
Key Zeroization	W

Figure 12 Access to keys by services

Note: Key zeroization zeroes all keys and CSPs, this is a “write” operation in that all keys are overwritten with zeroes.

2.8 Self-Tests

The module implements the self-tests required by FIPS 140-2. The following two sections outline the tests that are performed.

2.8.1 Power-up self-tests

OBJECT	TEST
AES-256	A separate encryption and decryption Known answer test for each AES implementation within the module
Module software	HMAC SHA-256 Integrity Check

Figure 13 Power-up self-tests

2.8.2 Conditional self-tests

There are no conditional tests that are run by the module.

2.9 Design Assurance

McAfee, Inc. employ industry standard best practices in the design, development, production and maintenance of all its products, including the FIPS 140-2 module.

This includes the use of an industry standard configuration management system that is operated in accordance with the requirements of FIPS 140-2, such that each configuration item that forms part of the module is stored with a label corresponding to the version of the module and that the module and all of its associated documentation can be regenerated from the configuration management system with reference to the relevant version number.

Design documentation for the module is maintained to provide clear and consistent information within the document hierarchy to enable transparent traceability between corresponding areas throughout the document hierarchy, for instance, between elements of this Cryptographic Module Security Policy (CMSP) and the design documentation.

Guidance appropriate to an operator's Role is provided with the module and provides all of the necessary assistance to enable the secure operation of the module by an operator, including the Approved security functions of the module.

Delivery of the Cryptographic Module to customers from the vendor is via the internet. When a customer purchases a license to use the Cryptographic Module software, they are issued with a grant number as part of the sales process. This is then used as a password to allow them to download the software that they have purchased. The delivery channel is protected using secured sockets. Once the Cryptographic Officer has downloaded the cryptographic module, it is his responsibility to ensure its secure delivery to the users that he is responsible for.

2.10 Mitigation of Other Attacks

The module does not mitigate any other attacks.