McAfee, Inc.

McAfee Endpoint Encryption for PCs

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation

Document revision 0.5, April 2009

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054,
888.847.8766
www.mcafee.com

Table of Contents

1 INTRODUCTION 3
1.1 PURPOSE 3
1.2 REFERENCES 3
1.3 DOCUMENT ORGANIZATION 3
2 MCAFEE ENDPOINT ENCRYPTION FOR PCS 4
2.1 MCAFEE ENDPOINT ENCRYPTION FOR PCS 5
2.2 MODULE INTERFACES 5
2.3 OPERATIONAL ENVIRONMENT 6
2.4 ROLES AND SERVICES 6
2.5 ACCESS TO SERVICES 7
2.6 PHYSICAL SECURITY 7
2.7 CRYPTOGRAPHIC KEY MANAGEMENT 8
2.7.1 Key generation 8
2.7.2 Key entry and output 8
2.7.3 Key storage 8
2.7.4 Zeroization of key material 9
2.7.5 Access to key material 9
2.8 CRYPTOGRAPHIC ALGORITHMS 10
2.9 SELF-TESTS 10
2.9.1 Power-up self-tests 10
2.9.2 Conditional self-tests 11
2.10 DESIGN ASSURANCE 11
3 FIPS MODE 12
4 APPENDIX A – CREATING THE FIPS ENABLE SCRIPT 13

Table of Figures

Figure 1: Block Diagram of the cryptographic boundary 4
Figure 2: Security Level specification per individual areas of FIPS 140-2 5
Figure 3: Roles 6
Figure 4: Services Authorized for Roles 7
Figure 5: CSPs used by McAfee Endpoint Encryption for PCs 8
Figure 6: Public Keys used by McAfee Endpoint Encryption for PCs 8
Figure 7: User Role 9
Figure 8: Crypto-Officer Role 9
Figure 9: Power-up Self-tests 10

1 INTRODUCTION

1.1 Purpose

This is the non-proprietary FIPS 140-2 Security Policy for the McAfee Endpoint Encryption for PCs cryptographic module, also referred to as "the module" within this document. This Security Policy details the secure operation of McAfee Endpoint Encryption for PCs 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.

1.2 References

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

1.3 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.

2 McAfee Endpoint Encryption for PCs

McAfee Endpoint Encryption for PCs (SW Version 5.1.6), also referred to simply as “module”, is a Software Only Module which resides on a General Purpose Computer (see Figure 1). In simple terms, McAfee Endpoint Encryption for PCs takes control of a user’s hard disk away from the operating system. McAfee Endpoint Encryption encrypts data written to the disk, and decrypts data read from the disk. If the hard disk drive is read directly, one would find only encrypted data, even in the Windows swap file and temporary file areas.

The cryptographic boundary of the module is the case of the Personal Computer (PC) on which it is installed. See Figure 1. The module is a software module running on a standard General Purpose Computing (GPC) device. The processor of the GPC device 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.

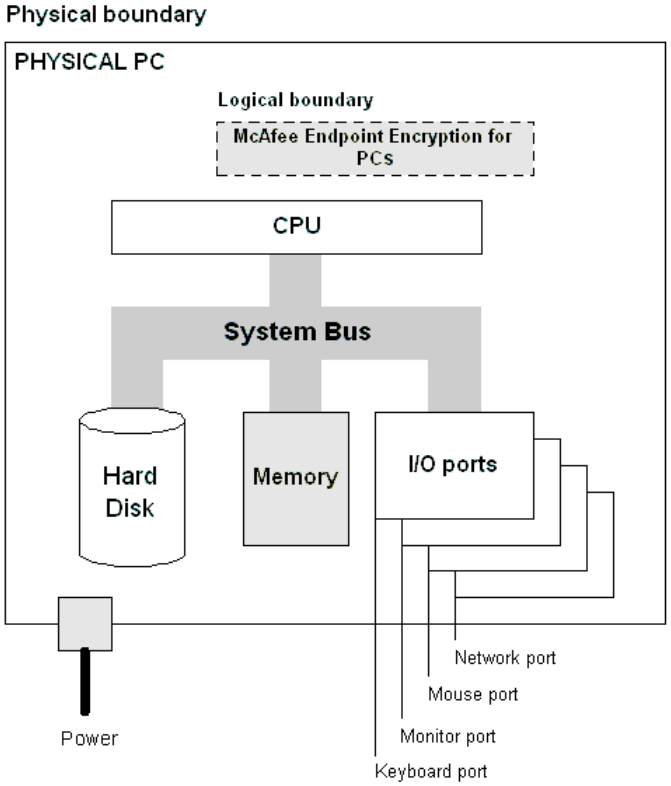

Figure 1: Block Diagram of the cryptographic boundary

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

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	**1**
Mitigation of Other Attacks	**N/A**

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

McAfee Endpoint Encryption for PCs has the option of being configured in different ways. At installation, the McAfee Endpoint Encryption Crypto Officer can specify how the hard disk can be encrypted by choosing one of three encryption modes: full, partial, or none. Full encryption mode encrypts an entire partition. Partial encryption mode encrypts only a portion of a partition or hard disk. 'None' encryption mode leaves the partition in plaintext with no encryption. (Refer to section 3 for FIPS compliant configuration.)

2.1 McAfee Endpoint Encryption for PCs

McAfee Endpoint Encryption for PCs is an application that consists of a number of individual drivers to handle encryption and synchronization. There is also a system tray application which provides a Graphical User Interface (GUI) to the operator via the GPC devices display. These components comprise the validated module. McAfee Endpoint Encryption hooks into a number of Windows system interfaces and is seamlessly integrated into the device operating system, with the only outward signs that it is installed being the proprietary logon screen and tray application. The McAfee Endpoint Encryption for PCs can be managed both locally as well as externally via an external Software Application called the Admin Server. Synchronization is the service used to securely manage and configure the McAfee Endpoint Encryption for PCs cryptographic module remotely using the Admin Server.

2.2 Module Interfaces

McAfee Endpoint Encryption for PCs 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.

McAfee Endpoint Encryption provides a logical interface via an Application Programming Interface (API) and a Graphical User Interface (GUI). This logical interface exposes services (described in section 2.4) that the User and operating system may utilize directly.

The logical interfaces provided by McAfee Endpoint Encryption for PCs are mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, and status output as follows:

- Data Input – Input to all driver functions, Software Interface (SWI), GUI
- Data Output – Output from all driver functions, GUI, Software Interface (SWI)
- Control Input – Input from TCP/IP interface, IPC interface, GUI, Software Interface (SWI)
- Status Output – Return codes from driver functions, GUI, Software Interface (SWI)

2.3 Operational Environment

The McAfee Endpoint Encryption for PCs 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:

- Microsoft Windows Vista 64
- Microsoft Windows XP
- Microsoft Windows Vista 32

The McAfee Endpoint Encryption for PCs is also supported on Microsoft Windows 2000.

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. For the purposes of FIPS 140-2, each of the Windows operating systems listed above must be configured as a single user operating system.

2.4 Roles and Services

McAfee Endpoint Encryption for PCs implements both a Crypto Officer role and a User role. Roles are assumed implicitly upon accessing the associated services. Figure 4 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 3: Roles

2.5 Access to Services

The following table, Figure 4, lists the authorized services linked to each of the Roles offered by the module.

Role	Authorized Services	Description
User	Synchronization	Establishes a secure network connection between the module and the remote Admin Server for the purpose of configuring the module.
	Encryption/Decryption	Encryption/Decryption of data written to the hard drive.
	Self-test Functions	Performs all FIPS 140-2 defined self tests.
	Recovery request	If the User is denied access to the module then the recovery request can be used to re-allow access. (Note: Successful utilization of this service requires Crypto Officer assistance.)
	Uninstall	Uninstalls the module from the host platform and zeroizes the Device Encryption Key and the Server Public Key
	Power Cycle	Power Cycles the host device and zeroizes CSPs in RAM
Crypto Officer	Synchronization	Establishes a secure network connection between the module and the remote Admin Server for the purpose of configuring the module.
	Configuration	Configuration of the module.
	View audit	View audit log information.
	Clear audit	Deletes the audit log.
	File Updates	This service is used to update or add-on module functionality as opposed to performing a full software update.
	Manage McAfee Endpoint Encryption for PCs (Cryptographic & Key Management Functions)	Manage McAfee Endpoint Encryption for PCs (Cryptographic & Key Management Functions)
	Software Updates	Loads new module software.
	Recovery	Will allow a User to access a module to which they are currently disallowed access.
	Set Attributes	Set module Attributes
	Change Attributes	Change module Attributes

Figure 4: Services Authorized for Roles

2.6 Physical Security

McAfee Endpoint Encryption for PCs is a software only cryptographic module and therefore the physical security requirements of FIPS 140-2 do not apply.

2.7 Cryptographic Key Management

The following tables list all Critical Security Parameters (CSPs) and public keys used within the McAfee Endpoint Encryption module. Currently, AES-256 is the only Approved encryption algorithm in McAfee Endpoint Encryption for PCs product and all encryption keys are AES-256 keys. The server public key is a DSA key.

Key type	Purpose
Device Encryption Key	To encrypt local storage, application databases, and external storage.
Session Key	Key used to encrypt traffic between device and remote server
Diffie-Hellman Shared Secret	Shared secret generated by the Diffie-Hellman Key exchange.
Diffie-Hellman Private Key	Private Diffie-Hellman component used during Session Key agreement.
DRNG Seed Key	Seed values and seed key used as input into the FIPS 186-2 DRNG.

Figure 5: CSPs used by McAfee Endpoint Encryption for PCs

Key type	Purpose
Server Public Key	DSA Key used to authenticate software during power-up self tests and software updates.
Diffie-Hellman Server Public Key	The Server Public Diffie-Hellman component used during Session Key agreement.
Diffie-Hellman Client Public Key	The Client Public Diffie-Hellman component generated internally by the module and used during Session Key agreement.

Figure 6: Public Keys used by McAfee Endpoint Encryption for PCs

2.7.1 Key generation

McAfee Endpoint Encryption for PCs generates symmetric key material and CSPs (and the Diffie-Hellman public/private key components used in session CSP establishment) using a FIPS 186-2 Appendix 3.1 compliant deterministic random number generator. The only symmetric keys/CSPs generated in this way are the Device Encryption Key and the Session Key.

2.7.2 Key entry and output

The module supports the following key entry:

- Entry of the Diffie-Hellman Server Public Key signed with the Server Private Key

The module supports the following key output:

- Plaintext output of the Diffie-Hellman Client Public Key
- Encrypted output of the Device Encryption Key

2.7.3 Key storage

Key material is stored in the McAfee Endpoint Encryption datastore in local GPC storage.

2.7.4 Zeroization of key material

All key material managed by the McAfee Endpoint Encryption for PCs has the ability to be zeroized. Zeroization is a two step procedure, which initiates two events. During uninstall, the module calls a zeroize command, which zeroizes the Device Encryption Key and Server Public Key; it also causes a power-cycle, which zeroizes all keys stored in RAM.

2.7.5 Access to key material

The following matrices (Figures 7 and 8) show 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.

	Key							
Service	**DK**	**SPK**	**DRNGSK**	**DHK**	**DHSPK**	**DHCPK**	**DHSS**	**SK**
Synchronization	R, O	R,W	R, W	W	W, E	W, O	W, R	R, W
Encryption/Decryption	R							
Self-test Functions								
Recovery Request								
Uninstall	Z	Z						
Power Cycle			Z	Z	Z	Z	Z	Z

Figure 7: User Role

	Key							
Service	**DK**	**SPK**	**DRNGSK**	**DHK**	**DHSPK**	**DHCPK**	**DHSS**	**SK**
Synchronization	R, O	R	R, W	W	W, E	W, O	W, R	R, W
View audit		R						R
Clear audit		R						R
Configuration	R	R						R
File Updates		R						R
Manage McAfee Endpoint Encryption for PCs (Cryptographic & Key Management Functions)	R	R						R
Software Updates		R, E, W						R
Recovery	R							R
Set Attributes		R						R
Change Attributes		R						R

Figure 8: Crypto-Officer Role

Access rights	
Blank	Not Applicable
W	Write access
R	Read Access
E	Key Entry
O	Key Output
Z	Zeroize Access

Keys	
DK	Device Encryption Key
SPK	Server Public Key
DRNGSK	DRNG Seed Key
DHK	Diffie-Hellman Private Key
DHSS	Diffie-Hellman Shared Secret
DHSPK	Diffie-Hellman Server Public Key
DHCPK	Diffie-Hellman Client Public Key
SK	Session Key

Note: If a service requires read or write access, it is the service as realized by module processes that requires access to the keys or CSPs. The operator (either User or Crypto Officer) does not have access to the CSPs themselves. The operator may change keys or use keys, but in all cases has no plaintext access to key material or CSPs.

2.8 Cryptographic Algorithms

McAfee Endpoint Encryption for PCs supports the following algorithms:

- FIPS-approved algorithms
  - AES-256
  - DSA
  - SHA-1
  - FIPS 186 Appendix 3.1 DRNG.
- Non FIPS-approved algorithms:
  - Diffie-Hellman (key establishment methodology provides 80 bits of security)
  - NDRNG (Used to seed the FIPS approved DRNG)

2.9 Self-Tests

McAfee Endpoint Encryption for PCs implements both power-up and conditional self tests as required by FIPS 140-2. The following two sections outline the tests that are performed.

2.9.1 Power-up self-tests

The following table, Figure 9, lists the power-up self-tests performed by the module:

SHA-1 known answer test
DSA known answer test
AES-256 known answer test
Software integrity test (DSA Signature verification)
Deterministic Random Number Generator Known Answer Test

Figure 9: Power-up Self-tests

Each of these tests is executed when the computer is turned on and the module first executes. If any of these tests fail, the module will not load. The module must be reset to re-execute these tests.

2.9.2 Conditional self-tests

There are a number of conditional tests that are run by the module. A continuous random number generator test is run every time the module requests a random number from either the FIPS Approved 186-2 DRNG or the NDRNG. Failure of this test may result in keys not being generated and an appropriate error message will be given. A test is also done when a software update or file update occurs. All files are digitally signed and this signature is checked prior to any update of the software.

2.10 Design Assurance

McAfee, Inc. employ industry standard best practices in the design, development, production and maintenance of the McAfee Endpoint Encryption product, 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.

3 FIPS Mode

The following procedures must be followed to operate McAfee Endpoint Encryption for PCs cryptographic module in a FIPS Approved mode. For more information please refer to the McAfee Administrators Guide for Endpoint Encryption for PCs:

1. The module software must be operating in “FIPS” mode. This is done by setting the FIPS registry key value from 0 (disabled) to 1 (enabled). The first step is to create a FIPS registry script (see Appendix A for details). Once the file is created, right click on the newly created .reg file and select merge from the drop down menu.
2. To verify that the registry has been updated properly the user must install a registry editor and navigate to `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier and verify the value of FipsMode equals 1.` .
3. All application databases and media on the device where McAfee Endpoint Encryption for PCs has been installed MUST be fully encrypted by selection of full encryption mode. This is performed by setting the module’s internal memory encryption parameter to “Encrypt Entire Device”.
4. The PC used to run McAfee Endpoint Encryption for PCs Client must be built using production grade components and configured in a single operator mode. To do this, the following operating system services must be disabled:
    - Fast user switching
    - Terminal services
    - Remote registry service
    - Secondary logon service
    - Telnet service
    - Remote desktop and Remote assistance services

4 Appendix A – Creating the FIPS enable script

The following needs to be saved to a text file with the extension ".reg" and then merged into the registry as a requirement for installing the module in a FIPS-compliant mode of operation:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier]
"FipsMode"=dword:00000001

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\1]
"Path"="c:\\windows\\system32\\drivers\\SafeBoot.sys"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\2]
"Path"="c:\\windows\\system32\\drivers\\SbAlg.sys"
```

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054,
888.847.8766
www.mcafee.com