McAfee, Inc.

McAfee Endpoint Encryption Manager

FIPS 140-2 Non-Proprietary
Security Policy

Level 2 Validation

Document revision 0.25, May 2011

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

1 Revision History

Date	Revision	Description
17 December 2009	0.3	Updated to address TOR_EE_MGR_L2_Algorithm Certs(v1)
29 January 2010	0.4	Modified to address TOR_EE_MGR_L1_and_L2_service_input_output(v1)
4 February 2010	0.5	Modified to address TOR_EE_MGR_L1_and_L2_Password-only_Token(v1)
22 February 2010	0.6	Modified in response to TOR_EE_FF_Keys(v6.1) and TOR_EE_FF_Keys(v8.1)
23 February 2010	0.7	Modified in response to TOR_EE_FF_L2_Security Policy Comments(v5)
25 February 2010	0.8	Modified in response to TOR_EE_FF_L2_Security Policy Comments(v7)
25 February 2010	0.9	Modified in response to TOR_EE_MGR_L1_and_L2_Recovery_Process(v2)
2 March 2010	0.10	Modified in response to TOR_EE_MGR_L1_and_L2_Security Policy Comments(v1)_Response
12 March 2010	0.11	Modified in response to TOR_EE_MGR_L1_and_L2_Security Policy Comments(v2b)
18 August 2010	0.12	Modified in response to TOR_EE_MGR_L1_and_L2_Security Policy Comments(vdjc1) and TOR_EE_MGR_L1_and_L2_Security Policy Comments(vdjc2)
14 December 2010	0.13	Modified following code review
4 January 2011	0.14	Modified in response to TOR4_EE_MGR_5.2.6_L1_and_L2_Comments and TOR5_EE_MGR_5.2.6_L1_and_L2_Comments
14 January 2011	0.15	Modified in response to TOR6_EE_MGR_5.2.6_L1_and_L2_Comments
19 January 2011	0.16	Modification to “FipsMode” script instructions
26 January 2011	0.17	Modification to installation instructions
28 January 2011	0.18	Updated PIV authentication notes and Table 11, 12
29 January 2011	0.19	Modified in response to TOR11_EE_MGR_5.2.6_L1_and_L2_Comments
31 January 2011	0.20	Modified in response to TOR12_EE_MGR_5.2.6_L1
9 March 2011	0.21	Modified following comments from NIST
10 March 2011	0.22	Modified following comments from NIST
18 March 2011	0.23	Modified in response to TOR_EE_MGR_L1_and_L2_Security Policy Comments(v3)
26 April 2011	0.24	Modified in response to TOR_EE_MGR_L1_and_L2_Security Policy Comments(v4)
10 May 2011	0.25	Modified in response to TOR_EE_MGR_L1/L2 SPs

Table of Contents

Table of Figures

2 INTRODUCTION

2.1 Purpose

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

2.2 References

For more information on McAfee Endpoint Encryption Manager and the McAfee Endpoint Encryption product range 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.

2.3 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.

3 McAfee Endpoint Encryption Manager

McAfee Endpoint Encryption Manager (SW Version 5.2.6), 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 Manager is a management console application that allows an authorized Crypto Officer to manage, configure and deploy McAfee Endpoint Encryption point product software.

In order to install the module it is first necessary to install the core McAfee Endpoint Encryption Manager software (Endpoint Encryption Manager v5.2.6, file download McAfee_EEM_526.zip) and then to install the McAfee Endpoint Encryption for PC software (Endpoint Encryption for PC v5.2.6, file download McAfee_EEPC_526.zip).

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 Common Criteria EAL2 certified operating environment. 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.

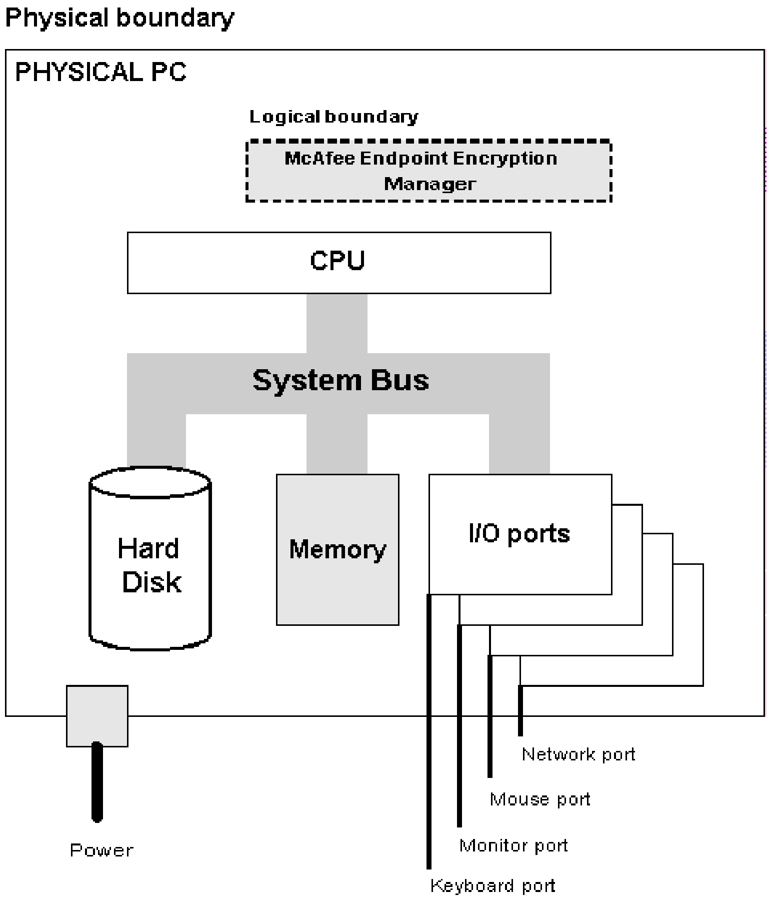

Figure 1: Block Diagram of the cryptographic boundary

However, the module consists of a number of components:

- The McAfee Endpoint Encryption Manager Management Console GUI application,
- Token modules to facilitate user identification and authentication,
- The Object Directory, a central repository for system objects (Supported accessible Objects are Users, Machines, Servers, Files, Directories, and Groups),
- The McAfee Endpoint Encryption Database Server that allows McAfee Endpoint Encryption point products to connect to and synchronize with the Object Directory,
- The McAfee Endpoint Encryption Connector Manager is responsible for managing the association of information between the Endpoint Encryption Object Directory and another data source. This remote source may be another Object Directory, or may be some third party system (for example an X500 directory over LDAP, or Microsoft Active Directory).

For FIPS 140-2 purposes, all of the components of the module are installed and running on a single General Purpose Computer (GPC).

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

Security Requirements Section	**Level**
Cryptographic Module Specification	**2**
Module Ports and Interfaces	**2**
Roles, Services and Authentication	**3**
Finite State Model	**2**
Physical Security	**N/A**
Operational Environment	**2**
Cryptographic Key Management	**2**
EMI/EMC	**2**
Self-Tests	**2**
Design Assurance	**3**
Mitigation of Other Attacks	**N/A**

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

3.1 McAfee Endpoint Encryption Manager

McAfee Endpoint Encryption Manager is a Windows GUI whose purpose is to allow McAfee Endpoint Encryption Systems to be deployed, configured and synchronized.

McAfee Endpoint Encryption Manager is able to manage a number of McAfee Endpoint Encryption products, including:

- McAfee Endpoint Encryption for PCs
- McAfee Endpoint Encryption for Files and Folders
- McAfee Endpoint Encryption for Mobile

User and Machine configurations are created and modified using McAfee Endpoint Encryption Manager and stored in a central database, the Object Directory.

Every time a Endpoint Encryption protected system starts, and optionally every time the user initiates a remote access connection or after a set period of time, Endpoint Encryption tries to contact its Object Directory.

Endpoint Encryption applications query the directory for any updates to their configuration, and if needed download and apply them. Typical updates could be a new user assigned to the machine by an administrator, a change in password policy, or an upgrade to the Endpoint Encryption operating system or a new file specified by the administrator. At the same time Endpoint Encryption uploads details like the latest audit information, any user password changes, and security breaches to the Object Directory. In this way, transparent synchronization of the enterprise becomes possible.

3.2 Module Interfaces

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

McAfee Endpoint Encryption Manager provides a logical interface via a Graphical User Interface (GUI) and a secure communications channel via a TCP/IP interface with McAfee Endpoint Encryption applications. This logical interface exposes services (described in section 3.4) that the User and McAfee Endpoint Encryption applications may utilize directly.

McAfee Endpoint Encryption Manager provides a logical interface to physical tokens outside of the cryptographic boundary to provide user authentication.

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

- Data Input – Input from TCP/IP interface during application synchronization, GUI, token input
- Data Output – Output to TCP/IP interface during application synchronization, GUI, user authentication to physical token
- Control Input – Input from TCP/IP interface, GUI
- Status Output –GUI

3.3 Operational Environment

The cryptographic module is capable of running and tested in FIPS 140-2 Level 2 mode on the following Common Criteria-evaluated platforms:

- Windows Server 2003 SP1 on Dell Optiplex GX620
- Windows Server 2008 on Dell PowerEdge 2970

Windows Server Enterprise 2008 (64 bit) and Dell PowerEdge 2970, 1.7 GHz quad core AMD Opteron 2344 Processor (2 CPUs), 64-bit
http://www.commoncriteriaportal.org/files/epfiles/st_vid10291-st.pdf

Windows Server 2003 SP1 Dell Optiplex GX620 and 3.0 GHz Intel Pentium D Processor 830 (1 CPU), 32-bit
http://www.commoncriteriaportal.org/files/epfiles/20080303_st_vid10184-st.pdf

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

- Microsoft Windows 7
- Microsoft Windows Vista 64
- Microsoft Windows XP
- Microsoft Windows Vista 32
- 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.

For the purposes of FIPS 140-2 validation, the module supports only one single user and only one operator can have access to the GPC 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.

3.4 Roles and Services

McAfee Endpoint Encryption Manager implements both a Crypto Officer role and a User role. The module provides identity-based authentication for both Users and Crypto Officers. 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, with only read access to the objects in the directory.

Figure 3: Roles

Each object in the directory has a certain "administration privilege" with a range of between 1 (lowest) to 32 (root administrator), no object except the root administrator can change the attributes of an object of its privilege or above, but some attributes can be read regardless. This mechanism stops low privilege users from changing their own configuration, and protects high-level administrators from the activities of lower levels.

For the purposes of FIPS 140-2 validation, a Crypto Officer has an administration privilege level of 32, and a User has an administration privilege level of 1. Further, the configuration of the module is required to restrict access for all Users to “View” operations, that is, read-only operations.

3.4.1 User and Crypto Officer authentication

Users and Crypto Officers logon to the module in the same way: identity-based access control and authentication using tokens.

The module supports several different types of token to provide identity based authentication.

The CAC and PIV cards and card readers are outside of the cryptographic boundary but the module provides an interface to these for authentication purposes.

The CAC and PIV smartcards are PKI tokens. Access control to the token is provided via a user name and a password, that is access to the token is password protected. Once access to the token is granted, the certificate on the token is used to decrypt an encrypted user CSP which is then used to decrypt the machine key. Each user is assigned a unique user name. Possession of the physical token, the ability to access it using a secret password, allows the module to use the token key to decrypt the user key matching the user. This provides identity based authentication of that user.

Note regarding PIV authentication:
In order to use PIV Authentication you need to do the following:
a. The full Principal Name of the user must be used in the EE MGR username field. This can be found in the PIV certificate.
b. In the file SbTokenPIV.ini file the usernametype field must be set to 0 (This is so the software checks against the full principal name).

Figure 4 summarizes the authentication mechanism for each of these roles, and Figure 5 describes the strength of these mechanisms.

Role	Type of Authentication	Authentication Data
User	Identity-based	1024 bit tokens for CAC and PIV are used for User and Crypto Officer authentication to the module. A password is used to access the token.
Crypto Officer	Identity-based	1024 bit tokens for CAC and PIV are used for User and Crypto Officer authentication to the module. A password is used to access the token.

Figure 4 Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Password	It is possible to configure the minimum password length and the type of characters that can be used in a password. It is also possible to configure the client to lock up after a specified number of unsuccessful password entry attempts. If a minimum password length of 4 is used, and the password is restricted to alphanumeric characters, this gives a chance of success of 1 in 62^4 or 1 in 14,776,336 for guessing a password, which is greater than required. McAfee, Inc. recommends a minimum password length of 5 characters, giving a random chance of success of 1 in 916,132,832. If 10 login attempts are possible in one minute, this gives a chance of successfully guessing the password at 1 in 91,613,283. This is significantly better than the acceptable probability of 1 in 100,000.
PKI encryption	1024 bit tokens for CAC and PIV are used for User and Crypto Officer authentication to the module.

Figure 5 Strength of Authentication Mechanisms

3.5 Access to Services

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

Role **User**	**Crypto Officer**	**Authorized Services**	**Description**	**Service Input**	**Service Output**
	X	Create Installation Set	Creates an installation set that contains all of the software needed to deploy the particular Endpoint Encryption point product that the installation set represents.	Crypto Officer chooses "Create Installation Set" option	Installation set
	X	Synchronization	Establishes a secure network connection between the module and a McAfee Endpoint Encryption point product for the	Synchronization request either triggered manually or according to a predetermined	Updated client module. Client module datastore synchronized

Role				Service Input	Service Output
User	Crypto Officer	Authorized Services	Description		
			purpose of configuring the module.	policy	with Object Directory
X	X	Self-test Functions	Performs all FIPS 140-2 defined self tests.	power cycle	Self-test results
	X	Recovery	If the Endpoint Encryption point product user is denied access to their PC/device then the recovery service can be used to enable access again.	Offline Challenge/ Response	Restored user access to Client CM
X	X	Uninstall	Uninstalls the module from the host platform. Uninstallation does not remove the Object Directory. This must be manually deleted after software uninstallation is complete.	User uninstalls software	All keys and CSPs zeroized.
	X	Configuration	Configuration of the module.	Crypto Officer makes changes to Object Directory using the McAfee Endpoint Encryption Manager GUI	Updated Object Directory
X	X	View audit	View audit log information.	Crypto Officer or User chooses to view audit from McAfee Endpoint Encryption Manager GUI	Audit log information displayed by GUI
	X	Clear audit	Deletes the audit log.	Crypto Officer uses McAfee Endpoint Encryption Manager GUI to clear audit information	Specific Audit information is deleted

Role				Service Input	Service Output
User	Crypto Officer	Authorized Services	Description		
	X	File Updates	This service is used to update or add-on functionality to Endpoint Encryption point products as opposed to performing a full software update.	Crypto Officer uses McAfee Endpoint Encryption Manager GUI to configure file updates	Updated files are stored in the Object Directory ready to be deployed via synchronization
	X	Machine Control	Functionality in McAfee Endpoint Encryption for Devices point products allows a Crypto Officer using the module to “force synchronization”, “reboot machine” or “lock machine” for a device connected to the McAfee Endpoint Encryption Manager.	Crypto Officer uses the McAfee Endpoint Encryption Manager GUI control a connected client module	Client module is synchronized, rebooted or locked as appropriate
	X	Create, Modify and Delete Objects and their properties	Supported accessible Objects are Users, Machines, Servers, Files, Directories, and Groups. McAfee Endpoint Encryption Manager provides a GUI to allow authorized operators to create, modify and delete Objects and their properties and for any changes to be stored in the Object Directory	Crypto Officer uses the McAfee Endpoint Encryption Manager GUI to make changes to objects and their properties	Changes are stored in the Object Directory
X	X	View objects and their properties	McAfee Endpoint Encryption Manager provides a GUI to allow authorized operators to view Objects and their properties.	Crypto Officer or User uses the McAfee Endpoint Encryption Manager GUI to view objects and their properties	The requested information is displayed by the GUI
X	X	Show self-test	Each of the Endpoint	Crypto Officer	The requested

Role User	Crypto Officer	Authorized Services	Description	Service Input	Service Output
		status	Encryption Manager Components displays its own self-test results. The failure of core components is reported in a Windows dialogue box. Failure of other components is reported in the Windows Application Event Log, success is reported in the Endpoint Encryption Manager Management Console status log window, the status bar in the Endpoint Encryption Manager Connector Manager, or the Endpoint Encryption Database Server server window, as appropriate	or User uses the McAfee Endpoint Encryption Manager GUI, Database server or Operating System Event Log to view self-test results.	information is displayed by the GUI or associated application

Figure 6: Services Authorized for Roles

3.6 Physical Security

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

3.7 Cryptographic Key Management

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

Key type	Purpose
Database Key	To encrypt the Object Directory.
Machine Key	Each PC/device has a key that is used to encrypt its hard disk/data. This key is also used to authenticate an Endpoint Encryption point product to the McAfee Endpoint Encryption Manager.
User Key	To encrypt secure user attributes.
User Recovery Key	To recover the user key.
Machine Recovery Key	To recover the machine key

Key type	Purpose
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. Used to derive the session key.
Diffie-Hellman Private Key	Private Diffie-Hellman component used during Session Key agreement.
User password	To authenticate users to the product.
DRNG Seed Key	Seed key used as input into the FIPS 186-2 DRNG.
DRNG Seed Values	Seed values used as input into the FIPS 186-2 DRNG.
Server Private Key	Private portion of the key pair used to authenticate the remote server and verify the authenticity of a software image or update during the module integrity test.

Figure 7: CSPs used by McAfee Endpoint Encryption Manager

Key type	Purpose
Manufacturer Public Key	DSA Key used to authenticate software during power-up self tests and software updates.
User Authentication Certificate	CAC/PIV Cards only: Employed in the user identification process during logon.
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 8: Public Keys used by McAfee Endpoint Encryption Manager

Key type	Key length/ strength	Storage location	Encrypted /Plaintext	Generation/ establishment	Entry/output
Database Key	AES 256 bit	Object Database	Encrypted	FIPS 186-2 DRNG	N/A
Machine Key	AES 256 bit	Object Database	Encrypted	Externally	Received from client application during installation
User Key	AES 256 bit	Object Database	Encrypted	FIPS 186-2 DRNG	Sent to client during client installation
User Recovery Key	AES 256 bit	Object Database	Encrypted	FIPS 186-2 DRNG	Manually output as obfuscated plaintext during user recovery
Machine Recovery Key	AES 256 bit	Object Database	Encrypted	Externally	1) Manually output as obfuscated plaintext during

Key type	Key length/ strength	Storage location	Encrypted /Plaintext	Generation/ establishment	Entry/output
					machine recovery. 2) Received from client application during client installation
Session Key	AES 256 bit	Ephemeral	Plaintext	Diffie-Hellman key establishment protocol	N/A
Diffie-Hellman Shared Secret	1024 bits	Ephemeral	Plaintext	Diffie-Hellman key establishment protocol	N/A
Diffie-Hellman Private Key	1024/2048 bit	Ephemeral	Plaintext	Diffie-Hellman key establishment protocol	N/A
User password	5+ characters	N/A	N/A	N/A	N/A
DRNG Seed Key	320 bit	Ephemeral	Plaintext	MD5	N/A
DRNG Seed Values	160 bit	Ephemeral	Plaintext	MD5	N/A
Server Private Key	1024 bit	Object Database	Encrypted	FIPS 186-2 DRNG	N/A
Manufacturer Public Key	1024 bit	Object Database	Plaintext	N/A	Deployed with installation
User Authentication Certificate	1024 bits	Object Database	Plaintext	N/A	Installed during configuration
Diffie-Hellman Server Public Key	1024/2048 bit	Ephemeral	Plaintext	Diffie-Hellman key establishment protocol	Exchanged with client during session key establishment
Diffie-Hellman Client Public Key	1024/2048 bit	Ephemeral	Plaintext	Diffie-Hellman key establishment protocol	Exchanged with server during session key establishment

Figure 9 Key information

3.7.1 Key generation

McAfee Endpoint Encryption Manager 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 Database Key, User Key, User recovery key and the Session Key.

3.7.2 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 electronic output of the Diffie-Hellman Client Public Key
- Encrypted electronic output of the User Key
- Obfuscated plaintext manual output of the Machine Recovery Key
- Obfuscated plaintext manual output of the User Recovery Key

Note: The Diffie Hellman key exchange takes place between a Server (the cryptographic module) and a Client machine (e.g. Endpoint Encryption for PC Client). The corresponding keys are referred to as Diffie-Hellman Server keys and Diffie-Hellman Client keys.

3.7.3 Key storage

Key material is stored in the McAfee Endpoint Encryption Manager Object Directory in local GPC storage.

3.7.4 Zeroization of key material

All key material managed by the McAfee Endpoint Encryption Manager has the ability to be zeroized.

In meeting the requirements of IG 7.9 for key zeroization, in order to zeroize all keys and CSPs, the operator should to be uninstall the module and then the hard drive on which it was installed should be reformatted and overwritten at least once. The operator should remain present during this process. Uninstallation will remove any plaintext keys and CSPs from memory and from the hard disk. Reformatting the hard drive will remove any encrypted or public keys from the hard disk. In this way all key material is zeroized. There are no user-accessible plaintext keys or CSPs in the module. Following the zeroization process, all keys and CSPs have been erased and overwritten.

3.7.5 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	**MPK**	**DRNGSK**	**DHK**	**UAC**	**DHSPK**	**DHCPK**	**DHSS**	**SK**
Create Installation Set								
Synchronization	R,W	R, W	W		W, E	W, O	W, R	R, W
Self-test Functions								
Recovery								
Uninstall								
Configuration	R,W	R, W	W		W, E	W, O	W, R	R, W
View audit								
Clear audit								

File Updates	R,W	R, W	W		W, E	W, O	W, R	R, W
Machine Control	R,W	R, W	W		W, E	W, O	W, R	R, W
Create, Modify and Delete Objects and their properties	R,W	R, W	W		W, E	W, O	W, R	R, W
View objects and their properties	R,W	R, W	W		W, E	W, O	W, R	R, W

Figure 10: Key usage part 1

	Key							
Service	**DBK**	**MEK**	**UEK**	**URK**	**MRK**	**PW**	**DRNGSD**	**SSK**
Create Installation Set								
Synchronization		R						
Self-test Functions							R, W	
Recovery	R			R	R			
Uninstall								
Configuration	R							
View audit								
Clear audit								
File Updates								
Machine Control	R	R						
Software Updates								
Create, Modify and Delete Objects and their properties	R		W	W		W		
View objects and their properties	R							

Figure 11: Key usage part 2

Access rights

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

Keys

DBK	Database Key
MEK	Machine Key
UEK	User Key
URK	User Recovery Key
MRK	Machine Recovery Key
MPK	Manufacturer Public Key
UAC	User Authentication Certificate
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
PW	User password
DRNGSD	DRNG Seed Values
SSK	Server Private 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 other than user or machine recovery, has no plaintext access to key material or CSPs. When carrying out user recovery or machine recovery, a Crypto Officer is required to read recovery keys to a remote user of a client module. Such recovery keys are manually output in obfuscated plaintext.

3.8 Cryptographic Algorithms

McAfee Endpoint Encryption Manager supports the following algorithms:

- FIPS-approved algorithms
  - AES-256 (CAVP Certificate #1366)
  - DSA (CAVP Certificate #446)
  - SHA-1 (CAVP Certificate #1247)
  - FIPS 186 Appendix 3.1 DRNG (CAVP Certificate #752).
- Non FIPS-approved algorithms:
  - Diffie-Hellman (key establishment methodology provides 80-112 bits of encryption strength since the module may use 1024 and 2048 bit DH keys)
  - MD5-based NDRNG (Used to seed the FIPS approved DRNG)

3.9 Self-Tests

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

3.9.1 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 12: 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.

3.9.2 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 MD5-based NDRNG. Failure of this test may result in keys not being generated and an appropriate error message will be given. A software integrity test is also done whenever a component is dynamically loaded into the module. All files are digitally signed and this signature is checked prior to any load operation.

3.10 Design Assurance

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

3.11 Mitigation of Other Attacks

The module does not mitigate other attacks.

4 FIPS Mode

The following procedures must be followed to operate McAfee Endpoint Encryption Manager 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 freshly installed in order to operate in FIPS mode, and not installed as an upgrade to an existing installation.
2. When installing the module, accept the default options. However, in the “Optional Components” page, deselect “Endpoint Encryption Web Recovery (Apache/CGI), and deselect all tokens except for “ActivIdentity Certificate Smartcard/USB Key” and “PIV Smart Card (PKI)”, that is “ActivIdentity Certificate Smartcard/USB Key” and “PIV Smart Card (PKI)” are the only tokens selected.
3. 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.
4. To verify that the registry has been updated properly the user must install a registry editor and navigate to `HKEY_LOCAL_MACHINE\Software\SafeBoot International` and verify the value of `FipsMode` equals 1.
5. The McAfee Endpoint Encryption Manager must be configured so that all Crypto Officers have an administration privilege level of 32 and the all Users have an administration privilege level of 1, and that users only have view access to audit data and to objects and their properties and that Users are not allowed to control machines, create installation sets or perform recovery operations.
6. Users of the cryptographic modules must use one of the tokens defined in section 3.4.1 to authenticate themselves to the module.
7. The PC operating environment must match one of those defined in section 3.3.
8. The PC used to run McAfee Endpoint Encryption Manager Client must be built using production grade components.

5 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\Software\SafeBoot International]
"FipsMode"=dword:00000001
```