Protect what you value.

McAfee, Inc.

McAfee Endpoint Encryption for PCs

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation

Document revision 1.33, September 2011

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

TABLE OF CONTENTS

Table of Figures

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/products/data-protection/endpoint-encryption.aspx. 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 5.2.6), 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 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 in a Windows operating environment 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.

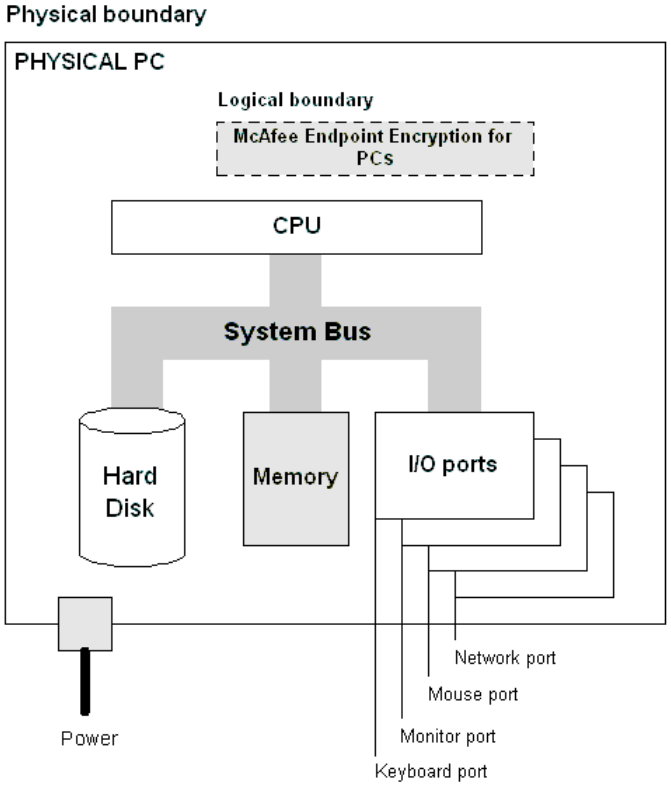

Figure 1: Block Diagram of the cryptographic boundary

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 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 a pre-boot driver to handle user logon and authentication in the pre-Windows environment. There are separate Windows drivers providing: AES Encryption services; a disk encryption driver; a client management driver that downloads configuration changes from a central management server and uploads audit data; a system tray application which provides a Graphical User Interface (GUI) to the operator via the GPC devices display; and a lock driver that prevents any of the other drivers from being inadvertently deleted and also provides integrity testing functionality.

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), TCP/IP secure management channel
- 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 cryptographic module is capable of running and tested in FIPS 140-2 Level 1 mode on the following Common Criteria-evaluated platforms:

- Windows XP 32-bit on an Intel Pentium D processor
- Windows Vista 64-bit on an Intel Core 2 Duo processor

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:

- Microsoft Windows 2000.
- Microsoft Windows Vista 32 bit
- Microsoft Windows 7

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. The module provides identity-based authentication for both Users and Crypto Officers for all services except for the Recovery Service. Therefore the module claims level 1 for authentication because the Recovery Service is not an authenticated Service. Figure 6 summarizes the services available to each role.

Role	Description
Crypto Officer	the Crypto Officer role is performed by the synchronization of the cryptographic module to Endpoint Encryption Manager
User	General User of the module

Figure 3: Roles

2.4.1 User authentication

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

The module uses CAC and PIV tokens to authenticate to the module for all User Role services, except the Recovery Service which does not have authentication. Since there is one service that is not authenticated, the module only claims Roles, Services and Authentication at level 1. 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.

The Common Access Card (CAC) is a United States Department of Defense (DoD) smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, other non-DoD government employees, state employees of the National Guard, and eligible contractor personnel.

The CAC is used for general identification as well as to provide authentication access to DoD computers, networks, and some DoD sites. The CAC enables encryption and signing of email and facilitates the use of PKI authentication tools.

PIV smart cards comply with the United States federal government FIPS 201 standard that specifies Personal Identity Verification (PIV) requirements for Federal employees and contractors.

CAC and PIV smartcards provide identity based authentication because each user has a unique user name and each user has a unique token. When the user of the module authenticates using the CAC or PIV smartcard, they use a password or PIN to unlock the token which is then read by the card reader. The minimum password or PIN length is 5 characters.

The CAC and PIV tokens are not within the scope of the validation. They are outside of the cryptographic boundary.

The Recovery Service is not an authenticated service.

2.4.2 Crypto Officer Authentication

The Crypto Officer role is performed by the cryptographic module performing synchronization to the Endpoint Encryption Manager. DSA is used to perform authentication of the Crypto Officer to the cryptographic module.

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	Password (and possession of token.)
Crypto Officer	Identity-based	DSS authenticated challenge-response mechanism to connect authenticated Crypto Officer to module

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. 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. PIV smartcards have a maximum password/PIN length of eight characters. CAC PINs consist of a number between six and eight digits in length.
DSS authenticated challenge-response mechanism	DSS provides a strength of 80 bits, that amounts to 2^{80} (approximately 1.2×10^{24}) possible outcomes. This greatly exceeds the requirement that the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. The key size is sufficiently large that many repeated attempts will not reduce the likelihood of success to 1 in 100,000

Figure 5 Strength of Authentication Mechanisms

2.5 Access to Services

The following table, Figure 6, lists the authorized services linked to each of the Roles offered by the module.

Role	Authorized Services	Description	Service Input	Service Output
User	Encryption/Decryption	Encryption/Decryption of data written to the hard drive.	Encryption: Plaintext data Decryption: Encrypted data	Encrypted data Plaintext data
	Self-test Functions	Performs all FIPS 140-2 defined self tests.	N/A	Self-test results
	Uninstall	Uninstalls the module from the host platform and zeroizes the Machine Key and the Server Public Key. To complete the process the hard disk on which the module was installed then needs to be reformatted.	N/A	All keys and CSPs zeroized.
	Show status	Show the status of the hard disk encryption and self-test results	N/A	Tray menu status window displays module status
	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.)	Offline Challenge/ Response	Restored user access to CM
Crypto Officer	Synchronization	Establishes a secure network connection between the module and the remote Admin Server for the purpose of configuring the module. Synchronization allows configuration changes to be deployed to the module (including setting, changing, and deleting attributes), file updates, and also allows audit data to be transferred to the Admin Server.	N/A	Synchronized datastore. Synchronized audit data. Updated policies

Figure 6: 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
Machine 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 key used as input into the FIPS 186-2 DRNG.
DRNG Seed Values	Seed values used as input into the FIPS 186-2 DRNG.
User Encryption CSP	To encrypt secure user attributes
Machine Recovery CSP	To recover machine key
User Recovery CSP	To recover user encryption CSP
User password	To authenticate users to the token.

Figure 7: CSPs used by McAfee Endpoint Encryption for PCs

Key type	Purpose
Server DSA Public Key	Used by the Cryptographic Module to authenticate the identity of the Database server.
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 for PCs

McAfee Endpoint Encryption for PC uses a hard coded DSA public key for signature verification in the software integrity test and this hard coded key is not a CSP.

Key type	Key length/ strength	Storage location	Encrypted /Plaintext	Generation/ establishment	Entry/output
Machine Key	AES 256 bit	Client Datastore	Encrypted	FIPS 186-2 DRNG	Send to server during client installation
User Encryption CSP	AES 256 bit	Client	Encrypted	Externally	Received by

Key type	Key length/ strength	Storage location	Encrypted /Plaintext	Generation/ establishment	Entry/output
		Datastore			client during synchronization with administration server, during a secure management session.
User Recovery CSP	AES 256 bit	Ephemeral	Encrypted	Externally	Manually input as obfuscated plaintext during user recovery
Machine Recovery CSP	AES 256 bit	Client Datastore	Encrypted	FIPS 186-2 DRNG	1) Manually input as obfuscated plaintext during machine recovery. 2) Send to server 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 DSA Public Key	1024 bits	This is stored in plaintext in a configuration file, SDMCFG.INI.	Plaintext	Externally	Deployed with the installation.
User Authentication Certificate	1024 bits	Client Datastore	Plaintext	N/A	Installed during configuration

Key type	Key length/ strength	Storage location	Encrypted /Plaintext	Generation/ establishment	Entry/output
Diffie-Hellman Server Public Key	1024/2048 bit	Ephemeral	Plaintext	Diffie-Hellman key establishment protocol	Exchanged with server 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

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 Machine Key and the Machine Recovery Key. The secure management Session Key is a shared secret that is established to enable secure communication using a Diffie-Hellman key exchange mechanism.

2.7.2 Key entry and output

The module supports the following key entry:

- Diffie-Hellman Server Public Key – entered signed with the Server DSA Private Key.
- User Recovery CSP - Manually input as obfuscated plaintext
- Machine Recovery CSP - Manually input as obfuscated plaintext
- Machine Key - encrypted by the User Encryption CSP over a secure session
- User Encryption CSP – input encrypted by the CAC/PIV RSA Public Key over an encrypted session.
- User Encryption CSP – input encrypted by the User Recovery CSP over an encrypted session.
- User Encryption CSP – Input as plaintext from the CAC/PIV over a trusted path.
- User Authentication Certificate – Input over an encrypted session.

The module supports the following key output:

- Machine Key – Output to the Admin Database server over a secure session
- Machine Recovery Key – output to the Admin Database server over a secure session
- Diffie-Hellman Client Public Key – output in plaintext
- User Encryption CSP - encrypted by the CAC/PIV RSA Public 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 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 operator 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.

During uninstallation, the module calls a zeroize command, which zeroizes the Machine Key and Server Public Key. 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 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 matrices (Figure 10 and Figure 11) 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**	**PK**	**DRNGSK**	**DHK**	**DHSPK**	**DHCPK**	**DHSS**	**SK**
Encryption/Decryption	R							
Self-test Functions								
Uninstall	R, Z	Z	Z	Z	Z	Z	Z	Z
Show status								
Recovery Request								

	Key					
Service	**UAC**	**UEK**	**URK**	**MRK**	**PWD**	**SV**
Encryption/Decryption		R				R, W
Self-test Functions						
Uninstall	Z	R, Z	Z	Z	Z	Z
Show status						
Recovery Request		R	R	R		

Figure 10: User Role

	Key							
Service	**DK**	**PK**	**DRNGSK**	**DHK**	**DHSPK**	**DHCPK**	**DHSS**	**SK**
Synchronization	R, O	R	R, W	W	W, E	W, O	W, R	R, W
Recovery	R							R

	Key					
Service	**UAC**	**UEK**	**URK**	**MRK**	**PWD**	**SV**
Synchronization	R	R	R, W	R, W	W	
Recovery		R	R	R		

Figure 11: 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	Machine Key
PK	Server DSA 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
UAC	User Authentication Certificate
SK	Session Key
UEK	User Encryption CSP
URK	User Recovery CSP
MRK	Machine Recovery CSP
PWD	User Password
SV	DRNG Seed Values

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 recovery or machine recovery, has no plaintext access to key material or CSPs. When carrying out user recovery or machine recovery, a user is required to manually enter an obfuscated plaintext recovery key received from a McAfee Endpoint Encryption Manager Crypto Officer into the module.

2.8 Cryptographic Algorithms

McAfee Endpoint Encryption for PCs 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 either 80 bits or 112 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 12, lists the power-up self-tests performed by the module:

SHA-1 known answer test
DSA known answer test (DSA Signature Verification)
AES-256 known answer test (Encrypt/Decrypt)
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, if the failure is in the Pre-boot phase, then an error message is displayed and the system halted. If the failure is in the Windows phase, then the GPC is halted with a blue stop error screen and an appropriate error message is displayed. The module must be reset to re-execute these tests.

2.9.1.1 Power-up self-test errors

Phase	**Test**	**Action on failure**
Preboot	AES and RNG KAT	E_SB_ALG_DLM_INIT_FAILED error displayed in message box and then system halts.
	DSA and SHA-1 KAT	Throws an E_SB_GEN_MODULE_VERIFY error. This is displayed in a message box and then when closed, system halts.
	Integrity check	Throws an E_SB_GEN_MODULE_VERIFY error. This is displayed in a message box and then when closed, system halts.
Windows	AES and RNG KAT	AES Driver is unloaded with an STATUS_INSUFFICIENT_RESOURCES stop error.
	DSA and SHA-1 KAT	Blue screens with a STATUS_IMAGE_CHECKSUM_MISMATCH stop error
	Integrity check	Blue screens with a STATUS_IMAGE_CHECKSUM_MISMATCH stop error

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. This E_SBALG_KEY_DATA_INVALID error is stored in the client status log and can be viewed by selecting the client status window from the GPC Windows task bar.

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.

Delivery of the Crypographic 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.

2.11 Mitigation of Other Attacks

The module does not mitigate other attacks.

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. The Cryptographic Module Boot Protection functionality must be enabled.
3. 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. .`
4. 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”.
5. Users of the cryptographic modules must use one of the tokens defined in section 2.4.1 to authenticate themselves to the module.
6. 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.

4 Appendix A – Creating the FIPS enable script

The cryptographic module has been tested in Windows XP and Windows Vista 64-bit operating environments. Each of these needs to run a different registry script in order to be configured to run in a FIPS-compliant mode of operation. These two scripts are listed below.

The script text needs to be saved to a text file with the extension ".reg" and then merged into the registry.

4.1 Windows XP

```
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"


[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\3]

"Path"="c:\\Program Files\\McAfee\\Endpoint Encryption for PC\\SbClientStatus.dll"


[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\4]

"Path"="c:\\windows\\system32\\drivers\\SbFlop.sys"


[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\5]

"Path"="c:\\windows\\system32\\drivers\\SbFsLock.sys"
```

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\6]

"Path"="c:\\windows\\system32\\drivers\\SbPrcCtl.sys"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\7]

"Path"="c:\\windows\\system32\\drivers\\RsvLock.sys"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\8]

"Path"=" C:\\Program Files\\McAfee\\Endpoint Encryption for PC\\SbClientManager.exe"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\9]

"Path"=" C:\\Program Files\\McAfee\\Endpoint Encryption for PC\\SbGinaLib.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\10]

"Path"=" C:\\Program Files\\McAfee\\Endpoint Encryption for PC\\SbComms.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\11]

"Path"=" C:\\Program Files\\McAfee\\Endpoint Encryption for PC\\SbDbMgr.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\12]

"Path"=" C:\\Program Files\\McAfee\\Endpoint Encryption for PC\\SbFileDb.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\13]

"Path"=" C:\\Program Files\\McAfee\\Endpoint Encryption for PC\\SbReaderPcsc.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\14]

"Path"=" C:\\Program Files\\McAfee\\Endpoint Encryption for PC\\SbXferDb.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\15]

"Path"=" C:\\Program Files\\McAfee\\Endpoint Encryption for PC\\SbUiLib.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\16]

"Path"=" C:\\Program Files\\McAfee\\Endpoint Encryption for PC\\SbAlgs\\SbAlg.dll"

4.2 Windows Vista 64-bit

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"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\3]

"Path"=" C:\\Program Files(x86)\\McAfee\\Endpoint Encryption for PC\\SbAlgs\\SbAlg.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\4]

"Path"="c:\\windows\\system32\\drivers\\SbFlop.sys"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\5]

"Path"="c:\\windows\\system32\\drivers\\SbFsLock.sys"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\6]

"Path"="c:\\windows\\system32\\drivers\\RsvLock.sys"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\7]

"Path"="c:\\windows\\system32\\drivers\\SbRegFlt.sys"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\8]

"Path"="c:\\windows\\system32\\drivers\\SbHiber.sys"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\9]

"Path"="c:\\Program Files(x86)\\McAfee\\Endpoint Encryption for PC\\SbCredProv.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\10]

"Path"= "c:\\Program Files(x86)\\McAfee\\Endpoint Encryption for PC\\SbTokWatch.exe"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\11]

"Path"=" C:\\Program Files(x86)\\McAfee\\Endpoint Encryption for PC\\SbClientManager.exe"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\12]

"Path"=" C:\\Program Files(x86)\\McAfee\\Endpoint Encryption for PC\\SbClientStatus.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\13]

"Path"=" C:\\Program Files(x86)\\McAfee\\Endpoint Encryption for PC\\SbComms.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\14]

"Path"=" C:\\Program Files(x86)\\McAfee\\Endpoint Encryption for PC\\SbDbMgr.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\15]

"Path"=" C:\\Program Files(x86)\\McAfee\\Endpoint Encryption for PC\\SbFileDb.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\16]

"Path"=" C:\\Program Files(x86)\\McAfee\\Endpoint Encryption for PC\\SbReaderPcsc.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\17]

"Path"=" C:\\Program Files(x86)\\McAfee\\Endpoint Encryption for PC\\SbXferDb.dll"

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RsvLock\Verifier\18]

"Path"=" C:\\Program Files(x86)\\McAfee\\Endpoint Encryption for PC\\SbUiLib.dll"

5 Components excluded from the cryptographic module

A number of components are included in the product but are not security relevant and so are excluded from the cryptographic module.

5.1 Localization

A number of files are required to localize the EEPC Client. The localization under test is the English (US) standard McAfee Theme.

[AppDir]\Graphics\1024x768\Bar.png
[AppDir]\Graphics\1024x768\Middle.png
[AppDir]\Graphics\1024x768\Stripe.png
[AppDir]\Graphics\640x480\Bar.png
[AppDir]\Graphics\640x480\Middle.png
[AppDir]\Graphics\640x480\Stripe.png
[AppDir]\Graphics\800x600\Bar.png
[AppDir]\Graphics\800x600\Middle.png
[AppDir]\Graphics\800x600\Stripe.png
[AppDir]\Graphics\Graphics.ini
[AppDir]\Graphics\LatinASCII\Tahoma12B.pbf
[AppDir]\Graphics\LatinASCII\Tahoma18B.pbf
[AppDir]\Graphics\LatinASCII\Tahoma8.pbf
[AppDir]\Graphics\LatinASCII\Tahoma8B.pbf
[AppDir]\Graphics\Shared\Logonbanner.png
[AppDir]\Graphics\Shared\Options.png
[AppDir]\Graphics\Shared\Recovery.png
[AppDir]\Locale\Locale.ini

5.2 EEPC Client Core Components

[AppDir]\SbChkDsk.dll
[AppDir]\SbClientSupportInfoPlugin.dll
[AppDir]\SbCmaDe.dll
[AppDir]\SbKbeDe5.dll
[AppDir]\SbPostInstall.dll
[AppDir]\SbPreInstall.dll
[AppDir]\SbSetup.exe
[Tray Manager AppDir]\SbTrayManager.exe
[WinDir]\SafeBoot.scr

5.3 Windows XP components

[WinSysDir]\SbNp.dll
[AppDir]\SbGina.dll

5.4 Windows Vista64 Components

[WinSysDir]\SbNp.dll