FIPS 140-2 Non-Proprietary Security Policy

McAfee EMM Cryptographic Module (Version 1.0)

Document Version 1.2

March 1, 2012

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the EMM Cryptographic Module (Version 1.0).

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment of Canada (CSEC) Cryptographic Module Validation Program (CMVP) runs the FIPS 140 program. The CMVP accredits independent testing labs to perform FIPS 140 testing; the CMVP also validates test reports for products meeting FIPS 140 validation. *Validated* is the term given to a product that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the EMM Cryptographic Module (Version 1.0) from McAfee provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

The McAfee EMM Cryptographic Module (Version 1.0) may also be referred to as the "module" in this document.

1.3 External Resources

The McAfee website (http://www.mcafee.com) contains information on the full line of products from McAfee, including a detailed overview of the EMM Cryptographic Module (Version 1.0). The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm) contains links to the FIPS 140-2 certificate and McAfee contact information.

1.4 Notices

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
API	Application Programming Interface
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DTR	Derived Testing Requirement
ECB	Electronic Code Book
EDC	Error Detection Code
EMM	Enterprise Mobility Management
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GPOS	General Purpose Operating System
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
MDM	Mobile Device Manager
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adelman
SHA	Secure Hashing Algorithm

Table 1 – Acronyms and Terms

2 McAfee EMM Cryptographic Module (Version 1.0)

2.1 Product Overview

The McAfee EMM platform provides secure management of mobile devices. McAfee EMM allows integration of smartphones into enterprise networks with the same level of security protection enabled on laptops and desktops. With McAfee EMM, System Administrators have the tools and capabilities needed to effectively secure mobile devices in the enterprise network, seamlessly manage them in a scalable architecture, and efficiently assist users when problems arise.

McAfee EMM is a web-based solution that helps manage the entire life cycle of the mobile device. McAfee EMM's unique combination of device management, on-device security, network control, and compliance reporting delivers a powerful mobile device security solution.

2.2 Cryptographic Module Specification

The module is the McAfee EMM Cryptographic Module (Version 1.0), provides the EMM solution with cryptographic functionality. The module is a software-only, multi-chip standalone embodiment that runs on a General Purpose Computer running a Microsoft Windows Server 2008 R2 (x64 Version). The module provides cryptographic services to the McAfee EMM application.

The module is a uniquely identifiable set of libraries built into the EMM console application; it does not install or execute on a mobile platform. All operations of the module occur via calls from the EMM application and its internal processes, and all calls are authenticated via digital signature verification. As such there are no untrusted services or processes calling the services of the module. No security functions outside the cryptographic module provide FIPS-relevant functionality to the module.

Once configured for FIPS mode of operation (see the Guidance and Secure Operation section), the module cannot be placed into a non-FIPS mode.

2.3 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1

FIPS 140-2 Section Title	Validation Level
Cryptographic Key Management	1
Electromagnetic Interference / Electromagnetic Compatibility	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 2 – Validation Level by DTR Section

The "Mitigation of Other Attacks" section is not relevant as the module does not implement any countermeasures towards special attacks.

2.4 Cryptographic Algorithms

2.4.1 Algorithm Implementation Certificates

The module's cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	CAVP Certificate	Use
Hashing	SHS	1081	Hashing
Symmetric Key	AES-128 ECB Mode	1168	Data encryption / decryption
Keyed Hash	HMAC	687	Module integrity

Table 3 – Algorithm Certificates for FIPS-Approved Algorithms[1]

2.5 Module Interfaces

The figure below shows the module's physical and logical block diagram:

[1] Note this implementation has received FIPS 140-2 Level 1 validation 1337: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm#1337

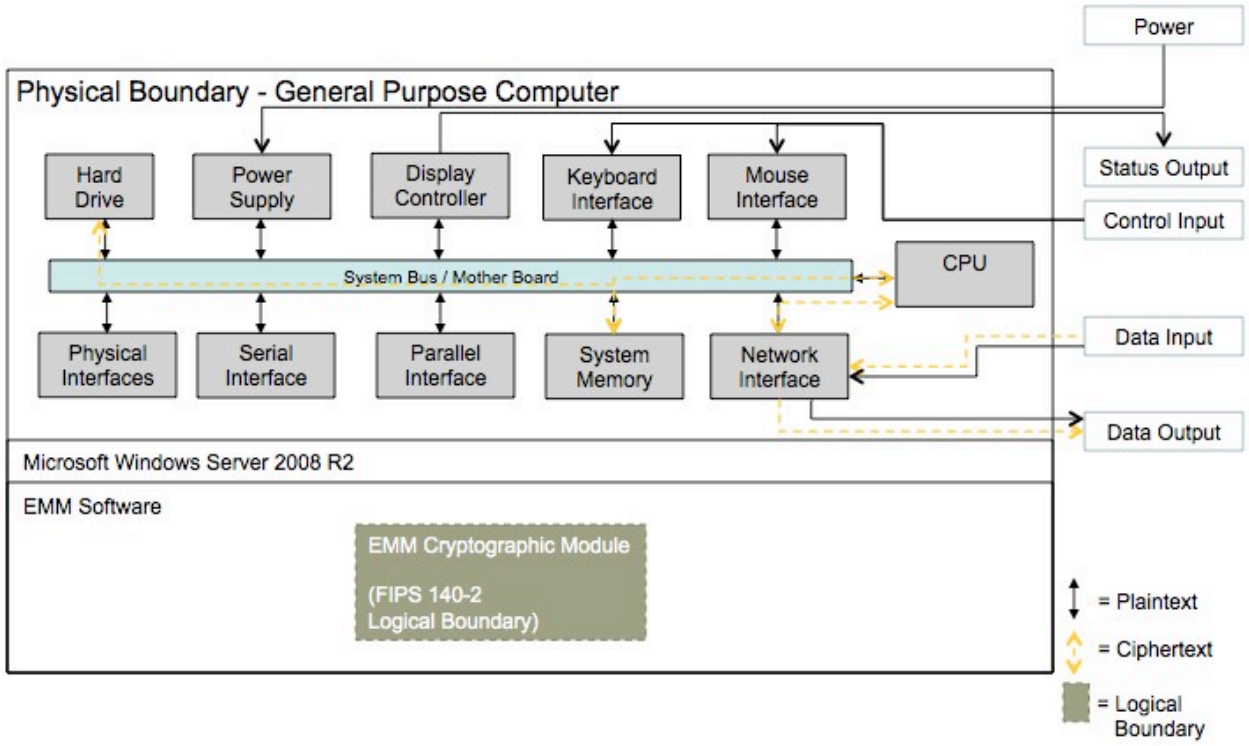

Figure 1 – Module Interfaces Diagram

The interfaces (ports) for the physical boundary are shown in Figure 1 – Module Interfaces Diagram and Table 4 – Logical Interface / Physical Interface Mapping. When operational, the module does not transmit any information across these physical ports because it is a software cryptographic module. Therefore, the module's interfaces are purely logical and are provided through the Application Programming Interface (API) that a calling process can operate. The logical interfaces expose services that applications directly call, and the API provides functions that may be called by a referencing application (see Section 2.6 – Roles, Services, and Authentication for the list of available functions).

The API provided by the module is mapped onto the FIPS 140- 2 logical interfaces: data input, data output, control input, and status output. Each of the FIPS 140- 2 logical interfaces relates to the module's callable interface, as follows:

FIPS 140-2 Interface	Logical Interface	Module Physical Interface
Data Input	Input parameters of API function calls	Ethernet/Network port
Data Output	Output parameters of API function calls	Ethernet/Network port
Control Input	API function calls	Keyboard and mouse
Status Output	For FIPS mode, function calls returning status information and return codes provided by API function calls.	Display controller

FIPS 140-2 Interface	Logical Interface	Module Physical Interface
Power	None	Power supply/connector

Table 4 – Logical Interface / Physical Interface Mapping

The module's logical interfaces are provided only through the Application Programming Interface (API) that a calling process can operate. The module distinguishes between logical interfaces by logically separating the information according to the defined API.

As shown in Figure 1 – Module Interfaces Diagram and Table 5 – User Services and Descriptions, the output data path is logically disconnected from processes performing zeroization. No key information will be output through the data output interface when the module zeroizes keys.

2.6 Roles, Services, and Authentication

The module supports a Crypto Officer and a User role. The module does not support a Maintenance role. As allowed by Level 1, the module does not support authentication.

2.6.1 Operator Services and Descriptions

The services available to the User and Crypto Officer roles in the module are as follows:

Service	Description	Service Input/Output (API)	Key/CSP Access
Encrypt	Encrypts a block of data	`EncryptString()`	DB Key
Decrypt	Decrypts a block of data	`DecryptString()`	DB Key
Hash	Performs a message digest	`CreateHash()`	None
Self Test	Performs self tests defined in Section 2.10.1 - Power-On Self-Tests. Can be performed on demand by reloading / rebooting the module.	`Public static bool SelfTest()` `FipsEMMCryptoLibraryValid()`	Integrity Key
Show Status	Shows status of the module	`Public static bool IsFipsEnabled`	None

Table 5 – User Services and Descriptions

Service	Description	Service Input/Output (API)	Key/CSP Access
Initialize	Installs the module per Section 3	See Section 3	None

Service	Description	Service Input/Output (API)	Key/CSP Access
Zeroization	Zeroizes keys	Manual deletion of key file by Administrator	None

Table 6 – Crypto Officer Services and Descriptions

2.7 Physical Security

This section of requirements does not apply to this module. The module is a software-only module and does not implement any physical security mechanisms.

2.8 Operational Environment

The module operates on a general-purpose computer (GPC) running a general-purpose operating system (GPOS). The module was tested on the following:

- Microsoft Windows Server 2008 R2 (x64 Version)

Compliance is maintained on platforms for which the binary executables remain unchanged including:

- Microsoft Windows Server 2003 SP2 or greater

For FIPS purposes, the module is running on one of these platforms in single user mode and does not require any additional configuration to meet the FIPS requirements.

The GPC(s) used during testing met Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B. FIPS 140-2 validation compliance is maintained when the module is operated on other versions of the Microsoft Windows GPOS running in single user mode, assuming that the requirements outlined in NIST IG G.5 are met.

2.9 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

CSP / Details	DB Key	Integrity Key
Type	AES	HMAC-SHA1
Storage Location	On disk	On disk
Storage Method	Plaintext	Plaintext
Input	No	No
Input Method	NA	NA
Output	No	No

CSP / Details	DB Key	Integrity Key
Output Method	NA	NA
Generated	No	At build time
Zeroized	Yes (Uninstall and format the disk)	Yes (Uninstall and format the disk)
CO Access	Read / Write / Delete	Read / Delete
User Access	Read / Write / Delete	Read

Table 7 – Module Keys/CSPs

The DB key enters the module via the EMM application, which resides within the module's physical boundary. Keys / CSPs are protected from unauthorized disclosure, unauthorized modification, and unauthorized substitution because only authorized users are allowed access to the GPOS and EMM application. The EMM application ensures that no keys or CSPs leave the physical boundary of the module in plaintext. The module does not output intermediate key values, nor does it generate keys with non-Approved key generation methods.

Ephemeral CSPs are zeroized by the RAM clearing processes, and static CSPs are zeroized by uninstalling the module and formatting the hard drive. All keys and CSPs are stored in memory, and zeroization has been implemented to ensure no traces are left of any CSPs upon termination of the service using the CSP. Zeroization has been implemented by overwriting the allocated memory buffer with zeros before freeing the memory to other uses. Any service using a CSP will zeroize the CSP upon normal termination and when transitioning into error states. Zeroization is initiated by terminating the process and powering off the module. Zeroization will complete before any other malicious command could compromise the keys currently being zeroized because the module will not process additional commands until it finishes executing the current command.

2.10 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module/EMM application will output an error to the audit log and will shutdown. In addition to self-test failures, successful loading of the module is also logged. To access status of self-tests, success or failure, the application provides access to the audit log. Status is viewable via operating environment's audit mechanism and by verifying proper loading and operation of the EMM application. While the module is running self-tests, the module will not output data. The EMM application makes calls to the EMM Cryptographic Module (Version 1.0), and data will not be returned until the self-tests complete.

No keys or CSPs will be output when the module is in an error state. The module will halt and the process will terminate; as such, no data will be output via the data output interface. Additionally, the module does not support a bypass function, and the module does not allow plaintext cryptographic key

components or other unprotected CSPs to be output on physical ports. No external software or firmware is allowed to be loaded in a FIPS mode of operation.

The following sections discuss the module's self-tests in more detail.

2.10.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the users. The module implements the following power-on self-tests:

- Module integrity check via HMAC-SHA1
- Triple-DES ECB encrypt/decrypt KAT
- SHA-384 KAT
- SHA-512 KAT
- SHA-1 HMAC KAT
- SHA-256 HMAC KAT
- RSA sign/verify power up test
- AES 128 ECB encrypt/decrypt KAT
- SP 800-90 CTR_DRBG KAT

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by reinitializing the module in FIPS approved Mode of Operation. Upon passing the power-on self-tests, the module will log the success and will continue to boot normally; successful loading of the EMM application will indicate that all self-tests have passed. If a self-test fails an error will be logged in the event viewer and the module will halt.

2.10.2 Conditional Self-Tests

Conditional self-tests are on-demand tests and tests run continuously during operation of the module. The module performs the following conditional tests:

- RSA pairwise consistency test
- Continuous random number generator test.

2.11 Mitigation of Other Attacks

The module does not mitigate other attacks.

3 Guidance and Secure Operation

This section describes how to configure the module for FIPS-approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 Software Packaging and OS Requirements

The module is included with EMM version 9.6 and is not available for direct download. The EMM application must be installed on Microsoft Windows Server 2008 R2 (x64 Version) running in single user mode. To configure single-user mode, the following must be disabled:

- Remote registry and remote desktop services
- Remote assistance
- Guest accounts
- Server and terminal services

Contact Microsoft support for configuration details; specific configuration steps are beyond the scope of this document.

3.1.2 Enabling FIPS Mode

FIPS mode within the module is enabled by default. There is no non-FIPS mode, and there are no specific commands to enable FIPS mode.

3.1.3 Additional Rules of Operation

1. All host system components that can contain sensitive cryptographic data (main memory, system bus, disk storage) must be located in a secure environment.
2. The writable memory areas of the Module (data and stack segments) are accessible only by the EMM application so that the Module is in "single user" mode, i.e. only the EMM application has access to that instance of the Module.
3. The operating system is responsible for multitasking operations so that other processes cannot access the address space of the process containing the Module.

3.2 User Guidance

3.2.1 General Guidance

The User must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation:

1. The end user of the operating system is responsible for zeroizing CSPs by via wipe/secure delete procedures.