Security Policy

FIPS 140-2 Level 1

Mobile Armor Cryptographic Module

3.0

Version: 1.5

Date: 05/4/2009

This document is provided for informational purposes about the non-proprietary structure of the Mobile Armor Cryptographic Module 3.0 as it pertains to FIPS 140-2 validation.

Contact Mobile Armor

Mobile Armor, Inc.
400 South Woods Mill Road
Suite 300
St. Louis, MO, 63017 USA

Telephone: +1 (314) 590-0900
Fax: +1 (314) 590-0995

Website: http://www.mobilearmor.com

Email: sales@mobilearmor.com

Revisions

Date	Version	Author	Description
11/12/07	0.1	Brian E Wood	Initial version
11/13/07	0.2	Brian E Wood	Updates with input from Brendan Johnson
11/27/07	0.3	Brian E Wood	Updates with input from Brendan Johnson
12/3/07	0.4	Brian E Wood	Updates based on Palm differences
4/15/08	1.0	Brian E Wood	Updated platforms to be supported
10/21/08	1.1	Brian E Wood	Updated platforms to be supported to final list
10/31/08	1.2	Brian E Wood	Replaced “generic PC” with “IBM Compatible PC”, edited Apple computer platform
11/10/08	1.3	Brian E Wood	Updated integrity check text and added block diagrams
03/30/2009	1.4	Brian E Wood	Updated several section based on feedback from SAIC
05/4/2009	1.5	Brian E Wood	Updated several section based on feedback from SAIC

Contents

Tables

Figures

1 Security Policy Introduction

1.1 Security Policy, Product and Evaluation Identification

SP Title: Mobile Armor Cryptographic Module 3.0 Security Policy

SP Version: Version 1.3

Product Identification: Mobile Armor Cryptographic Module 3.0

FIPS Evaluation Identification: FIPS 140-2

Evaluation Level: 1

1.2 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Mobile Armor Cryptographic Module 3.0. This security policy describes how the Mobile Armor Cryptographic Module 3.0 meets the Level 1 security requirements of FIPS 140-2. While the product will be evaluated on Microsoft Windows Vista, Microsoft Windows Mobile 6, Mac OS 10.4, Red Hat Enterprise Linux 5.0 and Ubuntu 7.10, it is a cross-platform module also capable of running on Microsoft Windows 2000/XP, Microsoft Windows Mobile 5, Mac OS 10.5 and other platforms with no modifications. This policy was prepared as part of FIPS 140-2 validation of the Mobile Armor Cryptographic Module 3.0.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 - Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.3 References

This document deals only with operations and capabilities of the Mobile Armor Cryptographic Module 3.0 in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the Mobile Armor Cryptographic Module 3.0 application from the following sources:

- Overview information of Mobile Armor products and services as well as answers to technical or sales related questions, refer to: http://www.mobilearmor.com.

Acronym	Definition
AES	Advanced Encryption Standard
Triple-DES	Triple Data Encryption Standard
PRNG	Pseudo Random Number Generator
SHA	Secure Hash Algorithm

Acronym	Definition
HMAC	Hash Message Authentication Code
API	Application Programming Interface
DLL	Dynamic Link Library

Table 1 – Acronyms

For the purposes of this document, the term “mobile device” will be used to designate a device such as a PDA or smartphone, as opposed to a PC. These devices run the Windows Mobile OS.

2 Mobile Armor Cryptographic Module 3.0

2.1 Overview

The Mobile Armor Cryptographic Module 3.0 provides cryptographic support for all Mobile Armor products. The Cryptographic Module is used to create, manage and delete cryptographic keys as well as to perform cryptographic operations.

To provide cryptographic security services, the Cryptographic Module provides access to symmetric key based encryption algorithms, message digest, message authentication code, and pseudo random number generation functions. The keys and information provided by the user is used by the Cryptographic Module for encryption/decryption operations.

The Cryptographic Module is designed for multiple functions within Mobile Armor applications. It provides a structured set of APIs to expose these functions, giving flexibility to add new applications for the Cryptographic Module functions in the future without changing the module itself.

2.2 Cryptographic Module

The Mobile Armor Cryptographic Module 3.0 is classified as a multi-chip standalone module for FIPS 140-2 purposes.

The cryptographic module is capable of running on any commercially available IBM compatible PC running the following list of Operating Systems (OS).

- Microsoft Windows Vista
- Microsoft Windows Vista 64-bit
- Microsoft Windows Mobile 6
- Apple Mac OS X 10 on Intel hardware
- Red Hat Enterprise Linux 5.1
- Red Hat Enterprise Linux 5.1 64-bit
- Fedora Core 8
- Fedora Core 8 64-bit
- Ubuntu 7.10
- Ubuntu 7.10 64-bit

The module is capable of running on any commercially available Microsoft Windows Mobile-based device (note the device must be capable of running Windows Mobile 5 or 6, and not earlier versions of the OS). A partial list of devices currently available (in the United States) that meet this requirement can be found at http://www.microsoft.com/windowsmobile/devices/default.mspx.

The module is capable of running on the commercially available Intel-based Apple Mac computers. Non-Intel-based Apple systems are not supported.

The module was tested for FIPS 140-2 compliance on the following platforms:

- An IBM compatible PC running Microsoft Windows Vista configured in the single user mode
- An IBM compatible PC running Microsoft Windows Vista 64-bit configured in the single user mode
- An IBM compatible PC running Red Hat Enterprise Linux 5.1 configured in single user mode
- An IBM compatible PC running Red Hat Enterprise Linux 5.1 64-bit configured in single user mode
- An IBM compatible PC running Fedora Core 8 configured in single user mode
- An IBM compatible PC running Fedora Core 8 64-bit configured in single user mode
- An IBM compatible PC running Ubuntu 7.10 configured in single user mode
- An IBM compatible PC running Ubuntu 7.10 64-bit configured in single user mode
- An Apple-based computer with an Intel processor running OSX 10.5
- A mobile device running Windows Mobile 6

The module is compiled into libraries that are specific to each platform. The only changes between these platforms are those necessary for porting the Cryptographic Module, and these are handled through compiler options.

2.3 Module Ports and Interfaces

The Mobile Armor Cryptographic Module 3.0 is classified as a multi-chip standalone module for FIPS 140-2 purposes. As such, the module's logical cryptographic boundary includes the library binary. The physical boundary includes a PC or mobile device running an operating system and interfacing with the device, and external components such as keyboard, mouse, touch screen, screen, floppy drive, CD-ROM drive, speaker, serial ports, parallel ports, USB ports and power plug. This boundary is shown in **Error! Reference source not found.**.

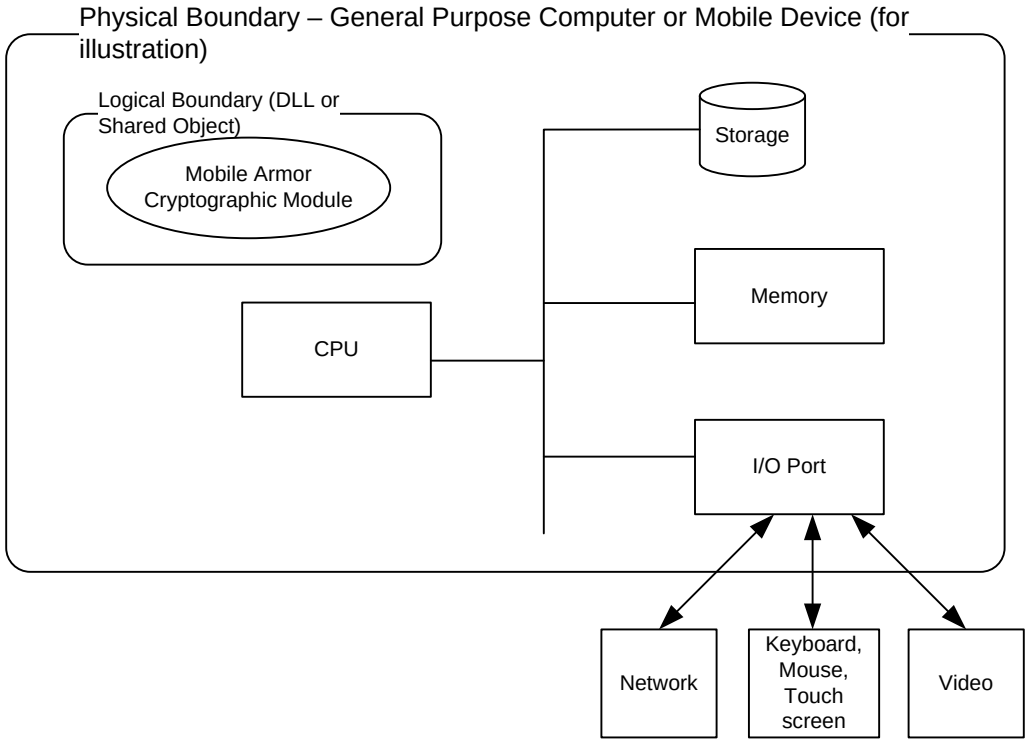

Figure 1– Logical Block Diagram

The Mobile Armor Cryptographic Module 3.0 provides a logical interface via an Application Programming Interface (API). The API provided by the module is mapped to the FIPS 140-2 logical interfaces: data input, data output, control input, and status output. All of these physical interfaces are separated into the logical interfaces from FIPS as described in the following table:

FIPS 140-2 Logical Interface	Module Mapping
Data Input Interface	Parameters passed to the module via API calls
Data Output Interface	Data returned by the module via the API
Control Input Interface	Control input through the API function calls
Status Output Interface	Information returned via exceptions and calls
Power Interface	Does not provide a separate power or maintenance access interface beyond the power interface provided by the computer itself

Table 2 - FIPS 140-2 Logical Interfaces

2.4 Roles, Services and Authentication

The Mobile Armor Cryptographic Module 3.0 does not provide any identification or authentication for any user that is accessing the module, and is only acceptable for FIPS 140-2 level 1 validation. The module provides a Crypto Officer and a User role (there is no Maintenance role). Since the module does not provide any identification or authentication services, the level of access granted to any functionality of the module is implicitly determined

by the service calling the module; the module itself makes no determination about the role itself. The Crypto Officer is expected to install and uninstall the module.

Table 3 - Cryptographic Module Services provides a description of the services which are made available by the module to the calling application.

Service	API Calls	Purpose and Use
AES	aes_encrypt aes_encrypt_padded aes_decrypt aes_decrypt padded aes_cbc_encrypt aes_cbc_decrypt aes_cfb_encrypt aes_cfb_decrypt	Allows Users to encrypt/decrypt data using AES algorithm
Triple-DES	des3_encrypt des3_decrypt des3_cbc_encrypt des3_cbc_decrypt	Allows Users to encrypt/decrypt data using Triple-DES algorithm
SHS	sha1 sha224 sha256 sha384 sha512	Allows Users to generate message digests
HMAC	sha1_hmac sha224_hmac sha256_hmac sha384_hmac sha512_hmac	Allows Users to generate MAC values
RNG	CryptGenRand	Allows Users to generate deterministic random numbers which can be used for algorithm keys
Initialization Self-Tests	FIPS_SelfTests	Allows Users to determine if the module is functioning properly (this service only executes when the module is started)
Show Status	API function return values	Allow Users to observe module operation status
Zeroization	aes_clear_context des3_clear_context	Allows Users to zeroize key data

Table 3 - Cryptographic Module Services

2.5 Physical Security

The Mobile Armor Cryptographic Module 3.0 is a software module intended for use with Microsoft Windows Vista, Fedora Core 8, Ubuntu 7.10 and Red Hat Enterprise Linux 5.0 in single user modes on a PC, an Intel-based Mac and Microsoft Windows Mobile on a mobile device. Since the module is implemented solely in software, the physical security section of FIPS 140-2 is not applicable.

2.6 Operational Environment

The Mobile Armor Cryptographic Module 3.0 is compiled into separate modules for each supported platform from the same cryptographic source. The only differences are those necessary to port the Cryptographic Module between platforms.

Platform	Implementation
Microsoft Windows Vista	Normal C Dll (MAFips.dll)
Microsoft Windows Vista 64	Normal C Dll (MAFips64.dll)
Microsoft Windows Mobile	Normal C Dll (MAFips.dll)
Linux (all)	Shared Object (libMAFips.so)
Linux (all) 64-bit	Shared Object (libMAFips64.so)
Mac OS X	Shared Object (libMAFips.dylib)
Mac OS X	Shared Object (libMAFips64.dylib)

Table 4 – Cryptographic Module Implementations

The only differences in the Cryptographic Module are those necessary to port the Cryptographic Module between the different platforms.

The Mobile Armor Cryptographic Module 3.0 is a single user module that is always distributed in binary form to discourage unauthorized access or modification to source. Additionally, an HMAC SHA1 software integrity check is run when the modules are loaded to help ensure that the code has not been modified from its validated configuration.

2.7 Cryptographic Key Management

The Mobile Armor Cryptographic Module 3.0 implements the following algorithms. The FIPS approved column specifies whether the algorithm is available in the FIPS-mode.

Algorithm	FIPS Approved	Certificate #
AES (CBC, ECB 256-bit	Yes	820

Algorithm	FIPS Approved	Certificate #
keys)		
Triple-DES (CBC, ECB 168-bit keys)	Yes	692
SHA1	Yes	818
HMAC SHA1	Yes	453
SHA256 (SHA224)	Yes	818
HMAC SHA256	Yes	453
SHA512 (SHA384)	Yes	818
HMAC SHA512	Yes	453
ANSI X9.31 PRNG	Yes	472

Table 5 - FIPS Cryptographic Algorithms

All keys are generated by using the ANSI X9.31 PRNG which is based on the validated Triple-DES algorithm.

The following list of keys and CSPs is used by the module. They are generated or inserted as specified and stored within the Cryptographic Module as necessary. Here inserted is used to mean the key is provided be the calling application, as opposed to internally generated.

Name	Created	Size(s) in bits	Purpose	Zeroization method
AES-key	Generated/Inserted	128, 192, 256	Data Encryption, Decryption	Function aes_clear_context
Triple-DES-key	Generated/Inserted	112, 168	Data Encryption, Decryption	Function des3_clear_context
SHA1 HMAC integrity check key	Hard coded	112	Verify driver integrity	Uninstallation of module
PRNG key	Generated	168	Random Number Generation	Unload module from memory
PRNG seed	Generated	64	Random Number Generation	Unload module from memory
HMAC key	Generated/Inserted	N/A	MAC	Functions sha1_clear_context, sha256_clear_context, sha512_clear_context, and memset

Table 6 - Key Generation

Keys are stored in the Cryptographic Module's internal data structures, which are not exposed to external access. When keys are set for deletion, the key is zeroized by overwriting the key once with zeroes to ensure it cannot be retrieved. This function is only used for securely wiping keys in memory, not from magnetic media.

The Cryptographic Module implements the following access control policy on keys and CSPs in the module shown in Table 7 – Cryptographic Module CSP Access Control Policy. The Access Policy is noted by R=Read, W=Write and X=Execute.

Services	CSP Access	Access Rights
AES	AES-key	RX
Triple-DES	Triple-DES-key	RX
SHS		
HMAC	HMAC key	RX
RNG	PRNG key, PRNG seed	RWX
Initialization Self-Tests	SHA1 HMAC integrity check key	RX
On-demand Self-Tests	SHA1 HMAC integrity check key	RX
Zeroization	AES-key, Triple-DES-key	RW

Table 7 – Cryptographic Module CSP Access Control Policy

2.8 Self-Tests

Upon startup, the Mobile Armor Cryptographic Module 3.0 performs several power-up self-tests including known answer tests for all algorithms. The Cryptographic Module performs an HMAC SHA1 self-integrity check to verify the module has not been damaged or tampered with. The hash value for this integrity check is stored in a hidden file kept in the same directory as the module. The file is hidden according to standard file handling practices for the operating system.

The Cryptographic Module performs continuous tests on the PRNG (approved as well as non-approved) each time it is used to generate random data.

Algorithm	Known Answer Tests	Monte Carlo Tests
AES	Yes	Yes
Triple-DES	Yes	Yes
SHA1	Yes	No
HMAC SHA1	Yes	No
SHA224	Yes	No
HMAC SHA224	Yes	No
SHA256	Yes	No

Algorithm	Known Answer Tests	Monte Carlo Tests
HMAC SHA256	Yes	No
SHA384	Yes	No
HMAC SHA384	Yes	No
SHA512	Yes	No
HMAC SHA512	Yes	No
Integrity Test (HMAC-SHA1)	Yes	No
ANSI X9.31 PRNG	Yes	Yes

Table 8 - FIPS Algorithm Self-Tests

Upon failure of a self-test, an error message indicating the failure is sent to the calling application and the module enters the Error state where no operations are permitted. To transition out of the Error state, the module must be uninstalled and installed by the crypto officer only.

The module does not provide a direct means for executing an on-demand self-test, though every time the calling application is restarted, the module is also restarted, and the self-tests are automatically executed. To run self-tests on request, restart the application which is using the module.

2.9 Design Assurance

Mobile Armor maintains versioning for all source code through Subversion 1.4. Documentation is managed through Microsoft SharePoint Portals.

2.10 Mitigation of Other Attacks

The Mobile Armor Cryptographic Module 3.0 does not employ security mechanisms to mitigate specific attacks.

3 Operation of the Mobile Armor Cryptographic Module 3.0

The Mobile Armor Cryptographic Module 3.0 contains only FIPS-approved algorithms and operates only in FIPS mode after installation.

The Mobile Armor Cryptographic Module 3.0 is designed for installation and use on a computer or mobile device configured in single user mode, and is not designed for use on systems where multiple, concurrent users are active.