Security Policy
FIPS 140-2 Level 2

Mobile Armor Cryptographic Module

3.5

Version: 1.3

Date: 3/30/2009

This document is provided for informational purposes about the non-proprietary structure of the Mobile Armor Cryptographic Module 3.5 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

Contents

Tables

Figures

1 Security Policy Introduction

1.1 Security Policy, Product and Evaluation Identification

SP Title: Mobile Armor Cryptographic Module 3.5 Security Policy

SP Version: Version 1.2

Product Identification: Mobile Armor Cryptographic Module 3.5

FIPS Evaluation Identification: FIPS 140-2

FIPS 140-2 Level: 2

1.2 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Mobile Armor Cryptographic Module 3.5. This security policy describes how the Mobile Armor Cryptographic Module 3.5 meets the Level 2 security requirements of FIPS 140-2. This module will be evaluated on Microsoft Windows XP, Windows Server 2003, Windows 2000, SUSE 10, and Red Hat Enterprise Linux 5. The module is also capable of running on Microsoft Windows Vista, Microsoft Windows Mobile 5 and 6, Mac OS 10 and Ubuntu 7 and is based on the Mobile Armor Cryptographic Module 3.0, allowing it to run as a FIPS 140-2 Level 2 compliant module on those operating systems.

This policy was prepared as part of FIPS 140-2 validation of the Mobile Armor Cryptographic Module 3.5.

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 3.5 in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the Mobile Armor Cryptographic Module 3.5 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
API	Application Programming Interface
CC	Common Criteria
DLL	Dynamic Link Library
HMAC	Hash Message Authentication Code
OS	Operating System
PRNG	Pseudo Random Number Generator
SHA	Secure Hash Algorithm
Triple-DES	Triple Data Encryption Standard

Table 1 – Acronyms

2 Mobile Armor Cryptographic Module 3.5

2.1 Overview

The Mobile Armor Cryptographic Module 3.5 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 3.5 is classified as software which is designed to run on a multi-chip standalone module for FIPS 140-2 purposes. Designed around the Mobile Armor Cryptographic Module 3.0 module (validated at FIPS 140-2 Level 1), the module is able to run on several operating systems as a Level 2 module.

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

- Windows XP Professional SP2 running on Dell Optiplex GX270 (http://www.commoncriteriaportal.org/files/epfiles/st_vid9506-vr.pdf)
- Windows 2000 Professional SP3 running on Dell Optiplex GX400 (http://www.commoncriteriaportal.org/files/epfiles/CCEVS_VID402-VR.pdf)
- Windows Server 2003 SP1 running on Dell Optiplex GX270 (http://www.commoncriteriaportal.org/files/epfiles/ST_VID4025-VR.pdf)
- Red Hat Enterprise Linux Version 5 running on IBM System x3455 (32 bit binary) (http://www.commoncriteriaportal.org/files/epfiles/st_vid10125-vr.pdf)
- Red Hat Enterprise Linux Version 5 running on IBM System x3455 (64 bit binary) (http://www.commoncriteriaportal.org/files/epfiles/st_vid10125-vr.pdf)
- SUSE Linux Enterprise Server 10 SP1 running on IBM System x3455 (32 bit binary) (http://www.commoncriteriaportal.org/files/epfiles/st_vid10271-vr.pdf)
- SUSE Linux Enterprise Server 10 SP1 running on IBM System x3455 (64 bit binary) (http://www.commoncriteriaportal.org/files/epfiles/st_vid10271-vr.pdf)

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.

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 Vista

- Microsoft Windows Vista 64-bit
- Ubuntu 7.10
- Ubuntu 7.10 64-bit
- Apple Mac OS X 10.4, 10.5 (on Intel)
- Microsoft Windows Mobile 5
- Microsoft Windows Mobile 6

2.3 Module Ports and Interfaces

The Mobile Armor Cryptographic Module 3.5 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 as defined by the Common Criteria evaluation for the operating environment. This boundary is shown in Figure 1 - Logical Block Diagram.

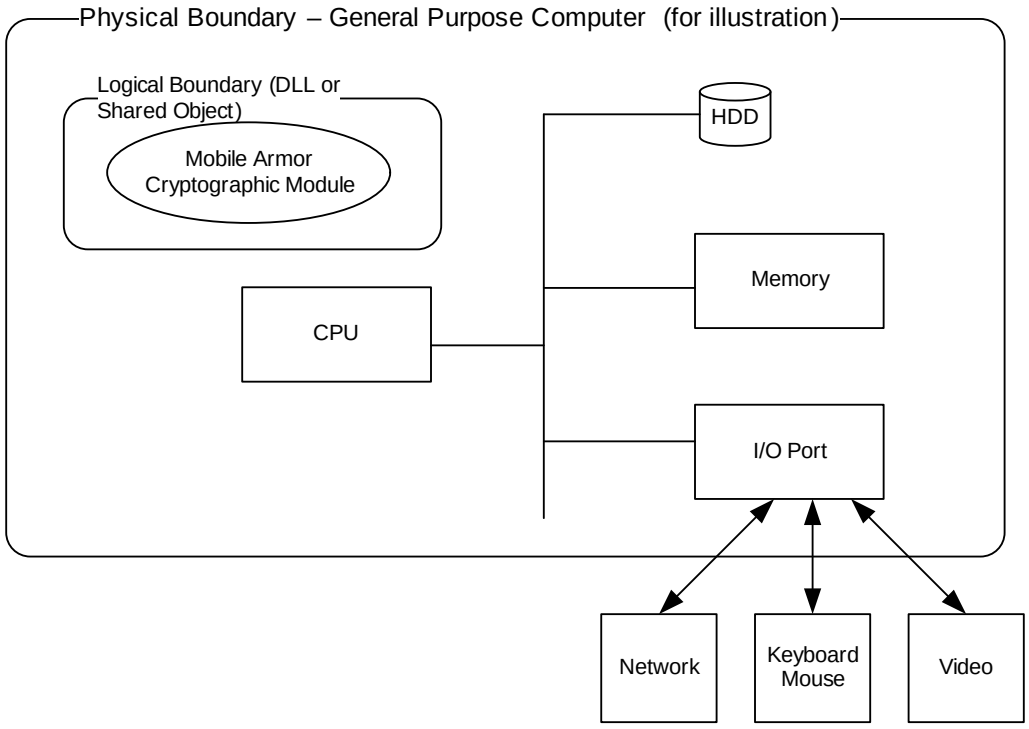

Figure 1 - Logical Block Diagram

The Mobile Armor Cryptographic Module 3.5 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 3.5 supports two roles, the Crypto Officer and the User; there is no Maintenance role. The module relies on the operational environment authentication to distinguish the role an operator should have. The OS on which the module runs must provide a minimum length password of 6 characters to satisfy the FIPS 140-2 authentication requirements. The module assigns the Crypto Officer role to an operating system account with the username "maco" (Mobile Armor Crypto Officer). The maco user must be an administrator, but only the maco account is assigned the Crypto Officer role. All other users are automatically assigned to the User role.

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

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 aes_ofb_encrypt aes_ofb_decrypt aes_ctr_encrypt aes_ctr_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
On-demand Self-Tests	SelfTest	Allows Crypto Officers to determine if the module is functioning properly at any time

Service	API Calls	Purpose and Use
Zeroization	aes_clear_context des3_clear_context	Allows Users to zeroize key data

Table 3 - Cryptographic Module Services

The Cryptographic Module implements an access control policy to ensure proper authorization to the provided services. Table 4 - Cryptographic Module Services Access Control Policy shows the policy and the services which are accessible by the Roles available in the module.

Service	User	Crypto Officer
AES	X	X
Triple-DES	X	X
SHS	X	X
HMAC	X	X
RNG	X	X
Initialization Self-Tests	X	X
On-demand Self-Tests		X
Zeroization	X	X

Table 4 - Cryptographic Module Services Access Control Policy

2.5 *Physical Security*

The Mobile Armor Cryptographic Module 3.5 is a software module intended for use with a Common Criteria evaluated operating system such as Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Server 2003, Red Hat Enterprise Linux 5 and SUSE 10. 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 3.5 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	Normal C Dll (MAFips.dll)
Microsoft Windows 64	Normal C Dll (MAFips64.dll)

Linux	Shared Object (libMAFips.so)
Linux 64-bit	Shared Object (libMAFips64.so)

Table 5 – Cryptographic Module Implementations

The Mobile Armor Cryptographic Module 3.5 is a single user module that is always distributed in binary form to discourage unauthorized access or modification to source. Additionally, a software integrity check is run when the modules are loaded to help ensure that the code has not been accidentally or ineptly modified from its validated configuration.

2.7 Cryptographic Key Management

The Mobile Armor Cryptographic Module 3.5 implements the following algorithms. The FIPS approved column specifies whether the algorithm is available in the FIPS-mode.

Algorithm	FIPS Approved	Cert Number
AES (CBC,OFB, CFB, CTR, ECB 256-bit, 192-bit, 128bit keys)	Yes	920
Triple-DES (CBC, ECB 112, 168-bit keys)	Yes	740
SHA1	Yes	907
SHA224	Yes	
SHA256	Yes	
SHA384	Yes	
SHA512	Yes	
SHA1 HMAC	Yes	514
SHA224 HMAC	Yes	
SHA256 HMAC	Yes	
SHA384 HMAC	Yes	
SHA512 HMAC	Yes	
ANSI X9.31 PRNG	Yes	528
DES	No	-
Non-Approved RNG	No	-

Table 6 - FIPS Cryptographic Algorithms

All keys are generated by using the ANSI X9.31 PRNG.

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.

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 7 - 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 8 – 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

Services	CSP Access	Access Rights
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 8 – Cryptographic Module CSP Access Control Policy

2.8 Self-Tests

Upon startup, the Mobile Armor Cryptographic Module 3.5 performs several power-up self-tests including known answer tests for all algorithms. The Cryptographic Module also performs a self-integrity check (in the form of an HMAC-SHA-1 digest comparison) to verify the module has not been damaged or tampered with.

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
SHA1 HMAC	Yes	No
SHA224	Yes	No
SHA224 HMAC	Yes	No
SHA256	Yes	No
SHA256 HMAC	Yes	No
SHA384	Yes	No
SHA384 HMAC	Yes	No
SHA512	Yes	No
SHA512 HMAC	Yes	No
Integrity Test (HMAC-SHA1)	Yes	No
ANSI X9.31 PRNG	Yes	Yes

Table 9 - FIPS Algorithm Self-Tests

Upon failure of a self-test, an error message indicating the failure is logged to the operating system log and the module enters the Error state where no operations are permitted. To transition out of the Error state, the module must be reset.

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 3.5 does not employ security mechanisms to mitigate specific attacks.

3 Operation of the Mobile Armor Cryptographic Module 3.5

For operation in FIPS mode, the following steps must be performed:

1) Use one of the CC evaluated OS identified in section 2.2 as specified in the relevant Security Target (ST).
2) Define an account "maco" belonging to the Administrator group on the OS. This account will assume the role of the Crypto Officer. This account must adhere to the minimum password length requirement specified in section 2.4.
3) Use only FIPS Approved algorithms identified in table 3.
4) Guest account must be disabled and all accounts on the OS must be password protected.