# Mobile Armor™ Crypto Module 2.1.0.0

## Security Policy

**FIPS 140-2**

Level 1

Version 5.1

September 23, 2005

Mobile Armor Mobile Armor™ Crypto Module 2.1.0.0 Security Policy

This document is provided for informational purposes about the non-proprietary structure of the Mobile Armor™ Crypto Module 2.1.0.0 as it pertains to FIPS 140-2 validation.

Any reproduction of this document must include the Copyright notice of Mobile Armor, LLC.

Document ID Number: DACSPSP-51-01

Contact Mobile Armor

Mobile Armor, LLC.
400 South Woods Mill Road
Suite 110
St. Louis, MO, 63017 USA

| | |
|---|---|
| Telephone: | +1 (636) 449-0239 |
| Fax: | +1 (314) 205-2303 |
| Website: | http://www.mobilearmor.com |
| Email: | mailto:sales@mobilearmor.com |

# Table of Contents

# 1. Security Policy Introduction

## 1.1 Security Policy, Product and Evaluation Identification

**SP Title:** Mobile Armor Crypto Module 2.1.0.0 Security Policy

**SP Version:** Version 5.1

**Product Name:** Mobile Armor Crypto Module

**Product version:** 2.1.0.0

**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 Crypto Module 2.1.0.0. This security policy describes how the Mobile Armor Crypto Module 2.1.0.0 meets the Level 1 security requirements of FIPS 140-2. While the product was tested on Windows XP Professional SP2, PocketPC 2003 and Red Hat Enterprise Linux 3.0, it is a cross-platform module also capable of running on Microsoft Windows 2000 as well as other Linux distributions running the 2.6.8 or higher kernel. This policy was prepared as part of FIPS 140-2 validation of the Mobile Armor Crypto Module 2.1.0.0.

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/cryptval/.

## 1.3 References

This document deals only with operations and capabilities of the Mobile Armor Crypto Module 2.1.0.0 in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the Mobile Armor Crypto Module 2.1.0.0 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 |
|---|---|
| 3DES | Triple Data Encryption Standard |
| AES | Advanced Encryption Standard |
| PRNG | Pseudo Random Number Generator |
| SHA | Secure Hash Algorithm |
| API | Application Programming Interface |
| DLL | Dynamic Link Library |

**Table 1 – Acronyms**

# 2. Mobile Armor Crypto Module

## 2.1 Overview

The Mobile Armor Crypto Module 2.1.0.0 provides cryptographic support for the Mobile Armor Mobile Armor products. The Crypto Module is used to create, manage and delete cryptographic keys as well as to perform cryptographic operations.

To provide cryptographic security services, the Crypto 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 Crypto Module for encryption/decryption operations.

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

## 2.2 Cryptographic Module

The Mobile Armor Crypto Module 2.1.0.0 is classified as a multi-chip standalone module for FIPS 140-2 purposes. The cryptographic module is capable on running on any commercially available IBM compatible PC running the following list of Operating Systems (OS).

- Microsoft Windows XP Professional SP2
- Microsoft Windows 2000 SP4
- Red Hat Enterprise Linux 3.0

Further, the module is capable of running on any commercially available Microsoft Windows Mobile-based PDA (note the PDA must be capable of running Windows Mobile, and not earlier versions of the Pocket PC 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/pocketpc/ppc/americas.mspx.

The module was tested for FIPS 140-2 compliance on a generic PC running Windows XP Professional SP2 configured in the single user mode as well as Red Hat Enterprise Linux 3.0 configured in single user mode. The module was also tested on a generic Windows Mobile PDA running PocketPC 2003.

The module is compiled into two libraries, one for the Windows Mobile platform, and one for the PC platform. The only changes between these platforms are those necessary for porting the Crypto Module, and these are handled through compiler options.

## 2.3 Module Ports and Interfaces

The Mobile Armor Crypto Module 2.1.0.0 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 PDA 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.

The Mobile Armor Crypto Module 2.1.0.0 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 Crypto Module 2.1.0.0 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 the Crypto Officer and User roles which are combined into a single role. This role has access to all services, keys and CSPs of the module.

The Mobile Armor Crypto Module 2.1.0.0 provides the following API calls for access to the functions of the module:

| Exposed APIs | Description |
|---|---|
| CMAEncryption | Constructor |
| ~CMAEncryption | Destructor |
| SetEncryptionAlgorithm | Sets encryption algorithm |
| SetSecretKey | Sets encryption key |
| DeleteSecretKey | Deletes encryption key |
| CryptEncrypt | This will encrypt a block of text is specified chunks |
| CryptDecrypt | This will decrypt a block of text is specified chunks |
| CryptEncryptBlock | This will encrypt an algorithm-specific block of data |
| CryptDecryptBlock | This will decrypt an algorithm-specific block of data |
| CryptHash | Computes the hash of the input |
| CryptGenRand | Generates a random number |
| CryptGenKey | This generates a random key of the specified size |

**Table 3 – Application Programming Interface**

## 2.5 Physical Security

The Mobile Armor Crypto Module 2.1.0.0 is a software module intended for use with Microsoft Windows 2000, Microsoft Windows XP and Red Hat Enterprise Linux 3.0 in single user modes on a PC, and Microsoft Windows Mobile (Pocket PC 2003) on a PDA. 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 Crypto Module 2.1.0.0 is compiled into two separate modules with the same cryptographic source, one for the PC-based platforms, and one for the Windows Mobile PDA platform. The Crypto Module is implemented as a DLL on Windows platforms and as a Shared Object (SO) on Linux. The only differences in the Crypto Module are those necessary to port the Crypto Module from the PC to the PDA platform.

The Mobile Armor Crypto Module 2.1.0.0 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 Crypto Module 2.1.0.0 implements the following algorithms. The FIPS approved column specifies whether the algorithm is available in the FIPS-mode.

| Algorithm | FIPS Approved |
|---|---|
| AES (ECB-256-bit keys) | Yes |
| TDES (ECB, Keying Options 1,2,3) | Yes |
| SHA-256 | Yes |
| HMAC SHA-1 | Yes |
| SHA-1 | Yes |
| ANSI X9.31 PRNG | Yes |

**Table 4 – 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 Crypto Module as necessary.

| Name | Created | Size(s) in bits | Purpose |
|---|---|---:|---|
| AES-key | Generated/Inserted | 256 | Data Encryption, Decryption |
| 3DES-key | Generated/Inserted | 168 | Data Encryption, Decryption |
| HMAC-SHA-1 integrity check key | Hard coded | N/A | Verify driver integrity |
| PRNG key<br>PRNG seed | Generated<br>Generated | 168-bits<br>64-bits | Random Number Generation<br>Random Number Generation |

**Table 5 – Key Generation**

Keys are stored in the Crypto 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 multiple times to ensure it cannot be retrieved.

## 2.8 Self-Tests

The Mobile Armor Crypto Module 2.1.0.0 performs several power up self-tests including known answer tests and monte carlo tests for the algorithms (AES, 3DES, SHA-1, SHA-256, HMAC-SHA-1, and PRNG). The crypto module also performs a self-integrity check to verify the module has not been damaged or tampered with.

The crypto 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 |
| TDES | Yes | Yes |
| SHA-256 | Yes | No |
| SHA-1 | Yes | No |
| HMAC SHA-1 | Yes | No |
| ANSI X9.31 PRNG | Yes | Yes |

**Table 6 – FIPS Algorithm Self Tests**

## 2.9 Design Assurance

Mobile Armor maintains versioning for all source code and associated documentation through Microsoft Visual SourceSafe 6.0.

## 2.10 Mitigation of Other Attacks

The Mobile Armor Crypto Module 2.1.0.0 does not employ security mechanisms to mitigate specific attacks.

# *3. Operation of the Mobile Armor Crypto Module*

The Mobile Armor Crypto Module 2.1.0.0 contains only FIPS-approved algorithms and operates only in FIPS mode after installation.

The Mobile Armor Crypto Module 2.1.0.0 is designed for installation and use on a computer configured in single user mode, and is not designed for use on systems where multiple, concurrent users are active.