

*Mocana Cryptographic Loadable
Kernel Module
Software Version 5.4f*

*Security Policy
Document Version 1.2*

Mocana Corporation

October 17, 2011

TABLE OF CONTENTS

1. MODULE OVERVIEW.....3

2. SECURITY LEVEL4

3. MODES OF OPERATION.....5

 APPROVED MODE OF OPERATION5

 NON-FIPS APPROVED ALGORITHMS5

4. PORTS AND INTERFACES.....6

5. IDENTIFICATION AND AUTHENTICATION POLICY6

 ASSUMPTION OF ROLES.....6

6. ACCESS CONTROL POLICY.....6

 ROLES AND SERVICES.....6

 OTHER SERVICES.....7

 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPs).....8

 DEFINITION OF PUBLIC KEYS:9

 DEFINITION OF CSPS MODES OF ACCESS9

7. OPERATIONAL ENVIRONMENT.....10

8. SECURITY RULES10

9. PHYSICAL SECURITY11

10. MITIGATION OF OTHER ATTACKS POLICY.....11

11. CRYPTOGRAPHIC OFFICER GUIDANCE.....11

 KEY DESTRUCTION SERVICE11

12. DEFINITIONS AND ACRONYMS.....12

1. Module Overview

The Mocana Cryptographic Loadable Kernel Module (Software Version 5.4f) is a software only, multi-chip standalone cryptographic module that runs on a general purpose computer. The primary purpose of this module is to provide FIPS Approved cryptographic routines to consuming applications via an Application Programming Interface. The physical boundary of the module is the case of the general purpose computer. The logical boundary of the cryptographic module is the kernel module, moc_crypto.ko.

The cryptographic module runs on the following operating environments:

- Android 2.2 (single-user mode)
- WindRiver 4.0 using Linux 2.6.34 (single-user mode)

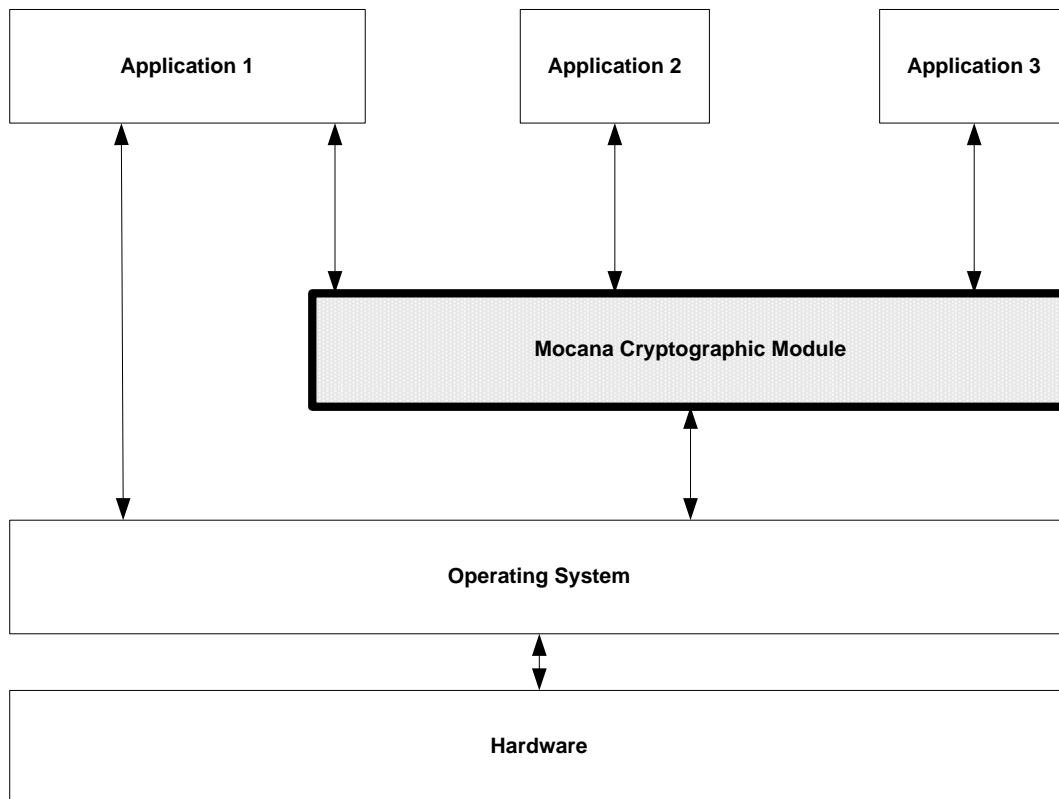


Figure 1 – Cryptographic Module Interface Diagram

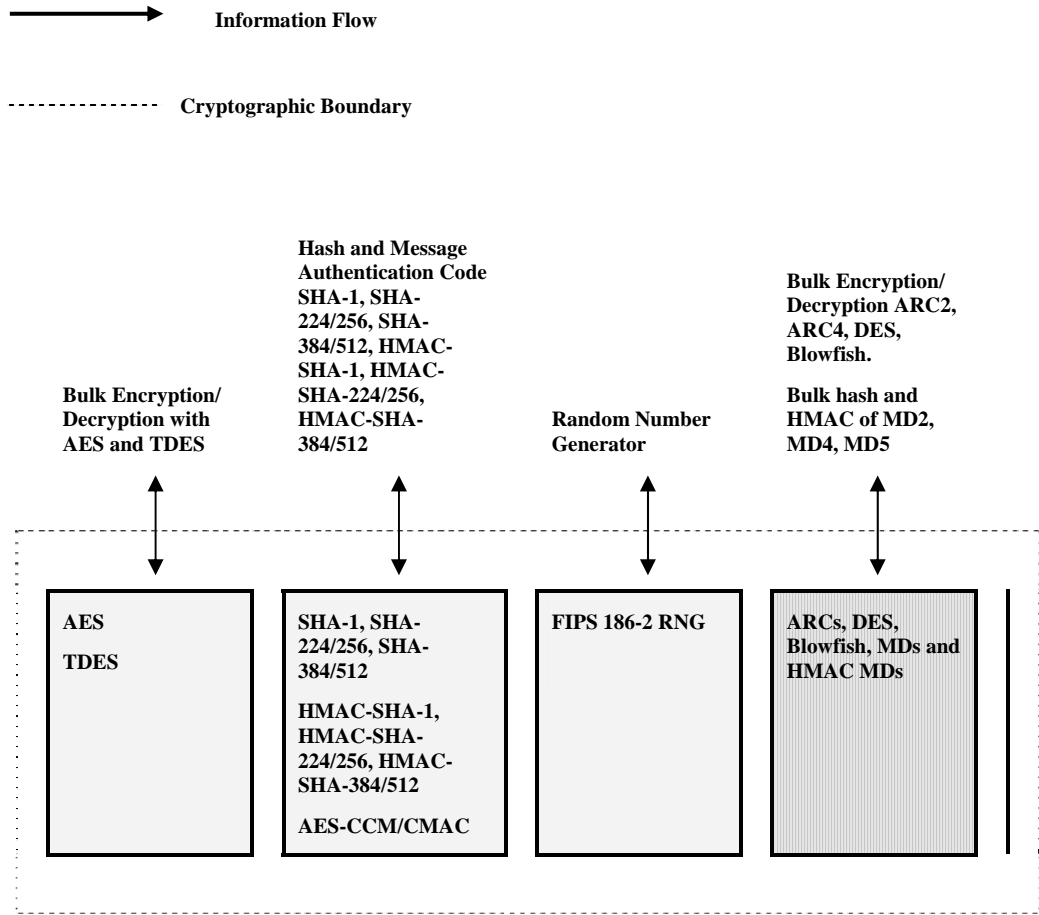


Figure 2 – Logical Cryptographic Boundary

2. Security Level

The cryptographic module meets the overall requirements applicable to Security Level 1 of FIPS 140-2.

Table 1 - Module Security Level Specification

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	1
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The module supports both a FIPS Approved and non-Approved mode of operation. The following FIPS Approved algorithms are supported:

- AES (ECB, CBC, CFB, CTR and GCM modes; E/D; 128, 192 and 256)
- AES (CCM, CMAC; 128, 192 and 256)
- AES XTS (128 and 256)
- Triple-DES (3-key and 2-key; TCBC mode; E/D)
- HMAC-SHA-1
- HMAC-SHA-224
- HMAC-SHA-256
- HMAC-SHA-384
- HMAC-SHA-512
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512
- FIPS 186-2 RNG

Non-FIPS Approved mode of operation

In addition to the above algorithms, the following algorithms are available in the non-FIPS Approved mode of operation:

- DES, Blowfish, ARC2, ARC4, MD2, MD4, MD5, HMAC-MD5, AES EAX, AES XCBC

The module will transition to the non-Approved mode of operation when one of the above algorithms is utilized. The module can transition back to the Approved mode of operation by utilizing an Approved security function listed above.

4. Ports and Interfaces

The physical ports of the module are provided by the general purpose computer on which the module is installed. The logical interfaces are defined as the API of the cryptographic module. The module's API supports the following logical interfaces: data input, data output, control input, and status output.

5. Identification and Authentication Policy

Assumption of roles

The Mocana Cryptographic Loadable Kernel Module shall support two distinct roles (User and Cryptographic Officer). The cryptographic module does not provide any identification or authentication methods of its own. The Cryptographic Officer and the User roles are implicitly assumed based on the service requested.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	N/A	N/A
Cryptographic Officer	N/A	N/A

6. Access Control Policy

Roles and Services

Table 3 – Services Authorized for Roles

Role	Authorized Services
User	<ul style="list-style-type: none"> • Self-tests • Show Status
Cryptographic-Officer	<ul style="list-style-type: none"> • AES Encryption • AES Decryption • AES Message Authentication Code • TDES Encryption • TDES Decryption • SHA-1 • SHA-224/256 • SHA-384/512 • HMAC-SHA-1 Message Authentication Code • HMAC-SHA-224/256 Message Authentication Code • HMAC-SHA-384/512 Message Authentication Code

	<ul style="list-style-type: none">• FIPS 186-2 Random Number Generation• Key Destruction
--	---

Other Services

The cryptographic module supports the following service that does not require an operator to assume an authorized role:

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2. It is invoked by reloading the library into executable memory.

Definition of Critical Security Parameters (CSPs)

The following are CSPs that may be contained in the module:

Table 4 - CSP Information

Key	Description/Usage	Generation	Storage	Entry / Output	Destruction
TDES Keys	Used during TDES encryption and decryption	Externally.	Temporarily in volatile RAM	Entry: Plaintext Output: N/A	An application program which uses the API may destroy the key. The Key Destruction service zeroizes this CSP.
AES Keys	Used during AES encryption, decryption, and CMAC operations	Externally.	Temporarily in volatile RAM	Entry: Plaintext Output: N/A	An application program which uses the API may destroy the key. The Key Destruction service zeroizes this CSP.
HMAC Keys	Used during HMAC-SHA-1, 224, 256, 384, 512 operations	Externally.	Temporarily in volatile RAM	Entry: Plaintext Output: N/A	An application program which uses the API may destroy the key. The Key Destruction service zeroizes this CSP.

Note: Key Entry and Output refers to keys crossing the logical boundary of the cryptographic module, and not the physical boundary of the GPC.

Definition of Public Keys:

The module does not contain any public keys.

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services.

Table 5 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	User		
X		AES Encryption	Use AES Key
X		AES Decryption	Use AES Key
X		AES Message Authentication Code	Use AES Key
X		TDES Encryption	Use TDES Key
X		TDES Decryption	Use TDES Key
X		SHA-1	Generate SHA-1 Output; no CSP access
X		SHA-224/256	Generate SHA-224/256 Output; no CSP access
X		SHA-384/512	Generate SHA-384/512 Output; no CSP access
X		HMAC-SHA-1 Message Authentication Code	Use HMAC-SHA-1 Key Generate HMAC-SHA-1 Output
X		HMAC-SHA-224/256 Message Authentication Code	Use HMAC-SHA-224/256 Key Generate HMAC-SHA-224/256 Output
X		HMAC-SHA-384/512 Message Authentication Code	Use HMAC-SHA-384/512 Key Generate HMAC-SHA-384/512 Output
X		FIPS 186-2 Random Number Generation	N/A
X		Key Destruction	Destroy All CSPs
	X	Show Status	N/A
	X	Self-Tests	N/A

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are applicable because the Mocana Cryptographic Loadable Kernel Module operates in a modifiable operational environment.

The module was operational tested on the following platforms:

- Android 2.2
- WindRiver 4.0 using Linux 2.6.34

8. Security Rules

The Mocana Cryptographic Loadable Kernel Module design corresponds to the following security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module shall provide two distinct roles. These are the User role and the Cryptographic Officer role.
2. The cryptographic module does not provide any operator authentication.
3. The cryptographic module shall encrypt/decrypt message traffic using the Triple-DES or AES algorithms.
4. The cryptographic module shall perform the following self-tests:

Power-up Self-Tests:

- Cryptographic Algorithm Tests:
 - AES - ECB, CBC, CFB, CCM, CMAC, CTR, GCM, and XTS Known Answer Test
 - Triple-DES Known Answer Test
 - HMAC-SHA-1 Known Answer Test
 - HMAC-SHA-224 1 Known Answer Test
 - HMAC-SHA-256 Known Answer Test
 - HMAC-SHA-384 Known Answer Test
 - HMAC-SHA-512 Known Answer Test
 - SHA-1 Known Answer Test
 - SHA-224 Known Answer Test
 - SHA-256 Known Answer Test
 - SHA-384 Known Answer Test
 - SHA-512 Known Answer Test
 - FIPS 186-2 RNG Known Answer Test
- Software Integrity Test: HMAC-SHA-1
- Critical Functions Tests: N/A

Conditional Tests:

- FIPS 186-2 RNG Continuous Test
5. At any time, the operator shall be capable of commanding the module to perform the power-up self-tests by reloading the cryptographic module into memory.
 6. The cryptographic module is available to perform services only after successfully completing the power-up self-tests.
 7. Data output shall be inhibited during self-tests, zeroization, and error states.
 8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
 9. The module shall not support concurrent operators.
 10. The module does not support key generation.
 11. DES, Blowfish, ARC2, ARC4, MD2, MD4, MD5, HMAC-MD5, AES EAX, and AES XCBC are not allowed for use in the FIPS Approved mode of operation. When these algorithms are used, the module is no longer operating in the FIPS Approved mode of operation. It is the responsibility of the consuming application to zeroize all keys and CSPs prior to and after utilizing these non-Approved algorithms. CSPs shall not be shared between the Approved and non-Approved modes of operation.

9. Physical Security

The FIPS 140-2 Area 5 Physical Security requirements are not applicable because the Mocana Cryptographic Loadable Kernel Module is software only.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks outside the scope of FIPS 140-2 requirements.

11. Cryptographic Officer Guidance

The operating systems running the Mocana Cryptographic Loadable Kernel Module must be configured in a single-user mode of operation.

Key Destruction Service

There is a context structure associated with every cryptographic algorithm available in this module. Context structures hold sensitive information such as cryptographic keys. These context structures must be destroyed via respective API calls when the application software no longer needs to use a specific algorithm any more. This API call will zeroize all sensitive information including cryptographic keys before freeing the dynamically allocated memory. See the *Mocana Cryptographic API Reference* for additional information.

12. Definitions and Acronyms

AES	Advanced Encryption Standard
API	Application Program Interface
CO	Cryptographic Officer
CSP	Critical Security Parameter
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DLL	Dynamic Link Library
ECDSA	Elliptic Curve Digital Signature Standard
RNG	Random Number Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
LKM	Loadable Kernel Module
RAM	Random Access Memory
RNG	Random Number Generator
TDES	Triple-DES
SHA	Secure Hash Algorithm
SO	Shared Object