Mocana Cryptographic Loadable Kernel Module

Software Version 5.5f and 5.5.1f

Non-Proprietary Security Policy

Document Version 3.1

Mocana Corporation

March 30, 2016

TABLE OF CONTENTS

1. Module Overview

The Mocana Cryptographic Loadable Kernel Module (Software Version 5.5f, 5.5.1f) 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:

Table 1 – Operational Environments

SW Version	Operating System	Platform
5.5f	Android 2.2 (single-user mode)	LG Optimus 3D
5.5f	Android 2.3 (single-user mode)	LG G2X
5.5f	Android 4.0 (single-user mode)	Samsung Nexus-S
5.5f	Android 4.1 (single-user mode)	LG Optimus 3D
5.5f	Ubuntu Linux 32 bit (single-user mode)	Dell Dimension 9200
5.5f	Ubuntu Linux 64 bit (single-user mode)	Dell Dimension 9200
5.5.1f	Android 4.3(single-user mode)	Asus TF 700 Tablet
5.5.1f	Android 4.4 (single-user mode)	Nexus 7 Tablet
5.5.1f	Android Lollipop Linux 3.4 (single-user mode)	Qualcomm Snapdragon MSM8974 development device
5.5.1f	Android Lollipop Linux 3.10 (single-user mode)	Qualcomm Snapdragon MSM8992 development device

The cryptographic module is also supported on the following operating environments for which operational testing was not performed:

- Linux Kernel version 3.4.0
- Linux Kernel version 3.1.10
- Linux Kernel version 3.0.31
- Linux Kernel version 2.6.32
- Linux Kernel version 3.0.27
- Linux Kernel version 2.6.32.45
- Linux Kernel version 2.6.35.7
- Android 4.2
- Android 5.0

Note: the CMVP makes no statement as to the correct operation of the module on the operational environments for which operational testing was not performed.

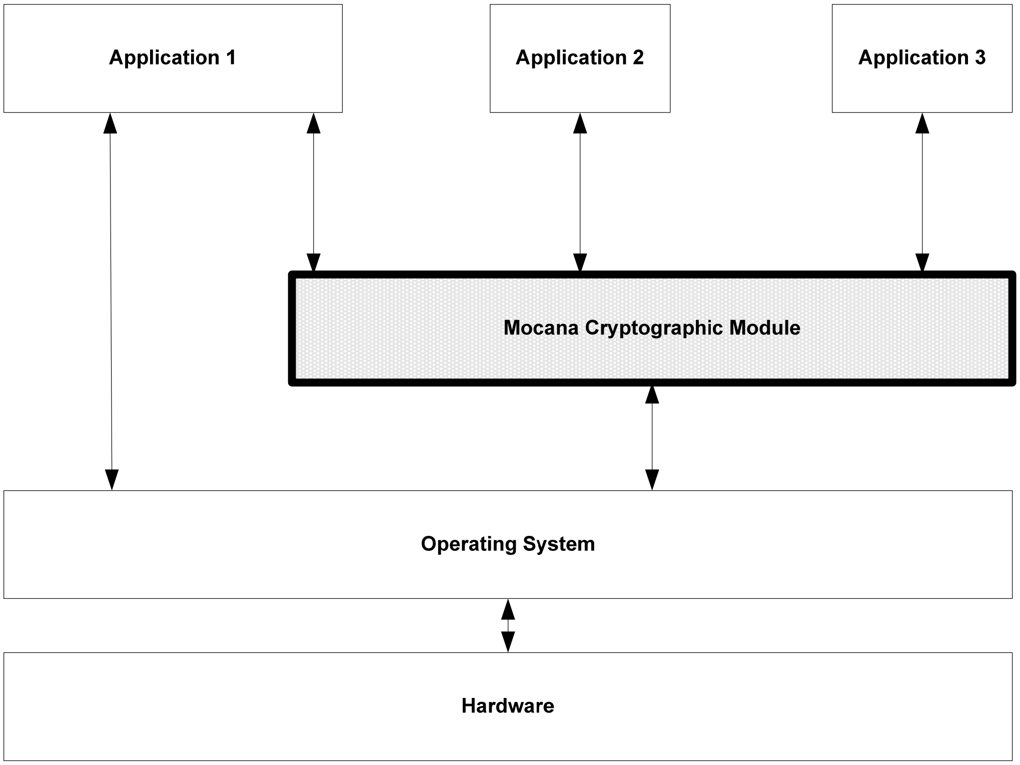

Figure 1 – Cryptographic Module Interface Diagram

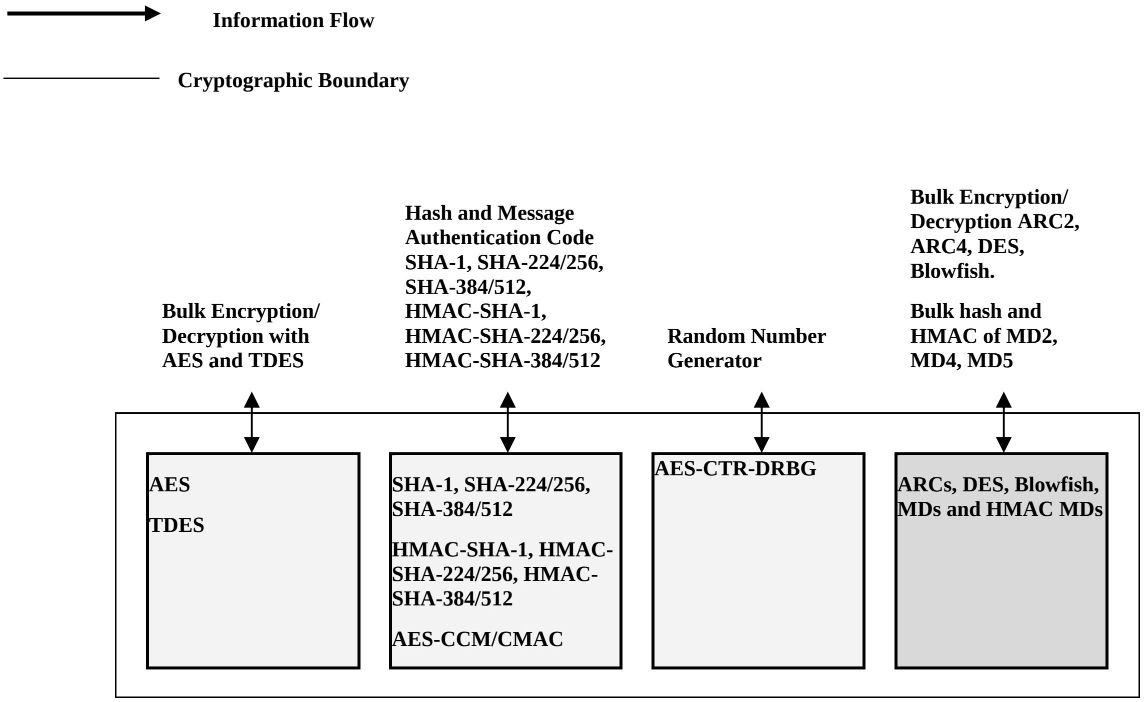
Information Flow
Cryptographic Boundary
Bulk Encryption/ Decryption with AES and TDES
Hash and Message Authentication Code SHA-1, SHA-224/256, SHA-384/512, HMAC-SHA-1, HMAC-SHA-224/256, HMAC-SHA-384/512
Random Number Generator
Bulk Encryption/ Decryption ARC2, ARC4, DES, Blowfish.
Bulk hash and HMAC of MD2, MD4, MD5
AES
TDES
SHA-1, SHA-224/256, SHA-384/512
HMAC-SHA-1, HMAC-SHA-224/256, HMAC-SHA-384/512
AES-CCM/CMAC
AES-CTR-DRBG
ARCs, DES, Blowfish, MDs and HMAC MDs

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 2 – 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 multiple Approved modes of operation. Upon module initialization, a consuming application can configure the module to utilize all, or any subset of the following FIPS Approved algorithms:

Table 3 - Algorithms and Software Versions

Algorithms	Software Version 5.5f	Software Version 5.5.1f
AES (ECB, CBC, OFB, CFB, CTR and GCM modes; E/D; 128, 192 and 256)	Certs. #2039 and #2272	Cert. #2741
AES (CCM, CMAC 128, 192 and 256)	Certs. #2039 and #2272	Cert. #2741
AES XTS (128 and 256)	Certs. #2039 and #2272	Cert. #2741
Triple-DES (3-key and 2-key[1]; TCBC mode; E/D)	Cert. #1316	Cert. #1650
HMAC-SHA-1; HMAC-SHA-224; HMAC-SHA-256; HMAC-SHA-384; HMAC-SHA-512	Cert. #1238	Cert. #1718
SHA-1 SHA-2: SHA-224; SHA-256; SHA-384; SHA-512	Cert. #1785	Cert. #2313
AES-CTR based DRBG	Cert. #201	Cert. #460

[1] Per NIST SP 800-131A: Through December 31, 2015, the use of 2-key Triple DES for encryption is restricted: the total number of blocks of data encrypted with the same cryptographic key shall not be greater than 2^{20}. After December 31, 2015, 2-key Triple DES shall not be used for encryption. Decryption using 2-key Triple DES is allowed for legacy-use.

Non-Approved but Allowed Algorithms

Within the FIPS Approved mode of operation, the module supports the following allowed algorithms:

- NDRNG – Used to seed the Approved DRBGs

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, FIPS 186-2 RNG, Dual EC DRBG

During module initialization, the module may be configured to use one of these non-Approved security functions in lieu of an Approved one. In this case, during operation, the module can switch service by service between an Approved mode of operation and a non-Approved mode of operation. 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.

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 4 – 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 5 – Services Authorized for Use in the Approved modes of operation

Role	Authorized Services
User	• Self-tests • Show Status • Read Version
Cryptographic-Officer	• 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 • AES-CTR-DRBG Random Number Generation • Key Destruction

Note: The module may be configured to support only a subset of the Approved security functions listed in Section 3 above. In this case, not all of the services listed in Table 3 would be available.

Other Services

Table 6 – Services Authorized for Use in the non-Approved mode of operation

Role	Authorized Services
User	• Self-tests • Show Status • Read Version
Cryptographic-Officer	• DES Encryption • DES Decryption • AES Message Authentication Code • Blowfish Encryption • Blowfish Decryption • ARC2, ARC4 Encryption • ARC2, ARC4 Decryption • MD2 Hash • MD4 Hash • MD5 Hash • HMAC-MD5 Message Authentication Code • AES EAX Encryption

Role	Authorized Services
	• AES EAX Decryption • AES XCBC Encryption • AES XCBC Decryption • FIPS 186-2 Random Number Generation • Dual EC DRBG Random Number Generation

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 7 – 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.
Seed and Seed Keys	Used to seed the DRBG for random number generation	Internally via NDRNG or externally	Temporarily in volatile RAM	Entry: Plaintext if generated externally Output: N/A	Automatically after use

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 8 – 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		AES-CTR-DRBG Random Number Generation	Use Seed and Seed Key to generate random number Destroy Seed and Seed Key after use
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.

Please refer to Table 1 for a list of environments for which operational testing of the module was performed.

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, OFB. 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
     - AES-CTR DRBG Known Answer Test
   - Software Integrity Test: HMAC-SHA-1
   - Critical Functions Tests: N/A

Conditional Tests:

- FIPS 186-2 RNG Continuous Test
- AES-CTR DRBG Continuous Test
- Dual EC DRBG Continuous Test
- NDRNG Continuous Test

The module can be configured to utilize all or only a subset of the Approved security functions listed in Section 3 above. Only the self-tests of the algorithms that are to be utilized will be run at power up. When reconfigured, the module will run all self-tests associated with the new configuration.

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. In the event of a self-test failure, the module will enter an error state and a specific error code will be returned indicating which self-test or conditional test has failed. The module will not provide any cryptographic services while in this state.
10. The module shall not support concurrent operators.
11. The module does not support key generation.
12. The module supports multiple approved modes of operation.
13. Upon re-configuration from one Approved mode of operation to another, the cryptographic module shall reinitialize and preform all power-up self-tests associated with the new Approved mode of operation.
14. DES, Blowfish, ARC2, ARC4, MD2, MD4, MD5, HMAC-MD5, AES EAX, AES XCBC, FIPS 186-2 RNG, and Dual EC DRBG 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