

# *Mocana Cryptographic Suite B Module*

*Software Version 5.4fm*

## *Security Policy*

*Document Version 1.0*

*Mocana Corporation*

August 4, 2011

**TABLE OF CONTENTS**

**1. MODULE OVERVIEW.....3**

**2. SECURITY LEVEL .....4**

**3. MODES OF OPERATION.....5**

    APPROVED MODE OF OPERATION .....5

    NON-FIPS APPROVED ALGORITHMS .....5

**4. PORTS AND INTERFACES.....6**

**5. IDENTIFICATION AND AUTHENTICATION POLICY .....6**

    ASSUMPTION OF ROLES.....6

**6. ACCESS CONTROL POLICY.....7**

    ROLES AND SERVICES.....7

    OTHER SERVICES.....8

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

    DEFINITION OF PUBLIC KEYS: .....10

    DEFINITION OF CSPs MODES OF ACCESS .....11

**7. OPERATIONAL ENVIRONMENT.....13**

**8. SECURITY RULES .....13**

**9. PHYSICAL SECURITY .....14**

**10. MITIGATION OF OTHER ATTACKS POLICY.....14**

**11. CRYPTOGRAPHIC OFFICER GUIDANCE.....14**

    KEY DESTRUCTION SERVICE .....14

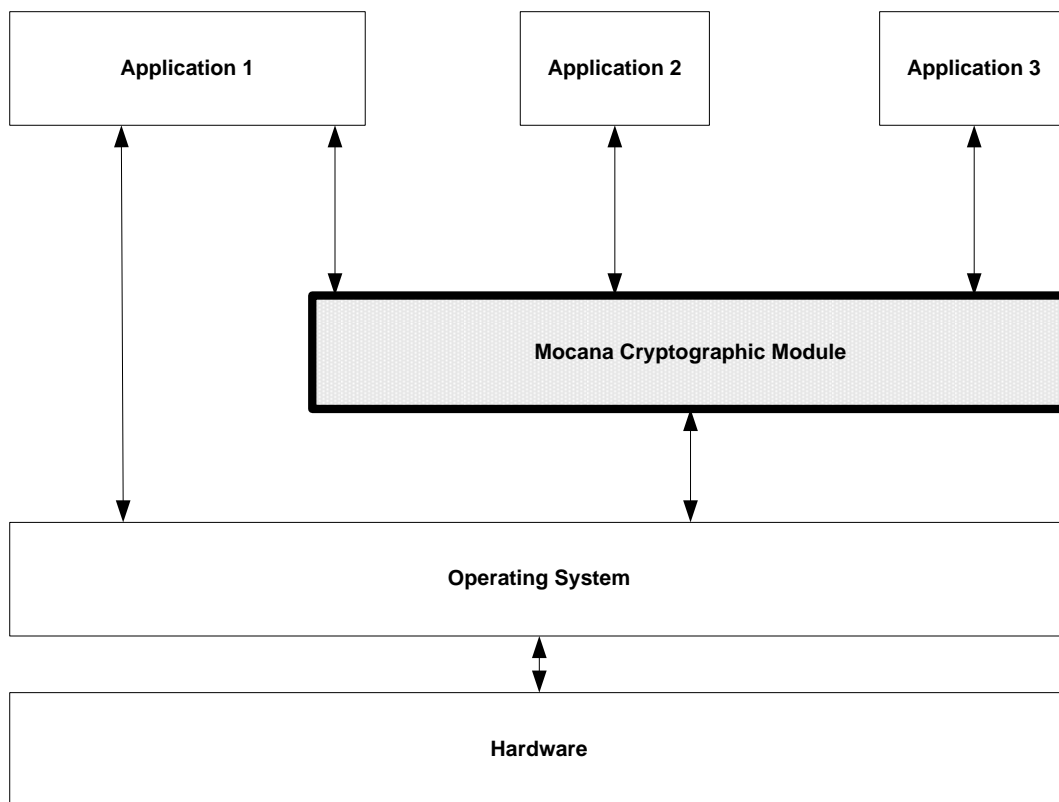
**12. DEFINITIONS AND ACRONYMS.....15**

# 1. Module Overview

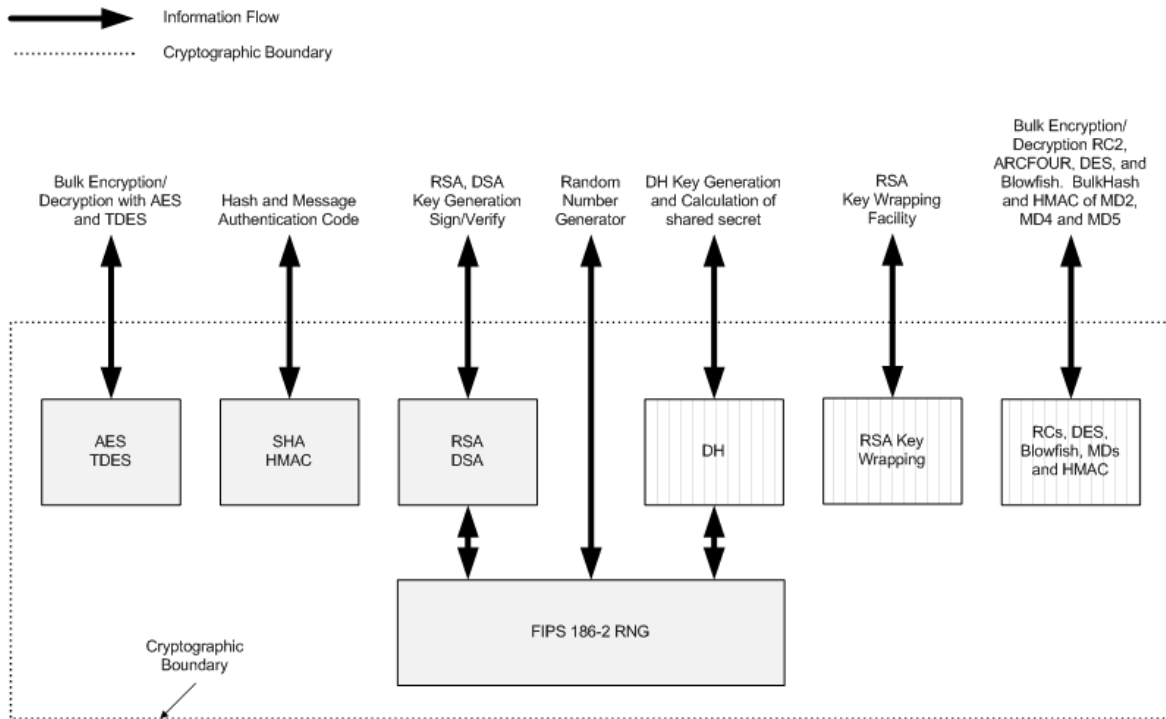
The Mocana Cryptographic Suite B Module (Software Version 5.4fm) is a software only, multi-chip standalone cryptographic module that runs on a general purpose computer. The primary purpose of this module is to provide FIPS Approved cryptographic routines to consuming applications via an Application Programming Interface. The physical boundary of the module is the case of the general purpose computer. The logical boundary of the cryptographic module is the single shared object (SO).

The cryptographic module runs on the following operating environments:

- Android 2.3 (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 a FIPS Approved mode of operation. By default, the module is running in the FIPS Approved mode of operation after installation. 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
- RSA key generation, signature generation and verification (Gen Key X9.31; PKCS #1 1.5, Sig Gen and Sig Ver: 1024, 1536, 2048, 3072, 4096; PSS Sig Gen and Sig Ver: 1024, 1536, 2048, 3072, 4096)
- DSA key generation, signature generation and verification (PQG Gen/Ver, Key Pair Gen, Sig Gen/Ver; 1024)
- FIPS 186-2 RNG

#### *Non-FIPS Approved Algorithms*

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

- Diffie-Hellman (for key agreement; provides 80 or 112 bits of encryption strength)
- RSA Key Wrapping (provides between 80 and 150 bits of encryption strength)

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
- RSA PKCS #1 v2.1 RSAES-OAEP encryption/decryption

## 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 Suite B 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**

| <b>Role</b>           | <b>Type of Authentication</b> | <b>Authentication Data</b> |
|-----------------------|-------------------------------|----------------------------|
| 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"> <li>• Self-tests</li> <li>• Show Status</li> </ul>   |
| Cryptographic-Officer | <ul style="list-style-type: none"> <li>• DH Key Generation</li> <li>• DH Key Exchange</li> <li>• RSA Key Generation</li> <li>• RSA Signature Generation</li> <li>• RSA Signature Verification</li> <li>• RSA Key Wrapping Encryption</li> <li>• RSA Key Wrapping Decryption</li> <li>• DSA Key Generation</li> <li>• DSA Signature Generation</li> <li>• DSA Signature Verification</li> <li>• AES Encryption</li> <li>• AES Decryption</li> <li>• AES Message Authentication Code</li> <li>• TDES Encryption</li> <li>• TDES Decryption</li> <li>• SHA-1</li> <li>• SHA-224/256</li> <li>• SHA-384/512</li> <li>• HMAC-SHA1 Message Authentication Code</li> <li>• HMAC-SHA224/256 Message Authentication Code</li> <li>• HMAC-SHA384/512 Message Authentication Code</li> <li>• FIPS 186-2 Random Number Generation</li> <li>• Key Destruction</li> </ul> |

### 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   |
|------------------------------|--|---|-----------------------------|---|---|
| DH Private Components        | Used to derive the secret session key during DH key agreement protocol | Internally using the FIPS 186-2 RNG   | Temporarily in volatile RAM | N/A   | An application program which uses the API may destroy the key. The Key Destruction service zeroizes this CSP. |
| DRNG Seed Key                | Used to seed the RNG for key generation                                | Externally  | Temporarily in volatile RAM | Entry: Plaintext<br>Output: N/A                               | Automatically after use   |
| DRNG Seed                    | Used to seed the RNG for key generation                                | Externally  | Temporarily in volatile RAM | Entry: Plaintext<br>Output: N/A                               | Automatically after use   |
| RSA Private Key              | Used to create RSA digital signatures                                  | May be generated internally using the FIPS 186-2 RNG or generated externally. | Temporarily in volatile RAM | Entry: Plaintext if generated externally<br>Output: Plaintext | An application program which uses the API may destroy the key. The Key Destruction service zeroizes this CSP. |
| RSA Key Wrapping Private Key | Used for RSA Key Wrapping decryption operation                         | May be generated internally using the FIPS 186-2 RNG or generated externally. | Temporarily in volatile RAM | Entry: Plaintext if generated externally<br>Output: Plaintext | An application program which uses the API may destroy the key. The Key Destruction service zeroizes this CSP. |
| DSA Private Key              | Used to create DSA digital signatures                                  | May be generated internally using the FIPS 186-2 RNG or generated externally  | Temporarily in volatile RAM | Entry: Plaintext if generated externally<br>Output: Plaintext | An application program which uses the API may destroy the key. The Key Destruction service zeroizes this CSP. |



| Key       | Description/Usage   | Generation  | Storage                     | Entry / Output                        | Destruction   |
|-----------|---|-------------|-----------------------------|---------------------------------------|---|
| TDES Key  | Used during TDES encryption and decryption                  | Externally. | Temporarily in volatile RAM | Entry:<br>Plaintext<br>Output:<br>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:<br>Plaintext<br>Output:<br>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:<br>Plaintext<br>Output:<br>N/A | An application program which uses the API may destroy the key. The Key Destruction service zeroizes this CSP. |

**Definition of Public Keys:**

The following are the public keys contained in the module:

**Table 5: Public Key Information**

| Key                          | Description/Usage  | Generation  | Storage                     | Entry/Output  |
|------------------------------|--|---|-----------------------------|---|
| DH Public Component          | Used to derive the secret session key during DH key agreement protocol | Internally using the FIPS 186-2 RNG   | Temporarily in volatile RAM | Entry: Receive Client Public Component during DH exchange.<br><br>Output: Transmit Host Public Component during DH exchange |
| RSA Public Keys              | Used to verify RSA signatures  | May be generated internally using the FIPS 186-2 RNG or generated externally. | Temporarily in volatile RAM | Input: Plaintext if generated externally<br>Output: Plaintext   |
| RSA Key Wrapping Public Keys | Used for RSA Key Wrapping encryption operation                         | May be generated internally using the FIPS 186-2 RNG or generated externally. | Temporarily in volatile RAM | Input: Plaintext if generated externally<br>Output: Plaintext   |
| DSA Public Keys              | Used to verify DSA signatures  | May be generated internally using the FIPS 186-2 RNG or generated externally  | Temporarily in volatile RAM | Input: Plaintext if generated externally<br>Output: Plaintext   |

**Definition of CSPs Modes of Access**

Table 6 defines the relationship between access to CSPs and the different module services.

**Table 6 – CSP Access Rights within Roles & Services**

| Role |      | Service                         | Cryptographic Keys and CSPs Access Operation                |
|------|------|---------------------------------|---|
| C.O. | User |                                 |   |
| X    |      | DH Key Generation               | Use DH Parameters<br>Generate DH Key pair                   |
| X    |      | DH Key Exchange                 | Use DH Private Component<br>Generate DH shared secret       |
| X    |      | RSA Key Generation              | Generate RSA Public/Private Key pair                        |
| X    |      | RSA Signature Generation        | Use RSA Private Key<br>Generate RSA Signature               |
| X    |      | RSA Signature Verification      | Use RSA Public Key<br>Verify RSA Signature                  |
| X    |      | RSA Key Wrapping Encryption     | Use RSA Public Key<br>Performs Key Wrapping Encryption      |
| X    |      | RSA Key Wrapping Decryption     | Use RSA Private Key<br>Performs Key Wrapping Decryption     |
| X    |      | DSA Key Generation              | Generate DSA Key Pair for Signature Generation/Verification |
| X    |      | DSA Signature Generation        | Use DSA Private Key<br>Generate DSA Signature               |
| X    |      | DSA Signature Verification      | Use DSA Public Key<br>Verify DSA Signature                  |
| 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              | Use HMAC-SHA-1 Key  |

| Role |      | Service                                      | Cryptographic Keys and CSPs Access Operation   |
|------|------|--|--|
| C.O. | User |  |  |
|      |      | Authentication Code                          | Generate HMAC-SHA-1 Output   |
| X    |      | HMAC-SHA-224/256 Message Authentication Code | Use HMAC-SHA-224/256 Key<br>Generate HMAC-SHA-224/256 Output                           |
| X    |      | HMAC-SHA-384/512 Message Authentication Code | Use HMAC-SHA-384/512 Key<br>Generate HMAC-SHA-384/512 Output                           |
| X    |      | FIPS 186-2 Random Number Generation          | Use Seed and Seed Key to generate random number<br>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 Suite B Module operates in a modifiable operational environment.

Operational testing of the module was performed on the following environments:

- Android 2.3 (single-user mode)

## 8. Security Rules

The Mocana Cryptographic Suite B 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 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
  - RSA Pairwise Consistency Test
  - RSA Encrypt/Decrypt Known Answer Test
  - DSA Pairwise Consistency Test
  - DH Pairwise Consistency Test
  - FIPS 186-2 RNG Known Answer Test
- Software Integrity Test: HMAC-SHA-1

- Critical Functions Tests: N/A

#### Conditional Tests:

- DSA Pairwise Consistency Test
  - RSA Pairwise Consistency Test
  - 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 key generation, 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. DES, Blowfish, ARC2, ARC4, MD2, MD4, MD5, HMAC-MD5, AES EAX, AES XCBC, and RSA PKCS #1 v2.1 RSAES-OAEP encryption/decryption are not allowed for use in the FIPS Approved mode of operation.

## 9. Physical Security

The FIPS 140-2 Area 5 Physical Security requirements are not applicable because the Mocana Cryptographic Suite B 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 system running the Mocana Cryptographic Suite B 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                |
| DH   | Diffie-Hellman                          |
| DSA  | Digital Signature Algorithm             |
| EMC  | Electromagnetic Compatibility           |
| EMI  | Electromagnetic Interference            |
| FIPS | Federal Information Processing Standard |
| HMAC | Keyed-Hash Message Authentication Code  |
| RAM  | Random Access Memory                    |
| RNG  | Random Number Generator                 |
| RSA  | Rivest, Shamir and Adleman Algorithm    |
| TDES | Triple-DES                              |
| SHA  | Secure Hash Algorithm                   |
| SO   | Shared Object                           |