Mocana Cryptographic Module

Software Version 3.06.1 and 3.06.1a

Security Policy

Document Version 1.05

Mocana Corporation

April 17, 2008

TABLE OF CONTENTS

1. Module Overview

The Mocana Cryptographic Module is a software only, multi-chip standalone cryptographic module that runs on a general purpose computer. The 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 module is the single cryptographic module dynamic link library (DLL) for Windows and the shared object (SO) for Linux.

The cryptographic module runs on the Microsoft Windows CE 4.2, Linux Kernel 2.6 and uClinux Kernel 2.4 operating systems.

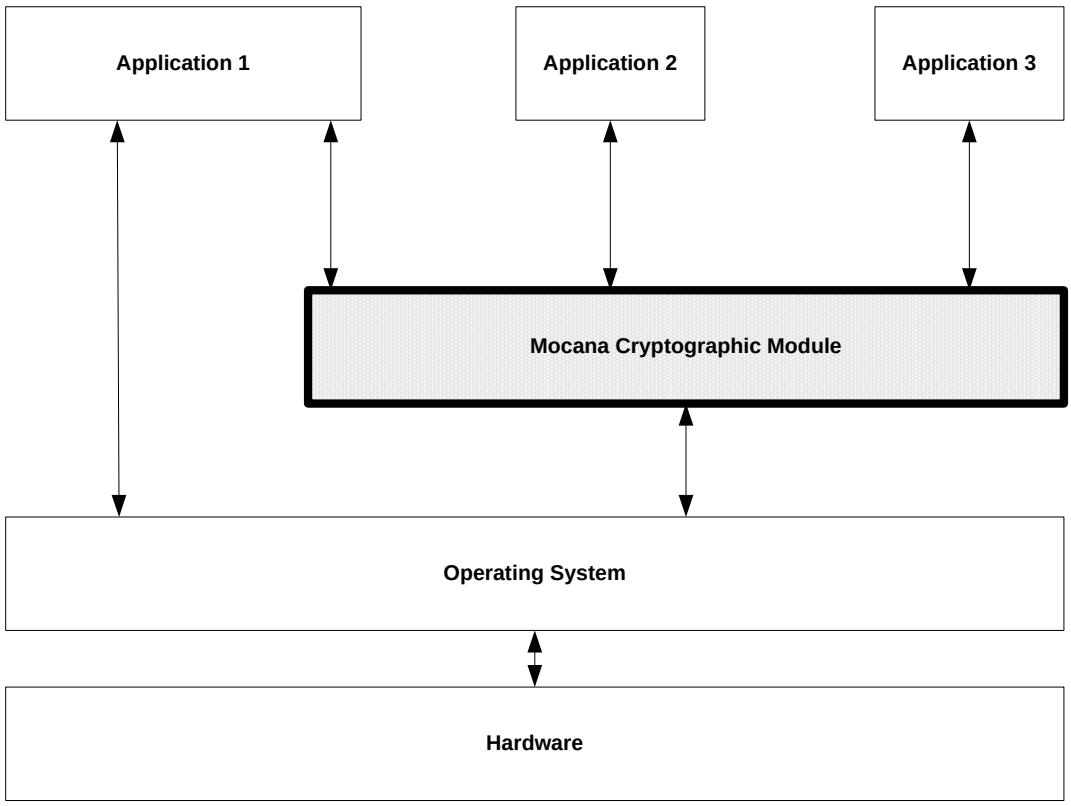

Figure 1 – Cryptographic Module Interface Diagram

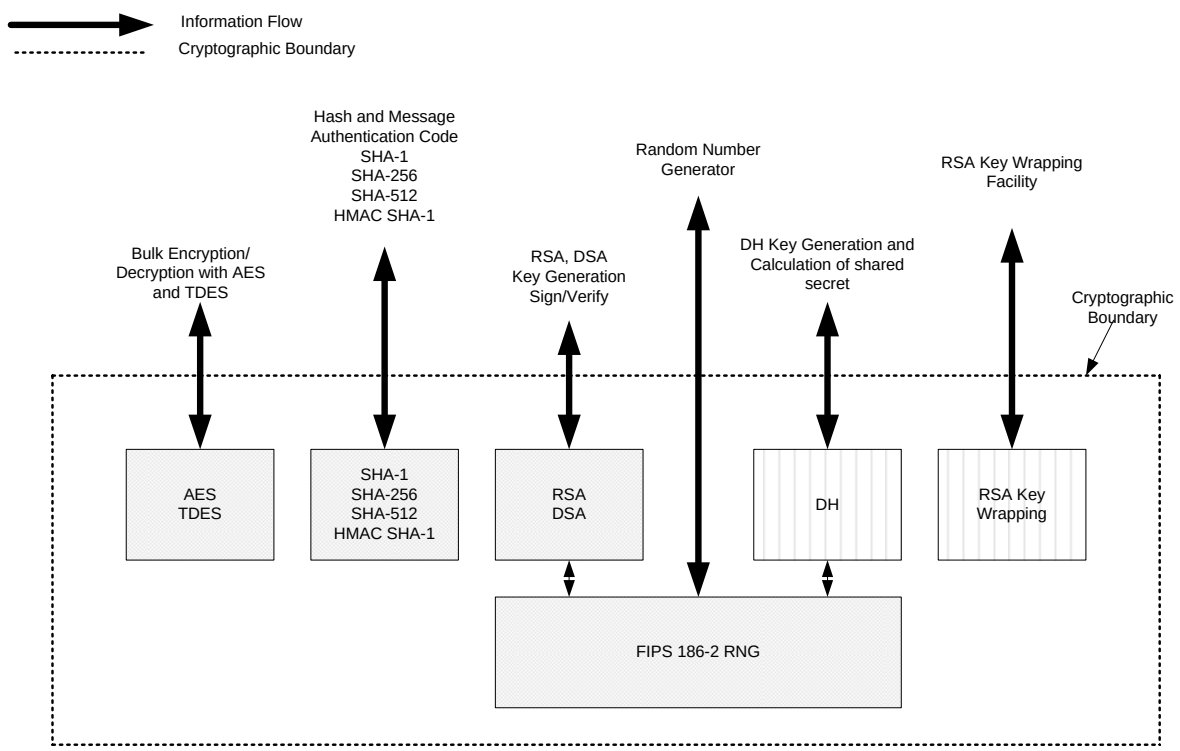

Figure 2 – Logical Cryptographic Boundary

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. In the FIPS Approved mode of operation, RSA key generation is not allowed. The following FIPS Approved algorithms are supported:

- AES (CBC mode; E/D; 128, 192 and 256)
- Triple-DES (3-key and 2-key; TCBC mode; E/D)
- HMAC-SHA-1
- SHA-1
- SHA-256
- SHA-512
- RSA signature generation and verification (PKCS #1 1.5, 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; 512, 576, 640, 704, 768, 832, 896, 960, 1024)
- FIPS 186-2 DRNG

Non-FIPS Approved Algorithms

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

- Diffie-Hellman for SSH v2 (for key agreement; provides 80 or 112 bits of encryption strength)
- RSA Key Wrapping (provides between 80 and 128 bits of encryption strength)

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

- RSA Key Generation (not algorithm tested)

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 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

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
N/A	N/A

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User	• Self-tests • Show Status
Cryptographic-Officer	• DH Key Generation • DH Key Exchange • RSA Signature Generation • RSA Signature Verification • RSA Key Wrapping Encryption • RSA Key Wrapping Decryption • DSA Key Generation • DSA Signature Generation • DSA Signature Verification • AES Encryption • AES Decryption • TDES Encryption • TDES Decryption • SHA-1 • SHA-256 • SHA-512 • HMAC-SHA1 Message Authentication Code • FIPS 186-2 Random Number Generation • Key Destruction • Self-tests • Show Status

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 contained in the module:

Table 5: 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 DRNG	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 DRNG for key generation	Externally	Temporarily in volatile RAM	Entry: Plaintext Output: N/A	Automatically after use
RSA Private Key	Used to create RSA digital signatures	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.

Key	Description/Usage	Generation	Storage	Entry / Output	Destruction
RSA Key Wrapping Private Key	Used for RSA Key Wrapping decryption operation	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.
DSA Private Key	Used to create DSA digital signatures	May be internally generated using the FIPS 186-2 DRNG or generated externally	Temporarily in volatile RAM	Entry: Plaintext if generated externally Output: Plaintext	An application program which uses the API may destroy the key. The Key Destruction service zeroizes this CSP.
TDES Key	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 Key	Used during AES 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.

Key	Description/Usage	Generation	Storage	Entry / Output	Destruction
HMAC Key	Used during HMAC-SHA-1 operation	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.

Definition of Public Keys:

The following are the public keys contained in the module:

Table 6: 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 DRNG	Temporarily in volatile RAM	Entry: Receive Client Public Component during DH exchange. Output: Transmit Host Public Component during DH exchange
RSA Public Keys	Used to verify RSA signatures	Externally	Temporarily in volatile RAM	Input: Plaintext Output: N/A
RSA Key Wrapping Public Keys	Used for RSA Key Wrapping encryption operation	Externally	Temporarily in volatile RAM	Input: Plaintext Output: N/A
DSA Public Keys	Used to verify DSA signatures	May be internally generated using the FIPS 186-2 DRNG or generated externally	Temporarily in volatile RAM	Input: Plaintext if generated externally Output: Plaintext

Definition of CSPs Modes of Access

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

Table 7 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	**User**		
X		DH Key Generation	Use DH Parameters Generate DH Key pair
X		DH Key Exchange	Use DH Private Component Generate DH shared secret
X		RSA Signature Generation	Use RSA Private Key Generate RSA Signature
X		RSA Signature Verification	Use RSA Public Key Verify RSA Signature
X		RSA Key Wrapping Encryption	Use RSA Public Key Performs Key Wrapping Encryption
X		RSA Key Wrapping Decryption	Use RSA Private Key Performs Key Wrapping Decryption
X		DSA Key Generation	Generate DSA Key Pair for Signature Generation/Verification
X		DSA Signature Generation	Use DSA Private Key Generate DSA Signature
X		DSA Signature Verification	Use DSA Public Key Verify DSA Signature
X		AES Encryption	Use AES Key
X		AES Decryption	Use AES Key
X		TDES Encryption	Use TDES Key

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

7. Operational Environment

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

- Windows CE 4.2 (single-user mode)
- Linux Kernel 2.6 (single-user mode)
- uClinux Kernel 2.4 (single-user mode)

8. Security Rules

The Mocana Cryptographic 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 Known Answer Test
   - Triple-DES Known Answer Test
   - HMAC-SHA-1 Known Answer Test
   - SHA-1 Known Answer Test
   - SHA-256 Known Answer Test
   - SHA-512 Known Answer Test
   - RSA Pairwise Consistency Test
   - RSA Key Wrapping Known Answer Test
   - DSA Pairwise Consistency Test
   - FIPS 186-2 DRNG Known Answer Test

   Software Integrity Test: HMAC-SHA-1

   Critical Functions Tests: N/A

   Conditional Tests:

   - DSA Pairwise Consistency Test
   - FIPS 186-2 DRNG 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. RSA key generation is not allowed 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 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

There are no installation or configuration instructions required for the Mocana Cryptographic Module. RSA key generation is not allowed in the FIPS Approved 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
DLL	Dynamic Link Library
DRNG	Deterministic Random Number Generator
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
SSH	Secure Shell