Mocana Cryptographic Suite B Hybrid Module

Software Version 5.5fi
Hardware Version: Freescale P2020 SEC 3.1

Security Policy

Document Version 1.3

Mocana Corporation

March 30, 2016

TABLE OF CONTENTS

1. Module Overview

The Mocana Cryptographic Suite B Hybrid Module (Hardware Version: Freescale P2020 SEC 3.1; Software Version 5.5fi) is a software hybrid, 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.

For the purposes of FIPS 140-2 the module is classified as a software-hybrid module. This module includes the following components:

- Single-chip hardware component, Freescale P2020 SEC3.1.
- Mocana cryptographic software component to drive the hardware component.

The hardware component consists of a single chip that is physically protected by a hard tamper-resistant epoxy layer. The physical boundary of the hardware component is the boundary of the epoxy layer. 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).

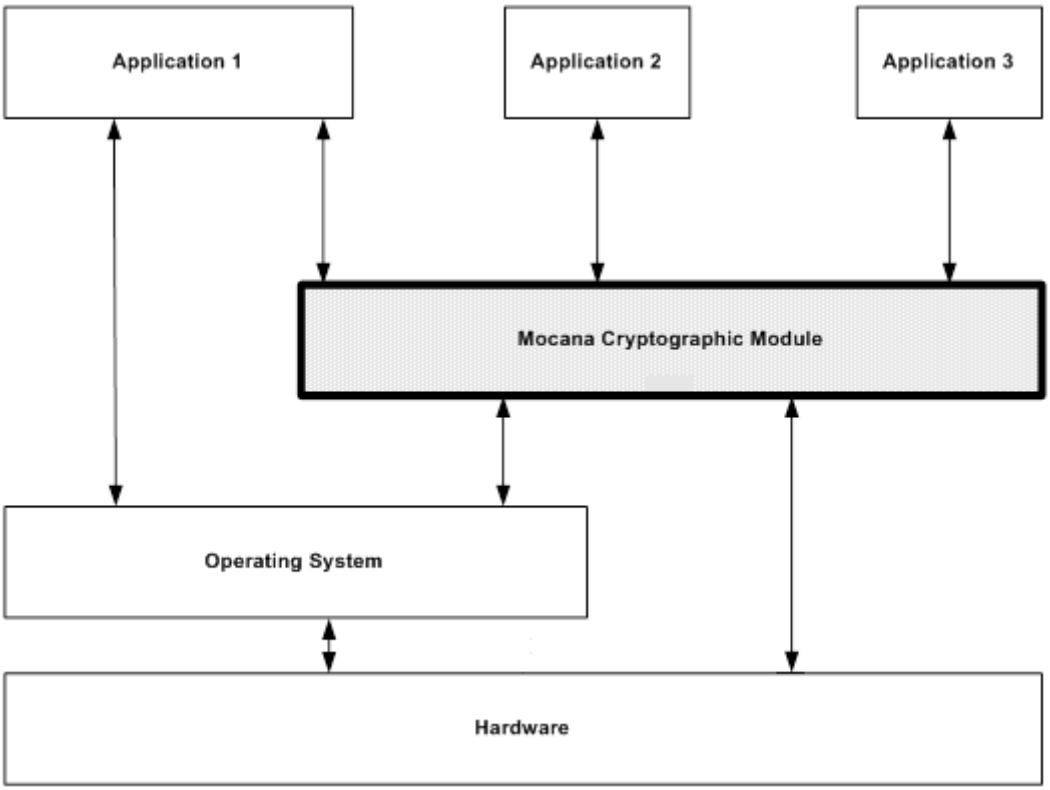
The cryptographic module runs on the following operating environments:

- VxWorks 6.8 running on a XPedite5500 with a Freescale P2020 SEC3.1 processor (Single-user mode)

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

- VxWorks version 6.x

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.



Cryptographic Boundary

The cryptographic boundary of the module includes the software binary (software component) as well as the P2020 chip (hardware component).

All module interfaces, inputs and outputs are provided by the software component.

Figure 1 – Cryptographic Module Interface Diagram

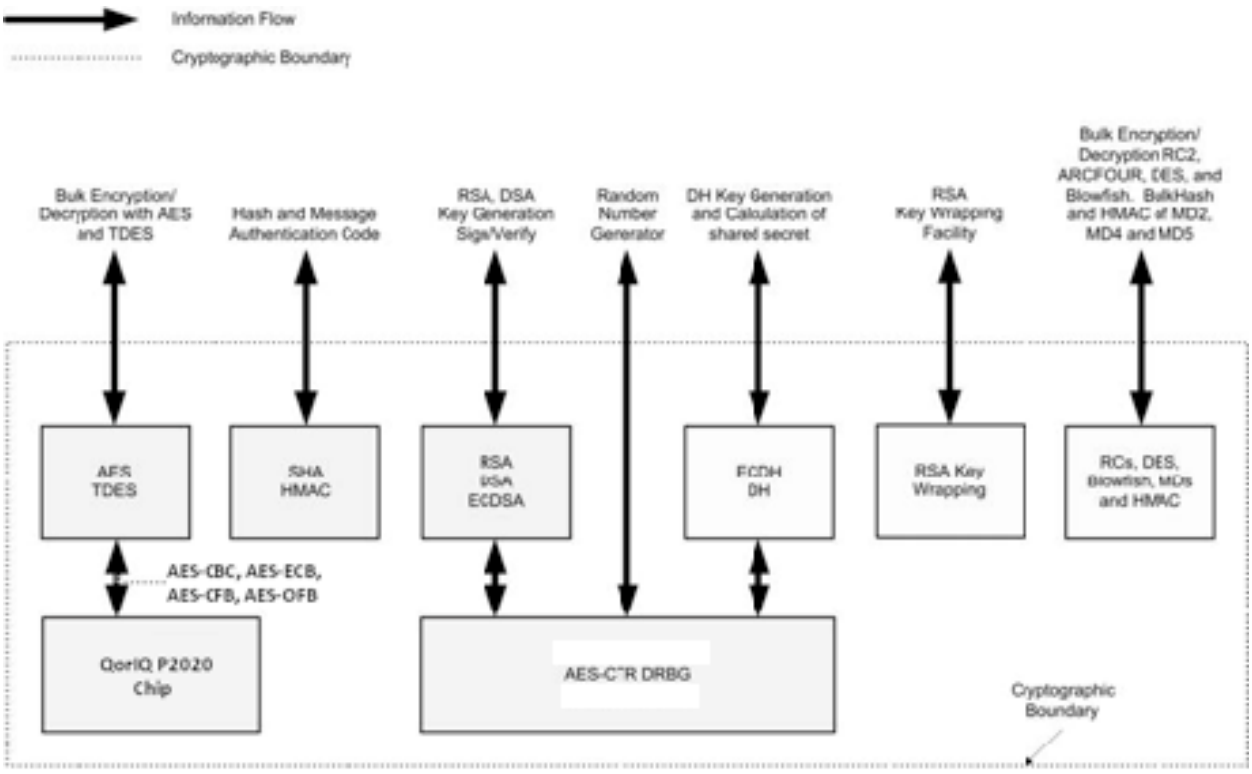


Figure 2 – Logical Cryptographic Boundary

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	1
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 an Approved and non-Approved mode of operation. The following FIPS Approved algorithms are available for use in the Approved mode:

Algorithms	Certificate #
AES (ECB, CBC, OFB, CFB, CTR and GCM modes; E/D; 128, 192 and 256)	Cert. #2291
AES (CCM, CMAC 128, 192 and 256)	Cert. #2290
AES XTS (128 and 256)	Cert. #2290
Triple-DES (3-key and 2-key[1]; TCBC mode; E/D)	Cert. #1440
HMAC-SHA-1; HMAC-SHA-224; HMAC-SHA-256; HMAC-SHA-384; HMAC-SHA-512	Cert. #1407
SHA-1 SHA-2: SHA-224; SHA-256; SHA-384; SHA-512	Cert. #1974

[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.

Algorithms	Certificate #
FIPS 186-2 RSA: - ANSI X9.31 key generation: 2048, 3072, and 4096-bit - PKCS #1 1.5 and PSS signature generation: 2048, 3072, and 4096-bit using SHA-2 - PKCS #1 1.5 and PSS signature verification: 1024, 1536, 2048, 3072, and 4096-bit using SHA-1 and SHA-2	Cert. #1179
FIPS 186-2 DSA: - PQG Ver: 1024-bit using SHA-1 - Sig Ver: 1024-bit using SHA-1	Cert. #717
FIPS 186-2 ECDSA: Key Gen: CURVES P; 224, 256, 384, 521 Sig Ver: CURVES P; 192, 224, 256, 384, 521 using SHA-1 PKV: CURVES P; 192, 224, 256, 384, 521 using SHA-1	Cert. #372
AES-CTR based DRBG	Cert. #284

During module initialization, a consuming application can configure the module to utilize all, or any subset of the above Approved algorithms. The module's FIPS_powerupSelfTest_Ex() function, which is called during module startup, takes a parameter that points to a configuration table data structure. This data structure contains an array of booleans indexed by an internal Algorithm-ID that will indicate to the module which FIPS algorithms should be initialized for use. The only configuration that was tested as part of the FIPS validation is the configuration which utilized ALL of the Approved algorithms. The CMVP makes no statement as to the correct operation of the module for all other configurations for which operational testing was not performed.

Non-FIPS Approved Algorithms

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

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength)
- EC Diffie Hellman (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength)
- NDRNG – Used to seed the Approved DRBG

Non-FIPS Approved mode:

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
- FIPS 186-2 RNG, Dual EC DRBG

The following algorithms are Disallowed as of January 1, 2014 per the NIST SP 800-131A algorithm transitions:

- FIPS 186-2 RSA (Certs. #1059 and #1437)
    - ANSI X9.31 key generation: 1024 and 1536-bit
    - PKCS #1 1.5 and PSS signature generation: 1024 and 1536-bit using SHA-1 and SHA-2; 2048, 3072 and 4096-bit using SHA-1
- FIPS 186-2 DSA using SHA-1 (Certs. #647 and 840)
    - PQG generation: 1024-bit
    - Key generation: 1024-bit
    - Signature generation: 1024-bit
- FIPS 186-2 ECDSA using SHA-1 (Certs. #298 and #479)
    - Signature generation: P-192, P-224 P-256, P-384, P521 curves
    - Key generation: P-192 curve
- Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength; non-compliant)
- RSA (key wrapping; key establishment methodology provides less than 112 bits of encryption strength; non-compliant)
- EC Diffie Hellman (key agreement; key establishment methodology provides less than 112 bits of encryption strength; non-compliant)

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 non-Approved security functions is utilized in lieu of an Approved one. 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 Suite B Hybrid 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 Use in the Approved modes of operation

Role	Authorized Services
User	• Self-tests • Show Status • Read Version
Cryptographic-Officer	• DH Key Generation • DH Key Exchange • ECDH Key Exchange • RSA Key Generation • RSA Signature Generation • RSA Signature Verification • RSA Key Wrapping Encryption • RSA Key Wrapping Decryption • DSA Key Generation • DSA Signature Generation • DSA Signature Verification • ECDSA Key Generation • ECDSA Signature Generation • ECDSA Signature Verification • AES Encryption (supported by hardware) • AES Decryption (supported by hardware) • AES Message Authentication Code • TDES Encryption • TDES Decryption • SHA-1 • SHA-224/256 • SHA-384/512 • HMAC-SHA1 Message Authentication Code • HMAC-SHA224/256 Message Authentication Code • HMAC-SHA384/512 Message Authentication Code • AES-CTR DRBG Random Number Generation • Seed PRNG • Key Destruction

Note: The module may be configured to support all or only a subset of the Approved security functions listed in Section 3 above. The services available in each Approved mode of operation depend on which algorithms were configured for use. Table 3 lists all of the module services. The following services will be available regardless of which Approved algorithms are configured for use:

- Self-tests
- Show Status
- Read Version
- Key Destruction

Other Services

Table 4 – 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 • AES EAX Decryption • AES XCBC Encryption • AES XCBC Decryption • RSA PKCS #1 v2.1 RSAES-OAEP Encryption • RSA PKCS #1 v2.1 RSAES-OAEP Decryption • Dual EC DRBG Random Number Generation • FIPS 186-2 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 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 AES-CTR DRBG	Temporarily in volatile RAM	N/A	An application program which uses the API may destroy the key. The Key Destruction service zeroizes this CSP.
ECDH Private Components	Used to derive the secret session key during ECDH key agreement protocol	Internally using the AES-CTR DRBG	Temporarily in volatile RAM	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 key generation	Internally via NDRNG or externally	Temporarily in volatile RAM	Entry: Plaintext if generated externally Output: N/A	Automatically after use
RSA Private Key	Used to create RSA digital signatures	May be generated internally using the AES-CTR DRBG 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.
RSA Key Wrapping Private Key	Used for RSA Key Wrapping decryption operation	May be generated internally using the AES-CTR DRBG 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.
DSA Private Key	Used to create DSA digital signatures	May be generated internally using the AES-CTR DRBG 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.

Key	Description/Usage	Generation	Storage	Entry / Output	Destruction
ECDSA Private Key	Used to create DSA digital signatures	May be generated internally using the AES-CTR DRBG 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 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: *No assurance of the minimum strength of externally provided entropy; the module generates cryptographic keys whose strengths are modified by available entropy; no assurance of the minimum strength of generated keys.*

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 AES-CTR DRBG	Temporarily in volatile RAM	Entry: Receive Client Public Component during DH exchange. Output: Transmit Host Public Component during DH exchange
ECDH Public Component	Used to derive the secret session key during ECDH key agreement protocol	Internally using the AES-CTR DRBG	Temporarily in volatile RAM	Entry: Receive Client Public Component during ECDH exchange. Output: Transmit Host Public Component during ECDH exchange
RSA Public Keys	Used to verify RSA signatures	May be generated internally using the AES-CTR DRBG or generated externally	Temporarily in volatile RAM	Input: Plaintext if generated externally t Output: Plaintext
RSA Key Wrapping Public Keys	Used for RSA Key Wrapping encryption operation	May be generated internally using the AES-CTR DRBG or generated externally	Temporarily in volatile RAM	Input: Plaintext if generated externally Output: Plaintext
DSA Public Keys	Used to verify DSA signatures	May be generated internally using the AES-CTR DRBG or generated externally	Temporarily in volatile RAM	Input: Plaintext if generated externally Output: Plaintext

Key	Description/Usage	Generation	Storage	Entry/Output
ECDSA Public Keys	Used to verify ECDSA signatures	May be generated internally using the AES-CTR DRBG or generated externally	Temporarily in volatile RAM	Input: Plaintext if generated externally Output: Plaintext

Note: *No assurance of the minimum strength of externally provided entropy; the module generates cryptographic keys whose strengths are modified by available entropy; no assurance of the minimum strength of generated keys.*

Definition of CSPs Modes of Access

Table 6 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		ECDH Key Exchange	Use ECDH Private Component Generate ECDH shared secret
X		RSA Key Generation	Generate RSA Public/Private Key pair
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		ECDSA Key Generation	Generate ECDSA Key Pair for Signature Generation/Verification
X		ECDSA Signature Generation	Use DSA Private Key Generate ECDSA Signature
X		ECDSA Signature Verification	Use ECDSA Public Key Verify ECDSA Signature
X		AES Encryption	Use AES Key
X		AES Decryption	Use AES Key
X		AES Message Authentication	Use AES Key

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	**User**		
		Code	
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 Key to generate random number Destroy Seed Key after use
X		Seed PRNG	Initialize RNG or DRBG with external Seed Key
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 Hybrid Module operates in a modifiable operational environment.

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

- VxWorks 6.8 running on a XPedite5500 with a Freescale P2020 SEC3.1 processor (Single-user mode)

8. Security Rules

The Mocana Cryptographic Suite B Hybrid 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, and CTR Known Answer Test
     - AES- CCM, CMAC, 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 Encrypt Known Answer Test
     - RSA Decrypt Known Answer Test
     - RSA Sign Known Answer Test
     - RSA Verify Known Answer Test
     - DSA Pairwise Consistency Test

  - ECDSA Pairwise Consistency Test
  - ECDH Pairwise Consistency Test
  - DH Pairwise Consistency Test
  - AES-CTR DRBG Known Answer Test
- Software Integrity Test: HMAC-SHA-1
- Critical Functions Tests: N/A

Conditional Tests:

- DSA Pairwise Consistency Test
- RSA Pairwise Consistency Test
- ECDSA Pairwise Consistency Test
- 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. The self-tests that are run at module power up depend on which Approved algorithms have been configured for use. The module's FIPS_powerupSelfTest_Ex() function, which is called during module startup, takes a parameter that points to a configuration table data structure. This data structure contains an array of booleans indexed by an internal Algorithm-ID that will indicate to the module which FIPS algorithms should be initialized for use. Only the self-tests of the algorithms that are to be utilized will be run at power up. Upon re-configuration, the module will reinitialize and perform all power-up self-tests associated with the new Approved mode of operation.

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. 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. DES, Blowfish, ARC2, ARC4, MD2, MD4, MD5, HMAC-MD5, AES EAX, AES XCBC, FIPS 186-2 RNG, Dual EC DRBG, and RSA PKCS #1 v2.1 RSAES-OAEP encryption/decryption 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 applicable to the Freescale P2020 SEC3.1 hardware component only. An image of the hardware component protected by hard epoxy is provided below:

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 Hybrid 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
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve 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