# FIPS 140-2 Non-Proprietary Security Policy

## Symantec Messaging Gateway Cryptographic Module

Software Version 1.0

Document Version 1.6

March 18, 2019

*Prepared For:*

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
www.symantec.com

*Prepared By:*

SafeLogic Inc.
530 Lytton Ave, Suite 200
Palo Alto, CA 94301
www.safelogic.com

# Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for Symantec Messaging Gateway Cryptographic Module.

# Table of Contents



  

# List of Tables



# List of Figures

# 1 Introduction

## 1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) run the FIPS 140-2 program. The NVLAP accredits independent testing labs to perform FIPS 140 testing; the CMVP validates modules meeting FIPS 140-2 validation. *Validated* is the term given to a module that is documented and tested against the FIPS 140-2 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

## 1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the Messaging Gateway Cryptographic Module from Symantec provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

Symantec Messaging Gateway Cryptographic Module may also be referred to as the "module" in this document.

## 1.3 External Resources

The Symantec website (www.symantec.com) contains information on Symantec services and products. The Cryptographic Module Validation Program website contains links to the FIPS 140-2 certificate and Symantec contact information.

## 1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

## 1.5 Acronyms

The following table defines acronyms found in this document:

| Acronym | Term |
|---|---|
| AES | Advanced Encryption Standard |
| ANSI | American National Standards Institute |
| API | Application Programming Interface |
| CMVP | Cryptographic Module Validation Program |
| CO | Crypto Officer |
| CSE | Communications Security Establishment |
| CSP | Critical Security Parameter |
| DES | Data Encryption Standard |
| DH | Diffie-Hellman |
| DRBG | Deterministic Random Bit Generator |
| DSA | Digital Signature Algorithm |
| EC | Elliptic Curve |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FCC | Federal Communications Commission |
| FIPS | Federal Information Processing Standard |
| GPC | General Purpose Computer |
| GUI | Graphical User Interface |
| HMAC | (Keyed-) Hash Message Authentication Code |
| KAT | Known Answer Test |
| MAC | Message Authentication Code |
| MD | Message Digest |
| NIST | National Institute of Standards and Technology |
| OS | Operating System |
| PKCS | Public-Key Cryptography Standards |
| PSS | Probabilistic Signature Scheme |
| RNG | Random Number Generator |
| RSA | Rivest, Shamir, and Adleman |
| SHA | Secure Hash Algorithm |
| SHS | Secure Hash Standard |
| SSL | Secure Sockets Layer |
| Triple-DES | Triple Data Encryption Algorithm |
| TLS | Transport Layer Security |
| USB | Universal Serial Bus |

**Table 1 – Acronyms and Terms**

# 2 Symantec Messaging Gateway Cryptographic Module

## 2.1 Cryptographic Module Specification

The Symantec Messaging Gateway Cryptographic Module provides cryptographic functions for the Messaging Gateway platforms software.

The module's logical cryptographic boundary is the shared library files and their integrity check HMAC files. The module is a multi-chip standalone embodiment installed on a General Purpose Device.

All operations of the module occur via calls from host applications and their respective internal daemons/processes. As such there are no untrusted services calling the services of the module.

### 2.1.1 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

| FIPS 140-2 Section Title | Validation Level |
|---|---|
| Cryptographic Module Specification | 1 |
| Cryptographic 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 |
| Electromagnetic Interference / Electromagnetic Compatibility | 1 |
| Self-Tests | 1 |
| Design Assurance | 1 |
| Mitigation of Other Attacks | N/A |

**Table 2 – Validation Level by FIPS 140-2 Section**

### 2.1.2 Approved Cryptographic Algorithms

The module's cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

| CAVP Cert. | Algorithm | Standard | Mode/ Method | Key Lengths, Curves or Moduli | Use |
|---|---|---|---|---|---|
| #4124 | AES | FIPS 197, SP 800-38A | ECB, CBC, CFB1, CFB8, OFB, CFB128, CTR | 128, 192, 256 | Data Encryption and Decryption |
| #4124 | AES | SP 800-38B | CMAC | 128, 192, 256 | Generation and Verification |
| #4124 | AES | SP 800-38C | CCM | 128, 192, 256 | Data Encryption and Decryption |
| #4124 | AES | SP 800-38D | GCM, GMAC | 128, 192, 256 | Data Encryption and Decryption |
| #931 | CVL Partial EC DH | SP 800-56A | ECC CDH KAS | All allowed curves | Shared Secret Computation |
| #1244 | DRBG | SP 800-90A | Hash_DRBG | - | Deterministic Random Bit Generation |
| #1244 | DRBG | SP 800-90A | HMAC_DRBG | - | Deterministic Random Bit Generation |
| #1244 | DRBG | SP 800-90A | CTR_DRBG | - | Deterministic Random Bit Generation |
| #1117 | DSA2 | FIPS 186-4 | PQG Gen, PQG Ver, Key Pair, Sig Gen, Sig Ver | 1024 (for PQG Ver only), 2048, 3072 | Digital Signature Generation and Verification |
| #939 | ECDSA2 | FIPS 186-4 | Key Pair Generation Test, Public Key Validation Test, Signature Generation Test, Signature Verification Test | All allowed curves | Digital Signature Generation and Verification |

| CAVP Cert. | Algorithm | Standard | Mode/ Method | Key Lengths, Curves or Moduli | Use |
|---|---|---|---|---|---|
| #2695 | HMAC | FIPS 198-1 | HMAC-SHA-1 | 112 | Message Authentication |
| #2695 | HMAC | FIPS 198-1 | HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-512 | 224, 256, 512 | Message Authentication |
| #2238 | RSA | FIPS 186-2 | RSASSA-PSS Signature Verification | 1024, 1536, 2048, 3072, 4096 | Legacy use Digital Signature Verification |
| #2238 | RSA | FIPS 186-4 | ANSI X9.31 Signature Verification, RSASSA-PKCS#1-v1.5 Signature Verification | 1024, 2048, and 3072 | Digital Signature Verification |
| #2238 | RSA2 | FIPS 186-4 | ANSI X9.31 Signature Generation, RSASSA-PKCS#1-v1.5 Signature Generation, RSASSA-PSS Signature Generation | 2048, 3072, 4096 | Digital Signature Generation and Verification |
| #3393 | SHS | FIPS 180-4 | SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | - | Message Digest |
| #2255 | Triple-DES | SP 800-67 | TECB, TCBC, TCFB1, TCFB8, TCFB64, TOFB | 3-Key | Data Encryption and Decryption |
| #2255 | Triple-DES | SP 800-38B | CMAC | 3-Key | Generation and Verification |

**Table 3 – FIPS-Approved Algorithm Certificates**

### 2.1.3 Non-Approved Cryptographic Algorithms

The module supports the following non-FIPS 140-2 approved but allowed algorithms:

| Algorithm | Caveat | Use |
|---|---|---|
| RSA Key Wrapping | Key wrapping; key establishment methodology provides between 112 and 256 bits of encryption strength | Key Establishment |
| EC Diffie-Hellman | Key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength | Key Establishment |
| NDRNG | Produces output that is dependent on unpredictable physical sources that are outside human control | Seed Material |

**Table 4 – Non-Approved Cryptographic Algorithms**

### 2.1.4 Non-Approved Mode of Operation

The module supports a non-approved mode of operation. The algorithms listed in this section are not to be used by the operator in the FIPS Approved mode of operation.

| Algorithm | Use |
|---|---|
| AES-XTS | Non-compliant |
| CVL | ECC CDH KAS – non-compliant less than 112 bits of encryption strength |
| DSA (FIPS 186-2) | Key Generation and Signature Generation with SHA-1 and 1024 bit keys |
| RNG (ANS X9.31) | Random Number Generation |
| RSA | Key Wrapping – non-compliant less than 112 bits of encryption strength |

**Table 5 – Algorithms in the Non-Approved Mode of Operation**

## 2.2 Module Interfaces

The figure below shows the module's physical and logical block diagram:

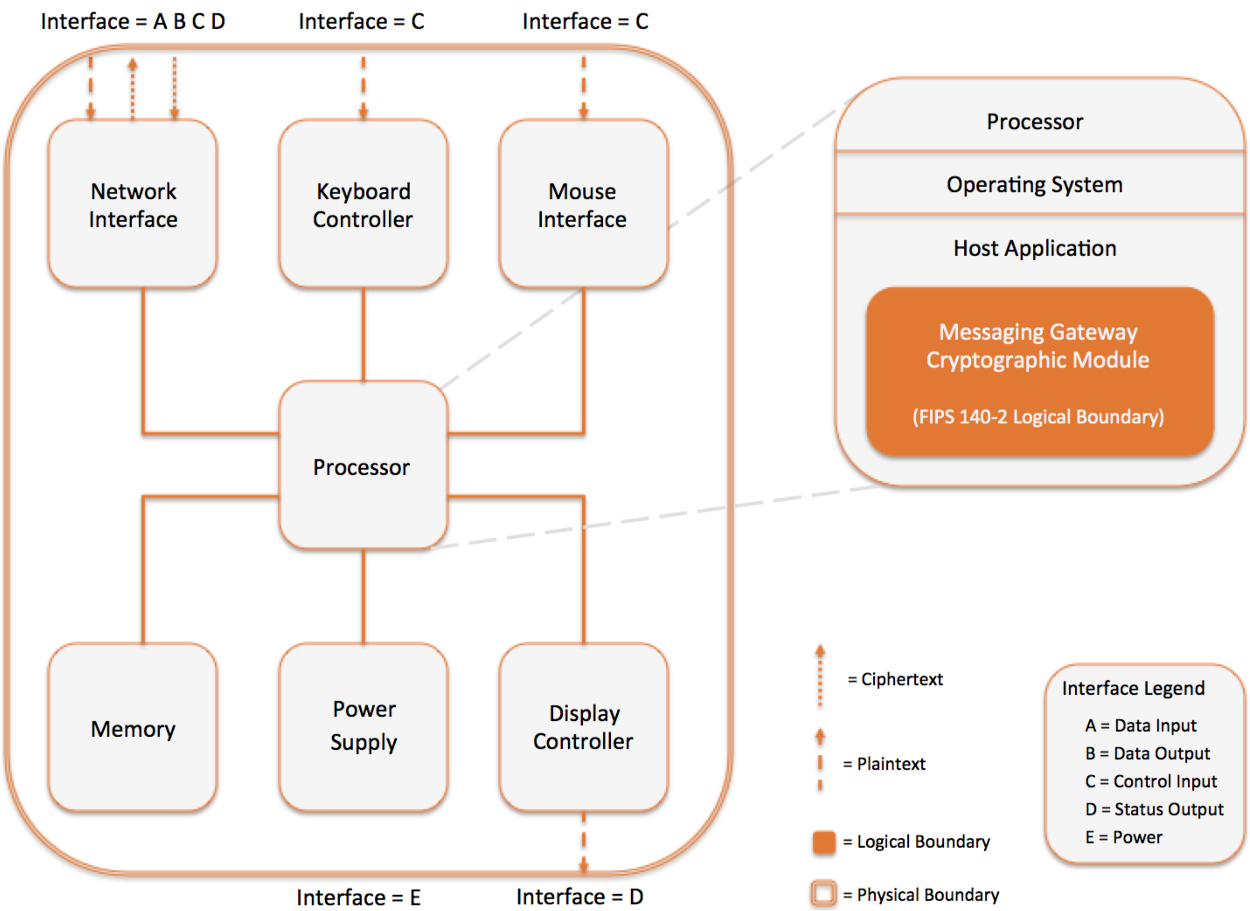


**Figure 1 – Module Boundary and Interfaces Diagram**

The interfaces (ports) for the physical boundary include the computer keyboard port, mouse port, network port, USB ports, display and power plug. When operational, the module does not transmit any information across these physical ports because it is a software cryptographic module. Therefore, the module's interfaces are purely logical and are provided through the Application Programming Interface (API) that a calling daemon can operate. The logical interfaces expose services that applications directly call, and the API provides functions that may be called by a referencing application (see Section 2.3 – Roles, Services, and Authentication for the list of available functions). The module distinguishes between logical interfaces by logically separating the information according to the defined API.

The API provided by the module is mapped onto the FIPS 140- 2 logical interfaces: data input, data output, control input, and status output. Each of the FIPS 140- 2 logical interfaces relates to the module's callable interface, as follows:

| FIPS 140-2 Interface | Logical Interface | Module Physical Interface |
|---|---|---|
| Data Input | Input parameters of API function calls | Network Interface |
| Data Output | Output parameters of API function calls | Network Interface |
| Control Input | API function calls | Keyboard Interface, Mouse Interface |
| Status Output | For FIPS mode, function calls returning status information and return codes provided by API function calls. | Display Controller |
| Power | None | Power Supply |

**Table 6 – Logical Interface / Physical Interface Mapping**

As shown in Figure 1 – Module Boundary and Interfaces Diagram and Table 7 – Module Services, Roles, and Descriptions, the output data path is provided by the data interfaces and is logically disconnected from processes performing key generation or zeroization. No key information will be output through the data output interface when the module zeroizes keys.

## 2.3 Roles, Services, and Authentication

The module supports a Crypto Officer and a User role. The module does not support a Maintenance role. The User and Crypto-Officer roles are implicitly assumed by the entity accessing services implemented by the Module.

### 2.3.1 Operator Services and Descriptions

The module supports services that are available to users in the various roles. All of the services are described in detail in the module's user documentation. The following table shows the services available to the various roles and the access to cryptographic keys and CSPs resulting from services:

| Service | Roles | CSP / Algorithm | Permission |
|---|---|---|---|
| Module initialization | Crypto Officer | None | No Access to Keys or CSPs |
| Symmetric encryption/decryption | User | AES Key, Triple-DES Key | User: read/write/execute |
| Digital signature[1]* | User | RSA Private Key, DSA Private Key, ECDSA Private Key | User: read/write/execute |
| Symmetric key generation | User | AES Key, Triple-DES Key | User: read/write/execute |

[1] Note that per SP800-131A, issuing 1024-bit signatures with SHA-1 is disallowed as of the end of 2013.
* Indicates non-Approved services if non-Approved key sizes are utilized (<112 bits)

| Service | Roles | CSP / Algorithm | Permission |
|---|---|---|---|
| Asymmetric key generation | User | RSA Private Key, DSA Private Key, ECDSA Private Key, EC DH Private Components | User: read/write/execute |
| Keyed Hash (HMAC)* | User | HMAC Key<br>HMAC SHA-1, HMAC SHA- 224, HMAC SHA-256, HMAC SHA-512 | User: read/write/execute |
| Message digest (SHS) | User | SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | User: read/write/execute |
| Random number generation | User | DRBG Seed and Seed Key | User: read/write/execute |
| Show status | Crypto Officer<br>User | None | No Access to Keys or CSPs |
| Self test | User | All CSPs | User: read/execute |
| Zeroize | Crypto Officer<br>User | All CSPs | User and CO: delete |

**Table 7 – Module Services, Roles, and Descriptions**

### 2.3.2 Operator Authentication

As required by FIPS 140-2, there are two roles (a Crypto Officer role and User role) in the module that operators may assume. As allowed by Level 1, the module does not support authentication to access services. As such, there are no applicable authentication policies. Access control policies are implicitly defined by the services available to the roles as specified in Table 7 – Module Services, Roles, and Descriptions.

## 2.4 Physical Security

This section of requirements does not apply to this module. The module is a software-only module and does not implement any physical security mechanisms.

## 2.5 Operational Environment

The module operates on a general purpose computer (GPC) running a general purpose operating system (GPOS). For FIPS purposes, the module is running on this operating system in single user mode and does not require any additional configuration to meet the FIPS requirements.

The module was tested on the following platforms:

- CentOS 6 running on a Dell PowerEdge R430 with Intel Xeon E5-2600

The cryptographic module is also supported on the following operating systems for which operational testing and algorithm testing was not performed. The cryptographic module is "vendor affirmed" by Symantec to operate properly for Symantec products using these operating systems; no claim can be made as to the correct operation of the module or the security strengths of the generated keys:

- CentOS 7

Compliance is maintained for other versions of the respective operating system family where the binary is unchanged. No claim can be made as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate.

The GPC(s) used during testing met Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B. FIPS 140-2 validation compliance is maintained when the module is operated on other versions of the GPOS running in single user mode, assuming that the requirements outlined in NIST IG G.5 are met.

## 2.6 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

| Keys and CSPs | Storage Locations | Storage Method | Input Method | Output Method | Zeroization | Access |
|---|---|---|---|---|---|---|
| AES Key | RAM | Plaintext | API call parameter | None | power cycle<br>cleanse() | CO: D<br>U: RWD |
| Triple-DES Key | RAM | Plaintext | API call parameter | None | power cycle<br>cleanse() | CO: D<br>U: RWD |
| RSA Public Key | RAM | Plaintext | API call parameter | None | power cycle<br>cleanse() | CO: D<br>U: RWD |
| RSA Private Key | RAM | Plaintext | API call parameter | None | power cycle<br>cleanse() | CO: D<br>U: RWD |
| DSA Public Key | RAM | Plaintext | API call parameter | None | power cycle<br>cleanse() | CO: D<br>U: RWD |
| DSA Private Key | RAM | Plaintext | API call parameter | None | power cycle<br>cleanse() | CO: D<br>U: RWD |
| HMAC Key | RAM | Plaintext | API call parameter | None | power cycle<br>cleanse() | CO: D<br>U: RWD |
| Integrity Key | Module Binary | Plaintext | None | None | None | CO: D<br>U: RWD |
| EC DSA Private Key | RAM | Plaintext | None | None | power cycle<br>cleanse() | CO: D<br>U: RWD |
| EC DSA Public Key | RAM | Plaintext | None | None | power cycle<br>cleanse() | CO: D<br>U: RWD |

| Keys and CSPs | Storage Locations | Storage Method | Input Method | Output Method | Zeroization | Access |
|---|---|---|---|---|---|---|
| EC DH Public Components | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |
| EC DH Private Components | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |
| CTR_DRBG V Value | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |
| CTR_DRBG Key | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |
| CTR_DRBG Entropy | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |
| Hash_DRBG V Value | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |
| Hash_DRBG C Value | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |
| Hash_DRBG Entropy | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |
| HMAC_DRBG Entropy | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |
| HMAC_DRBG V Value (Seed Length) | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |
| HMAC_DRBG Key | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |
| HMAC_DRBG init_seed | RAM | Plaintext | None | None | power cycle cleanse() | CO: D<br>U: RWD |

R = Read W = Write D = Delete

**Table 8 – Module Keys/CSPs**

The application that uses the module is responsible for appropriate destruction and zeroization of the key material. The module provides functions for key allocation and destruction which overwrite the memory that is occupied by the key information with zeros before it is deallocated.

### 2.6.1 Random Number Generation

The module uses SP800-90A DRBGs for creation of asymmetric and symmetric keys.

The module accepts input from entropy sources external to the logical cryptographic boundary, but located within the operational environment inside the module's physical boundary for use as seed material for the module's Approved DRBGs. The calling application of the module shall use entropy sources that meet the security strength required for the random bit generation mechanism as shown in NIST Special Publication 800-90A Table 2 (Hash_DRBG, HMAC_DRBG) and Table 3 (CTR_DRBG).

The module performs continual tests on the random numbers it uses to ensure that the seed and seed key input to the Approved DRBGs do not have the same value. The module also performs continual tests on the output of the Approved DRBGs to ensure that consecutive random numbers do not repeat.

### 2.6.2 Key/Critical Security Parameter (CSP) Authorized Access and Use by Role and Service/Function

An authorized application as user (the User role) has access to all key data generated during the operation of the module.

### 2.6.3 Key/CSP Storage

Public and private keys are provided to the module by the calling process and are destroyed when released by the appropriate API function calls or during power cycle. The module does not perform persistent storage of keys.

### 2.6.4 Key/CSP Zeroization

The application is responsible for calling the appropriate destruction functions from the API. The destruction functions then overwrite the memory occupied by keys with zeros and deallocates the memory. This occurs during process termination / power cycle. Keys are immediately zeroized upon deallocation, which sufficiently protects the CSPs from compromise.

## 2.7 Self-Tests

FIPS 140-2 requires that the module perform self-tests to ensure the integrity of the module and the correctness of the cryptographic functionality at start up. In addition some functions require continuous verification of function, such as the random number generator. All of these tests are listed and described in this section.  In the event of a self-test error, the module will log the error and will halt. The module must be initialized into memory to resume function.

The following sections discuss the module's self-tests in more detail.

### 2.7.1 Power-On Self-Tests

Power-on self-tests are executed automatically when the module is loaded into memory. The module verifies the integrity of the runtime executable using a HMAC-SHA256 digest computed at build time. If the fingerprints match, the power-up self-tests are then performed. If the power-up self-test is successful, a flag is set to place the module in FIPS mode.

| Type | Detail |
|---|---|
| Software Integrity Check | • HMAC-SHA256 on all module components |
| Known Answer Tests[2] | • AES separate encrypt and decrypt<br>• AES GCM separate encrypt and decrypt<br>• AES CCM separate encrypt and decrypt<br>• AES CMAC sign and verify<br>• Triple-DES CMAC sign and verify<br>• ECDH<br>• HMAC-SHA1<br>• HMAC-SHA224<br>• HMAC-SHA256<br>• HMAC-SHA512<br>• RSA sign and verify<br>• SHA-1<br>• SHA-224<br>• SHA-256<br>• SHA-384<br>• SHA-512<br>• SP 800-90A DRBG (Hash_DRBG, HMAC_DRBG, CTR_DRBG)<br>• Triple-DES separate encrypt and decrypt (3-key)<br>• ECC CDH |
| Pair-wise Consistency Tests | • DSA<br>• RSA<br>• ECDSA |

**Table 9 – Power-On Self-Tests**

Input, output, and cryptographic functions cannot be performed while the Module is in a self-test or error state because the module is single-threaded and will not return to the calling application until the power-up self-tests are complete. If the power-up self-tests fail, subsequent calls to the module will also fail - thus no further cryptographic operations are possible.

[2] Note that all SHA-X KATs are tested as part of the respective HMAC SHA-X KAT. SHA-1 is also tested independently.

### 2.7.2 Conditional Self-Tests

The module implements the following conditional self-tests upon key generation, or random number generation (respectively):

| TYPE | DETAIL |
|---|---|
| Pair-wise Consistency Tests | • DSA<br>• RSA<br>• ECDSA |
| Continuous RNG Tests | • Performed on all Approved DRBGs and the non-approved X9.31 RNG |
| DRBG Health Tests | • Health testing per SP 800-90A Section 11 |

**Table 10 – Conditional Self-Tests**

### 2.7.3 Cryptographic Function

The module verifies the integrity of the runtime executable using a HMAC-SHA256 digest which is computed at build time. If this computed HMAC-SHA256 digest matches the stored, known digest, then the power-up self-test (consisting of the algorithm-specific Pairwise Consistency and Known Answer tests) is performed. If any component of the power-up self-test fails, an internal global error flag is set to prevent subsequent invocation of any cryptographic function calls. Any such power-up self-test failure results in a transition to the error state that can only be recovered by reloading the module[3]. The power-up self-tests may be performed at any time by reloading the module.

No operator intervention is required during the running of the self-tests.

## 2.8 Mitigation of Other Attacks

The Module does not contain additional security mechanisms beyond the requirements for FIPS 140-2 Level 1 cryptographic modules.

[3] The initialization function could be re-invoked but such re-invocation does not provide a means from recovering from an integrity test or known answer test failure

# 3 Guidance and Secure Operation

## 3.1 Crypto Officer Guidance

### 3.1.1 Software Installation

The module is provided directly to solution developers and is not available for direct download to the general public. The module and its host application are to be installed on an operating system specified in Section 2.5 or one where portability is maintained.

To enter the Approved Mode of Operation, the Crypto Officer must invoke the command "fipsmode on", upon which the module will initiate a restart, effectively zeroizing keys and CSPs currently stored in memory that were intended for use in the Non-Approved Mode of Operation. While in the Approved Mode of Operation, the Crypto Officer can revert to the Non-Approved Mode of Operation by invoking the command "fipsmode off", upon which the module will initiate a restart (zeroizing keys and CSPs that were intended for use in the Approved Mode).

### 3.1.2 Additional Rules of Operation

1. The writable memory areas of the module (data and stack segments) are accessible only by the application so that the operating system is in "single user" mode, i.e. only the application has access to that instance of the module.

2. The operating system is responsible for multitasking operations so that other processes cannot access the address space of the process containing the module.

## 3.2 User Guidance

### 3.2.1 General Guidance

The module is not distributed as a standalone library and is only used in conjunction with the solution.

The end user of the operating system is also responsible for zeroizing CSPs via wipe/secure delete procedures.

If the module power is lost and restored, the calling application shall reset the IV to the last value used.