# Symantec SymSSLf Cryptographic Module FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.0
November 22nd, 2017
Symantec Corporation

Symantec™
Confidence in a connected world.

## Table of Contents

# 1. Introduction

## 1.1 Purpose

This is the non-proprietary Cryptographic Module Security Policy for the Symantec SymSSLf Cryptographic Module (Software Version: 1.0.1) from Symantec Corporation. This security policy documents how the SymSSLf Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2.
More information about the FIPS 140-2 standard and the Cryptographic Module Validation Program (CMVP) is available online from the National Institute of Standards and Technology (NIST) website. Please visit http://csrc.nist.gov/groups/STM/cmvp/.

## 1.2 Scope

The scope of this document is limited to cover only the capabilities and operations of the Symantec SymSSLf Cryptographic Module as it relates to the technical requirements of the FIPS 140-2 cryptographic module security policy.
Additional information on the Symantec product line and contact information for sales and technical support can be found online at the Symantec website. Please visit https://www.symantec.com/.

# 2. Module Overview

The Symantec SymSSLf Cryptographic Module (Software Version: 1.0.1) is a software-only cryptographic module designed to provide low-level cryptographic algorithm support to Symantec products. Symantec products will commonly use the module as a basis for implementation of higher level secure networking protocols like Transport Layer Security (TLS). The Symantec SymSSLf Cryptographic Module may also be hereafter referred to as the cryptographic module or the Module.

The cryptographic module was tested on the following general-purpose operating environments:

| Operational Environment | Processor | Optimizations |
|---|---|---|
| Windows 7 SP1 | Intel Xeon E5620 | AES-NI |
| Windows 7 SP1 | Intel Xeon E5620 | None |

*Table 1. Tested Configurations*

Figure 1 below illustrates the Module's cryptographic boundary:

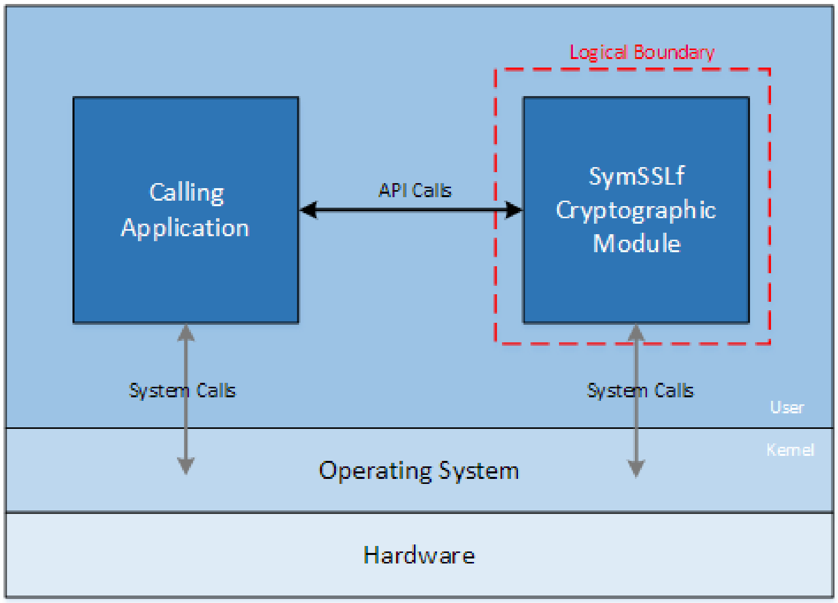

*Figure 1. Specification of Cryptographic Boundary*

# 3. Security Level

The cryptographic module meets the overall requirements of Level 1 security as per FIPS 140-2.

| **Security Requirements** | **Security 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 |

*Table 2. Security Levels of FIPS 140-2*

# 4. Modes of Operation

The cryptographic module supports a FIPS Approved mode of operation and a non-Approved mode of operation.

## 4.1 FIPS Approved Mode of Operation

The cryptographic module supports the following Approved algorithms in FIPS Approved mode:

| CAVP Cert. | Algorithm | Standard | Mode/Method | Key Lengths, Curves or Moduli | Use |
|---|---|---|---|---|---|
| #4515, #4516 | AES | FIPS 197, SP 800-38A | ECB, CBC, CFB1, CFB8, CFB128, OFB, CTR | 128, 192, 256 | Data Encryption / Decryption |
| | AES | FIPS 197, SP 800-38B | CMAC | 128, 192, 256 | Key Generation / Verification |
| | AES | FIPS 197, SP 800-38C | CCM | 128, 192, 256 | Generation-Encryption, Decryption-Verification |
| | AES | FIPS 197, SP 800-38D[1] | GCM | 128, 192, 256 | Authentication Encryption / Decryption |
| #1198, #1199 | CVL | SP 800-56A rev.1 | ECC CDH Primitive | P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 | Shared Secret Computation |
| #1476, #1477 | DRBG | SP 800-90A rev. 1 | Hash_Based DRBG, HMAC_Based DRBG, CTR_DRBG[2] | | Deterministic Random Bit Generation |

[1] This module meets the requirements of IG A.5 “Key/IV Pair Uniqueness Requirements from SP 800-38D” Scenario 3. The IV is constructed in its entirety internally deterministically as per SP 800-38D section 8.2.1.

[2] The CTR-DRBG implementation supports the Derivation Function by default in the FIPS Approved mode of operation. CTR_DRBG “without Derivation Function” is latent-functionality.

| CAVP Cert. | Algorithm | Standard | Mode/Method | Key Lengths, Curves or Moduli | Use |
|---|---|---|---|---|---|
| #1202, #1203 | DSA | FIPS 186-4 | PQG(gen), PQG(ver), KeyPairGen, SIG(gen), SIG(ver) | 1024[3], 2048, 3072 | Digital Signature Generation and Verification |
| #1098, #1099 | ECDSA | FIPS 186-4 | PKG, PKV, SigGen, SigVer | P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 | Digital Signature Generation and Verification |
| #2982, #2983 | HMAC | FIPS 198-1 | HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 | 112, 128, 192, 256, 320, 384 | Message Authentication |
| #2460, #2461 | RSA | FIPS 186-4 | RSASSA-PKCS1_V1_5 (SigGen and SigVer)<br>RSASSA-PSS (SigGen and SigVer) | 2048, 3072 | Digital Signature Generation / Verification |
| #3703, #3704 | SHS | FIPS 180-4 | SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | | Message Digest |
| #2410, #2411 | Triple-DES | SP 800-67 | TECB, TCBC, TCFB1, TCFB8, TCFB64, TOFB | 192 | Data Encryption / Decryption |
| | Triple-DES | SP 800-67, SP 800-38B | Triple-DES CMAC | 192 | Key Generation / Verification |

*Table 3. FIPS Approved Algorithm Certificates*

Operators should reference the transition tables that will be available at the CMVP Web site (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf). The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

[3] DSA 1024-bit key size is only supported for PQG(ver) and SIG(ver).

The cryptographic module supports the following non-Approved but Allowed algorithms in FIPS Approved mode:

| Algorithm | Caveat |
|---|---|
| Elliptic Curve Diffie-Hellman | key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength |
| RSA Key Wrapping | key wrapping; key establishment methodology provides 112 bits of encryption strength |

*Table 4. Non-Approved Algorithms Allowed in FIPS Approved Mode*

## 4.2 Non-Approved Mode of Operation

The following table lists services implemented by the cryptographic module that shall not be used when operating in the FIPS Approved mode of operation. If any of these services are used, the cryptographic module is no longer considered to be in the FIPS Approved mode of operation. In the event that the Crypto Officer or User violates or attempts to violate such restrictions, the cryptographic module is in strict violation of this Security Policy and is deemed fully non-compliant and unfit for service to protect sensitive unclassified data with cryptography. Both the Crypto Officer Role and the User Role have access to the non-Approved services listed in table below.

| **Function** | **Algorithm** | **Options** |
|---|---|---|
| Random Number Generation; Symmetric key generation | ANSI X9.31 RNG | AES 128, 192 and 256-bit |
| | [SP800-90A] DRBG (non-compliant) | Dual EC DRBG |
| Digital Signature and Asymmetric Key Generation | [FIPS 186-2] RSA (non-compliant) | GenKey9.31, SigGen9.31, SigGenPKCS1.5, SigGenPSS (1024/1536 with all SHA sizes, 2048/3072/4096 with SHA1) |
| | [FIPS 186-2] DSA (non-compliant) | PQG Gen, Key Pair Gen, Sig Gen (1024 with all SHA sizes, 2048/3072 with SHA1) |
| | [FIPS 186-4] DSA (non-compliant) | PQG Gen, Key Pair Gen, Sig Gen (1024 with all SHA sizes, 2048/3072 with SHA1) |
| | [FIPS 186-2] ECDSA (non-compliant) | PKG: CURVES (P-192 K-163 B-163)<br>SIG(gen): CURVES (P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 B-571) |
| | [FIPS 186-4] ECDSA (non-compliant) | PKG: CURVES (P-192 K-163 B-163)<br>SigGen: CURVES (P-192:(SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384:(SHA-1) P-521:(SHA-1) K-163:(SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163:(SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283:(SHA-1) B-409:(SHA-1) B-571:(SHA-1)) |
| ECC CDH (KAS) | [SP800-56A] (§5.7.1.2) (non-compliant) | All NIST Recommended B, K and P curves sizes 163 and 192 |
| Key Wrapping | [SP800-56B] RSA Key Wrapping (non-compliant) | RSA 1024, 1536, and 3072 |

*Table 5. Non-Approved Algorithms Disallowed in FIPS Approved Mode*

## 5. Physical Ports and Logical Interfaces

The physical ports of the cryptographic module are the same as the computer system on which the cryptographic module runs. The logical interface of the cryptographic module is via the application program interface (API).

| Logical Interface | Description |
|---|---|
| Data Input | Parameters passed to the module through API calls. |
| Control Input | API function calls. |
| Power Input | Not Applicable |
| Data Output | Data returned by the module through API calls. |
| Status Output | Error and status codes returned by API calls. |

*Table 6. Specification of Cryptographic Module Logical Interfaces*

The cryptographic module does not support a cryptographic bypass mode.

All Data Output is inhibited when the module is performing self-tests, zeroization, or in an error state.

The following is the mapping of the physical ports/interfaces to the logical ports/interfaces available to the module:

| Physical Ports / Interfaces | Description | Logical Ports / Interfaces |
|---|---|---|
| Power supply unit | Provides power to the cryptographic module | Power Input |
| Video connector | Connects a monitor to the general purpose computing platform | Data Output, Status Output |
| Serial connector | Connects peripheral general purpose I/O devices such as mouse, keyboard, and monitor | Data Input, Data Output, Control Input, Status Output |
| USB connectors | Connects peripheral general purpose I/O devices such as mouse, keyboard, and monitor | Data Input, Data Output, Control Input, Status Output |
| Ethernet connectors | Provides network connectivity | Data Input, Data Output, Control Input, Status Output |

*Table 7. Mapping of physical ports/interfaces to the logical ports/interfaces*

# 6. Identification and Authentication Policy

The role of the operator of the cryptographic module is identified implicitly from the API function. The cryptographic module is designed to meet the requirements specified for a Level 1 software-only cryptographic module as per FIPS 140-2 and therefore does not support operator authentication, as shown in Table 8 and Table 9 below.

| Role | Type of Authentication | Authentication Data |
|---|---|---|
| User | N/A | N/A |
| Crypto Officer | N/A | N/A |

*Table 8. Roles and Required Identification and Authentication*

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| N/A | N/A |

*Table 9. Strengths of Authentication Mechanisms*

# 7. Access Control Policy

## 7.1 Roles and Services

The cryptographic module operator is any software application which dynamically links the cryptographic module shared library.

The cryptographic module supports two roles: User and Crypto Officer. An operator assesses both roles while using the cryptographic module and the means of access is the same for both roles. A role is implicitly assumed based on the services that are accessed. These roles are defined as the following.

- User Role: allowed to perform all services provided by the cryptographic module.
- Crypto Officer Role: allowed to perform all services provided by the cryptographic module and also responsible for the installation of the module.

The Crypto Officer is any entity that can install the module library onto a general purpose computer system, configure the operating system and validate the compliance of the module. This role is implicitly selected when the cryptographic module is installed or the operating system is configured.

The Crypto Officer must have permission to write the library comprising the cryptographic module into an operating system directory. This typically requires administrator access to the operating system.

The run self-tests service is ran automatically when the Module is loaded.

## 7.2 Service Inputs and Outputs

The following table summarizes which CSPs are accessed by each service and how the CSP is accessed on behalf of the operator when the service is performed in FIPS mode of operation. All services are available to both the Crypto Officer (CO) and User roles

| Service | Role | Cryptographic Keys & CSPs | Type(s) of Access |
|---|---|---|---|
| Initialize | CO, User | None | - |
| Self-test | CO, User | None | - |
| Show status | CO, User | None | - |
| Zeroize | CO, User | DRBG V Value, DRBG C Value, DRBG Key Value | D |
| Random number generation | CO, User | DRBG V Value, DRBG C Value, DRBG Key Value | C, D, R, W |
| Asymmetric key generation | CO, User | DSA Private Key, ECDSA Private Signature Key, DSA Public Key, ECDSA Public Signature Key | C, W |
| Symmetric encrypt/decrypt | CO, User | AES Secret Key, Three-Key Triple-DES Secret Key | R, W |
| Symmetric digest | CO, User | AES CMAC Key, Three-Key Triple-DES CMAC Key | D, R, W |
| Message digest | CO, User | None | - |
| Keyed Hash | CO, User | HMAC Secret Key | D, R, W |
| Key transport | CO, User | RSA Private Key for Key Transport | R, W |
| Key agreement | CO, User | ECC CDH Private Key, ECC CDH Shared Secret, ECC CDH Public Key | W |
| Digital signature | CO, User | RSA Private Signature Key, ECDSA Private Signature Key, RSA Public Signature Key, ECDSA Public Signature Key | R, W |
| Utility | CO, User | None | - |

*Table 10. Services. Please see Table 11 for more information*

Table 11 below defines the relationship between access to CSPs and the different Module services. The modes of access shown in table 10 are defined as follows:

| **Access** | **Identifier** | **Description** |
|---|---|---|
| Create | C | An object is created |
| Destroy | D | An object is destroyed and memory that it used is released |
| Read | R | Data stored by an object is accessed for use |
| Write | W | An object is modified |

*Table 11. CSP Access Rights within Roles & Services*

The software-only cryptographic module contains an approved DRBG (see Appendix A: Critical Security Parameters and Public Keys for a description and bit-length of the associated CSPs). Entropy is loaded into the cryptographic module from the calling application (software outside of the cryptographic module's logical boundary but within the operational environment within the cryptographic module's physical boundary). A minimum of 112-bits of entropy shall be provided by the calling application when the cryptographic module is in FIPS mode or this Security Policy is violated, the cryptographic module is fully non-compliant and is operating in non-FIPS mode and shall not be used to protect sensitive unclassified data. This satisfies FIPS 140-2 Implementation Guidance, Section 7.14, Scenario 2.B.

The identifier “C” in Table 10 represents the creation of the CSP from the output of the approved DRBG.

The identifier “W” in Table 10 represents the import of such CSP by the calling application.

Please see Appendix A for more information.

## 7.3 Definition of Critical Security Parameters (CSPs)

The following list enumerates the secret keys, private keys, and CSPs contained in the cryptographic module:

- AES Secret Key
- DSA Private Key
- RSA Private Signature Key
- RSA Private Key for Key Transport
- ECDSA Private Signature Key
- ECC CDH Private Key
- ECC CDH Shared Secret
- DRBG V Value
- DRBG C Value
- DRBG Key Value
- HMAC Secret key
- AES CMAC Key
- Three-Key Triple-DES Secret Key
- Three-Key Triple-DES CMAC Key

The following list enumerates the public keys contained in the Module:

- DSA Public Key
- RSA Public Signature Key
- RSA Public Key for Key Transport
- ECDSA Public Signature Key
- ECC CDH Public Key

Please see section Appendix A: Critical Security Parameters and Public Keys for more details.

# 8. Operational Environment

The operational environment for the cryptographic module is a “modifiable operational environment”.

The FIPS 140-2 Operational Environment requirements for Security Level 1 are satisfied in the following way:

When the cryptographic module is operated in FIPS approved mode, the environment is restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded). The tested operating systems separate user processes into separate address spaces, where each space is logically separated from any other address space by the operating systems and the hardware on which it runs. The cryptographic module runs entirely within the address space of the calling application so it implicitly satisfies the requirement for a single user mode of operation.

Processes that are spawned by the cryptographic module are owned by the cryptographic module and are not owned by external processes/operators. Non-cryptographic processes shall not interrupt the cryptographic module during execution.

The cryptographic module software is installed in a form that protects the software and executable code from unauthorized disclosure and modification.

# 9. Security Rules

This section specifies the security rules under which the cryptographic module shall operate.

1. The Module must be used as described in this document
2. Installation of the Module is the responsibility of the Crypto Officer
3. Before the Module can be used in Approved mode, it must be initialized as described in the "FIPS Mode Operating Procedure" section of this document
4. Only Approved cryptographic algorithms as enumerated in the "FIPS Approved Mode of Operation" section of this document may be used.
5. The Module does not perform key generation
6. The Module inhibits Data Output during self-tests and error states. The Data Output interface is logically disconnected from the processes performing self-tests and zeroization.
7. The zeroization process must be implemented using the appropriate API function.
8. The Module is designed to satisfy the requirements of FIPS 140-2 Level 1, therefore the Module does not provide authentication mechanisms.
9. The Module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e. for Home use) which vacuously satisfies Class A.
10. The cryptographic module fully implements the SP800-90A Section 11.3 requirements, and therefore meets the requirements of SP800-90A Section 11.3
11. Power-up self-tests do not require any operator intervention.
12. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
13. The Module does not support a maintenance interface or role.
14. The Module does not support manual key entry.
15. The Module does not support bypass mode.
16. The Module receives plaintext keys from the calling application and outputs plaintext keys to the calling application; however the requirements of key entry/output are not applicable as per FIPS 140-2 IG 7.7.
17. The Module does not output intermediate key values.
18. The Module enforces logical separation of all data inputs, data outputs, control inputs, and status outputs.
19. The general purposes-computing platform includes a power port.
20. Role are implicitly assumed based upon the service requested.
21. The User and Crypto Officer are responsible for ensuring the cryptographic module is compliant with the requirements of FIPS 140-2 IG A.13 SP 800-67rev1 Transition: *The cryptographic module shall perform a maximum of 2 ^28 encryption operations with the same Triple-DES key*.
22. The User and Crypto Officer are responsible for ensuring that the IV is reset to the last one used in the event that the module's power is lost and then restored, as per FIPS-140-2 Implementation Guidance, Section A.5.

### 9.1 FIPS Mode Operating Procedure

The calling application must conform to the following procedure in order to correctly operate the cryptographic module in FIPS approved mode:

1. Application must call Windows system API function LoadLibary (or variant) to load the cryptographic module into the application's process. At that time, the module's self-test operations are run without further user intervention. If self-tests succeed, the module load operation will complete and the LoadLibary API will return a handle for the loaded module back to calling application. If self-tests fail for any reason, the module will fail to load and no handle will be returned to application. See section 9.2 below for more details.

2. After the module loads, application must call function FIPS_module_mode_set with parameter value 1 to complete the initialization procedure. If this function call returns 1, then the module is operating in FIPS mode so long as the operator ensures that algorithms, modes and key sizes are being used in accordance with section 4.1 FIPS Approved Mode of Operation. Any use of non-approved algorithms described in section 4.2 Non-Approved Mode of Operation is an explicit violation of this Security Policy and implicitly toggles the module into the Non-Approved Mode of Operation.

The module conforms to the IG 9.10 requirements by providing a Default Entry Point (DEP). The DEP is automatically executed, without requiring operator intervention (calling application).

## 9.2 Self-Test Operations

At the time the calling application attempts to load the cryptographic module, the following self-test operations are run without further user intervention. Failure in any of these test cases will result in failure of the module load operation and will prevent the application from being able to make any calls into the cryptographic module. If all power-up self-tests succeed, the FIPS_module_mode_set function will return a 1, and a "0" otherwise.

| Algorithm | Type | Test Attributes |
|---|---|---|
| Software integrity | KAT | HMAC-SHA-1 |
| HMAC | KAT | One KAT per SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. Per IG 9.3, this testing covers SHA POST requirements. |
| AES | KAT | Separate encrypt and decrypt, ECB mode, 128 bit key length |
| AES CCM | KAT | Separate encrypt and decrypt, 192 key length |
| AES GCM | KAT | Separate encrypt and decrypt, 256 key length |
| AES CMAC | KAT | Sign and verify CBC mode, 128, 192, 256 key lengths |
| Triple-DES | KAT | Separate encrypt and decrypt, ECB mode, 3Key |
| Triple-DES CMAC | KAT | CMAC generate and verify, CBC mode, 3Key |
| RSA | KAT | Sign and verify using 2048 bit key, SHA-256, PKCS#1 |
| DSA | PCT | Sign and verify using 2048 bit key, SHA-384 |
| DRBG | KAT | CTR_DRBG: AES, 256 bit with and without derivation function<br>HASH_DRBG: SHA-256<br>HMAC_DRBG: SHA-256 |
| ECDSA | PCT | Keygen, sign, verify using P-224, K-233 and SHA-512. The K-233 selftest is not performed for operational environments that support prime curve only (see Table 2). |
| ECC CDH | KAT | Shared secret calculation per SP 80056A §5.7.1.2, IG 9.6 |

*Table 12. Power-Up Self-Tests*

The Module also implements the following conditional tests:

| Algorithm | Test |
|---|---|
| DRBG | Continuous Random Number Generator Test |
| DRBG | Health Tests as required by Section 11 of SP800-90Arev1 |
| DSA | Pairwise consistency test on each generation of a key pair (Sign/Verify) |
| ECDSA | Pairwise consistency test on each generation of a key pair (Sign/Verify) |
| NDRNG | Continuous Random Number Generator Test |

*Table 13. Conditional Self-Tests*

In the event of a DRBG self-test failure the calling application must uninstantiate and reinstantiate the DRBG as per the requirements of SP800-90Arev1; this is not something the Module can do itself.

## 10. Physical Security Policy

The cryptographic module is a software module; therefore, the physical security requirements are not applicable.

| Physical Security Mechanisms | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details |
|---|---|---|
| N/A | N/A | N/A |

*Table 14. Inspection/Testing of Physical Security Mechanisms*

# 11. Mitigation of Other Attacks Policy

The cryptographic module is not designed to mitigate any other attacks.

| Other Attacks | Mitigation Mechanism | Specific Limitations |
|---|---|---|
| N/A | N/A | N/A |

*Table 15. Mitigation of Other Attacks*

## 12. Definitions and Acronyms

The following paragraphs define the acronyms used in this document.

**AES**. Advanced Encryption Standard secret key algorithm. See [FIPS-197].
**API**. Application Programming Interface
**CBC**. Cipher Block Chaining mode
**CFB**. Cipher Feedback mode
**CSP**. Critical Security Parameters
**DES**. Data Encryption Standard. See [SP800-67].
**DRBG**. Deterministic Random Bit Generator.
**DSS**. Digital Signature Standard. See [FIPS-186-4]
**ECB**. Electronic Codebook mode
**EMI**. Electromagnetic Interference
**EMC**. Electromagnetic Compatibility
**FIPS**. Federal Information Processing Standards of NIST.
**IV**. Initialization Vector
**KDF**. Key Derivation Function See [SP800-108, SP800-132]
**NIST**. National Institute of Standards and Technologies.
**OFB**. Output Feedback mode
**SHA-1**. Secure Hash Algorithm revision 1. See [FIPS-180-4].

# Appendix A: Critical Security Parameters and Public Keys

## A.1 Private Keys

The module supports the following secret keys, private keys, and CSPs:

1. AES Secret Key
- Description: 128-bit, 192-bit and 256-bit AES secret keys are used in ECB, CBC, CCM, OFB, GCM, CFB1, CFB8, CFB128 and CTR modes for encrypt/decrypt services
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

2. DSA Private Key
- Description: 2048-bit and 3072-bit DSA private key used for digital signature generation
- Generation: via DRBG. As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

3. RSA Private Signature Key
- Description: 2048-bit and 3072-bit RSA private key used for digital signature generation
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

4. RSA Private Key for Key Transport
- Description: 2048-bit RSA private key used for key transport
- Generation: N/A

- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

5. ECDSA Private Signature Key
- Description: ECDSA (P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571) key used for digital signature generation
- Generation: via DRBG. As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

6. ECC CDH Private Key
- Description: ECC CDH (P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571) private key
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

7. ECC CDH Shared Secret
- Description: ECC CDH (P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571) shared secret for the ECC CDH private key
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.

- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

8. DRBG V Value
- Description: Internal state of the DRBG: 128 bits (for AES-128, AES-192 and AES-256 constructions);160 bits (for HMAC-SHA-1 construction); 224 bits (for HMAC-SHA-224 construction); 256 bits (for HMAC-SHA-256 construction); 384 bits (for HMAC-SHA-384 construction); 512 bits (for HMAC-SHA-512 construction); 440 bits (for SHA-1, SHA-224 and SHA-256 constructions); 888 bits (for SHA-384 and SHA-512 constructions)
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

9. DRBG C Value
- Description: Internal state of the DRBG: 440 bits (for SHA-1, SHA-224 and SHA-256 constructions) or 888 bits (for SHA-384 and SHA-512 constructions)
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

10. DRBG Key Value
- Description: Internal state of the DRBG: 128 bits (for AES-128 construction); 192 bits (for AES-192 construction); 256 bits (for AES-256 construction); 160 bits (for HMAC-SHA-1 construction); 224 bits (for HMAC-SHA-224 construction); 256 bits (for HMAC-SHA-256 construction); 384 bits (for HMAC-SHA-384 construction); 512 bits (for HMAC-SHA-512 construction)
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.

- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

11. HMAC Secret key
- Description: HMAC-SHA-1 (128-bit key), HMAC-SHA-224 (112-bit and 192-bit keys), HMAC-SHA-256 (256-bit and 384-bit keys), HMAC-SHA-384 (256-bit and 384-bit keys), HMAC-SHA-512 (320-bit keys)
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

12. AES CMAC Key
- Description: 128-bit, 192-bit and 256-bit AES secret keys are used in CMAC mode for generation/verification services
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

13. Three-key Triple-DES Secret Key
- Description: 192-bit Triple-DES secret keys are used in TECB, TCBC, TCFB1, TCFB8, TCFB64 and TOFB mode for encrypt and decrypt services
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

14. Three-key Triple-DES CMAC Key
- Description: 192-bit secret key is used in CMAC mode for generation/verification services
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

## A.2 Public Keys

The module supports the following public keys:

1. DSA Public Key
- Description: 1024-bit or 2048-bit or 3072-bit DSA public key used for digital signature verification
- Generation: via DRBG. As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

2. RSA Public Signature Key
- Description: 2048-bit and 3072-bit RSA public key used for digital signature verification
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

3. RSA Public Key for Key Transport
- Description/Usage: 2048-bit RSA public key used for key transport
- Generation: N/A

- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

4. ECDSA Public Signature Key
- Description: ECDSA (P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571) public key used for digital signature verification
- Generation: via DRBG. As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program

5. ECC CDH Public Key
- Description: ECC CDH (P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571) public key
- Generation: N/A
- Establishment: N/A
- Storage: In RAM as plaintext
- Entry: N/A - the key is entered by the calling application; as per FIPS 140-2 IG 7.7 the calling application entering the key is considered as not applicable.
- Output: N/A - the key is output to the calling application; as per FIPS 140-2 IG 7.7 the module outputting the key to the calling application is considered as not applicable.
- Entity: Process
- Zeroization: Power off or actively overwritten by calling program