FIPS 140-2 Non-Proprietary Security Policy

SQLCipher Cryptographic Module (Mobile)

Software Version 2.1.2

Document Version 1.0

April 24, 2024

Prepared For:

Zetetic, LLC
PO Box 5018
Branchburg, NJ 08876
USA
www.zetetic.net

Prepared By:

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

Overview

This document provides a non-proprietary FIPS 140-2 Security Policy for SQLCipher Cryptographic Module (Mobile).

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 Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. The NVLAP accredits independent testing labs to perform FIPS 140 testing; the CMVP validates modules meeting FIPS 140 validation. *Validated* is the term given to a module that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for SQLCipher Cryptographic Module (Mobile) from Zetetic, LLC (Zetetic) 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 (CSPs). This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 Approved mode of operation.

SQLCipher Cryptographic Module (Mobile) may also be referred to as the "module" in this document.

1.3 External Resources

The Zetetic website (www.zetetic.net) contains information on Zetetic services and products. The CMVP website contains links to the FIPS 140-2 certificate and Zetetic contact information.

1.4 Notices

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

2 SQLCipher Cryptographic Module (Mobile)

2.1 Cryptographic Module Specification

The SQLCipher Cryptographic Module is a cryptographic engine that integrates with SQLCipher, enhancing encrypted database operations with a trusted security layer. SQLCipher provides full database encryption and data integrity protection for local storage at rest. This module guarantees that all data stored and retrieved through SQLCipher is encrypted, decrypted, and verified using a reliable implementation for applications demanding high levels of data security.

SQLCipher Cryptographic Module (Mobile) is used by supported Zetetic products, including SQLCipher Enterprise FIPS.

The module's software version is 2.1.2.

The module is a software module that relies on the physical characteristics of the host platform. The module's physical cryptographic boundary is defined by the enclosure of the host platform, which is the General Purpose Device that the module is installed on. For the purposes of FIPS 140-2 validation, the module's embodiment type is defined as multi-chip standalone.

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.

The module's logical cryptographic boundary is the shared library files and their integrity check HMAC files.

2.1.1 Validation Level Detail

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

Table 1 – Validation Level by FIPS 140-2 Section

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	3
Mitigation of Other Attacks	N/A

2.1.2 Modes of Operation

The module supports two modes of operation: FIPS Approved mode and non-Approved mode. The module will be in the FIPS Approved mode when all power-up self-tests have completed successfully, and only Approved algorithms are invoked. See Section 2.1.3 - Approved Cryptographic Algorithms below for a list of the supported Approved algorithms and Section 2.1.4 - Non-Approved but Allowed Cryptographic Algorithms for a list of supported allowed algorithms. The non-Approved mode is entered when a non-Approved algorithm is invoked. See Section 2.1.5 - Non-Approved Algorithms for a list of non-Approved algorithms.

2.1.3 Approved Cryptographic Algorithms

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

Table 2 – FIPS-Approved Algorithm Certificates

CAVP Cert.	Algorithm	Standard	Mode/Method and Key Lengths, Curves or Moduli[1]	Use
A4947	AES	FIPS 197, SP 800-38 series	**CBC** (e/d; 128, 192, 256) **CFB1** (e/d; 128, 192, 256) **CFB8** (e/d; 128, 192, 256) **CFB128** (e/d; 128, 192, 256) **ECB** (e/d; 128, 192, 256) **OFB** (e/d; 128, 192, 256) **CTR** (external counter only; 128, 192, 256) **CMAC** (Generation/Verification: 128, 192, 256) **CCM** (128, 192, 256) **GCM**[2] (e/d: 128, 192, 256)	Data encryption/ decryption and authentication
Vendor Affirmed	CKG	SP 800-133		Cryptographic key generation per IG D.12. The resulting symmetric key or asymmetric seed is an unmodified output from a DRBG. (Ref. Security Policy Section 2.6.1)

[1] The module's CAVP certificates include additional algorithm functionality that is not supported by the module. Algorithms supported by the module are as specified in this table.
[2] IV generation is compliant with IG A.5. See Security Policy Sections 2.6.1 and 3.2.1.

CAVP Cert.	Algorithm	Standard	Mode/Method and Key Lengths, Curves or Moduli[1]	Use
A4947	DRBG	SP 800-90A	Hash_DRBG (SHA-1, SHA-2) HMAC_DRBG (SHA-1, SHA-2) CTR_DRBG (128, 192, 256)	Random number generation. No assurance of the minimum strength of generated keys.
A4947	DSA	FIPS 186-4	**Key Pair Gen**: (2048, 224), (2048, 256), (3072, 256) **PQG Gen**: (2048, 224), (2048, 256), (3072, 256) (SHA-2) **PQG Ver**: (1024, 160), (2048, 224), (2048, 256), (3072, 256) (SHA-1 and SHA-2) **Sig Gen**: (2048, 224), (2048, 256), (3072, 256) (SHA-2) **Sig Ver**: (1024, 160), (2048, 224), (2048, 256), (3072, 256) (SHA-1 and SHA-2)	Digital signatures
A4947	ECDSA	FIPS 186-4	**Key Pair Gen**: P-224, P-256, P-384, P-521 K-233, K-283, K-409, K-571 B-233, B-283, B-409, B-571 **PKV**: P-192, P224, 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 **Sig Gen**: using (SHA-2) P-224, P-256, P-384, P-521 K-233, K-283, K-409, K-571 B-233, B-283, B-409 & B-571 **Sig Ver**: (using SHA-1 and SHA-2) P-192, P224, 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	Digital signatures
A4947	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	Message authentication

CAVP Cert.	Algorithm	Standard	Mode/Method and Key Lengths, Curves or Moduli[1]	Use
A4947	RSA	FIPS 186-4	**ANSI X9.31** Sig Gen: 2048, 3072, 4096 (using SHA-2) Sig Ver: 1024, 2048, 3072 (any SHA size) **PKCS1 V1.5** Sig Gen: 2048, 3072, 4096 (using SHA-2) Sig Ver: 1024, 2048, 3072 (any SHA size) **PSS** Sig Gen: 2048, 3072, 4096 (using SHA-2) Sig Ver: 1024, 2048, 3072 (any SHA size)	Digital signatures
		FIPS 186-2	**ANSI X9.31** Sig Ver: 1024, 1536, 2048, 3072, 4096 (any SHA size) **PKCS1 V1.5** Sig Ver: 1024, 1536, 2048, 3072, 4096 (any SHA size) **PSS** Sig Ver: 1024, 1536, 2048, 3072, 4096 (any SHA size)	
A4947	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Hashing
A4947	Triple-DES	SP 800-67	**TCBC** (KO 1 e/d, KO 2 d only) **TCFB1** (KO 1 e/d, KO 2 d only) **TCFB8** (KO 1 e/d, KO 2 d only) **TCFB64** (KO 1 e/d, KO 2 d only) **TECB** (KO 1 e/d, KO 2 d only) **TOFB** (KO 1 e/d, KO 2 d only) **CMAC** (KS: 3-Key; Generation/Verification; Block Size(s): Full / Partial)	Data encryption/ decryption and authentication

2.1.4 Non-Approved but Allowed Cryptographic Algorithms

The module does not support any FIPS 140-2 non-Approved but allowed algorithms that may be used in the FIPS Approved mode of operation.

2.1.5 Non-Approved Algorithms

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.

The following algorithms shall not be used:

- AES XTS (KS: XTS_128 (e/d) (f/p), KS: XTS_256 (e/d) (f/p)
- EC Diffie-Hellman
- RSA (key wrapping; key establishment methodology provides up to 256 bits of encryption strength)
- GMAC

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

- FIPS 186-4 DSA
  PQG Gen 1024-bit (any SHA size), 2048-bit, 3072-bit using SHA-1
  Key Gen 1024-bit (any SHA size), 2048-bit, 3072-bit using SHA-1
  Sig Gen 1024-bit (any SHA size), 2048-bit, 3072-bit using SHA-1
- FIPS 186-2 DSA
  PQG Gen 1024-bit (any SHA size)
  PQG Ver 1024-bit
  Key Gen 1024-bit
  Sig Gen 1024-bit (any SHA size), 2048-bit, 3072-bit using SHA-1
- FIPS 186-2 RSA
  ANSI X9.31
  Key Gen 1024 & 1536
  ANSI X9.31
  Sig Gen 1024 & 1536 (any SHA size); 2048, 3072 using SHA-1
  PKCSI V1 5
  Sig Gen 1024 & 1536 (any SHA size); 2048, 3072 using SHA-1
  PSS
  Sig Gen 1024 & 1536 (any SHA size); 2048, 3072 using SHA-1
- FIPS 186-4 RSA
  ANSI X9.31
  Sig Gen 1024 using SHA-1
  PKCSI V1 5
  Sig Gen 1024 using SHA-1
  PSS
  Sig Gen 1024 using SHA-1
- FIPS 186-2 ECDSA
  Key Pair Generation Curves P-192, K-163, B-163
  PKV All P, K & B
  Sig Gen Curves All P, K & B
  Sig Ver Curves All P, K & B
- FIPS 186-4 ECDSA
  Key Pair Generation: Curves P-192, K-163, B-163

Sig Gen Curves P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571) (using SHA-1)
P-192, K-163, B-163 (any SHA size)

- CVL (ECC CDH KAS)

The following algorithms are disallowed as of January 1, 2016 per the NIST SP 800-131A algorithm transitions:

- Random Number Generator Based on ANSI X9.31 Appendix A.2.4
- Two-Key Triple DES Encryption
- Dual EC DRBG

The following algorithms are disallowed as of September 1, 2020 per the FIPS 186-2 transitions:

- FIPS 186-2 RSA (X9.31, PKCS #1.5, PSS)
    - **ANSI X9.31**
        - Key Gen: 2048-bit, 3072-bit, 4096-bit
        - Sig Gen: 2048-bit, 3072-bit (any SHA size)
        - Sig Gen: 4096-bit using SHA-1
    - **PKCS1 V1.5**
        - Sig Gen: 2048-bit, 3072-bit (any SHA size)
        - Sig Gen: 4096-bit using SHA-1
    - **PSS**
        - Sig Gen: 2048-bit, 3072-bit (any SHA size)
        - Sig Gen: 4096-bit using SHA-1

2.2 Module Interfaces

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

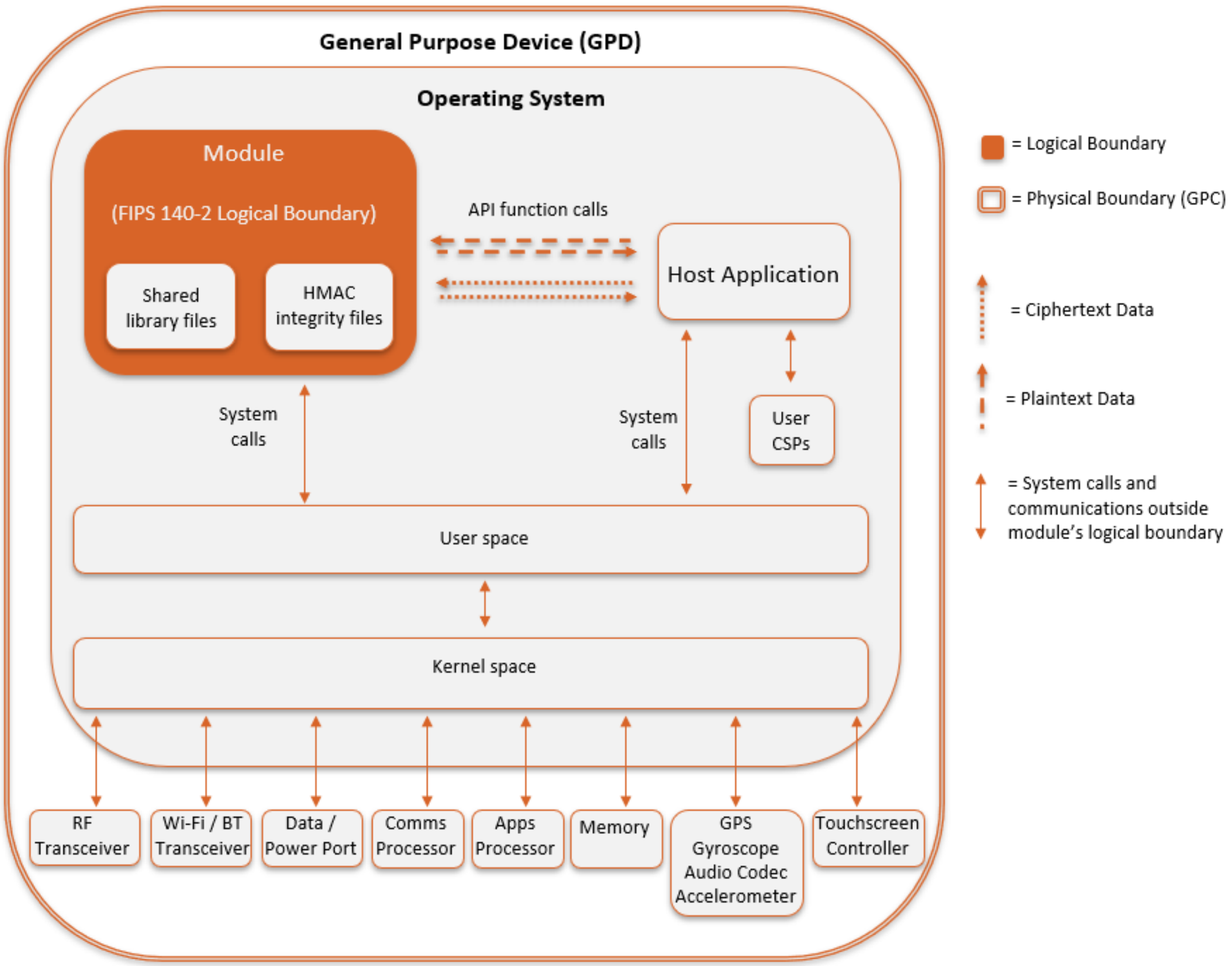

Figure 1 – Module Boundary and Interfaces Diagram

The module's physical boundary is the boundary of the General Purpose Device (GPD) on which the module is installed. The GPD includes processors and memory. The interfaces (ports) for the physical boundary include the RF Transceiver, Wi-Fi/BT Transceiver, data/power port, and touchscreen controller. 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.

The logical interface is provided through the Application Programming Interface (API) that a calling daemon can operate. The API itself defines the module's logical boundary, i.e. all access to the module is through this API. The API provides functions that may be called by an application; see Section 2.3 – Roles, Services, and Authentication for the list of available API 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, which relate to the module's callable interface as follows:

Table 3 – Logical Interface / Physical Interface Mapping

FIPS 140-2 Interface	Module Logical Interface	GPD Physical Interface
Data Input	Input parameters of API function calls	RF Transceiver, Wi-Fi/BT Transceiver, data/power port
Data Output	Output parameters of API function calls	RF Transceiver, Wi-Fi/BT Transceiver, data/power port
Control Input	API function calls	RF Transceiver, Wi-Fi/BT Transceiver, data/power port, touchscreen controller
Status Output	For FIPS Approved mode, function calls returning status information and return codes provided by API function calls.	touchscreen controller
Power	None	data/power port

As shown in Figure 1 – Module Boundary and Interfaces Diagram and Table 4 – 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 (CO) role 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 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:

Table 4 – Module Services, Roles, and Descriptions

Service	Roles	CSP / Algorithm	Permission
Module initialization	Crypto Officer	None	CO: execute
Symmetric encryption/decryption	User	AES Key, Triple-DES Key	User: read/write/execute

Service	Roles	CSP / Algorithm	Permission
Digital signature generation	User	RSA Private Key, DSA Private Key, ECDSA Private Key	User: read/write/execute
Digital Signature verification	User	RSA Public Key, DSA Public Key, ECDSA Public Key	User: read/write/execute
Symmetric key generation	User	AES Key, Triple-DES Key	User: read/write/execute
Asymmetric key generation	User	DSA Private Key, ECDSA Private Key	User: read/write/execute
Keyed Hash (HMAC)	User	HMAC Key HMAC SHA-1, HMAC SHA- 224, HMAC SHA-256, HMAC SHA-384, 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 Internal State, DRBG Entropy	User: read/write/execute
Show status	Crypto Officer User	None	User and CO: execute
Self-test	User	None	User: read/execute
Zeroize	Crypto Officer User	All CSPs	CO: read/write/execute

The operator is required to review Sections 2.1.3 - Approved Cryptographic Algorithms, 2.1.4 - Non-Approved but Allowed Cryptographic Algorithms, 2.1.5 - Non-Approved Algorithms, and 3 - Guidance and Secure Operation to ensure only Approved algorithms are used.

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 4 – 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 in a modifiable operational environment under the FIPS 140-2 definitions. The module operates on a General Purpose Device (GPD) running a General Purpose Operating System (GPOS). For FIPS purposes, the module runs on this operating system in single user mode and does not require any additional configuration to meet FIPS requirements.

The module was tested on the following platforms:

Table 5 – Tested Environments

Operating System	Hardware Platform	Processor (CPU)
Android 8	Galaxy Nexus 5X	Qualcomm Snapdragon 808
iPadOS 15	Apple iPad Air 2	Apple A8X

FIPS 140-2 validation compliance is maintained for compatible operating systems (in single user mode) where the module source code is unmodified, and the requirements outlined in NIST IG G.5 are met. 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 that is not listed on the validation certificate.

The module, when compiled from the same unmodified source code, is vendor-affirmed to be FIPS 140-2 compliant when running on the following supported operating systems for which operational testing and algorithm testing were not performed:

- iOS 15 on iPhone 12 (arm64)
- iOS 17 iPhone Simulator (x86_64)
- iOS 17 iPhone Simulator (arm64)
- Android 6 armeabi-v7a (arm32)
- Android 12 arm64-v8a (arm64)
- Android 6 Android Emulator (x86_64)
- Android on ChromeOS 123 (x86_64)

The GPD(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.

2.6 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters (CSPs) and keys used within the module. Access is indicated as follows:

R = Read W = Write D = Delete

Table 6 – Module Keys/CSPs

Keys and CSPs	Storage Locations	Storage Method	Input Method	Output Method	Zeroization	Access
AES Key (128, 192, 256 bits) Used for Encrypt/Decrypt operations. Used to generate and verify MACs with AES as part of the CMAC algorithm.	RAM	Plaintext	API call parameter	None	power cycle cleanse()	CO: RWD U: RWD
Triple-DES Key (168 bits, 112 bits – decrypt only) Used for Encrypt/Decrypt operations. Used for generating and verifying MACs with Triple-DES as part of the CMAC algorithm.	RAM	Plaintext	API call parameter	None	power cycle cleanse()	CO: RWD U: RWD
RSA Public Key (1024, 1536, 2048, 3072, 4096 bits) RSA public/private keys used to sign and verify data.	RAM	Plaintext	API call parameter	API call parameter	power cycle cleanse()	CO: RWD U: RWD
RSA Private Key (2048, 3072, 4096 bits) RSA public/private keys used to sign and verify data.	RAM	Plaintext	API call parameter	API call parameter	power cycle cleanse()	CO: RWD U: RWD
DSA Public Key (1024, 2048, 3072 bits) DSA public/private keys used to sign and verify data.	RAM	Plaintext	API call parameter	API call parameter	power cycle cleanse()	CO: RWD U: RWD

Keys and CSPs	Storage Locations	Storage Method	Input Method	Output Method	Zeroization	Access
DSA Private Key (2048, 3072 bits) DSA public/private keys used to sign and verify data.	RAM	Plaintext	API call parameter	API call parameter	power cycle cleanse()	CO: RWD U: RWD
HMAC Key (≥ 112 bits) HMAC keys used to generate and verify MACs on data.	RAM	Plaintext	API call parameter	API call parameter	power cycle cleanse()	CO: RWD U: RWD
Integrity Key	Module Binary	Plaintext	None	None	None	CO: RWD U: RWD
ECDSA Private Key (**PKG/SigGen**: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571) **PKV/SigVer**: All P, K & B curves) ECDSA public/private keys used to sign and verify data.	RAM	Plaintext	API call parameter	API call parameter	power cycle cleanse()	CO: RWD U: RWD
ECDSA Public Key (**PKG/SigGen**: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-233, B-283, B-409, B-571 **PKV/SigVer**: All P, K & B curves) ECDSA public/private keys used to sign and verify data.	RAM	Plaintext	API call parameter	API call parameter	power cycle cleanse()	CO: RWD U: RWD
DRBG Internal state (V, C, Key value) V and Key are used as part of HMAC and CTR DRBG process. V and C are used as part of HASH DRBG process.	RAM	Plaintext	None	None	power cycle cleanse()	CO: RWD U: RWD
DRBG Entropy Entropy input strings used as part of the DRBG process.	RAM	Plaintext	API call parameter	None	power cycle cleanse()	CO: RWD U: RWD

Please note that keys can be generated by the module for the services that require those keys, but the keys will always be input via an API call.

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 SP 800-90A DRBGs for creation of asymmetric and symmetric keys.

The module accepts input from entropy sources external to the cryptographic 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). At a minimum, the entropy source shall provide at least 128 bits of entropy to the DRBG.

The module performs continual tests on the random numbers it uses to ensure that the seed inputs 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.

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) for symmetric keys and asymmetric seeds per NIST SP 800-133rev2 (vendor affirmed). The resulting symmetric key or asymmetric seed is an unmodified output from a DRBG.

The AES GCM IV generation is in compliance with the RFC5288 and RFC5289 and shall only be used for the TLS protocol version 1.2 to be compliant with [FIPS140-2_IG] IG A.5, provision 1 ("TLS protocol IV generation"); thus, the module is compliant with [SP800-52]. Refer to Section 3.2.1 – General Guidance for additional detail.

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

An authorized application acting in 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 deallocate 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. 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 reloaded 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-SHA-1 digest computed at build time. If the fingerprints match, the power-up self-tests are then performed. If the power-up self-tests are successful, a flag is set to indicate the module is in FIPS Approved mode (the operator is still required to follow the guidance in Section 3 – Guidance and Secure Operation to ensure the module is running in FIPS Approved mode of operation).

Table 7 – Power-On Self-Tests

Test Type	Test Details
Software Integrity Check	• HMAC-SHA-1 on all module components (HMAC Cert. #A4947)
Known Answer Tests (KATs)	• AES ○ AES ECB 128 encrypt KAT ○ AES ECB 128 decrypt KAT ○ AES CMAC 128/192/256 encrypt KATs ○ AES CMAC 128/192/256 decrypt KATs ○ AES CCM 192 encrypt KAT ○ AES CCM 192 decrypt KAT ○ AES GCM 256 encrypt KAT ○ AES GCM 256 decrypt KAT ○ XTS-AES (legacy test) • DRBG ○ Hash_DRBG KATs ○ HMAC_DRBG KATs ○ CTR_DRBG KATs • EC Diffie-Hellman (legacy test) • HMAC ○ HMAC-SHA-1 KAT ○ HMAC-SHA-224 KAT ○ HMAC-SHA-256 KAT ○ HMAC-SHA-384 KAT ○ HMAC-SHA-512 KAT • RSA ○ RSA 2048 sign KAT (SHA-256, PKCS#1) ○ RSA 2048 verify KAT (SHA-256, PKCS#1) • SHS[3] ○ SHA-1 KAT • Triple-DES ○ Triple-DES ECB 3-key encrypt KAT ○ Triple-DES ECB 3-key decrypt KAT ○ Triple-DES CMAC 3-key generate KAT ○ Triple-DES CMAC 3-key verify KAT
Pairwise Consistency Tests (PCTs)	• DSA sign/verify PCT using 2048 bit key, SHA-384 • ECDSA sign/verify PCT using P-224, SHA-512 • ECDSA sign/verify PCT using K-233, SHA-512 • RSA PCT (legacy test)

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

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

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.

The module performs power-up self-tests automatically during loading of the module by making use of Default Entry Point (DEP) and no operator intervention is required.

2.7.2 Conditional Self-Tests

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

Table 8 – Conditional Self-Tests

Test Type	Test Details
Pairwise Consistency Tests	• DSA • RSA (legacy test not run in FIPS Approved mode) • ECDSA
Continuous RNG Tests	• Performed on all Approved DRBGs, the non-approved X9.31 RNG, and the non-approved DUAL_EC_DRBG Please note the DRBGs are tested as required by [SP800-90A] Section 11

2.7.3 Cryptographic Function

The module verifies the integrity of the runtime executable using a HMAC-SHA-1 digest that is computed at build time. If this computed HMAC-SHA-1 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. This power-up self-test failure is a hard error that can only be recovered by reloading the module. 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 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. Only the compiled module is provided to solution developers. The module and its host application are to be installed on an operating system specified in Section 2.5– Operational Environment or on an operating system where portability is maintained.

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 must ensure that any AES GCM keys used for encryption or decryption are redistributed.

The counter portion of the AES GCM IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party to encounter this condition shall trigger a handshake to establish a new encryption key in accordance with RFC 5246.

The AES GCM IV generation is in compliance with the RFC5288 and RFC5289 and shall only be used for the TLS protocol version 1.2 to be compliant with [FIPS140-2_IG] IG A.5, provision 1 (“TLS protocol IV generation”); thus, the module is compliant with [SP800-52].

In the event the `nonce_explicit` part of the IV exhausts the maximum number of possible values for a given session key, either party (the client or the server) that encounters this condition shall trigger a handshake to establish a new encryption key.

The same Triple-DES key shall not be used to encrypt more than 2^{16} 64-bit blocks of data in accordance with IG A.13.

At a minimum, the entropy source shall provide at least 128 bits of entropy to the DRBG.

4 References and Acronyms

4.1 References

Table 9 – References

Abbreviation	Full Specification Name
ANSI X9.31	*X9.31-1998, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), September 9, 1998*
FIPS 140-2	*Security Requirements for Cryptographic modules, May 25, 2001*
FIPS 180-4	*Secure Hash Standard (SHS)*
FIPS 186-4	*Digital Signature Standard (DSS)*
FIPS 197	*Advanced Encryption Standard*
FIPS 198-1	*The Keyed-Hash Message Authentication Code (HMAC)*
IG	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
SP 800-38B	*Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*
SP 800-38C	*Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*
SP 800-38D	*Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*
SP 800-67	*Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*
SP 800-90A	*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*

4.2 Acronyms

The following table defines acronyms found in this document:

Table 10 – Acronyms and Terms

Acronym	Term
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
BT	Bluetooth
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CCCS	Canadian Centre for Cyber Security
CKG	Cryptographic Key Generation
CSP	Critical Security Parameter
DEP	Default Entry Point
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EC	Elliptic Curve
EMI, EMC	Electromagnetic Interference, Electromagnetic Compatibility
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
GPD	General Purpose Device
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
RF	Radio Frequency
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SHA, SHS	Secure Hash Algorithm, Secure Hash Standard
SP	Special Publication (as used by NIST)
Triple-DES	Triple Data Encryption Algorithm
TLS	Transport Layer Security