Corsec Security, Inc.

CorSSL™

Software Version: 1.1.1s.005

FIPS 140-3 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.1

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
www.corsec.com

Abstract

This is a non-proprietary Cryptographic Module Security Policy for CorSSL™ (version: 1.1.1s.005) from Corsec Security, Inc. (Corsec). This Security Policy describes how CorSSL™ meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-3, which details the U.S. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-3 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-3 validation of the module. CorSSL™ is also referred to in this document as the module.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-3 cryptographic module security policy. More information is available on the module from the following sources:

- The Corsec website www.corsec.com contains information on the full line of services and solutions from Corsec.
- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

Document Organization

ISO/IEC 19790 Annex B uses the same section naming convention as *ISO/IEC 19790* section 7 - Security requirements. For example, Annex B section B.2.1 is named “General” and B.2.2 is named “Cryptographic module specification,” which is the same as *ISO/IEC 19790* section 7.1 and section 7.2, respectively. Therefore, the format of this Security Policy is presented in the same order as indicated in Annex B, starting with “General” and ending with “Mitigation of other attacks.” If sections are not applicable, they have been marked as such in this document.

Table of Contents

List of Tables

List of Figures

1. General

Corsec Security, Inc. is a privately owned company dedicated to assisting organizations through the security certification and validation process. Over the past 22 years, Corsec has grown significantly, becoming a global leader in product and corporate security, offering critical guidance and expertise to meet important business challenges in product security and third-party certifications and security validations, including FIPS 140-2, FIPS 140-3, Common Criteria, and the DoDIN[1] APL[2].

Corsec's certification methodology helps open doors to new markets and increase revenue for clients with products ranging from mobile phones to satellites. Corsec's broad knowledge safeguards against common pitfalls and thwarts delays, translating to a swift and seamless path to certification. Corsec has created the benchmark for providing business leaders with fast, flexible access to industry knowledge on security certifications and validations.

CorSSL™ v1.1.1s.005 is a software library providing a C language API[3] for use by other applications requiring cryptographic functionality. CorSSL™ v1.1.1s.005 offers symmetric encryption/decryption, digital signature generation/verification, hashing, cryptographic key generation, random number generation, message authentication, and key establishment functions to secure data-at-rest/data-in-flight and to support industry-standard secure communications protocols (including TLS[4] 1.2/1.3).

Corsec's CorSSL™ is built upon the OpenSSL 1.1.1 code base, providing engineering teams with a completely compatible cryptographic/protocol engine, allowing quick "drop-in" replacement into any existing OpenSSL 1.1.1-based architecture. CorSSL™ (which includes both the libcrypto crypto library and the libssl protocol library) does not modify the OpenSSL interface, maintaining complete compatibility, and eliminating engineering development time to meet FIPS 140-3 requirements.

CorSSL™ is validated at the FIPS 140-3 section levels shown in Table 1.

Table 1 – Security Levels

ISO/IEC 24579 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, and Authentication	1
5	Software/Firmware Security	1
6	Operational Environment	1
7	Physical Security	N/A
8	Non-Invasive Security	N/A

[1] DoDIN – Department of Defense Information Network
[2] APL – Approved Product List
[3] API – Application Programming Interface
[4] TLS – Transport Layer Security

ISO/IEC 24579 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
9	Sensitive Security Parameter Management	1
10	Self-tests	1
11	Life-Cycle Assurance	1
12	Mitigation of Other Attacks	N/A

The module has an overall security level of 1.

2. Cryptographic Module Specification

CorSSL™ v1.1.1s.005 is a software module with a multi-chip standalone embodiment. The module is designed to operate within a modifiable operational environment.

2.1 Operational Environments

The module was tested and found to be compliant with FIPS 140-3 requirements on the environments listed in Table 2.

Table 2 – Tested Operational Environments

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	Debian 9	Dell PowerEdge R440	Intel® Xeon Silver 4214R	With (AES-NI)
2	Debian 9	Dell PowerEdge R440	Intel® Xeon Silver 4214R	Without

The module is designed to utilize the AES-NI[5] extended instruction set when available on the host platform's CPU to accelerate the processing of its AES implementation.

There are no vendor-affirmed operational environments claimed.

The cryptographic module maintains validation compliance when operating on any general-purpose computer (GPC) provided that the GPC uses any single-user operating system/mode specified on the validation certificate, or another compatible single-user operating system. The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment not listed on the validation certificate.

2.2 Algorithm Implementations

The module implements cryptographic algorithms in the following providers:

- CorSSL (libcrypto) v1.1.1s.005 (Cert. A3254)
- CorSSL (libssl) v1.1.1s.005 (Cert. A3253)

Validation certificates for each Approved security function are listed in Table 3 below.

[5] AES-NI – Advanced Encryption Algorithm New Instructions

Table 3 – Approved Algorithms

CAVP Cert[6]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
CorSSL (libcrypto)				
A3254	**AES-CBC**[7] *FIPS PUB[8] 197* *NIST SP 800-38A*	CBC	128, 192, 256	Encryption/Decryption
A3254	**AES-CCM**[9] *NIST SP 800-38C*	CCM	128, 192, 256	Encryption/Decryption
A3254	**AES-CFB1**[10] *FIPS PUB 197* *NIST SP 800-38A*	CFB1	128, 192, 256	Encryption/Decryption
A3254	**AES-CFB128** *FIPS PUB 197* *NIST SP 800-38A*	CFB128	128, 192, 256	Encryption/Decryption
A3254	**AES-CFB8** *FIPS PUB 197* *NIST SP 800-38A*	CFB8	128, 192, 256	Encryption/Decryption
A3254	**AES-CMAC**[11] *NIST SP 800-38B*	CMAC	128, 192, 256	MAC Generation/Verification
A3254	**AES-CTR**[12] *FIPS PUB 197* *NIST SP 800-38A*	CTR	128, 192, 256	Encryption/Decryption
A3254	**AES-ECB**[13] *FIPS PUB 197* *NIST SP 800-38A*	ECB	128, 192, 256	Encryption/Decryption
A3254	**AES-GCM**[14] *NIST SP 800-38D*	GCM	128, 192, 256	Authenticated Encryption/Decryption
A3254	**AES-GMAC**[15] *NIST SP 800-38D*	GMAC	128, 192, 256	Encryption/Decryption
A3254	**AES-KW**[16] *NIST SP 800-38F*	KW	128, 192, 256	Encryption/Decryption
A3254	**AES-KWP**[17] *NIST SP 800-38F*	KWP	128, 192, 256	Encryption/Decryption
A3254	**AES-OFB**[18] *FIPS PUB 197* *NIST SP 800-38A*	OFB	128, 192, 256	Encryption/Decryption

[6] This table includes vendor-affirmed algorithms that are approved but CAVP testing is not yet available.
[7] CBC – Cipher Block Chaining
[8] PUB – Publication
[9] CCM – Counter with Cipher Block Chaining - Message Authentication Code
[10] CFB – Cipher Feedback
[11] CMAC – Cipher-Based Message Authentication Code
[12] CTR – Counter
[13] ECB – Electronic Code Book
[14] GCM – Galois Counter Mode
[15] GMAC – Galois Message Authentication Code
[16] KW – Key Wrap
[17] KWP – Key Wrap with Padding
[18] OFB – Output Feedback

CAVP Cert[6]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A3254	**AES-XTS**[19,20,21] **Testing Revision 2.0** *NIST SP 800-38E*	XTS[22,23,24]	128, 256	Encryption/Decryption
A3254	**Counter DRBG**[25] *NIST SP 800-90Arev1*	Counter-based	128, 192, 256-bit AES-CTR	Deterministic Random Bit Generation
A3254	**DSA**[26] **KeyGen (FIPS186-4)** *FIPS PUB 186-4*	DSA KeyGen	2048/224, 2048/256, 3072/256	Key Pair Generation
A3254	**DSA PQGGen (FIPS186-4)** *FIPS PUB 186-4*	DSA PQGGen	2048/224, 2048/256, 3072/256 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Domain Parameter Generation
A3254	**DSA PQGVer (FIPS186-4)** *FIPS PUB 186-4*	DSA PQGVer	1024/160, 2048/224, 2048/256, 3072/256 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Domain Parameter Verification
A3254	**DSA SigGen (FIPS186-4)** *FIPS PUB 186-4*	DSA SigGen	2048/224, 2048/256, 3072/256 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital Signature Generation
A3254	**DSA SigVer (FIPS186-4)** *FIPS PUB 186-4*	DSA SigVer	1024/160, 2048/224, 2048/256, 3072/256 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital Signature Verification
A3254	**ECDSA**[27] **KeyGen (FIPS186-4)** *FIPS PUB 186-4*	ECDSA KeyGen Secret generation mode: Testing candidates	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Key Pair Generation
A3254	**ECDSA KeyVer (FIPS186-4)** *FIPS PUB 186-4*	ECDSA KeyVer	B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Public Key Validation
A3254	**ECDSA SigGen (FIPS186-4)** *FIPS PUB 186-4*	ECDSA SigGen	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital Signature Generation

[19] XOR – Exclusive OR
[20] XEX – XOR Encrypt XOR
[21] XTS – XEX-Based Tweaked-Codebook Mode with Ciphertext Stealing
[22] XOR – Exclusive OR
[23] XEX – XOR Encrypt XOR
[24] XTS – XEX-Based Tweaked-Codebook Mode with Ciphertext Stealing
[25] DRBG – Deterministic Random Bit Generator
[26] DSA – Digital Signature Algorithm
[27] ECDSA – Elliptic Curve Digital Signature Algorithm

CAVP Cert[6]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A3254	**ECDSA SigVer (FIPS186-4)** *FIPS PUB 186-4*	ECDSA SigVer	B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-256, P-384, P-521 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital Signature Verification
A3254	**HMAC SHA-1** *FIPS PUB 198-1*	SHA-1	MAC: 80-160 Increment 8 Key Length: 8-524288 Increment 8	Message Authentication *The module also supports HMAC SHA-1-80.*
A3254	**HMAC SHA2-224** *FIPS PUB 198-1*	SHA2-224	MAC: 224 Key Length: 8-524288 Increment 8	Message Authentication
A3254	**HMAC SHA2-256** *FIPS PUB 198-1*	SHA2-256	MAC: 256 Key Length: 8-524288 Increment 8	Message Authentication
A3254	**HMAC SHA2-384** *FIPS PUB 198-1*	SHA2-384	MAC: 384 Key Length: 8-524288 Increment 8	Message Authentication
A3254	**HMAC SHA2-512** *FIPS PUB 198-1*	SHA2-512	MAC: 512 Key Length: 8-524288 Increment 8	Message Authentication
A3254	**HMAC SHA3-224** *FIPS PUB 198-1*	SHA3-224	MAC: 224 Key Length: 8-524288 Increment 8	Message Authentication
A3254	**HMAC SHA3-256** *FIPS PUB 198-1*	SHA3-256	MAC: 256 Key Length: 8-524288 Increment 8	Message Authentication
A3254	**HMAC SHA3-384** *FIPS PUB 198-1*	SHA3-384	MAC: 384 Key Length: 8-524288 Increment 8	Message Authentication
A3254	**HMAC SHA3-512** *FIPS PUB 198-1*	SHA3-512	MAC: 512 Key Length: 8-524288 Increment 8	Message Authentication
A3254	**KAS-ECC-SSC**[28] **Sp800-56Ar3** *NIST SP 800-56Arev3*	ephemeralUnified	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Shared Secret Computation
A3254	**KAS-FFC-SSC**[29] **Sp800-56Ar3** *NIST SP 800-56Arev3*	dhEphem	2048/224 (FB), 2048/256 (FC)	Shared Secret Computation
A3254	**PBKDF2**[30] *NIST SP 800-132*	Section 5.4, option 1a	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512	Password-Based Key Derivation

[28] KAS-ECC-SSC – Key Agreement Scheme - Elliptic Curve Cryptography - Shared Secret Computation
[29] KAS-FFC-SSC – Key Agreement Scheme - Finite Field Cryptography - Shared Secret Computation
[30] PBKDF2 – Password-based Key Derivation Function 2

CAVP Cert[6]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A3254	**RSA[31] KeyGen (FIPS186-4)** *FIPS PUB 186-4*	Key generation mode: B.3.3	2048, 3072, 4096	Key Pair Generation
A3254	**RSA[32] SigGen (FIPS186-4)** *FIPS PUB 186-4*	X9.31	2048, 3072, 4096 (SHA2-256, SHA2-384, SHA2-512)	Digital Signature Generation
		PKCS#1 v1.5	2048, 3072, 4096 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital Signature Generation
		PSS[33]	2048, 3072, 4096 (SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital Signature Generation
A3254	**RSA[34] SigVer (FIPS186-4)** *FIPS PUB 186-4*	X9.31	1024, 2048, 3072, 4096 (SHA-1, SHA2-256, SHA2-384, SHA2-512)	Digital Signature Verification
		PKCS#1 v1.5	1024, 2048, 3072, 4096 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital Signature Verification
		PSS[35]	1024, 2048, 3072, 4096 (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)	Digital Signature Verification
A3254	**SHA-1** *FIPS PUB 180-4*	SHA-1	Message Length: 0-65528 Increment 8	Message Digest
A3254	**SHA2-224** *FIPS PUB 180-4*	SHA2-224	Message Length: 0-65528 Increment 8	Message Digest
A3254	**SHA2-256** *FIPS PUB 180-4*	SHA2-256	Message Length: 0-65528 Increment 8	Message Digest
A3254	**SHA2-384** *FIPS PUB 180-4*	SHA2-384	Message Length: 0-65528 Increment 8	Message Digest
A3254	**SHA2-512** *FIPS PUB 180-4*	SHA2-512	Message Length: 0-65528 Increment 8	Message Digest
A3254	**SHA3-224** *FIPS PUB 202*	SHA3-224	Message Length: 0-65528 Increment 8	Message Digest
A3254	**SHA3-256** *FIPS PUB 202*	SHA3-256	Message Length: 0-65528 Increment 8	Message Digest
A3254	**SHA3-384** *FIPS PUB 202*	SHA3-384	Message Length: 0-65528 Increment 8	Message Digest
A3254	**SHA3-512** *FIPS PUB 202*	SHA3-512	Message Length: 0-65528 Increment 8	Message Digest
A3254	**SHAKE[36]-128** *FIPS PUB 202*	SHAKE-128	Output Length: 16-1024 Increment 8	Message Digest

[31] RSA – Rivest Shamir Adleman
[32] RSA – Rivest Shamir Adleman
[33] PSS – Probabilistic Signature Scheme
[34] RSA – Rivest Shamir Adleman
[35] PSS – Probabilistic Signature Scheme
[36] SHAKE – Secure Hash Algorithm KECCAK

CAVP Cert[6]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A3254	**SHAKE-256** *FIPS PUB 202*	SHAKE-256	Output Length: 16-1024 Increment 8	Message Digest
A3254	**TDES-CBC** *NIST SP 800-67rev2* *NIST SP 800-38A*	CBC	168	Decryption
A3254	**TDES-CFB1** *NIST SP 800-67rev2* *NIST SP 800-38A*	CFB1	168	Decryption
A3254	**TDES-CFB64** *NIST SP 800-67rev2* *NIST SP 800-38A*	CFB64	168	Decryption
A3254	**TDES-CFB8** *NIST SP 800-67rev2* *NIST SP 800-38A*	CFB8	168	Decryption
A3254	**TDES-CMAC** *NIST SP 800-67rev2* *NIST SP 800-38B*	CMAC	112, 168	MAC verification
A3254	**TDES-ECB** *NIST SP 800-67rev2* *NIST SP 800-38A*	ECB	168	Decryption
A3254	**TDES-OFB** *NIST SP 800-67rev2* *NIST SP 800-38A*	OFB	168	Decryption
A3254	**TLS v1.2 KDF RFC 7627** **CVL** *NIST SP 800-135rev1* *RFC 7627*	KDF (TLS[37] v1.2)	SHA2-256, SHA2-384, SHA2-512	Key Derivation *No part of the TLS 1.2 protocol, other than the KDF, has been tested by the CAVP and CMVP.*
CorSSL (libssl)				
A3253	**TLS v1.3 KDF** **CVL** *NIST SP 800-135rev1* *RFC 8446*	KDF (TLS v1.3)	SHA2-256, SHA2-384	Key Derivation *No part of the TLS 1.3 protocol, other than the KDF, has been tested by the CAVP and CMVP.*
Security Function Implementations (SFIs)				
KAS-ECC-SSC A3254 TLS v1.2 KDF RFC7627 A3254	**KAS**[38] *NIST SP 800-56Arev3* *NIST SP 800-135rev1* *RFC 7627*	*NIST SP 800-56Arev3*. KAS-ECC per IG D.F Scenario 2 path (2)	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, and P-521 curves providing between 112 and 256 bits of encryption strength	Key Agreement
KAS-ECC-SSC A3254 TLS v1.3 KDF A3253	**KAS** *NIST SP 800-56Arev3* *NIST SP 800-135rev1* *RFC 8446*	*NIST SP 800-56Arev3*. KAS-ECC per IG D.F Scenario 2 path (2)	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, and P-521 curves providing between 112 and 256 bits of encryption strength	Key Agreement

[37] TLS – Transport Layer Security
[38] KAS – Key Agreement Scheme

CAVP Cert[6]	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
KAS-FFC-SSC A3254 TLS v1.2 KDF RFC7627 A3254	**KAS** *NIST SP 800-56Arev3* *NIST SP 800-135rev1* *RFC 7627*	*NIST SP 800-56Arev3*. KAS-FFC per IG D.F Scenario 2 path (2)	2048-bit key providing 112 bits of encryption strength	Key Agreement
KAS-FFC-SSC A3254 TLS v1.3 KDF A3253	**KAS** *NIST SP 800-56Arev3* *NIST SP 800-135rev1* *RFC 8446*	*NIST SP 800-56Arev3*. KAS-FFC per IG D.F Scenario 2 path (2)	2048-bit key providing 112 bits of encryption strength	Key Agreement
AES-CCM A3254	**KTS**[39] *NIST SP 800-38C* *NIST SP 800-38F*	*NIST SP 800-38C* and *NIST SP 800-38F*. KTS (key wrapping and unwrapping) per IG D.G.	128, 192, and 256-bit keys provide between 128 and 256 bits of encryption strength	Key Wrap/Unwrap[40]
AES-GCM A3254	**KTS** *NIST SP 800-38D* *NIST SP 800-38F*	*NIST SP 800-38D* and *NIST SP 800-38F*. KTS (key wrapping and unwrapping) per IG D.G.	128, 192, and 256-bit keys provide between 128 and 256 bits of encryption strength	Key Wrap/Unwrap[41]
AES-KW A3254	**KTS** *NIST SP 800-38F*	*NIST SP 800-38F*. KTS (key wrapping and unwrapping) per IG D.G.	128, 192, and 256-bit keys provide between 128 and 256 bits of encryption strength	Key Wrap/Unwrap
AES-KWP A3254	**KTS** *NIST SP 800-38F*	*NIST SP 800-38F*. KTS (key wrapping and unwrapping) per IG D.G.	128, 192, and 256-bit keys provide between 128 and 256 bits of encryption strength	Key Wrap/Unwrap
Vendor Affirmed				
Vendor Affirmed	**CKG**[42] *NIST SP 800-133rev2*	-	-	Cryptographic Key Generation

The vendor affirms the following cryptographic security methods:

- Cryptographic key generation – In compliance with sections 4 and 5.1 of *NIST SP 800-133rev2*, the module uses its Approved DRBG to generate random values and seeds used for asymmetric key generation. The generated seed is an unmodified output from the DRBG. The cryptographic module invokes a GET command to obtain entropy for random number generation (the module requests 256 bits of entropy from the calling application per request), and then passively receives entropy from the calling application

[39] KTS – Key Transport Scheme
[40] Per FIPS 140-3 Implementation Guidance D.G, AES-CCM is Approved for key wrap/unwrap.
[41] Per FIPS 140-3 Implementation Guidance D.G, AES-GCM is Approved for key wrap/unwrap.
[42] CKG – Cryptographic Key Generation

while having no knowledge of the entropy source and exercising no control over the amount or the quality of the obtained entropy.

The calling application and its entropy sources are located within the operational environment inside the module's physical perimeter but outside the cryptographic boundary. Thus, there is no assurance of the minimum strength of generated SSPs (e.g., keys)

The module implements the Non-Approved but allowed algorithms shown in Table 4 below.

Table 4 – Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	Caveat	Use / Function
AES	Cert. #A3254, Key Unwrapping. Per IG D.G.	Symmetric Key Unwrapping (using any approved mode)
Triple-DES	Cert. #A3254, Key Unwrapping. Per IG D.G.	Symmetric Key Unwrapping (using any approved mode with two-key or three-key)

The module does not implement any Non-Approved algorithms allowed in the approved mode of operation for which no security is claimed.

The module employs the Non-Approved algorithms shown in Table 5 below. These algorithms shall not be used in the module's Approved mode of operation.

Table 5 – Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

Algorithm / Function	Use / Function
AES-GCM (non-compliant with external IV)	Encryption/Decryption
AES-OCB[43]	Authenticated Encryption/decryption
ANSI X9.31 RNG (with 128-bit AES core)	Random Number Generation
ARIA	Encryption/Decryption
Blake2	Encryption/Decryption
Blowfish	Encryption/Decryption
Camellia	Encryption/Decryption
CAST, CAST5	Encryption/Decryption
ChaCha20	Encryption/Decryption
DES	Encryption/Decryption
DRBG (non-compliant when using Hash_DRBG and HMAC_DRBG)	Random Bit Generation
DSA, ECDSA, and RSA (non-compliant when used with SHA-1 outside the TLS protocol)	Digital Signature Generation
DH (non-compliant with key sizes below 2048 bits)	Key Agreement

[43] OCB – Offset Codebook

Algorithm / Function	Use / Function
DSA (non-compliant with key sizes below the minimums for Approved mode)	Key Pair Generation; Digital Signature Generation; Digital Signature Verification
ECDH (non-compliant with curves P-192, K-163, B-163, and non-NIST curves)	Key Agreement
ECDSA (non-compliant with curves P-192, K-163, B-163, and non-NIST curves)	Key Pair Generation; Digital Signature Generation; Digital Signature Verification
EdDSA[44]	Key Pair Generation; Digital Signature Generation; Digital Signature Verification
IDEA	Encryption/Decryption
KDF	Key Derivation Functions for TLS 1.0/1.1; HKDF; X9.42
MD2, MD4, MD5	Message Digest
Poly1305	Message Authentication Code
RC2[45], RC4, RC5	Encryption/Decryption
RIPEMD	Message Digest
RMD160	Message Digest
RSA (non-compliant with non-approved/untested key sizes, and functions)	Key Pair Generation; Digital Signature Generation; Digital Signature Verification; Key Transport
SEED	Encryption/Decryption
SHA-1 (non-compliant)	Signature Generation for TLS 1.0/1.1
SM2, SM3	Message Digest
SM4	Encryption/Decryption
Triple-DES (non-compliant)	Encryption; MAC Generation; Key Wrapping
Whirlpool	Message Digest

2.3 Cryptographic Boundary

As a software cryptographic module, the module has no physical components. The physical perimeter of the cryptographic module is defined by each host platform on which the module is installed. Figure 1 below illustrates a block diagram of a typical GPC and the module's physical perimeter.

[44] EdDSA – Edwards-curve Digital Signature Algorithm
[45] RC – Rivest Cipher

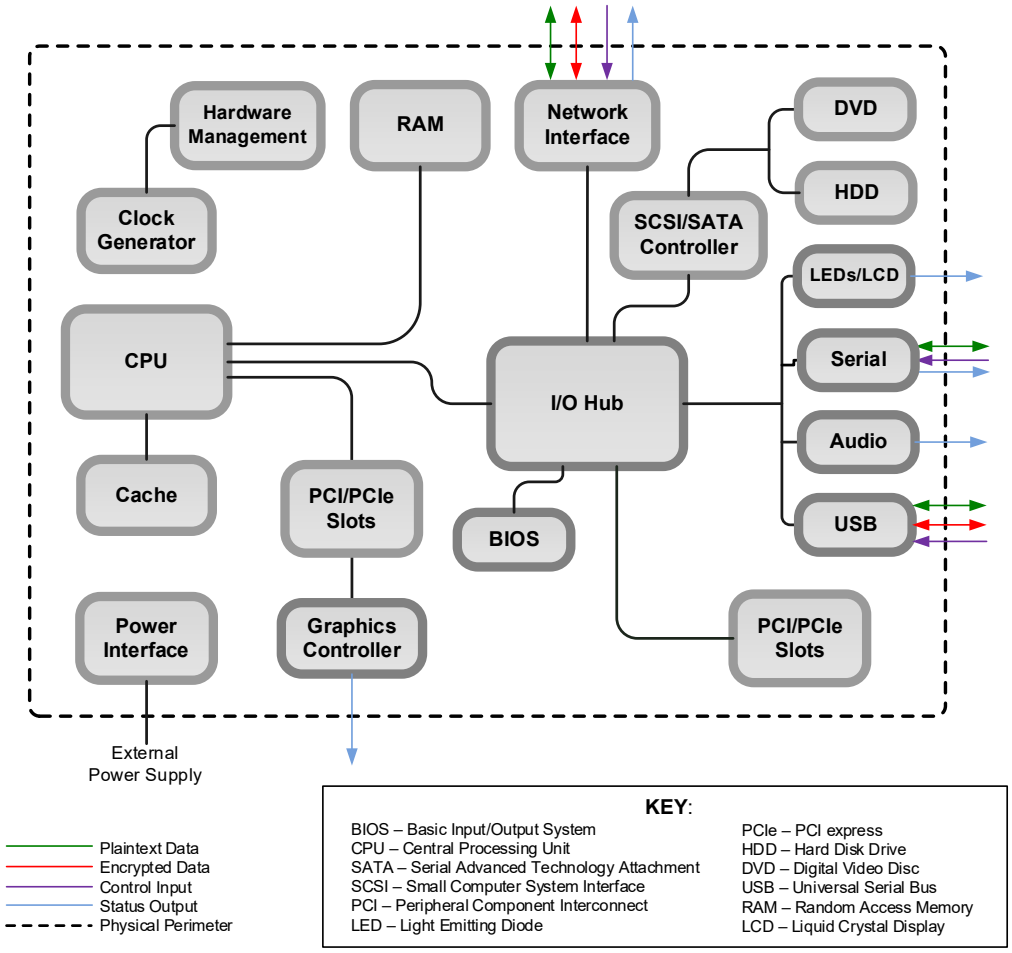

Figure 1 – GPC Block Diagram

The module's cryptographic boundary consists of all functionalities contained within the module's compiled source code. Including:

- libcrypto (cryptographic primitives library file)
- libssl (TLS protocol library file)
- libcrypto.hmac (an HMAC digest file for libcrypto integrity checks)
- libssl.hmac (an HMAC digest file for libssl integrity checks)

The cryptographic boundary is the contiguous perimeter that surrounds all memory-mapped functionality provided by the module when it is loaded and stored in the host platform's memory. The module is entirely contained within the physical perimeter.

Figure 2 shows the logical block diagram of the module executing in memory, its interactions with surrounding software components, and the module's physical perimeter and cryptographic boundary.

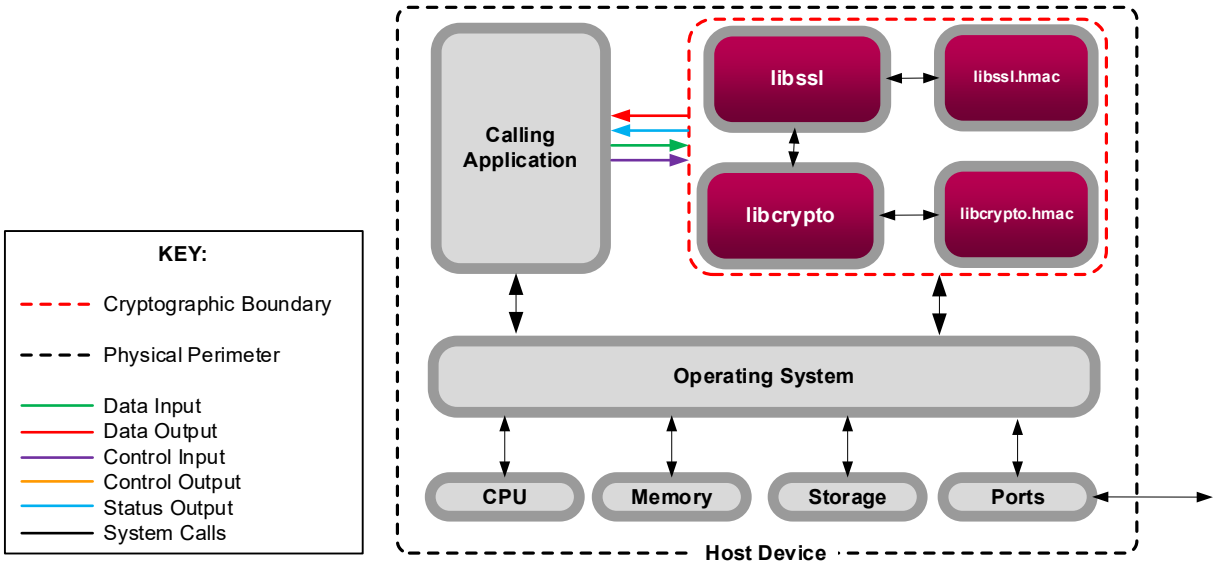

Figure 2 – Module Block Diagram (with Cryptographic Boundary)

2.4 Modes of Operation

The module supports two modes of operation: Approved and Non-Approved. The module operates in the Approved mode when all pre-operational self-tests have completed successfully, and only Approved services are invoked. Table 3 and Table 4 list the Approved and allowed algorithms, while Table 8 provides descriptions of the Approved services.

The module alternates on a service-by-service basis between Approved and Non-Approved modes of operation. The module will implicitly switch to the Non-Approved mode upon execution of a Non-Approved service. The module will implicitly switch back to the Approved mode upon execution of an Approved service. Table 5 lists the Non-Approved algorithms implemented by the module, while Table 9 below lists the services that constitute the Non-Approved mode.

When following the guidance in section 11.5 of this document, CSPs are not shared between Approved and non-Approved services and modes of operation.

3. Cryptographic Module Interfaces

FIPS 140-3 defines the following logical interfaces for cryptographic modules:

- Data Input
- Data Output
- Control Input
- Control Output
- Status Output

As a software library, the cryptographic module has no direct access to any of the host platform's physical ports, as it communicates only to the calling application via its well-defined API. A mapping of the FIPS-defined interfaces and the module's logical ports and interfaces can be found in Table 6. Note that the module does not output control information, and thus has no specified control output interface.

Table 6 – Ports and Interfaces

Physical Port	Logical Interface	Data That Passes Over Port/Interface
Physical data input port(s) of the tested platforms	Data Input • API input arguments that provide input data for processing	• Data to be encrypted, decrypted, signed, verified, or hashed • Keys to be used in cryptographic services • Random seed material for the module's DRBG • Keying material to be used as input to key establishment services
Physical data output port(s) of the tested platforms	Data Output • API output arguments that return generated or processed data back to the caller	• Data that has been encrypted, decrypted, or verified • Digital signatures • Hashes • Random values generated by the module's DRBG • Keys established using module's key establishment methods
Physical control input port(s) of the tested platforms	Control Input • API input arguments that are used to initialize and control the operation of the module	• API commands invoking cryptographic services • Modes, key sizes, etc. used with cryptographic services
Physical status output port(s) of the tested platforms	Status Output • API call return values	• Status information regarding the module • Status information regarding the invoked service/operation

4. Roles, Services, and Authentication

The sections below describe the module's authorized roles, services, and operator authentication methods.

4.1 Authorized Roles

The module supports a Crypto Officer (CO) that authorized operators can assume. The CO role performs cryptographic initialization or management functions and general security services.

The module also supports the following role(s):

- User – The User role performs general security services, including cryptographic operations and other approved security functions.

The module does not support multiple concurrent operators. The calling application that loaded the module is its only operator.

Table 7 below lists the supported roles, along with the services (including input and output) available to each role.

Table 7 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Show Status	API call parameters	Current operational status
CO	Perform Self-Tests On-Demand	Re-instantiate module; API call parameters	Status
CO	Zeroize	Restart calling application; reboot or power-cycle host platform	None
CO	Show Versioning Information	API call parameters	Module name, version
User	Perform Symmetric Encryption	API call parameters, key, plaintext	Status, ciphertext
User	Perform Symmetric Decryption	API call parameters, key, ciphertext	Status, plaintext
User	Generate Symmetric Digest	API call parameters, key, plaintext	Status, digest
User	Verify Symmetric Digest	API call parameters, digest	Status
User	Perform Authenticated Symmetric Encryption	API call parameters, key, plaintext	Status, ciphertext
User	Perform Authenticated Symmetric Decryption	API call parameters, key, ciphertext	Status, plaintext
User	Generate Random Number	API call parameters	Status, random bits
User	Perform Keyed Hash Operation	API call parameters, key, message	Status, MAC[46]
User	Perform Hash Operation	API call parameters, message	Status, hash
User	Generate DSA Domain Parameters	API call parameters	Status, domain parameters
User	Verify DSA Domain Parameters	API call parameters	Status, domain parameters
User	Generate Asymmetric Key Pair	API call parameters	Status, key pair
User	Verify ECDSA Public Key	API call parameters, key	Status
User	Generate Digital Signature	API call parameters, key, message	Status, signature

[46] MAC – Message Authentication Code

Role	Service	Input	Output
User	Verify Digital Signature	API call parameters, key, signature, message	Status
User	Perform Key Wrap	API call parameters, encryption key, key	Status, encrypted key
User	Perform Key Unwrap	API call parameters, decryption key, key	Status, decrypted key
User	Compute Shared Secret	API call parameters	Status, shared secret
User	Derive Keys via TLS KDF	API call parameters, TLS pre-master secret	Status, TLS keys
User	Perform Key Agreement Functions	API call parameters	Status, symmetric key
User	Derive Key via PBKDF2	API call parameters, password	Status, key

4.2 Authentication Methods

The module does not support authentication methods; operators implicitly assume an authorized role based on the service selected.

4.3 Services

Descriptions of the approved services available to the authorized roles are provided in Table 8 below.

This module is a software library that provides cryptographic functionality to calling applications. As such, the security functions provided by the module are considered the module's security services. Indicators for Approved services (in the case of this module, those security functions with algorithm validation certificates and all required self-tests) are provided via API return value.

When invoking a security function, the calling application provides inputs via an internal structure, or "context". Upon each service invocation, the module will determine if the invoked security function is an Approved service. To access the resulting value, the calling application must pass the finalized context to the indicator API associated with that security function (note the indicator check must be performed prior to any context cleanup is performed). The indicator API will return "1" to indicate the usage of an Approved service. Indicators for services providing Non-Approved security functions (as well as for services not requiring an indicator) will have a value other than "1", ensuring that the indicators for Approved services are unambiguous. Additional details on the APIs used for the Approved service indicators are provided in Appendix B below.

The keys and Sensitive Security Parameters (SSPs) listed in the table indicate the type of access required using the following notation:

- G = Generate: The module generates or derives the SSP.
- R = Read: The SSP is read from the module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the module.
- E = Execute: The module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The module zeroizes the SSP.

Table 8 – Approved Services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Show Status	Return Approved mode status	None	None	CO	N/A	N/A
Perform Self-Tests On-Demand	Perform pre-operational self-tests	None	Integrity Test Key - libcrypto Integrity Test Key - libssl	CO	Integrity Test Key – libcrypto – E Integrity Test Key - libssl – E	API return value
Zeroize	Zeroize and de-allocate memory containing sensitive data	None	All SSPs	CO	All SSPs – Z	N/A
Show Versioning Information	Return module versioning information	None	None	CO	N/A	N/A
Perform Symmetric Encryption	Encrypt plaintext data	AES-CBC (Cert. A3254) AES-CCM (Cert. A3254) AES-CFB1 (Cert. A3254) AES-CFB128 (Cert. A3254) AES-CFB8 (Cert. A3254) AES-CTR (Cert. A3254) AES-ECB (Cert. A3254) AES-GMAC (Cert. A3254) AES-KW (Cert. A3254) AES-KWP (Cert. A3254) AES-OFB (Cert. A3254) AES-XTS Testing Revision 2.0 (Cert. A3254)	AES key AES GMAC key AES XTS key	User	AES key – WE AES GMAC key – WE AES XTS key – WE	API return value
Perform Symmetric Decryption	Decrypt ciphertext data	AES-CBC (Cert. A3254) AES-CCM (Cert. A3254) AES-CFB1 (Cert. A3254) AES-CFB128 (Cert. A3254) AES-CFB8 (Cert. A3254) AES-CTR (Cert. A3254) AES-ECB (Cert. A3254) AES GMAC (Cert. A3254) AES-KW (Cert. A3254) AES-KWP (Cert. A3254) AES-OFB (Cert. A3254) AES-XTS Testing Revision 2.0 (Cert. A3254) TDES-CBC (Cert. A3254) TDES-CFB1 (Cert. A3254) TDES-CFB64 (Cert. A3254) TDES-CFB8 (Cert. A3254) TDES-ECB (Cert. A3254) TDES-OFB (Cert. A3254)	AES key AES GMAC key AES XTS key Triple-DES key	User	AES key – WE AES GMAC key – WE AES XTS key – WE Triple-DES key – WE	API return value
Generate Symmetric Digest	Generate symmetric digest	AES-CMAC (Cert. A3254)	AES CMAC key	User	AES CMAC key – WE	API return value
Verify Symmetric Digest	Verify symmetric digest	AES-CMAC (Cert. A3254) TDES-CMAC (Cert. A3254)	AES CMAC key Triple-DES CMAC key	User	AES CMAC key – WE Triple-DES CMAC key – WE	API return value
Perform Authenticated Symmetric Encryption	Encrypt plaintext using supplied AES GCM key and IV	AES-GCM (Cert. A3254)	AES GCM key AES GCM IV	User	AES GCM key – WE AES GCM IV – WE	API return value
Perform Authenticated Symmetric Decryption	Decrypt ciphertext using supplied AES GCM key and IV	AES-GCM (Cert. A3254)	AES GCM key AES GCM IV	User	AES GCM key – WE AES GCM IV – WE	API return value
Generate Random Number	Generate random bits using DRBG	Counter DRBG (Cert. A3254)	DRBG entropy input DRBG seed DRBG 'V' value DRBG 'Key' value	User	DRBG entropy input – WE DRBG seed – GE DRBG 'V' value – GE DRBG 'Key' value – GE	API return value
Perform Keyed Hash Operation	Compute a message authentication code	HMAC SHA-1 (Cert. A3254) HMAC SHA2-224 (Cert. A3254) HMAC SHA2-256 (Cert. A3254) HMAC SHA2-384 (Cert. A3254) HMAC SHA2-512 (Cert. A3254) HMAC SHA3-224 (Cert. A3254) HMAC SHA3-256 (Cert. A3254) HMAC SHA3-384 (Cert. A3254) HMAC SHA3-512 (Cert. A3254)	HMAC key	User	HMAC key – WE	API return value

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Perform Hash Operation	Compute a message digest	SHA-1 (Cert. A3254) SHA2-224 (Cert. A3254) SHA2-256 (Cert. A3254) SHA2-384 (Cert. A3254) SHA2-512 (Cert. A3254) SHA3-224 (Cert. A3254) SHA3-256 (Cert. A3254) SHA3-384 (Cert. A3254) SHA3-512 (Cert. A3254)	None	User	N/A	API return value
Generate DSA Domain Parameters	Generate DSA domain parameters	DSA PQGGen (FIPS186-4) (Cert. A3254)	None	User	N/A	API return value
Verify DSA Domain Parameters	Verify DSA domain parameters	DSA PQGVer (FIPS186-4) (Cert. A3254)	None	User	N/A	API return value
Generate Asymmetric Key Pair	Generate a public/private key pair	DSA KeyGen (FIPS186-4) (Cert. A3254) ECDSA KeyGen (FIPS186-4) (Cert. A3254) RSA KeyGen (FIPS186-4) (Cert. A3254)	DSA public key DSA private key ECDSA public key ECDSA private key RSA public key RSA private key	User	DSA public key – GR DSA private key – GR ECDSA public key – GR ECDSA private key – GR RSA public key – GR RSA private key – GR	API return value
Verify ECDSA Public Key	Verify an ECDSA public key	ECDSA KeyVer (FIPS186-4) (Cert. A3254)	ECDSA public key	User	ECDSA public key – W	API return value
Generate Digital Signature	Generate a digital signature	DSA SigGen (FIPS186-4) (Cert. A3254) ECDSA SigGen (FIPS186-4) (Cert. A3254) RSA SigGen (FIPS186-4) (Cert. A3254)	DSA private key ECDSA private key RSA private key	User	DSA private key – WE ECDSA private key – WE RSA private key – WE	API return value
Verify Digital Signature	Verify a digital signature	DSA SigVer (FIPS186-4) (Cert. A3254) ECDSA SigVer (FIPS186-4) (Cert. A3254) RSA SigVer (FIPS186-4) (Cert. A3254)	DSA public key ECDSA public key RSA public key	User	DSA public key – WE ECDSA public key – WE RSA public key – WE	API return value
Perform Key Wrap	Perform key wrap	KTS (AES-CCM) (Cert. A3254) KTS (AES-GCM) (Cert. A3254) KTS (AES-KW) (Cert. A3254) KTS (AES-KWP) (Cert. A3254)	AES key AES GCM key AES GCM IV	User	AES key – WE AES GCM key – WE AES GCM IV – WE	API return value
Perform Key Unwrap	Perform key unwrap	KTS (AES-CCM) (Cert. A3254) KTS (AES-GCM) (Cert. A3254) KTS (AES-KW) (Cert. A3254) KTS (AES-KWP) (Cert. A3254)	AES key AES GCM key AES GCM IV	User	AES key – WE AES GCM key – WE AES GCM IV – WE	API return value
Compute Shared Secret	Compute DH/ECDH shared secret suitable for use as input to a TLS KDF	KAS-ECC-SSC Sp800-56Ar3 (Cert. A3254) KAS-FFC-SSC Sp800-56Ar3 (Cert. A3254)	DH public key DH private key ECDH public key ECDH private key TLS pre-master secret	User	DH public key – WE DH private key – WE ECDH public key – WE ECDH private key – WE TLS pre-master secret – GE	API return value
Derive Keys via TLS KDF	Derive TLS session and integrity keys	TLS v1.2 KDF RFC7627 (Cert. A3254) TLS v1.3 KDF (Cert. A3253)	TLS pre-master secret TLS master secret AES key AES GCM key AES GCM IV HMAC key	User	TLS pre-master secret – WE TLS master secret – GE AES key – GR AES GCM key – GR AES GCM IV – GR HMAC key – GR	API return value
Perform Key Agreement Functions	Establish symmetric key using DH/ECDH key agreement	KAS (KAS-ECC_SSC/TLS v1.2 KDF RFC7627) (Certs. A3254, A3253) KAS (KAS-ECC_SSC/TLS v1.3 KDF) (Certs. A3254, A3253) KAS (KAS-FFC_SSC/TLS v1.2 KDF RFC7627) (Certs. A3254, A3253) KAS (KAS-FFC_SSC/TLS v1.3 KDF) (Certs. A3254, A3253)	DH public key DH private key ECDH public key ECDH private key TLS pre-master secret TLS master secret AES key AES GCM key AES GCM IV HMAC key	User	DH public key – WE DH private key – WE ECDH public key – WE ECDH private key – WE TLS pre-master secret – GE TLS master secret – GE AES key – GR AES GCM key – GR AES GCM IV – GR HMAC key – GR	API return value
Derive Key via PBKDF2	Derive key from PBKDF2	PBKDF2 (Cert. A3254)	Passphrase AES key Triple-DES key	User	Passphrase – WE AES key – GR Triple-DES key – GR	API return value

Per FIPS 140-3 Implementation Guidance 2.4.C, the **Show Status, **Zeroize**, and **Show Versioning Information** services do not require an Approve security service indicator.*

The following services/algorithms are allowed for legacy use only:

- Digital signature verification using ECDSA with curves B-163, K-163, and P-192

- Digital signature verification using DSA with key lengths of 1024 bits
- Digital signature verification using RSA with modulus lengths of 1024 bits
- Digital signature verification using SHA-1
- Symmetric decryption using two-key and three-key Triple DES
- Key unwrapping using two-key and three-key Triple DES
- MAC verification using two-key and three-key Triple DES CMAC

Table 9 below lists the Non-Approved services available to module operators.

Table 9 – Non-Approved Services

Service	Description	Algorithms Accessed	Role	Indicator
Perform Data Encryption (Non-Compliant)	Perform symmetric data encryption	ARIA, Blake2, Blowfish, Camellia, CAST, CAST5, ChaCha20, DES, IDEA, RC2, RC4, RC5, SEED, SM4, Triple-DES (non-compliant)	User	API return value
Perform Data Decryption (Non-Compliant)	Perform symmetric data decryption	ARIA, Blake2, Blowfish, Camellia, CAST, CAST5, ChaCha20, DES, IDEA, RC2, RC4, RC5, SEED, SM4	User	API return value
Perform MAC Operations (Non-Compliant)	Perform message authentication operations	Poly1305, Triple-DES/CMAC (non-compliant for MAC generation)	User	API return value
Perform Hash Operation (Non-Compliant)	Perform hash operation	MD2, MD4, MD5, RIPEMD, RMD160, SM2, SM3, SM4, Whirlpool	User	API return value
Perform Digital Signature Functions (Non-Compliant)	Perform digital signature functions	DSA (non-compliant), ECDSA (non-compliant), RSA (non-compliant)	User	API return value
Perform Key Agreement Functions (Non-Compliant)	Perform key agreement functions	DH (non-compliant), ECDH (non-compliant)	User	API return value
Perform Key Wrap (Non-Compliant)	Perform key wrap functions	Triple-DES/CMAC (non-compliant)	User	API return value
Perform Key Encapsulation (Non-Compliant)	Perform key encapsulation functions	RSA (non-compliant)	User	API return value
Perform Key Un-Encapsulation (Non-Compliant)	Perform key un-encapsulation functions	RSA (non-compliant)	User	API return value
Perform Key Derivation Functions (Non-Compliant)	Perform key derivation functions	HKDF, TLS v1.0/1.1 KDF (non-compliant)	User	API return value
Perform Authenticated Encryption/Decryption (Non-Compliant)	Perform authenticated encryption/decryption	AES-OCB	User	API return value
Perform Random Number Generation (Non-Compliant)	Perform random number generation	ANSI X9.31 RNG (with 128-bit AES core), Hash_DRBG (non-compliant), HMAC_DRBG (non-compliant)	User	API return value

Service	Description	Algorithms Accessed	Role	Indicator
Perform Key Pair Generation (Non-Compliant)	Perform key pair generation	DSA (non-compliant), ECDSA (non-compliant), EdDSA, RSA (non-compliant)	User	API return value

5. Software/Firmware Security

All software components within the cryptographic boundary are verified using an Approved integrity technique implemented within the cryptographic module itself. The module implements independent HMAC SHA2-256 digest checks to test the integrity of each library file; failure of the integrity test for either library file will cause the module to enter a critical error state. Details regarding the keys used for the integrity checks can be found in Table 10 below.

The module's integrity check is performed automatically at module instantiation (i.e., when the module is loaded into memory for execution) without action from the module operator. The CO can initiate the pre-operational tests on demand by re-instantiating the module or issuing the `FIPS_selftest()` API command.

CorSSL™ is not a standalone application; it is a cryptographic toolkit intended for use in a with a vendor's solution. The module will be linked to a host application, and the host application will be pre-installed onto a target platform by the vendor or installed onto target platforms by the end-user. The module requires no configuration steps to be performed by application developers or end-users, and no action is required from developers or end-users to initialize the module for operation. The module is designed with a default entry point (DEP) that ensures that the pre-operational tests and conditional CASTs are initiated automatically when the module is loaded.

6. Operational Environment

The CorSSL™ comprises a software cryptographic library that executes in a modifiable operational environment.

The cryptographic module has control over its own SSPs. The process and memory management functionality of the host device's OS prevents unauthorized access to plaintext private and secret keys, intermediate key generation values and other SSPs by external processes during module execution. The module only allows access to SSPs through its well-defined API. The operational environment provides the capability to separate individual application processes from each other by preventing uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless of whether this data is in the process memory or stored on persistent storage within the operational environment. Processes that are spawned by the module are owned by the module and are not owned by external processes/operators.

Please refer to section 2.1 of this document for a list/description of the applicable operational environments.

7. Physical Security

The cryptographic module is software module and does not include physical security mechanisms. Therefore, per *ISO/IEC 19790:2021* section 7.7.1, requirements for physical security are not applicable.

8. Non-Invasive Security

This section is not applicable. There is currently no approved non-invasive mitigation techniques referenced in *ISO/IEC 19790:2021* Annex F.

9. Sensitive Security Parameter Management

9.1 Keys and Other SSPs

The module supports the keys and other SSPs listed Table 10 below.

Table 10 – Keys

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroisation	Use & Related Keys
Keys								
Integrity Test Key - libcrypto (not an SSP)	256 bits	HMAC SHA2-256 (Cert. A2544)	-	-	Hardcoded in the module image	Plaintext in RAM	Not subject to zeroization requirements	Pre-operational verification of libcrypto library
Integrity Test Key - libssl (not an SSP)	256 bits	HMAC SHA2-256 (Cert. A2544)	-	-	Hardcoded in the module image	Plaintext in RAM	Not subject to zeroization requirements	Pre-operational verification of libssl library
AES Key (CSP)	Between 128 and 256 bits	AES-CBC (Cert. A3254) AES-CCM (Cert. A3254) AES-CFB1 (Cert. A3254) AES-CFB128 (Cert. A3254) AES-CFB8 (Cert. A3254) AES-CTR (Cert. A3254) AES-ECB (Cert. A3254) AES-KW (Cert. A3254) AES-KWP (Cert. A3254) AES-ECB (Cert. A3254) AES-KW (Cert. A3254) KTS (AES-CCM) (Cert. A3254) KTS (AES-GCM) (Cert. A3254) KTS (AES-KW) (Cert. A3254) KTS (AES-KWP)	-	Imported in plaintext via API parameter Never exported	Derived via TLS KDF	Plaintext in volatile memory	Unload module; Remove power	Symmetric Encryption, Decryption; Key Transport

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroisation	Use & Related Keys
		(Cert. A3254)						
AES GCM Key (CSP)	Between 128 and 256 bits	AES-GCM (Cert. A3254) KTS (AES-GCM) (Cert. A3254)	-	Imported in plaintext via API parameter Never exported	Derived via TLS KDF	Plaintext in volatile memory	Unload module; Remove power	Authenticated Symmetric Encryption, Decryption; Key Transport
AES XTS Key (CSP)	256 bits	AES-XTS (Cert. A3254)	-	Imported in plaintext via API parameter Never exported	-	Plaintext in volatile memory	Unload module; Remove power	Symmetric Encryption, Decryption
AES CMAC Key (CSP)	Between 128 and 256 bits	AES-CMAC (Cert. A3254)	-	Imported in plaintext via API parameter Never exported	-	Plaintext in volatile memory	Unload module; Remove power	MAC Generation, Verification
AES GMAC Key (CSP)	Between 128 and 256 bits	AES-GMAC (Cert. A3254)	-	Imported in plaintext via API parameter Never exported	-	Plaintext in volatile memory	Unload module; Remove power	MAC Generation, Verification
Triple-DES Key (CSP)	168 bits	TDES-CBC (Cert. A3254) TDES-CFB1 (Cert. A3254) TDES-CFB64 (Cert. A3254) TDES-CFB8 (Cert. A3254) TDES-ECB (Cert. A3254) TDES-OFB (Cert. A3254)	-	Imported in plaintext via API parameter Never exported	-	Plaintext in volatile memory	Unload module; Remove power	Symmetric Decryption; Key Unwrapping
Triple-DES CMAC Key (CSP)	168 bits	TDES-CMAC (Cert. A3254)	-	Imported in plaintext via API parameter Never exported	-	Plaintext in volatile memory	Unload module; Remove power	MAC Verification
HMAC Key (CSP)	112 bits (minimum)	HMAC SHA-1 (Cert. A3254) HMAC SHA2-224 (Cert. A3254) HMAC SHA2-256 (Cert. A3254) HMAC SHA2-384 (Cert. A3254) HMAC SHA2-512 (Cert. A3254) HMAC SHA3-224 (Cert. A3254) HMAC SHA3-256 (Cert. A3254) HMAC SHA3-384 (Cert. A3254) HMAC SHA3-512 (Cert. A3254)	-	Imported in plaintext via API parameter Never exported	Derived via TLS KDF	Plaintext in volatile memory	Unload module; Remove power	Keyed Hash
DSA Private Key (CSP)	112 or 128 bits	DSA SigGen (FIPS186-4) (Cert. A3254)	Generated internally via approved DRBG	Imported in plaintext via API parameter	-	Plaintext in volatile memory	Unload module; Remove power	Digital Signature Generation

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroisation	Use & Related Keys
				Exported in plaintext via API parameter				Paired with: DSA Public Key
DSA Public Key (PSP)	112 or 128 bits	DSA SigVer (FIPS186-4) (Cert. A3254)	Generated internally via approved DRBG	Imported in plaintext via API parameter Exported in plaintext via API parameter	-	Plaintext in volatile memory	Unload module; Remove power	Digital Signature Verification Paired with: DSA Private Key
ECDSA Private Key (CSP)	Between 112 and 256 bits	ECDSA SigGen (FIPS186-4) (Cert. A3254)	Generated internally via approved DRBG	Imported in plaintext via API parameter Exported in plaintext via API parameter	-	Plaintext in volatile memory	Unload module; Remove power	Digital Signature Generation Paired with: ECDSA Public Key
ECDSA Public Key (PSP)	Between 112 and 256 bits	ECDSA SigVer (FIPS186-4) (Cert. A3254)	Generated internally via approved DRBG	Imported in plaintext via API parameter Exported in plaintext via API parameter	-	Plaintext in volatile memory	Unload module; Remove power	Digital Signature Verification Paired with: ECDSA Private Key
RSA Private Key (CSP)	Between 112 and 150 bits	RSA SigGen (FIPS186-4) (Cert. A3254)	Generated internally via approved DRBG	Imported in plaintext via API parameter Exported in plaintext via API parameter	-	Plaintext in volatile memory	Unload module; Remove power	Digital Signature Generation Paired with: RSA Public Key
RSA Public Key (PSP)	Between 80 and 150 bits	RSA SigVer (FIPS186-4) (Cert. A3254)	Generated internally via approved DRBG	Imported in plaintext via API parameter Exported in plaintext via API parameter	-	Plaintext in volatile memory	Unload module; Remove power	Digital Signature Verification Paired with: RSA Private Key
DH Private Key (CSP)	112 bits	KAS-SSC-FFC Sp800-56Ar3 (Cert. A3254)	Generated internally via approved DRBG	Imported in plaintext via API parameter Exported in plaintext via API parameter	-	Plaintext in volatile memory	Unload module; Remove power	DH Shared Secret Computation Paired with: DH Public Key
DH Public Key (PSP)	112 bits	KAS-SSC-FFC Sp800-56Ar3 (Cert. A3254)	Generated internally via approved DRBG	Imported in plaintext via API parameter Exported in plaintext via API parameter	-	Plaintext in volatile memory	Unload module; Remove power	DH Shared Secret Computation Paired with: DH Public Key
ECDH Private Key (CSP)	Between 112 and 256 bits	KAS-SSC-ECC Sp800-56Ar3 (Cert. A3254)	Generated internally via approved DRBG	Imported in plaintext via API parameter Exported in plaintext via API parameter	-	Plaintext in volatile memory	Unload module; Remove power	ECDH Shared Secret Computation Paired with: ECDH Public Key
ECDH Public Key (PSP)	Between 112 and 256 bits	KAS-SSC-ECC Sp800-56Ar3 (Cert. A3254)	Generated internally via approved DRBG	Imported in plaintext via API parameter Exported in plaintext via API parameter	-	Plaintext in volatile memory	Unload module; Remove power	ECDH Shared Secret Computation Paired with: ECDH Private Key
Other SSPs								
Passphrase (PSP)	-	PBKDF2 (Cert. A3254)	-	Imported in plaintext via API parameter	-	Plaintext in volatile memory	Unload module; Remove power	Input to PBKDF for key derivation

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroisation	Use & Related Keys
				Never exported				
AES GCM IV (CSP)	-	AES-GCM (Cert. A3254)	Generated internally in compliance with the provisions of a peer-to-peer industry standard protocol	-	-	Plaintext in volatile memory	Unload module; Remove power	Initialization vector for AES GCM Paired with: AES GCM Key
TLS pre-master secret (CSP)	-	TLS v1.2 KDF RFC7627) (Cert. A3254) TLS v1.3 KDF (Cert. A3253)	-	Imported in plaintext via API parameter Never exported	-	Plaintext in volatile memory	Unload module; Remove power	Derivation of the TLS master secret
TLS master secret (CSP)	-	TLS v1.2 KDF RFC7627) (Cert. A3254) TLS v1.3 KDF (Cert. A3253)	-	-	Derived internally via TLS KDF	Plaintext in volatile memory	Unload module; Remove power	Derivation of the AES key, AES-GCM key, and HMAC key used for securing TLS connections Derived from: TLS pre-master secret
DRBG entropy input (CSP)	-	Counter DRBG (Cert. A3254)	-	Imported in plaintext via API parameter[47] Never exported	-	Plaintext in volatile memory	Unload module; Remove power	Entropy material for DRBG
DRBG seed (CSP)	-	Counter DRBG (Cert. A3254)	Generated internally using nonce along with DRBG entropy input	-	-	Plaintext in volatile memory	Unload module; Remove power	Seeding material for DRBG
DRBG 'V' value (CSP)	-	Counter DRBG (Cert. A3254)	Generated internally	-	-	Plaintext in volatile memory	Unload module; Remove power	State values for DRBG
DRBG 'Key' value (CSP)	-	Counter DRBG (Cert. A3254)	Generated internally	-	-	Plaintext in volatile memory	Unload module; Remove power	State values for DRBG

9.2 DRBGs

The module implements the following Approved DRBG:

- Counter-based DRBG

This DRBG is used to generate random values at the request of the calling application. Outputs from this DRBG are also used as seeds in the generation of asymmetric key pairs.

The module implements the following Non-Approved DRBGs (which are only available in the Non-Approved mode of operation):

- Hash-based DRBG (non-compliant)
- HMAC-based DRBG (non-compliant)
- ANSI X9.31 RNG (Non-Approved)

[47] The module obtains entropy input from the calling application (which is outside of the cryptographic boundary) but exercises no control over the amount or the quality of the obtained entropy. As such, there is no assurance of the minimum strength of generated SSPs (e.g., keys).

9.3 SSP Storage Techniques

There is no mechanism within the module's cryptographic boundary for the persistent storage of SSPs. The module stores DRBG state values for the lifetime of the DRBG instance. The module uses SSPs passed in on the stack by the calling application and does not store these SSPs beyond the lifetime of the API call.

9.4 SSP Zeroization Methods

Maintenance, including protection and zeroization, of any keys and CSPs that exist outside the module's cryptographic boundary are the responsibility of the end-user. For the zeroization of keys in volatile memory, module operators can unload the module from memory or reboot/power-cycle the host device.

9.5 RBG Entropy Sources

Table 11 below specifies the module's entropy sources.

Table 11 – Non-Deterministic Random Number Generation Specification

Entropy Sources	Minimum Number of Bits of Entropy	Details
Calling application	256	256 bits of seed material are provided to the module's DRBG by the calling application. The calling application and its entropy sources are outside the module's cryptographic boundary. The calling application shall use entropy sources that meet the security strength required for the CTR_DRBG as shown in *NIST SP 800-90Arev1*, Table 3. This entropy shall be supplied by means of a callback function. The callback function must return an error if the minimum entropy strength cannot be met.

10. Self-Tests

Both pre-operational and conditional self-tests are performed by the module. Pre-operational tests are performed between the time the cryptographic module is instantiated and before the module transitions to the operational state. Conditional self-tests are performed by the module during module operation when certain conditions exist. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

10.1 Pre-Operational Self-Tests

The module performs the following pre-operational self-test(s):

- Software integrity test for libcrypto (using an HMAC SHA2-256 digest)
- Software integrity test for libssl (using an HMAC SHA2-256 digest)

10.2 Conditional Self-Tests

The module performs the following conditional self-tests:

- Conditional cryptographic algorithm self-tests (CASTs)
  - AES ECB encrypt KAT[48] (128-bit)
  - AES ECB decrypt KAT[49] (128-bit)
  - AES CCM encrypt KAT (192-bit)
  - AES CCM decrypt KAT (192-bit)
  - AES GCM encrypt KAT (128-bit)
  - AES GCM decrypt KAT (128-bit)
  - AES XTS encrypt KAT (128/256-bit)
  - AES XTS decrypt KAT (128/256-bit)
  - AES CMAC generate KAT (CBC mode; 128/192/256-bit)
  - AES CMAC verify KAT (CBC mode; 128/192/256-bit)
  - Triple-DES ECB decrypt KAT (3-Key)
  - Triple-DES CMAC verify KAT (CBC mode; 3-Key)
  - CTR_DRBG KAT (AES, 256-bit, with derivation function)
  - CTR_DRBG generate/instantiate/reseed KAT (256-bit AES)
  - DSA sign KAT (2048-bit; SHA2-256)
  - DSA verify KAT (2048-bit; SHA2-256)
  - ECDSA sign KAT (P-224 and K-233 curves; SHA2-256)
  - ECDSA verify KAT (P-224 and K-233 curves; SHA2-256)
  - RSA sign KAT (2048-bit; SHA2-256; PKCS#1.5 scheme)
  - RSA verify KAT (2048-bit; SHA2-256; PKCS#1.5 scheme)
  - HMAC KATs (SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512)
  - SHA-1 KAT

[48] KAT – Known Answer Test
[49] KAT – Known Answer Test

- SHA-2 KATs (SHA2-224, SHA2-256, SHA2-384, SHA2-512)
- SHA-3 KAT (SHA3-256)
- FFC DH Shared Secret "Z" Computation KAT (2048-bit)
- ECC CDH Shared Secret "Z" Computation KAT (P-224 curve)
- PBKDF2 KAT (SHA2-256)
- TLS 1.2 KDF KAT
- TLS 1.3 KDF KAT

To ensure all CASTs are performed prior to the first operational use of the associated algorithm, all CASTs are performed during the module's initial power-up sequence. The SHA and HMAC KATs are performed prior to the pre-operational software integrity test; all other CASTs are executed after the successful completion of the software integrity test.

- Conditional pair-wise consistency tests (PCTs)
  - DSA sign/verify PCT[50]
  - ECDSA sign/verify PCT
  - RSA sign/verify PCT
  - DH key generation PCT
  - ECDH key generation PCT

- Conditional critical functions tests
  - XTS AES duplicate key test

10.3 On-Demand Self-Testing

The CO can initiate the pre-operational self-tests and conditional CASTs on demand for periodic testing of the module by re-instantiating the module, rebooting/power-cycling the host device, or issuing the `FIPS_selftest()` API command.

10.4 Self-Test Failure Handling

The module reaches the critical error state when any self-test fails. Upon test failure, the module immediately terminates the calling application's API call with a returned error code and sets an internal flag, signaling the error condition. For any subsequent request made by the calling application for cryptographic services, the module will return a failure indicator, thereby disabling all access to its cryptographic functions, sensitive security parameters (SSPs), and data output services while the error condition persists.

To recover, the module must be re-instantiated by the calling application. If the pre-operational self-tests complete successfully, then the module can resume normal operations. If the module continues to experience self-test failures after reinitializing, then the module will not be able to resume normal operations, and the CO should contact Corsec Security, Inc. for assistance.

[50] PCT – Pairwise Consistency Test

11. Life-Cycle Assurance

The sections below describe how to ensure the module is operating in its validated configuration, including the following:

- Procedures for secure installation, initialization, startup, and operation of the module
- Maintenance requirements
- Administrator and non-Administrator guidance

Operating the module without following the guidance herein (including the use of undocumented services) will result in non-compliant behavior and is outside the scope of this Security Policy.

11.1 Secure Installation

The module is distributed as a package containing the binaries and HMAC digest files that the Crypto Officer is to install onto a target platform specified in section 2.1 or one where portability is maintained.

11.2 Initialization

This module is designed to support third-party vendor applications, and these applications are the sole consumers of the cryptographic services provided by the module. No end-user action is required to initialize the module for operation; the calling application performs any actions required to initialization the module.

The pre-operational integrity test and conditional CASTs are performed automatically via a default entry point (DEP) when the module is loaded for execution, without any specific action from the calling application or the end-user. End-users have no means to short-circuit or bypass these actions. Failure of any of the initialization actions will result in a failure of the module to load for execution.

11.3 Startup

No startup steps are required to be performed by end-users.

11.4 Administrator Guidance

There are no specific management activities required of the CO role to ensure that the module runs securely. If any irregular activity is observed, or if the module is consistently reporting errors, then Corsec Customer Support should be contacted.

The following list provides additional guidance for the CO:

- The `fips_post_status()` API can be used to determine the module's operational status. A non-zero return value indicates that the module has passed all pre-operational self-tests and is currently in its Approved mode.

- The `OpenSSL_version()` API can be used to obtain the module's versioning information. This information will include the module name and version, which can be correlated with the module's validation record.

11.5 Non-Administrator Guidance

The following list provides additional policies for the User role:

- The module uses PBKDF2 option 1a from section 5.4 of *NIST SP 800-132*. The iteration count shall be selected as large as possible, as long as the time required to generate the resultant key is acceptable for module operators. The minimum iteration count shall be 1000.

  The length of the password/passphrase used in the PBKDF shall be of at least 20 characters, and shall consist of lower-case, upper-case, and numeric characters. The upper bound for the probability of guessing the value is estimated to be $1/62^{20} = 10^{-36}$, which is less than 2^{-112}.

  As specified in *NIST SP 800-132*, keys derived from passwords/passphrases may only be used in storage applications.

- The cryptographic module's services are designed to be provided to a calling application. Excluding the use of the NIST-defined elliptic curves as trusted third-party domain parameters, all other assurances from *FIPS PUB 186-4* (including those required of the intended signatory and the signature verifier) are outside the scope of the module and are the responsibility of the calling application.

- The module performs assurances for its key agreement schemes as specified in the following sections of *NIST SP 800-56Arev3:*

  - Section 5.5.2 (for assurances of domain parameter validity)
  - Section 5.6.2.1 (for assurances required by the key pair owner)

  The module includes the capability to provide the required recipient assurance of ephemeral public key validity specified in section 5.6.2.2.2 of *NIST SP 800-56Arev3*. However, since public keys from other modules are not received directly by this module (those keys are received by the calling application), the module has no knowledge of when a public key is received. Invocation of the proper module services to validate another module's public key is the responsibility of the calling application.

- AES GCM encryption is used in the context of the TLS protocol versions 1.2 and 1.3. To meet the AES GCM (key/IV) pair uniqueness requirements from *NIST SP 800-38D*, the module complies with *FIPS 140-3 IG* C.H as follows:

  - For TLS v1.2, the counter portion of the IV is strictly increasing. When the IV exhausts the maximum number of possible values for a given session key, a failure in encryption will occur and a handshake to establish a new encryption key will be required. It is the responsibility of the module operator (i.e., the first party, client, or server) to trigger this handshake in accordance with *RFC 5246* when this condition is encountered.

The module supports acceptable AES GCM cipher suites from section 3.3.1 of *NIST SP 800-52rev2*. The AES GCM IV generation is performed internally, is compliant with the *RFC 5288,* and shall only be used for the TLS 1.2 protocol to be compliant with scenario 1 in *FIPS 140-3 IG* C.H; thus, the module is compliant with *NIST SP 800-52rev2*.

- For TLS v1.3, a 64-bit sequence number is maintained separately for reading and writing records. Each sequence number is set to zero at the beginning of a connection and is incremented by one after reading or writing each record. Because the size of sequence numbers is 64-bit, they should not wrap. If a sequence number needs to wrap, the TLS implementation is responsible for either rekeying or terminating the connection.

  The module supports the TLS 1.3 GCM cipher suite from section 3.3.1.2 of *NIST SP 800-52rev2*. The AES GCM IV generation is performed internally, is compliant with the *RFC 8446*, and shall only be used for the TLS 1.3 protocol to be compliant with scenario 5 in *FIPS 140-3 IG* C.H; thus, the module is compliant with *NIST SP 800-52rev2*.

The module also supports internal IV generation using the module's Approved DRBG. The IV is at least 96 bits in length per section 8.2.2 of *NIST SP 800-38D*. Per *NIST SP 800-38D* and scenario 2 of *FIPS 140-3 IG* C.H, the DRBG generates outputs such that the (key/IV) pair collision probability is less than 2^{-32}.

In the event that power to the module is lost and subsequently restored, the calling application must ensure that any AES GCM keys used for encryption or decryption are re-distributed.

- The length of a single data unit encrypted or decrypted with the AES-XTS shall not exceed 2^{20} AES blocks; that is, 16 MB of data per AES-XTS instance. An XTS instance is defined in section 4 of *NIST SP 800-38E*.

  The AES-XTS mode shall only be used for the cryptographic protection of data on storage devices. The AES-XTS shall not be used for other purposes, such as the encryption of data in transit. The module implements the check to ensure that the two AES keys used in the XTS-AES algorithm are not identical.

- The calling application is responsible for ensuring that CSPs are not shared between Approved and Non-Approved services and modes of operation.

- The calling application is responsible for using entropy sources that meet the minimum security strength of 112 bits required for the CTR_DRBG as shown in *NIST SP 800-90Arev1*, Table 3.

11.6 Common Vulnerabilities and Exposures

The Common Vulnerabilities and Exposures (CVE) program is a dictionary or glossary of vulnerabilities that have been identified for specific code bases, such as software applications or open libraries. This list allows interested parties to acquire the details of vulnerabilities by referring to a unique identifier known as the CVE ID.

11.6.1 Applicable CVEs

The following table lists the applicable CVEs impacting the module, as well as methods of mitigation.

Table 12 – CVEs

CVE Number	Severity	Mitigation
CVE-2023-3446	Low	Before calling DH_check(), DH_check_ex(), or EVP_PKEY_param_check(), operator should verify that the DH key or DH parameters were obtained from a trusted source.
CVE-2023-3817	Low	Before calling DH_check(), DH_check_ex(), or EVP_PKEY_param_check(), operator should verify that the DH key or DH parameters were obtained from a trusted source.
CVE-2024-4741	Low	Applications should not directly call the SSL_free_buffers function.

11.6.2 CVE Mitigation Plan

Post-submission, the module has been continually updated to provide mitigations for the CVEs listed above. These mitigations will be included in a future revalidation of the module.

12. Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-3 Level 1 requirements for this validation.

Appendix A. Acronyms and Abbreviations

Table 13 below provides definitions for the acronyms and abbreviations used in this document.

Table 13 – Acronyms and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CAST	Cryptographic Algorithm Self-Test
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CCM	Counter with Cipher Block Chaining - Message Authentication Code
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CMAC	Cipher-Based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DEP	Default Entry Point
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI/EMC	Electromagnetic Interference /Electromagnetic Compatibility
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode

Term	Definition
GMAC	Galois Message Authentication Code
GPC	General-Purpose Computer
HMAC	(keyed-) Hash Message Authentication Code
KAS	Key Agreement Scheme
KAT	Known Answer Test
KTS	Key Transport Scheme
KW	Key Wrap
KWP	Key Wrap with Padding
MD	Message Digest
NIST	National Institute of Standards and Technology
OCB	Offset Codebook
OFB	Output Feedback
OS	Operating System
PBKDF	Password-Based Key Derivation Function
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standard
PSS	Probabilistic Signature Scheme
PUB	Publication
RC	Rivest Cipher
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SHAKE	Secure Hash Algorithm KECCAK
SHS	Secure Hash Standard
SP	Special Publication
TLS	Transport Layer Security
XEX	XOR Encrypt XOR
XTS	XEX-Based Tweaked-Codebook Mode with Ciphertext Stealing

Appendix B. Approved Service Indicators

This appendix specifies the APIs that are externally accessible and return the Approved service indicators.

Synopsis

```
#include <openssl/service_indicator.h>
#include <openssl/ssl.h>

int EVP_cipher_get_service_indicator(EVP_CIPHER_CTX *ctx);
int DSA_get_service_indicator(DSA * ptr_dsa, DSA_MODES_t mode);
int RSA_key_get_service_indicator(RSA * ptr_rsa);
int PBKDF_get_service_indicator();
int EVP_Digest_get_service_indicator(EVP_MD_CTX *ctx);
int EC_key_get_service_indicator(EC_KEY *ec_key);
int CMAC_get_service_indicator(CMAC_CTX *cmac_ctx, CMAC_MODE_t mode);
int HMAC_get_service_indicator(HMAC_CTX *ctx);
int TLSKDF_get_service_indicator(EVP_PKEY_CTX *tls_ctx);
int TLS1_3_kdf_get_service_indicator(EVP_MD *md);
int TLS1_3_get_service_indicator(SSL *s);
int DRBG_get_service_indicator(RAND_DRBG *drbg);
```

Description

These APIs are high-level interfaces that return the Approved service indicator value based on the parameter(s) passed to them.

- **EVP_cipher_get_service_indicator()** is used to return the Approved service indicator status for block ciphers like AES and Triple-DES.
- **DSA_get_service_indicator()** is used to return the Approved service indicator status for the DSA algorithm and its modes. You must include the mode you want the indicator for, which are specified in the DSA_MODES_t enum.
- **RSA_key_get_service_indicator()** is used to return the Approved service indicator status for RSA algorithm and its modes.
- **PBKDF_get_service_indicator()** is used to return the Approved service indicator status for PBKDF usage.
- **EVP_Digest_get_service_indicator()** is used to return the Approved service indicator status for SHS algorithms like SHA-1 and SHAKE.
- **EC_key_get_service_indicator()** is used to return the Approved service indicator status for elliptic curve algorithms like ECDSA and its modes.

- **CMAC_get_service_indicator()** is used to return the Approved service indicator status for CMAC requests that use AES or Triple-DES. You must include the mode you want the indicator for, which are specified in the CMAC_MODE_t enum.

- **HMAC_get_service_indicator()** is used to return the Approved service indicator status for HMAC requests and the associated SHS algorithm.

- **TLSKDF_get_service_indicator()** is used to return the Approved service indicator status for TLS KDF usage excluding TLS 1.3.

- **TLS1_3_kdf_get_service_indicator()** is used to return the Approved service indicator status for TLS 1.3 KDF usage. This function requires the ssl.h file and is used to call the TLS1_3_get_service_indicator() function because of the SSL struct requirement. You cannot call TLS1_3_get_service_indicator() directly unless you have the SSL struct that was used.

- **DRBG_get_service_indicator()** is used to return the Approved service indicator status for DRBG usage.

Return Values

Each function returns “1” when indicating the usage of approved services and “0” for Non-Approved services.

Notes

When calling a I<get> function, always call it after the variables have been finalized but before they are freed or destroyed.

Examples

The code sample below provides examples of how to check the Approved service indicators for Triple-DES (3-key, in ECB mode) encryption and decryption:

```
int 3des_indicator_test()
 {
    static EVP_CIPHER *cipher = NULL;
    static EVP_CIPHER_CTX *ctx;
    int outLen;
    unsigned char pltmp[8];
    unsigned char citmp[8];
          unsigned char key[] = { 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,
                                  19,20,21,22,23,24};
          unsigned char plaintext[] = { 'e', 't', 'a', 'o', 'n', 'r', 'i', 's' };
    cipher = EVP_des_ede3_ecb();

    //Encrypt
    ctx = EVP_CIPHER_CTX_new();
    EVP_EncryptInit_ex(ctx, cipher, NULL, key, NULL);
    EVP_CIPHER_CTX_set_key_length(ctx, 24);
    EVP_EncryptUpdate(ctx, citmp, &outLen, plaintext, 8);

    // Check the indicator
    int NID = EVP_CIPHER_CTX_nid(ctx);
    fprintf(stdout,"EVP_des_ede3_ecb (NID %i) encrypt indicator = %i\n", NID, EVP_cipher_get_service_indicator(ctx));
    EVP_CIPHER_CTX_cleanup(ctx);
```

```
    //Decrypt
    ctx = EVP_CIPHER_CTX_new();
    EVP_DecryptInit_ex(ctx, cipher, NULL, key, NULL);
    EVP_CIPHER_CTX_set_key_length(ctx, 24);
    EVP_DecryptUpdate(ctx, pltmp, &outLen, citmp, 8);

    // Check the indicator
    fprintf(stdout,"EVP_des_ede3_ecb (NID %i) decrypt indicator = %i\n", NID, EVP_cipher_get_service_indicator(ctx));
    EVP_CIPHER_CTX_cleanup(ctx);
    EVP_CIPHER_CTX_free(ctx);
}
```

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com