

Qualcomm Technologies, Inc.

Qualcomm® Trusted Execution Environment (TEE) Software Cryptographic Library

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1

Last Update: 07-20-2026

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

www.atsec.com

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
1.3 Additional Information 5
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 9
2.6 Security Function Implementations 13
2.7 Algorithm Specific Information 15
2.7.1 AES-XTS 15
2.7.2 PBKDF 15
2.7.3 RSA Modulus Sizes 15
2.7.4 Use of SHA-1 15
2.7.5 FIPS 186-4 Transition 15
2.8 RBG and Entropy 16
2.9 Key Generation 16
2.10 Key Establishment 16
2.11 Industry Protocols 16
3 Cryptographic Module Interfaces 17
3.1 Ports and Interfaces 17
4 Roles, Services, and Authentication 18
4.1 Authentication Methods 18
4.2 Roles 18
4.3 Approved Services 18
4.4 Non-Approved Services 22
4.5 External Software/Firmware Loaded 24
5 Software/Firmware Security 25
5.1 Integrity Techniques 25
5.2 Initiate on Demand 25

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

6 Operational Environment 26
6.1 Operational Environment Type and Requirements 26
6.2 Configuration Settings and Restrictions 26
7 Physical Security 27
7.1 Mechanisms and Actions Required 27
8 Non-Invasive Security 28
9 Sensitive Security Parameters Management 29
9.1 Storage Areas 29
9.2 SSP Input-Output Methods 29
9.3 SSP Zeroization Methods 29
9.4 SSPs 30
10 Self-Tests 33
10.1 Pre-Operational Self-Tests 33
10.2 Conditional Self-Tests 33
10.3 Periodic Self-Test Information 34
10.4 Error States 35
10.5 Operator Initiation of Self-Tests 36
11 Life-Cycle Assurance 37
11.1 Installation, Initialization, and Startup Procedures 37
11.2 Administrator Guidance 37
11.3 Non-Administrator Guidance 38
11.4 End of Life 38
12 Mitigation of Other Attacks 39
12.1 Attack List 39
Appendix A. Glossary and Abbreviations 40
Appendix B. References 41

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) 8

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Table 3: Tested Module Identification – Hybrid Disjoint Hardware 8
Table 4: Tested Operational Environments - Software, Firmware, Hybrid 8
Table 5: Modes List and Description 9
Table 6: Approved Algorithms 12
Table 7: Vendor-Affirmed Algorithms 12
Table 8: Non-Approved, Not Allowed Algorithms 13
Table 9: Security Function Implementations 15
Table 10: Ports and Interfaces 17
Table 11: Roles 18
Table 12: Approved Services 22
Table 13: Non-Approved Services 23
Table 14: Mechanisms and Actions Required 27
Table 15: Storage Areas 29
Table 16: SSP Input-Output Methods 29
Table 17: SSP Zeroization Methods 29
Table 18: SSP Table 1 31
Table 19: SSP Table 2 32
Table 20: Pre-Operational Self-Tests 33
Table 21: Conditional Self-Tests 34
Table 22: Pre-Operational Periodic Information 35
Table 23: Conditional Periodic Information 35
Table 24: Error States 35

List of Figures

Figure 1: Block diagram 7
Figure 2: Snapdragon® 8 Gen 2 Mobile Platform 7

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

1 General

1.1 Overview

This Security Policy describes the features and design of the module named Qualcomm® Trusted Execution Environment (TEE) Software Cryptographic Library using the terminology contained in the FIPS 140-3 specification. The FIPS 140-3 Security Requirements for Cryptographic Module specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST/CCCS Cryptographic Module Validation Program (CMVP) validates cryptographic module to FIPS 140-3. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

This Non-Proprietary Security Policy may be reproduced and distributed, but only whole and intact and including this notice. Other documentation is proprietary to their authors.

1.2 Security Levels

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	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	1
	Overall Level	1

Table 1: Security Levels

1.3 Additional Information

In preparing the Security Policy document, the laboratory formatted the vendor-supplied documentation for consolidation without altering the technical statements therein contained. The further refining of the Security Policy document was conducted iteratively throughout the conformance testing, wherein the Security Policy was submitted to the vendor, who would then edit, modify, and add technical contents. The vendor would also supply additional documentation, which the laboratory formatted into the existing Security Policy, and resubmitted to the vendor for their final editing.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is used by secure applications. It is part of the common library and provides APIs to the secure applications for cryptography and hashing functions.

The Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library uses the Arm® v8 instruction set architecture for hash operations for SHA-1, SHA-256, and SHA-512.

The Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library cryptographic module (hereafter referred to as "the module") is a hybrid software single-chip cryptographic module that consists of components listed in the table below. The Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is bound to the on-chip Pseudo Random Number Generator module with version 3.1.0 validated to FIPS 140-3 under Cert. #4778. The existing validated module which this module is bound to resides within the same physical perimeter. Sections of this Security Policy which relate to the existing validated module are marked with [EVM] as per IG 1.A.

Module Type: Software-hybrid

Module Embodiment: Single Chip

Cryptographic Boundary:

The cryptographic boundary of the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is shown by a red box in Figure 1 below.

Tested Operational Environment's Physical Perimeter (TOEPP):

The physical perimeter of the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is the physical perimeter of the device that contains it. Consequently, the embodiment of the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is a single-chip cryptographic module. Figure 1 shows a block diagram of the module, with the cryptographic boundary indicated in red, the bound module in the dark green box, and the physical perimeter in black.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

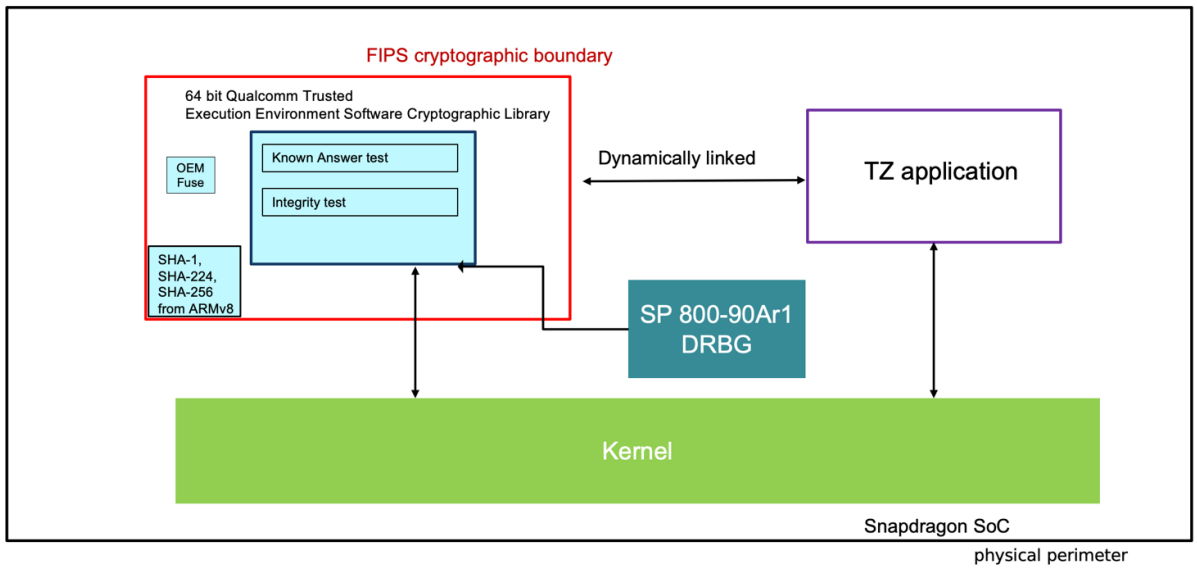


Figure 1: Block diagram

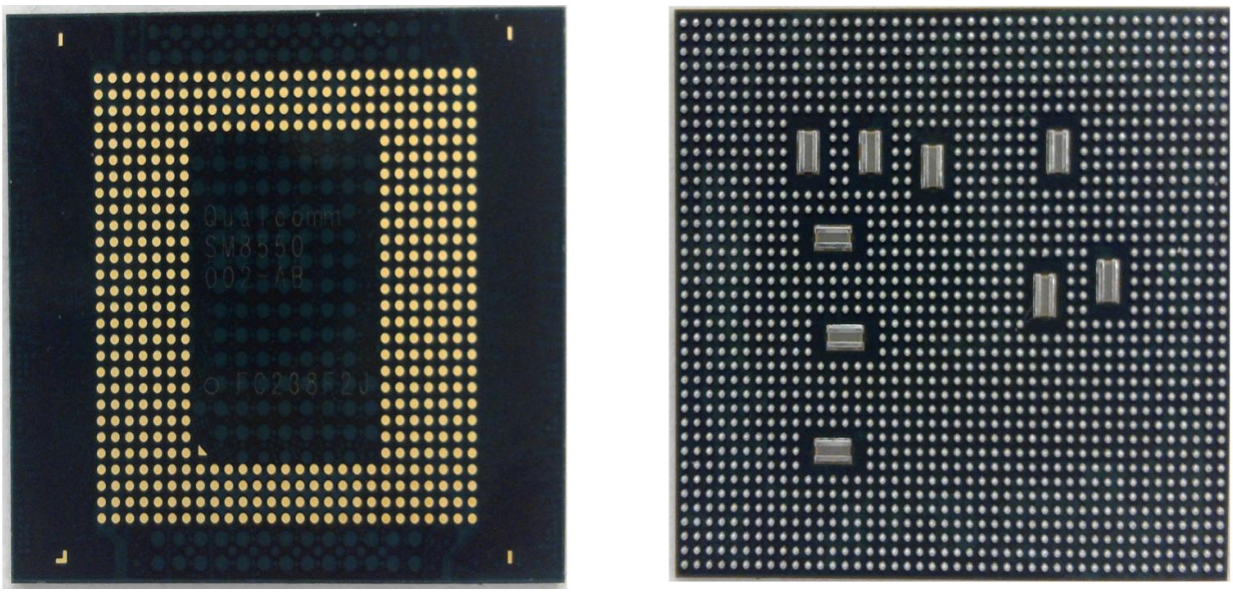


Figure 2: Snapdragon® 8 Gen 2 Mobile Platform

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Package or File Name	Software/ Firmware Version	Features	Integrity Test
Qualcomm® Trusted Execution Environment (TEE) Software Cryptographic Library	513b121d8d789b1e5a7fd22743994650a94b222d108c33b0d82c98ff282bac64	N/A	HMAC-SHA2-256

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Snapdragon 8 Gen 2 Mobile Platform	3.1.0	N/A	Snapdragon 8 Gen 2 Mobile Platform	N/A

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/ PAI	Hypervisor or Host OS	Version(s)
Qualcomm® Trusted Execution Environment (TEE) TZ.XF.5.24	Snapdragon 8 Gen 2 Mobile Platform	Snapdragon 8 Gen 2 Mobile Platform	No	N/A	513b121d8d789b1e5a7fd22743994650a94b222d108c33b0d82c98ff282bac64

Table 4: Tested Operational Environments - Software, Firmware, Hybrid

2.3 Excluded Components

There are no components within the cryptographic boundary excluded from the FIPS 140-3 requirements.

2.4 Modes of Operation

Modes List and Description:

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Mode Name	Description	Types of Services	Status Indicator
Approved	Automatically entered whenever an approved service is requested	Approved	qsee_get_fips_approval_status() returns 0 when called with appropriate enum
Non-Approved	Automatically entered whenever a non-approved service is requested	Non-Approved	none

Table 5: Modes List and Description

The module implements two modes of operation: (1) the approved mode, in which the approved services are available; and (2) the non-approved mode, in which the non-approved services are available. The current mode of operation of the module can be inferred by the service indicator, which indicates the approved state of the current service being invoked. No configuration is necessary for the module to operate and remain in the approved or non-approved modes. All SSPs are kept separate between the two modes.

Mode Change Instructions and Status:

To transition to the non-approved mode, one of the non-approved services in section 4 of this security policy can be requested. To transition to the approved mode, one of the approved services in Section 4.3 of this security policy can be requested.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A2940	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CBC-CS2	A2940	Direction - decrypt, encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 256-65536 Increment 8	SP 800-38A
AES-CCM	A2940	Key Length - 128, 192, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0, 256, 65536	SP 800-38C
AES-CFB128	A2940	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A2940	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 8-128 Increment	SP 800-38A

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Algorithm	CAVP Cert	Properties	Reference
		8 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	
AES-ECB	A2940	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-OFB	A2940	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A2940	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
ECDSA KeyGen (FIPS186-4)	A2940	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A2940	Component - No, Yes Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A2940	Component - No Curve - P-192, P-224, P-256, P-384, P-521 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
Hash DRBG	A2945	Prediction Resistance - No Supports Reseed - No Mode - SHA2-256 Entropy Input - Entropy Input: 256 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0, 32 Additional Input - Additional Input: 0, 0 Returned Bits - 1024	SP 800-90A Rev. 1
HMAC-SHA-1	A2940	MAC - MAC: 160 Key Length - Key Length: 8-4096 Increment 8	FIPS 198-1
HMAC-SHA2-224	A2940	MAC - MAC: 224 Key Length - Key Length: 8-4096 Increment 8	FIPS 198-1

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-256	A2940	MAC - MAC: 256 Key Length - Key Length: 8-4096 Increment 8	FIPS 198-1
HMAC-SHA2-384	A2940	MAC - MAC: 384 Key Length - Key Length: 8-4096 Increment 8	FIPS 198-1
HMAC-SHA2-512	A2940	MAC - MAC: 512 Key Length - Key Length: 8-4096 Increment 8	FIPS 198-1
PBKDF	A2940	Iteration Count - Iteration Count: 10-1000 Increment 1 HMAC Algorithm - SHA-1, SHA2-256, SHA2-512 Password Length - Password Length: 8-128 Increment 1 Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 128-4096 Increment 8	SP 800-132
RSA KeyGen (FIPS186-4)	A2940	Key Generation Mode - B.3.3 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Info Generated By Server - No Public Exponent Mode - Random Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A2940	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA2-224	FIPS 186-4
RSA Signature Primitive (CVL)	A2940	Private Key Format - standard Public Exponent Mode - fixed Fixed Public Exponent - 010001	FIPS 186-5
RSA SigVer (FIPS186-4)	A2940	Signature Type - PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4
SHA-1	A2940	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-224	A2940	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A2940	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A2940	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A2940	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric RSA modulus sizes:2048, 3072, 4096 bits ECDSA curves:P-224, P-256, P-384, P-521	N/A	SP 800-133 Rev. 2 Section 4 Example 1 with V=0

Table 7: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
DES	Encryption, Decryption
Triple DES	Encryption, Decryption
GCM/GMAC (external IV)	Encryption, Decryption, Message Authentication
HMAC (key sizes below 112 bits)	Message Authentication
RIPEMD-160	Hash
MD5	MD5
SM2	Signature Generation, Signature Verification, Hybrid Encryption, Hybrid Decryption
SM3	Hash
SM4	Encryption, Decryption
SHA-1, SHA-224 and SHA-256 (software) (not CAVP tested)	Hash

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Use and Function
ECDSA (secp160r1, P-192)	ECDSA (secp160r1, P-192)
ECDSA (secp160r1)	Signature Verification
ECDSA (P-192, P-224, P-256, P-384 and P-521)	Signature Verification - Component
Elliptic Curve Integrated Encryption Scheme (ECIES)	Hybrid Encryption, Hybrid Decryption
RSA-OAEP (not CAVP tested)	Key Encapsulation
RSA (1024 bit modulus)	Key Pair Generation, Signature Generation
Ed25519 (not CAVP tested)	Key Pair Generation, Signature Generation, Signature Verification
ECDH (no key assurances)	Shared Secret Computation
HKDF	Key Derivation

Table 8: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Symmetric Encryption	BC-UnAuthEncrypt	Encryption		AES-CBC: (A2940) AES-CBC-CS2: (A2940) AES-CFB128: (A2940) AES-CTR: (A2940) AES-ECB: (A2940) AES-OFB: (A2940) AES-XTS Testing Revision 2.0: (A2940)
Symmetric Decryption	BC-UnAuthDecrypt	Decryption		AES-CBC: (A2940) AES-CBC-CS2: (A2940) AES-CFB128: (A2940) AES-CTR: (A2940) AES-ECB: (A2940) AES-OFB: (A2940) AES-XTS Testing Revision 2.0: (A2940)

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Type	Description	Properties	Algorithms
Hashing	SHA	Hash		SHA-1: (A2940) SHA2-224: (A2940) SHA2-256: (A2940) SHA2-384: (A2940) SHA2-512: (A2940)
Message Authentication	BC-Auth	Computes the hash value of data		HMAC-SHA-1: (A2940) HMAC-SHA2-224: (A2940) HMAC-SHA2-256: (A2940) HMAC-SHA2-384: (A2940) HMAC-SHA2-512: (A2940)
Asymmetric Keygen	AsymKeyPair-KeyGen CKG	Asymmetric keygen		ECDSA KeyGen (FIPS186-4): (A2940) RSA KeyGen (FIPS186-4): (A2940) CKG: ()
Asymmetric Sign	DigSig-SigGen	Asymmetric siggen		ECDSA SigGen (FIPS186-4): (A2940) RSA SigGen (FIPS186-4): (A2940) RSA Signature Primitive: (A2940)
Asymmetric Verify	DigSig-SigVer	Asymmetric sigver		ECDSA SigVer (FIPS186-4): (A2940) RSA SigVer (FIPS186-4): (A2940)
Key Derivation	PBKDF	Password key derivation		PBKDF: (A2940)
Authenticated Symmetric Encryption	BC-AuthEncrypt	Authenticated symmetric encryption with CCM		AES-CCM: (A2940)
Authenticated Symmetric Decryption	BC-AuthDecrypt	Authenticated symmetric decryption with CCM		AES-CCM: (A2940)

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Type	Description	Properties	Algorithms
Random Number Generation	DRBG	[EVM] Random number generation		Hash DRBG: (A2945)

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES-XTS

AES-XTS is only approved for storage purposes. Per IG C.I, AES-XTS Key_1 and Key_2, when entered into the module by the operator, shall be generated and/or established independently of each other according to the rules for component symmetric keys from NIST SP 800-133rev2, Sec. 6.3. for an approved use of AES-XTS.

The length of a single data unit encrypted with the AES-XTS shall not exceed 2^{20} AES blocks. In compliance with IG C.I, the module verifies that the two keys used in AES-XTS are not equal.

2.7.2 PBKDF

The Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library implements Password-Based Key Derivation version 2 (PBKDF) as defined in SP800-132. The PBKDF function is provided as a service and returns the key derived from the provided password to the caller. The supported option is 1a from Section 5.4 of SP 800-132, whereby the Master Key (MK) is used directly as the Data Protection Key (DPK). The length of the salt should be at least 128 bits and the length of the password or passphrase should be at least 8 characters, which provides the probability of guessing this password or passphrase to be $(1/10)^8$ assuming a scenario where all characters are digits. The caller shall observe all requirements and should consider all recommendations specified in SP800-132 with respect to the strength of the generated key, including the length and source of the password, the length of the salt, and the number of iterations. The keys derived from passwords, as shown in SP 800-132, may only be used for storage applications.

2.7.3 RSA Modulus Sizes

In compliance with IG C.F, the module supports RSA signature generation with modulus lengths of 2048, 3072, and 4096 bits, and RSA signature generation has been CAVP tested for all of these modulus lengths. The number of Miller-Rabin tests are consistent with Appendix B of FIPS 186-4. The module performs RSA signature verification according to FIPS 186-4 with modulus lengths of 1024, 2048, 3072, and 4096 bits; RSA signature verification has been CAVP tested for all of these modulus lengths.

2.7.4 Use of SHA-1

Usages of SHA-1 which do not require collision resistance (e.g. standalone or in HMAC-SHA-1) are allowed through December 31, 2030. After December 31, 2030, usages of SHA-1 which do not require collision resistance are approved for legacy use, and may only be used to process previously protected information.

2.7.5 FIPS 186-4 Transition

FIPS 186-4 was superseded by FIPS 186-5 on February 4, 2024. Algorithms implemented in this module and tested under FIPS 186-4 may still be used in the approved mode as the module was submitted before the transition date. See IG C.K for details.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

2.8 RBG and Entropy

[EVM] The module does not implement a random bit generator. Instead, the module obtains random bits from the bound Qualcomm® Pseudo Random Number Generator module. The bound module implements a Hash DRBG and an entropy source to seed it. The Hash DRBG is compliant to SP 800-90A Rev. 1. The entropy source is compliant with SP 800-90B and validated under ESV certificate E67.

2.9 Key Generation

The SSP generation methods implemented in the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library for approved services are compliant with SP 800-133Rev2. ECDSA key pair generation is done according to FIPS 186-4, Appendix B.4.2 (Testing Candidates). RSA key pair generation is done according to FIPS 186-4, Appendix B.3.3 (Probable Prime Generation). The seeds (i.e., the random values) used in asymmetric key pair generation (CKG) are directly obtained from the SP 800-90Arev1 Hash DRBG provided by the bound Qualcomm Pseudo Random Number Generator module, compliant with SP 800-133r2 section 4 without the use of V (as specified in additional comment #2 to IG D.H).

The Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library also supports the derivation of symmetric keys in accordance with Section 6.2.3 of SP 800-133Rev2. Keys derived from passwords are only used for storage applications.

Intermediate key generation values are not output from the module during or after processing any key generation service.

2.10 Key Establishment

The module does not support any key establishment services.

2.11 Industry Protocols

The module does not implement any industry protocols, or provide services designed to be used as part of any industry protocol.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	Input parameters for data
N/A	Data Output	Input parameters for data
N/A	Control Input	Function calls, input parameters for control
N/A	Status Output	Return code, status values
SOC power port	Power	N/A

Table 10: Ports and Interfaces

All module interfaces are provided by the software API through which calling applications can interact with the module. The API design inherently provides logical separation between the different logical interfaces.

The module does not implement a control output interface.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not support authentication for roles.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer (CO)	Role	Crypto Officer	None

Table 11: Roles

The Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library supports only the Crypto Officer role. The role is implicitly assumed based on the services requested. The module does not support concurrent operators.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Encryption	Encrypts data using symmetric cryptography	0 return value with enum QSEE_FIPS_AES_*	AES key, plaintext	ciphertext	Symmetric Encryption	Crypto Officer (CO) - AES key: W,E
Decryption	Decrypts data using symmetric cryptography	0 return value with enum QSEE_FIPS_AES_*	AES key, ciphertext	plaintext	Symmetric Decryption	Crypto Officer (CO) - AES key: W,E
Authenticated Encryption	Authenticate and encrypt data	0 return value with enum QSEE_FIPS_AES_*	AES key, plaintext	ciphertext	Authenticated Symmetric Encryption	Crypto Officer (CO) - AES key: W,E
Authenticated Decryption	Verify and decrypt data	0 return value with enum QSEE_FIPS_AES_*	AES key, ciphertext	plaintext or fail	Authenticated Symmetric Decryption	Crypto Officer (CO) - AES key: W,E

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Hash	Computes the hash value of data	0 return value with enum QSEE_FIPS_SHA*	Message to be hashed	message digest	Hashing	Crypto Officer (CO)
Message Authentication	Computes the HMAC value of data	0 return value with enum QSEE_FIPS_HMAC*	Message	MAC	Message Authentication	Crypto Officer (CO) - HMAC key: W,E
Key Pair Generation	Generates asymmetric key pairs using random numbers from the bound module	0 return value with enum QSEE_FIPS_ECDSA_KEY_PAIR_GEN_* or 0 return value with enum QSEE_FIPS_RSA_KEY_PAIR_GEN_*	RSA modulus size or ECDSA curve	RSA or ECDSA key pair	Asymmetric Keygen Random Number Generation	Crypto Officer (CO) - ECDSA private key: G,R - ECDSA public key: G,R - RSA private key: G,R - RSA public key: G,R - Intermediate key generation value: G,E,Z
Signature Generation	Generates cryptographic signatures of data	0 return value with enum QSEE_FIPS_ECDSA_SIG_GEN_* or 0 return value with enum QSEE_FIPS_RSA_SIG_GEN_*	Message to sign	Digital Signature	Asymmetric Sign	Crypto Officer (CO) - ECDSA private key: W,E - RSA private key: W,E

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Signature Verification	Verifies cryptographic signatures of data	0 return value with enum QSEE_FIPS_ECDSA_SIG_VER_* or 0 return value with enum QSEE_FIPS_RSA_SIG_VER_*	Message, signature to verify	Pass or Fail	Asymmetric Verify	Crypto Officer (CO) - ECDSA public key: W,E - RSA public key: W,E
Signature Generation Component	Generates cryptographic signatures of prehashed data	0 return value with enum QSEE_FIPS_ECDSA_SIG_GEN_PRIMITIVE_* or 0 return value with enum QSEE_FIPS_RSA_SIG_GEN_PRIMITIVE_*	Hashed message	Digital Signature	Asymmetric Sign	Crypto Officer (CO) - ECDSA private key: W,E - RSA private key: W,E
Key Derivation	Derives a secret key	0 return value with enum QSEE_FIPS_PBKDF_*	Password	Derived Key	Key Derivation	Crypto Officer (CO) - Password: W,E - Derived key: G,R
Self-test	Self-Test is executed automatically when device is booted or restarted	None	N/A	Pass/Fail	Symmetric Encryption Symmetric Decryption Authenticated Symmetric Encryption Authenticated Symmetric Decryption Hashing Message Authentication	Crypto Officer (CO)

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Asymmetric Keygen Asymmetric Sign Key Derivation	
Show Status	Show status of the module state	None	N/A	status	None	Crypto Officer (CO)
Zeroization	Zeroizes all SSPs in the module	None	All SSPs	None	None	Crypto Officer (CO) - AES key: Z - HMAC key: Z - ECDSA private key: Z - ECDSA public key: Z - RSA private key: Z - RSA public key: Z - Password: Z - Derived key: Z - Intermediate key generation value: Z

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get FIPS Info (Show Version)	Show the versioning information of the module and execute self-tests on demand (pre-operational and CAST)	None	N/A	module version	None	Crypto Officer (CO)

Table 12: Approved Services

The module provides services to operators that assume the available role. Services are accessed through documented API interfaces from the calling application.

Additional services are provided by the bound Pseudo Random Number Generator module on the Snapdragon 8 Gen 2 Mobile Platform SoC. This Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library utilizes the random number generation service from the bound Pseudo Random Number Generator module.

The table above defines the services that utilize approved security functions in this module. For the respective tables, the convention below applies when specifying the access permissions (types) that the service has for each SSP.

- **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** = **Zeroise**: The module zeroises the SSP.

An operator can read the service indicator from a service by invoking the qsee_get_fips_approval_status() function with enum value for QSEE_FIPS_CRYPTO_SVC_TYPE. For details on the enum values please see the product documentation.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Encryption	Encrypts data using symmetric cryptography	DES Triple DES	CO

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Description	Algorithms	Role
		GCM/GMAC (external IV) SM4	
Decryption	Decrypts data using symmetric cryptography	DES Triple DES GCM/GMAC (external IV) SM4	CO
Hybrid Encryption	Encrypts data using symmetric cryptography	SM2 Elliptic Curve Integrated Encryption Scheme (ECIES)	CO
Hybrid Decryption	Decrypts data using symmetric cryptography	SM2 Elliptic Curve Integrated Encryption Scheme (ECIES)	CO
Hash	Computes the hash value of data	RIPEMD-160 MD5 SM3 SHA-1, SHA-224 and SHA-256 (software) (not CAVP tested)	CO
Message Authentication	Computes the MAC value of data	GCM/GMAC (external IV) HMAC (key sizes below 112 bits)	CO
Key Pair Generation	Generates asymmetric key pairs	ECDSA (secp160r1, P-192) RSA (1024 bit modulus) Ed25519 (not CAVP tested)	CO
Signature Generation	Generates cryptographic signatures of data	SM2 ECDSA (secp160r1, P-192) RSA (1024 bit modulus) Ed25519 (not CAVP tested)	CO
Signature Verification	Verifies cryptographic signatures of data	SM2 ECDSA (secp160r1) Ed25519 (not CAVP tested)	CO
Signature Verification - Component	Verifies cryptographic signatures of pre-hashed data	ECDSA (P-192, P-224, P-256, P-384 and P-521)	CO
Key Wrapping	Wraps a key using asymmetric cryptography	RSA-OAEP (not CAVP tested)	CO
Shared Secret Computation	Wraps a key using asymmetric cryptography	ECDH (no key assurances)	CO
Key Derivation	derives a key	HKDF	CO

Table 13: Non-Approved Services

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

4.5 External Software/Firmware Loaded

Not applicable. No external software or firmware is loaded.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the module is verified by comparing a HMAC-SHA-256 value calculated at run time with the HMAC-SHA-256 value stored in the module that was computed at build time. The HMAC key used to perform the integrity check is hardcoded in the module.

5.2 Initiate on Demand

The software integrity test is performed as part of the pre-operational self-tests. The software integrity test can also be invoked on-demand by calling the Get FIPS Info service.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

The procurement, build and configuring procedure are controlled. The Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is installed into a commercial off-the-shelf (COTS) mobile device by the customer.

The software components of this module are executed in the Qualcomm Trusted Execution Environment (TEE). Therefore, the operational environment is considered limited.

6.2 Configuration Settings and Restrictions

There are no security rules, settings or restrictions to the configuration of the operational environment.

The Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library does not have the capability of loading software or firmware from an external source.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper evident coating	N/A	N/A

Table 14: Mechanisms and Actions Required

The Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is a software-hybrid module implemented as part of the Snapdragon 8 Gen 2 Mobile Platform SoC, which is the physical perimeter of the single-chip software-hybrid module. The single-chip conforms to the Level 2 requirements for physical security.

At the time of manufacturing, the die of the Snapdragon 8 Gen 2 Mobile Platform SoC is embedded within a printed circuit board (PCB), which prevents visibility into the internal circuitry of the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library. The layering process which is used to embed the die into the PCB also prevents tampering of the physical components without leaving tamper evidence.

The Snapdragon 8 Gen 2 Mobile Platform SoC is further protected by being enclosed in commercial off the shelf mobile device utilizing production grade, commercially available components and said mobile device enclosure completely surrounds the Snapdragon 8 Gen 2 Mobile Platform SoC.

There are no steps required to ensure that physical security is maintained.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

8 Non-Invasive Security

The module does not support any non-invasive security techniques; therefore, this section is not applicable.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Temporary storage for SSPs used by the module as part of service execution	Dynamic

Table 15: Storage Areas

All SSPs are output from and entered into the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library by the calling process and are zeroized from memory when service execution completes. The module does not perform persistent storage of SSPs. The SSPs are only stored temporarily in plaintext in the RAM.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input API	RAM	RAM	Plaintext	Automated	N/A	
Output API	RAM	RAM	Plaintext	Automated	N/A	

Table 16: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power-Off	Temporary storage is zeroized at power off	RAM quickly loses state upon power-off.	Operator can initiate this zeroization method by powering off the module

Table 17: SSP Zeroization Methods

The module's functions deallocate and zeroize temporary SSP values in volatile memory used during the function's execution. The zeroization consists of writing zeroes to the memory location used by the SSP before deallocating the area. The module does not overwrite SSPs with other SSPs.

The zeroization service for the SSPs in volatile memory consists of powering off the module, which will remove power from the volatile memory. This action will cause the value of the SSPs in volatile memory to be overwritten by random values the next time the module is powered on. The successful act of powering off the module serves as the implicit indicator of zeroization. During power-off/zeroization, the module is unavailable, and the data output interface is inhibited.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	symmetric key for encryption/decryption	128, 192, 256 bits - 128, 192, 256 bits	Symmetric Key - CSP			Symmetric Decryption Symmetric Encryption
HMAC key	HMAC Key	112-256 bits - 112-256 bits	Authentication key - CSP			Message Authentication
ECDSA private key	private key for ECDSA	112-256 bits (P-224, P-256, P-384, P-521) - 112-256 bits	Private Key - CSP	Asymmetric Keygen		Asymmetric Sign
ECDSA public key	public key for ECDSA	96-256 bits (P-192, P-224, P-256, P-384, P-521) - 96-256 bits	Public Key - PSP	Asymmetric Keygen		Asymmetric Verify
RSA private key	private key for RSA	112-150 bits (2048, 3072, 4096 bit modulus) - 112-150 bits	Private Key - CSP	Asymmetric Keygen		Asymmetric Sign
RSA public key	public key for RSA	112-150 bits (2048, 3072,	Public Key - PSP	Asymmetric Keygen		Asymmetric Verify

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		4096 bit modulus) - 112-150 bits				
Password	password for PBKDF	N/A - N/A	password - CSP			Key Derivation
Derived key	key from PBKDF	128 - 256 bits - 128 - 256 bits	derived key - CSP	Key Derivation		
Intermediate key generation value	intermediate key	112-256 bits - 112-256 bits	intermediate value - CSP	Asymmetric Keygen		Asymmetric Keygen

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	Input API		For duration of the service	Power-Off	
HMAC key	Input API		For duration of the service	Power-Off	
ECDSA private key	Input API Output API		For duration of the service	Power-Off	ECDSA public key:Paired With Intermediate key generation value:Derived From
ECDSA public key	Input API Output API		For duration of the service	Power-Off	ECDSA private key:Paired With Intermediate key generation value:Derived From
RSA private key	Input API Output API		For duration of the service	Power-Off	RSA public key:Paired With Intermediate key generation value:Derived From
RSA public key	Input API Output API		For duration of the service	Power-Off	RSA private key:Paired With Intermediate key generation value:Derived From
Password	Input API		For duration of the service	Power-Off	Derived key:Derives

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Derived key	Output API		For duration of the service	Power-Off	Password:Derived From
Intermediate key generation value			For duration of the service	Power-Off	ECDSA private key:Derives ECDSA public key:Derives RSA private key:Derives RSA public key:Derives

Table 19: SSP Table 2

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

10 Self-Tests

The module performs pre-operational self-tests and conditional self-tests immediately when powered on. While the module is executing the self-tests, services are not available, and data output (via the data output interface) is inhibited until the tests are successfully completed. The module is not available to be used by the calling application until the pre-operational self-tests and cryptographic algorithm self-tests are completed successfully.

All the self-tests are listed below, with the respective condition under which those tests are performed. The software integrity test is performed after the HMAC cryptographic algorithm self-tests (CASTs) are performed. The self-tests for the DRBG and SHA used from the bound module are implemented by the bound module.

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A2940)	SHA2-256	HMAC-SHA2-256	SW/FW Integrity	Module is operational	N/A

Table 20: Pre-Operational Self-Tests

The integrity of the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is verified by comparing a HMAC-SHA-256 value calculated at run time with the HMAC-SHA-256 value stored in the module that was computed at build time. If the comparison verification fails, the module transitions to the error state (Section 10.4) The HMAC-SHA-256 algorithm goes through its cryptographic algorithm self-test before the integrity test is performed.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A2940)	128 and 256 bits	KAT	CAST	Module is operational	Decryption	Power Up
AES-CCM (A2940) - Encryption	128 and 256 bits	KAT	CAST	Module is operational	Encryption	Power Up
AES-CCM (A2940) - Decryption	128 and 256 bits	KAT	CAST	Module is operational	Decryption	Power Up
HMAC-SHA-1 (A2940)	SHA-1	KAT	CAST	Module is operational	N/A	Power Up
HMAC-SHA2-256 (A2940)	SHA2-256	KAT	CAST	Module is operational	N/A	Power Up
HMAC-SHA2-512 (A2940)	SHA2-512	KAT	CAST	Module is operational	N/A	Power Up

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-4) (A2940)	PKCS#1 V1.5 with SHA-256 and 2048 bit modulus	KAT	CAST	Module is operational	N/A	Power Up
RSA SigVer (FIPS186-4) (A2940)	PKCS#1 V1.5 with SHA-256 and 2048 bit modulus	KAT	CAST	Module is operational	N/A	Power Up
ECDSA SigGen (FIPS186-4) (A2940)	P-256 with SHA-256	KAT	CAST	Module is operational	N/A	Power Up
ECDSA SigVer (FIPS186-4) (A2940)	P-256 with SHA-256	KAT	CAST	Module is operational	N/A	Power Up
PBKDF (A2940)	SHA-1, SHA-256, SHA-512	KAT	CAST	Module is operational	N/A	Power Up
RSA KeyGen (FIPS186-4) (A2940)	PKCS#1 V1.5 with SHA-256	PCT	PCT	Successful key pair generation	N/A	Key generation is requested
ECDSA KeyGen (FIPS186-4) (A2940)	SHA-256	PCT	PCT	Successful key pair generation	N/A	Key generation is requested
Hash DRBG (A2945)	SHA2-256, Instantiate() -> Generate() test	KAT	CAST	Module is operational	[EVM] Implemented in and tested by bound module	Power Up

Table 21: Conditional Self-Tests

The module performs self-tests on all FIPS approved cryptographic algorithms as part of the approved services using the tests shown above. Data output through the data output interface is inhibited during the self-tests. The module transitions to the operational state only after the cryptographic algorithm self-tests are passed successfully.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A2940)	HMAC-SHA2-256	SW/FW Integrity	On Demand	Manual

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A2940)	KAT	CAST	On Demand	Manual
AES-CCM (A2940) - Encryption	KAT	CAST	On Demand	Manual
AES-CCM (A2940) - Decryption	KAT	CAST	On Demand	Manual
HMAC-SHA-1 (A2940)	KAT	CAST	On Demand	Manual
HMAC-SHA2-256 (A2940)	KAT	CAST	On Demand	Manual
HMAC-SHA2-512 (A2940)	KAT	CAST	On Demand	Manual
RSA SigGen (FIPS186-4) (A2940)	KAT	CAST	On Demand	Manual
RSA SigVer (FIPS186-4) (A2940)	KAT	CAST	On Demand	Manual
ECDSA SigGen (FIPS186-4) (A2940)	KAT	CAST	On Demand	Manual
ECDSA SigVer (FIPS186-4) (A2940)	KAT	CAST	On Demand	Manual
PBKDF (A2940)	KAT	CAST	On Demand	Manual
RSA KeyGen (FIPS186-4) (A2940)	PCT	PCT	On Demand	Manual
ECDSA KeyGen (FIPS186-4) (A2940)	PCT	PCT	On Demand	Manual
Hash DRBG (A2945)	KAT	CAST	On Demand	Manual

Table 23: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	Failure	Cryptographic Algorithm Self-Test or Software Integrity Test Failure Pair-wise consistency test failure	module restart	The module has halted and is unable to boot or the module returns ICryptoSelfTest_CRYPTO_SELFTEST_FAILED. No further operations are allowed.

Table 24: Error States

If the module fails any of the self-tests, the module enters the error state. In the error state, the module outputs the error type through the status output interface. In the error state, the data output interface is inhibited, and the module accepts no more inputs or requests. To recover from the error state, re-initialization is possible by successful execution of the pre-operational self-tests and cryptographic algorithm self-tests, which can be triggered by a power-off/power-on cycle.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

10.5 Operator Initiation of Self-Tests

The module performs on-demand self-tests initiated by calling the Get FIPS Info service. All self-tests marked as “Power up” are then executed. An operator can perform the pair-wise consistency tests on demand by requesting the Key Pair Generation service for RSA or ECDSA.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is a software-hybrid module that runs on the Snapdragon 8 Gen 2 Mobile Platform. This SoC is delivered from the vendor via a trusted delivery courier.

On the reception of the SoC, the operator shall first check all sides of the box to verify that it has not been tampered during the shipment. Then, after opening the box the operator shall verify that the moisture barrier bag is still sealed and does not present any trace of tampering. Finally, after retrieving the SoC, the operator shall perform a visual inspection of the external SoC package of the module, it should look similar to the pictures in Figure 2.

If one of these verifications fail, the operator shall contact their Qualcomm representative which released the delivery before operating the module.

Once the product is received by the customer, configured, and powered up, the test defined in Section 10 will be executed.

11.2 Administrator Guidance

To enable FIPS for the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library, the fuse must be set. The fuse enablement is mandatory to run as a FIPS validated module. This step needs to be performed only once during initial installation.

The information required for the Crypto Officer to verify the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is provided by the qsee_get_fips_info() function in qsee_fips_services.h. To verify that a Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is FIPS certified, the Crypto Officer should verify the following:

- The HMAC of the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library is on a list of HMACs of certified crypto modules.
    - This can be done by invoking the qsee_get_fips_info() function with the info_type parameter set to QSEE_FIPS_MODULE_HMAC (0). The buffer parameter should point to a buffer which is at least 32 bytes long, and the buffer_len parameter should be at least 32.
    - The result buffer should contain the HMAC-SHA-256 of the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library.
    - To get the HMAC of the 64-bit Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library, this should be run from a 64-bit Trusted Application.
- The FIPS enablement fuse is blown
    - This can be done by invoking the qsee_get_fips_info() function with the info_type parameter set to QSEE_FIPS_FUSE_STATUS (1). The buffer parameter should point to a 4-byte buffer (sizeof(uint32)) and the buffer_len parameter should equal 4.
    - The result buffer should contain the value QSEE_FIPS_FUSE_BLOWN (1).
- The pre-operational self-tests and cryptographic algorithm self-tests have passed.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

- This can be done by calling qsee_get_fips_info() with the info_type parameter set to QSEE_FIPS_SELFTEST_STATUS (2). The buffer parameter should point to a 4-byte buffer (sizeof(uint32)) and the buffer_len parameter should equal 4.
- The result buffer should contain the value QSEE_CRYPTO_SELFTEST_PASSED (1).
- If one or more of the self-tests failed, the TZ runtime environment will not be able to load Trusted Applications.

The operation of the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library does not need FIPS 140-3 specific guidance. The FIPS 140-3 functional requirements are always invoked. Once operational, if the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library enters the Error state, the Crypto Officer needs to re-initialize the library instance in order to recover from the Error state.

To use the cryptographic services of the Qualcomm Trusted Execution Environment (TEE) Software Cryptographic Library, please refer to 80-NH537-4: Qualcomm Trusted Execution Environment Version 5.0 User Guide.

11.3 Non-Administrator Guidance

There is no specific non-administrator guidance required for the module.

11.4 End of Life

As stated in Section 9 the module does not possess persistent storage of SSPs. The SSP values only exist in volatile memory and these values vanish when the module is powered off. The procedure for secure sanitization of the module at the end of life is simply to power it off, which is the action of zeroization of the SSPs (Section 9). As a result of this sanitization via power-off, all SSPs are removed from the module, so that the module may either be distributed to other operators or disposed.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

12 Mitigation of Other Attacks

12.1 Attack List

The elliptic curve implementation uses the Montgomery Ladder, as well as blinding of base points and private key multiplication. The RSA implementation uses base and modulus blinding to mitigate timing-based side-channel attacks. Blinding countermeasures add randomness to private key operations, making determination of secrets from observations more difficult for the attacker.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter Mode
DES	Data Encryption Standard
DF	Derivation Function
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
FIPS	Federal Information Processing Standards Publication
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OFB	Output Feedback
PSS	Probabilistic Signature Scheme
RNG	Random Number Generator
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Appendix B. References

FIPS140-3 **FIPS PUB 140-3 - Security Requirements For Cryptographic Modules**
March 2019
https://doi.org/10.6028/NIST.FIPS.140-3

FIPS140-3_IG **Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program**
March 2024
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements

FIPS180-4 **Secure Hash Standard (SHS)**
March 2012
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

FIPS186-4 **Digital Signature Standard (DSS)**
July 2013
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

FIPS197 **Advanced Encryption Standard**
November 2001
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

FIPS198-1 **The Keyed Hash Message Authentication Code (HMAC)**
July 2008
http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

PKCS#1 **Public Key Cryptography Standards (PKCS) #1: RSA Cryptography**
Specifications Version 2.1
February 2003
http://www.ietf.org/rfc/rfc3447.txt

SP800-38A **NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques**
December 2001
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

SP800-38C **NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality**
May 2004
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

SP800-38E	**NIST Special Publication 800-38E - Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices** January 2010 http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf
SP800-57	**NIST Special Publication 800-57 Part 1 Revision 4 - Recommendation for Key Management Part 1: General** January 2016 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
SP800-90Ar1	**NIST Special Publication 800-90A - Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
SP800-131Ar1	**NIST Special Publication 800-131A Revision 1- Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths** November 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf
SP800-132	**NIST Special Publication 800-132 - Recommendation for Password-Based Key Derivation - Part 1: Storage Applications** December 2010 http://csrc.nist.gov/publications/nistpubs/800-132/nist-sp800-132.pdf
SP800-133r2	**NIST Special Publication 800-133rev2 - Recommendation for Cryptographic Key Generation** December 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf
SP800-140Br1	**NIST Special Publication 800-140B Revision 1 - CMVP Security Policy Requirements** November 2023 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Br1.pdf

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.