Qualcomm® Trusted Execution Environment (TEE) Software Cryptographic Library

FIPS 140-2 Non-Proprietary Security Policy

Version: 1.1

2022-04-28

Prepared for:

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121

Prepared by:

atsec information security Corp.
9130 Jollyville Road, Suite 260
Austin, TX 78759

Table of Contents

1. Introduction

This document is a FIPS 140-2 Security Policy for the Qualcomm TEE Software Cryptographic Library. This document contains a specification of the rules under which the Qualcomm TEE Software Cryptographic Library must operate and describes how it meets the requirements as specified in Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2) for a Security Level 1 module. It is intended for the FIPS 140-2 testing lab, Cryptographic Module Validation Program (CMVP), developers working on the release, administrators and users of the Qualcomm TEE Software Cryptographic Library.

For more information about the FIPS 140-2 standard and validation program, refer to the NIST website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.1.Purpose of the Security Policy

There are three major reasons that a security policy is required

- It is required for FIPS 140-2 validation.
- It allows individuals and organizations to determine whether the Qualcomm TEE Software Cryptographic Library satisfies the stated security policy.
- It allows individuals and organizations to determine whether the described capabilities, the level of protection, and access rights provided by the Qualcomm TEE Software Cryptographic Library meet their security requirements.

2.Cryptographic Module Specification

2.1.Module description

The Qualcomm TEE Software Cryptographic Library is a single-chip software-hybrid cryptographic module.

The Qualcomm 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 TEE Software Cryptographic Library is determined to be a FIPS 140-2 validated module by blowing the TZ_SW_CRYPTO_FIPS_ENABLE fuse and by determining the version number based on its hash value combined with the register value of fuse.

The Qualcomm TEE Software Cryptographic Library uses the ARMv8 Cryptography Extensions (CE) for acceleration of cipher operations for SHA-1, SHA-224 and SHA-256.

The software-hybrid cryptographic module is specified in the following table:

Table 1-1: Components of the Software-hybrid Cryptographic Module

Component	Type	Version Number	Operating Environment
Qualcomm TEE Software Cryptographic Library	Software-hybrid	5.13-00023	Qualcomm TEE TZ.XF.5.13
ARM v*8* processor	Hardware	Snapdragon® 8cx Gen 3 Mobile Compute Platform	N/A

The modules have been tested on the following platform:
Snapdragon®[1] 8cx Gen 3 Mobile Compute Platform

Table 1-2 describes the software component versions that comprise the Qualcomm TEE Software Cryptographic Library while Table 1-3 describes the fuse setting that enables the FIPS validated module. The FIPS validated Qualcomm TEE Software Cryptographic Library comprises of a combination of the software component versions and fuse setting combined together.

Table 1-2: Software component versions for Qualcomm TEE Software Cryptographic Library

Software component	HMAC hash value
Qualcomm TEE Software Cryptographic Library (32 bit)	3e977120d3b0bda28f302df722ebf5d9b213da6982128b67234b44adeaf8279c
Qualcomm TEE Software Cryptographic library (64 bit)	6066189e342e0b8d68121dd4dbaee91a83a97a14b9fb3e808ef8f49460707516

[1] Snapdragon is a product of Qualcomm Technologies, Inc. and/or its subsidiaries.

Table 1-3: Fuse setting

Fuse name	1-bit fuse value	Descriptions
TZ_SW_CRYPTO_FIPS_ENABLE	1	Enable FIPS compliance for Qualcomm TEE Software Cryptographic Library. Disable by default and blow to enable.

2.1.1.Software description

The software cryptographic module consists of the Qualcomm TEE Software Cryptographic Library. The cryptographic functions are implemented within the library. The Qualcomm TEE Software Cryptographic Library is bound to the on-chip Pseudo Random Number Generator module with version 2.4.0 validated under FIPS 140-2 Cert. #3114. The bound module resides within the same physical boundary of the binding module.

2.1.2.Module Validation Level

The Qualcomm TEE Software Cryptographic Library is intended to meet requirements of FIPS 140-2 at an overall Security Level 1. The following table shows the security level claimed for each of the eleven sections that comprise the validation:

Table 2-1 Security Levels

FIPS 140-2 Section		Security Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	1
Overall Level		1

2.2.Description of Modes of Operations

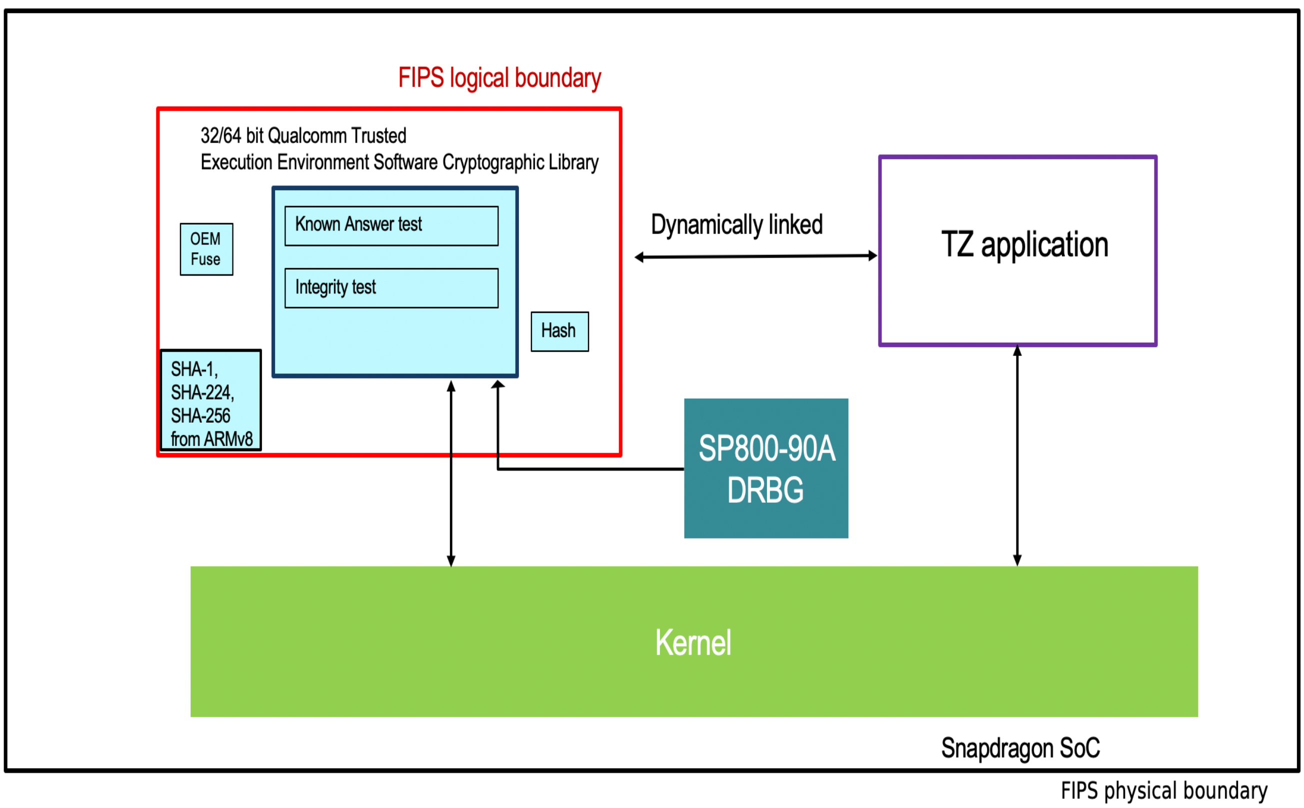
The Qualcomm TEE Software Cryptographic Library supports two modes of operation: FIPS approved mode and a non-approved mode. The mode of operation is implicitly assumed depending on the service invoked. The Qualcomm TEE Software Cryptographic Library enters FIPS approved mode after successful completion of the power up self-tests. Invoking a non-approved service will result in the Qualcomm TEE Software Cryptographic Library implicitly switching to non-approved mode. After completion of the service the Qualcomm TEE Software Cryptographic Library will immediately switch back to the FIPS approved mode and then depending on the next service call it will either remain in FIPS mode or will transition to non-approved mode. All CSPs are kept separate between the two modes.

Table 4-1 lists the roles and Table 4-2 along with Table 4-3 illustrates the services available to each role (Crypto Officer and User).

2.3.Cryptographic Module Boundary

The physical boundary of the Qualcomm TEE Software Cryptographic Library is the physical boundary of the device that contains it. Consequently, the embodiment of the Qualcomm TEE Software Cryptographic Library is a single-chip software-hybrid cryptographic module.

Figure 1: Cryptographic Boundary



3.Cryptographic Module Ports and Interfaces

Table 3-1 Ports and interfaces

FIPS Interface	Ports
Data Input	Input parameters of API calls
Data Output	Output parameters of API calls
Control Input	API calls
Status Output	Return values of API calls
Power Input	Physical power connector

As indicated in Table 3-1, all status ports and control ports are directed through the interface of the Qualcomm TEE Software Cryptographic Library's logical boundary, which is its software APIs.

The User or Crypto Officer interacts with the Qualcomm TEE Software Cryptographic Library in two distinct ways:

1. Initializing the Qualcomm TEE Software Cryptographic Library
2. The application services (API's) invoked by users

For the application services, the logical interfaces of the Qualcomm TEE Software Cryptographic Library are the library APIs. In detail, these interfaces are the following:

- Data input and data output are provided in the variables passed in the API and callable service invocations, generally through caller-supplied buffers.
- Control inputs are provided through dedicated parameters.
- Status output is provided in return codes and through messages. Documentation for each API lists possible return codes.

Once Qualcomm TEE Software Cryptographic Library initializes and the self-tests complete successfully, all cryptographic functions are made available. If its integrity test or KATs fail, the Qualcomm TEE Software Cryptographic Library goes into error state. To recover from a failure, the Qualcomm TEE Software Cryptographic Library will need to be re-initialized. When the Qualcomm TEE Software Cryptographic Library is in the error state, the data output is inhibited. The only way to recover from an integrity test failure is to reinstall the software and re-initialize.

Caller-induced or internal errors do not reveal any sensitive material to callers. The Qualcomm TEE Software Cryptographic Library ensures that there is no means to obtain data from itself by performing key zeroization. There is no means to obtain sensitive information from the Qualcomm TEE Software Cryptographic Library.

4.Roles, Services and Authentication

4.1.Roles

The Qualcomm TEE Software Cryptographic Library supports two roles: a Crypto Officer role and a User role. Roles are implicitly assumed based on the services requested.

The Qualcomm TEE Software Cryptographic Library supports multiple application sessions. Each application session is started with a separate instance of the library. Each session is protected by memory separation, process isolation and access control provided by the kernel.

4.1.1.Crypto Officer Role

The Crypto Officer role exists only while provisioning the Qualcomm TEE Software Cryptographic Library by the OEM.

4.1.2.User Role

The software applications assume the User role when requesting any services provided by the Qualcomm TEE Software Cryptographic Library. The User role has access to all its services except installation and configuration.

Table 4-1 Roles

Role	Services
User	Utilization of cryptographic services and re-initialization from Error state
Crypto Officer	Installation and Configuration

4.2.Services

The Qualcomm TEE Software Cryptographic Library does not provide a bypass capability through which some cryptographic operations are not performed or where certain controls are not enforced.

Services are accessed through documented API interfaces from the calling application.

Additional services are provided by bound Pseudo Random Number Generator module on the Snapdragon 8cx Gen 3 Mobile Compute Platform SoC. This Qualcomm TEE Software Cryptographic Library utilizes the random number generation service from the bound Pseudo Random Number Generator module.

The following tables (Table 4-2 and Table 4-3) illustrate the role and corresponding services of the Crypto Officer and User

Table 4-2 Approved, Allowed or Vendor Affirmed Services

Service	Roles User	Roles CO	CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
Symmetric Algorithms							
AES encryption and decryption	✓		AES Symmetric key (128, 192, 256 bit)	CBC, ECB, CTR, CCM, CFB128, XTS, OFB	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	FIPS 197, SP800-38A
AES cipher text stealing	✓		AES Symmetric key (128, 192, 256 bit)	AES-CBC-CS (CBC-CS2)	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	SP800-38A Addendum
Triple-DES encryption[2] and decryption	✓		Triple DES Symmetric key (192 bits)	CBC, ECB	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	SP 800-67r1 , SP800-38A
Hash Functions							
SHA-1 From ARMv8	✓		None	N/A	32-bit – Cert. #A1879 64-bit – Cert. #A1880	N/A	FIPS 180-4

[2] The use of three-key Triple-DES encryption will be disallowed after 2023.

Service	Roles: User	Roles: CO	CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
SHA-224 From ARMv8	✓		None	N/A	32-bit – Cert. #A1879 64-bit – Cert. #A1880	N/A	FIPS 180-4
SHA-256 From ARMv8	✓		None	N/A	32-bit – Cert. #A1879 64-bit – Cert. #A1880	N/A	FIPS 180-4
SHA-384 From software	✓		None	N/A	32-bit – Cert. #A1879 64-bit – Cert. #A1880	N/A	FIPS 180-4
SHA-512 From software	✓		None	N/A	32-bit – Cert. #A1879 64-bit – Cert. #A1880	N/A	FIPS 180-4
Message Authentication Codes (MACs)							
HMAC SHA-1	✓		HMAC SHA-1 key (key length between 112 bits and 512 bits)	N/A	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	FIPS 198-1

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
	User	CO					
HMAC SHA-224	✓		HMAC SHA-224 key (key length between 112 bits and 512 bits)	N/A	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	FIPS 198-1
HMAC SHA-256	✓		HMAC SHA-256 key (key length between 112 bits and 512 bits)	N/A	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	FIPS 198-1
HMAC SHA-384	✓		HMAC SHA-384 key (key length between 112 bits and 512 bits)	N/A	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	FIPS 198-1
HMAC SHA-512	✓		HMAC SHA-512 key (key length between 112 bits and 512 bits)	N/A	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	FIPS 198-1
Public Key Algorithms							
ECDSA Key-Pair	✓		ECDSA public/private key pair for P-224, P-256, P-384, P-521 curves	B.4.2	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Write	FIPS 186-4 SP800-133 (CKG) vendor affirmed

Service	Roles User	Roles CO	CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
ECDSA Sig Gen	✓		ECDSA private key according to P-224, P-256, P-384, P-521 curves	SHA-224, SHA-256, SHA-384, SHA-512	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	FIPS 186-4
ECDSA Sig Gen - component	✓		ECDSA private key according to P-224, P-256, P-384, P-521 curves	SHA-224, SHA-256, SHA-384, SHA-512	32-bit – CVL Cert. #A1879 64-bit – CVL Cert. #A1880	Read/Write	FIPS 186-4
ECDSA Sig Verify	✓		ECDSA public key according to P-192 to P-521 curves	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read	FIPS 186-4
RSA KeyGen 9.31	✓		RSA public and private key pair with 2048/3072/4096-bit modulus size	B.3.3	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Write	FIPS 186-4 SP800-133 (CKG) vendor affirmed
RSA SigGen PKCS1.5	✓		RSA private key with 2048/3072/4096-bit modulus size	SHA-224, SHA-256, SHA-384-SHA-512	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	FIPS 186-4

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
	User	CO					
RSA SigVer PKCS1.5	✓		RSA public key with 1024/2048/3072/ 4096-bit modulus size	SHA-1, SHA-256, SHA384, SHA-512	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read	FIPS 186-4
RSA SigGenPSS	✓		RSA private key with 2048/3072/4096-bit modulus size	SHA-224, SHA-256, SHA-384, SHA-512	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	FIPS 186-4
RSA SigVerPSS	✓		RSA public key with 1024/2048/3072/ 4096-bit modulus size	SHA-1, SHA-256, SHA-384, SHA-512	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read	FIPS 186-4
RSA SigGen - Primitive	✓		RSA private key with 2048-bit modulus size	N/A	32-bit – CVL Cert. #A1879 64-bit – CVL Cert. #A1880	Read/Write	FIPS 186-4
Key Derivation							
PBKDF2	✓		Password and derived key	SHA-1, SHA-256, SHA-512	32-bit – Cert. #A1879 64-bit – Cert. #A1880	Read/Write	SP 800-132

Service	Roles User	Roles CO	CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
Miscellaneous							
Installation and Configuration		✓	None	N/A	N/A	N/A	N/A
re-initialization from Error state	✓		None	N/A	N/A	N/A	N/A
Self-Tests	✓		None	N/A	N/A	N/A	N/A
Zeroization	✓		All CSPs	N/A	N/A	W	N/A
Show Status	✓		None	N/A	N/A	N/A	N/A
DRBG bound module							
SHA-256	✓		None	N/A	Certs. #A1630, #A1631	N/A	FIPS 180-4
SHA-256 Hash DRBG	✓		Seed, (i.e., entropy input string and nonce), Personalization string	SHA-256	Cert. #A1630	Read/Write	SP800-90A
				NDRNG – used to seed DRBG; provides 256 bits of entropy	N/A (Allowed in FIPS mode)	Read	N/A

Table 4-3 Non-Approved Services

Service	Roles	
	User	CO
Symmetric Algorithms		
DES	✓	
RIPEMD-160	✓	

Service	Roles	
	User	CO
GCM/GMAC[3]	✓	
HMAC SHA-1/SHA-256/SHA-384/ SHA-512 with key sizes below 112 bits	✓	
MD5	✓	
SM3	✓	
SM4	✓	
SHA-1, SHA-224 and SHA-256 from Software	✓	
Asymmetric algorithms		
ECDH key pair /shared secret computation[4]	✓	
ECDSA key pair/siggen with P-160/ P-192 and sigver with P-160	✓	
Elliptic Curve Integrated Encryption Scheme (ECIES)	✓	
RSA key wrapping with RSA OAEP	✓	
RSA keygen with 1024 bit keys and siggen with 1024 bit keys	✓	
SM2	✓	

4.3.Operator Authentication

There is no operator authentication; assumption of role is implicit by action.

[3] GCM is CAVP certified with CAVP *Certs. #A1879and #A1880*. However, there are two requirements from FIPS IG A.5 below that contributed to the non-compliance: 1) the IV uniqueness must be enforced by the Qualcomm Trusted Execution Environment Software Cryptographic Library ; 2) FIPS required that only 2^32 cipher operations are performed with a given key.

[4] ECDH is CAVP certified with CAVP Certs. *#A1879 and #A1880*. However, ECDH is not compliant with SP800-56A Rev 3 requirements.

5.Physical Security

The Qualcomm TEE Software Cryptographic Library is a software-hybrid module implemented as part of the Snapdragon 8cx Gen 3 Mobile Compute Platform SoC, which is the physical boundary of the single-chip software-hybrid module. The Snapdragon 8cx Gen 3 Mobile Compute Platform SoC is a single chip with a production grade enclosure and hence conform to the Level 1 requirements for physical security.

6.Operational Environment

6.1.Applicability

The operating system shall be restricted to a single operator mode of operation.
The procurement, build and configuring procedure are controlled. The Qualcomm TEE Software Cryptographic Library is installed into a commercial off-the-shelf (COTS) mobile device by the customer.

7.Cryptographic Key Management

7.1.Key Establishment/Key Derivation

The Qualcomm TEE Software Cryptographic Library implements Password-Based Key Derivation version 2 (PBKDFv2) as defined in [SP800-132]. The PBKDFv2 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 quality of the password, the quality of the salt as well as the number of iterations. The keys derived from passwords, as shown in SP 800-132, may only be used for storage applications.

7.2.Key Generation

Key Generation uses an approved DRBG algorithm provided as an approved service through the bound Pseudo Random Number Generator module.

The Key Generation methods implemented in the Qualcomm TEE Software Cryptographic Library for Approved services in FIPS mode are compliant with SP800- 133. RSA and ECDSA key generation is done according to FIPS Pub 186-4 [8]. For generating RSA and ECDSA keys, the Qualcomm TEE Software Cryptographic Library implements asymmetric key generation services compliant with FIPS Pub 186-4 and SP800-90A. A seed (i.e. the random value) used in asymmetric key generation is directly obtained from the SP800-90A DRBG provided by the bound module. The Qualcomm TEE Software Cryptographic Library does not generate symmetric keys.

7.3.Key Entry /Output

The Qualcomm TEE Software Cryptographic Library does not support manual key entry or intermediate key generation key output. The keys are provided to it via API input parameters in plaintext form and output via API output parameters in plaintext form. The Qualcomm TEE Software Cryptographic Library does not enter or output keys in plaintext format outside its physical boundary.

7.4.Key Storage

All keys are output from and entered into the Qualcomm TEE Software Cryptographic Library to and from the calling process, and are destroyed from memory when released. It does not perform persistent storage of keys. The keys and CSPs are stored encrypted in the RAM when the application is run out of protected memory. If the application chooses to run on un-protected memory or if protected memory is not supported in some hardware variants, the keys and CSPs will be stored temporarily in plaintext in the RAM.

7.5.Key Zeroization

The memory occupied by keys is allocated by regular memory allocation calls. The application is responsible for calling the appropriate zeroization functions provided in the Qualcomm TEE Software Cryptographic Library’s API.

Table 7-1 - Life cycle of Keys

Name	Generation	Entry and Output
AES keys	Not Applicable. Keys are provided by the calling application.	The key is passed into the Qualcomm TEE Software Cryptographic Library via API input parameters in plaintext.
Triple-DES keys		
HMAC key		
RSA private key	Key pairs are generated using FIPS 186-4 key generation method, and the random value used is generated using the SP800-90A DRBG provided by the bound module.	The key is passed into the Qualcomm TEE Software Cryptographic Library via API input parameters in plaintext. The key is passed out of the Qualcomm TEE Software Cryptographic Library via API output parameters in plaintext.
ECDSA private key		
Password	The Password is provided by the calling application	The password is passed into the Qualcomm TEE Software Cryptographic Library via API input parameters in plaintext.
Derived key	The derived key is generated by the PBKDF.	The derived key is passed out of the Qualcomm TEE Software Cryptographic Library via API output parameters in plaintext.

8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The Qualcomm TEE component cannot be certified by the FCC as it is not a standalone device. It is a software-hybrid module imbedded in the Snapdragon 8cx Gen 3 Mobile Compute Platform SoC, which is also not a standalone device. Instead, Snapdragon 8cx Gen 3 Mobile Compute Platform is intended to be used within a COTS device which would undergo standard FCC certification for EMI/EMC.

According to 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, the Qualcomm TEE is not subject to EMI/EMC regulations because it is a subassembly that is sold to an equipment manufacturer for further fabrication. That manufacturer is responsible for obtaining the necessary authorization for the equipment with the Qualcomm TEE embedded prior to further marketing to a vendor or to a user.

9.Power up Tests

The Qualcomm TEE Software Cryptographic Library performs power-up self-tests when it is loaded into memory, without operator intervention. Power-up self-tests ensure that it is not corrupted and that the cryptographic algorithms work as expected. The power-up self-tests consists of software integrity test and the known-answer tests.

While the Qualcomm TEE Software Cryptographic Library is executing the power-up self-tests, services are not available, and input and output are inhibited. It is not available to be used by the calling application until the power-up self-tests are completed successfully.

The integrity of the Qualcomm TEE Software Cryptographic Library is verified by checking a HMAC-SHA-256-based hash value of each Qualcomm TEE Software Cryptographic Library binary prior to being utilized. The binaries' hash values are generated during the final phase of the build process.

If any power-up test fails, the Qualcomm TEE Software Cryptographic Library enters an error state. The Trusted Application loading process will fail, so the application cannot be initialized and run. To recover from the error state, re-initialization is possible by successful execution of the power up tests which can be triggered by a power-off/power-on cycle. If the power-up tests complete successfully, the Qualcomm TEE Software Cryptographic Library will accept cryptographic operation service requests.

Pair-wise Consistency tests are run whenever the Qualcomm TEE Software Cryptographic Library generates a private-public key-pair. The private key structure always contains either the data of the corresponding public key or information sufficient for computing the corresponding public key.

If the pair-wise consistency check fails, the Qualcomm TEE Software Cryptographic Library enters an error state and returns an error status code. The calling application must recognize this error and handle it in a FIPS 140-2 appropriate manner, for example, by reinitializing the library instance.

The Qualcomm TEE Software Cryptographic Library implements the following self-tests to ensure its proper functioning. The implemented self-tests include power up self-tests of all approved algorithms.

9.1.Cryptographic Algorithm Tests

Table 9-1 Power up Tests

Algorithm	Test
AES encryption (CCM)	KAT
AES decryption (CCM)	KAT
AES decryption (ECB)	KAT
Triple-DES encryption (ECB)	KAT
Triple-DES decryption (ECB)	KAT
HMAC SHA-1	KAT
HMAC SHA-256	KAT
HMAC SHA-512	KAT
RSA Signature Generation/Signature Verification	KAT
ECDSA Signature Generation/Signature Verification	KAT

Algorithm	Test
PBKDF	KAT
HMAC SHA-256	Integrity test

Table 9-2 Pair-wise Consistency Tests

Algorithm	Test
RSA	PCT
ECDSA	PCT

10.Design Assurance

10.1.Configuration Management

Perforce Visual Client(P4V), a version control system from Perforce, is used to manage the revision control of the Qualcomm TEE software code. The Perforce Visual Client provides version control, branching and merging of code lines, and concurrent development.

Git, a version control system from Open Source Community., is also used to manage the revision control of the Qualcomm TEE unified crypto software code. The Git product provides version control, branching and merging of code lines, and concurrent development.

10.2.Crypto Officer Guidance

To enable FIPS for the Qualcomm TEE Software Cryptographic Library, the fuse must be set according to Table 1. The fuse enablement is mandatory to run as a FIPS validated module. This step is required to perform only once during initial configuration.

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

- The HMAC of the Qualcomm TEE Software Cryptographic Library is on a list of HMACs of certified crypto modules.
    - This can be done by calling qsee_get_fips_info() with the info_type parameter set to QSEE_FIPS_MODULE_HMAC (0). The buffer parameter should point to a buffer which is a least 32 bytes long, and the buffer_len parameter should be at least 32.
    - The result buffer should contain the SHA256 HMAC of the Qualcomm TEE Software Cryptographic Library.
    - To get the HMAC of the 32bit Qualcomm TEE Software Cryptographic Library, this should be run from a 32 bit Trusted Application. To get the HMAC of the 64bit Qualcomm 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 calling qsee_get_fips_info() 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 crypto self test has passed.
    - 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 the self test fails, the TZ runtime environment will not be able to load Trusted Applications.

10.3.User Guidance

The operation of the Qualcomm TEE Software Cryptographic Library does not need FIPS 140-2 specific guidance. The FIPS 140-2 functional requirements are always invoked.

Once operational, if the Qualcomm TEE Software Cryptographic Library enters Error state, the User needs to re-initialize the library instance in order recover from the Error state.

For using the cryptographic services of the Qualcomm TEE Software Cryptographic Library, please refer to 80-NH537-4: Qualcomm TEE Version 5.0 User Guide.

NOTE:

- AES counter mode uses a 128-bit counter. The counter will roll over after 2^128 blocks of encrypted data.
- According to IG A.13, the same Triple-DES key shall not be used to encrypt more than 2^16 64-bit blocks of data and the user is responsible to ensure that this compliance is met.
- The AES algorithm in XTS mode can be only used for the cryptographic protection of data on storage devices, as specified in [SP800-38E]. In addition, the length of a single data unit encrypted with the AES-XTS shall not exceed 2^20 AES blocks.

11. Mitigation of Other Attacks

The RSA implementation uses Montgomery Ladder and base/modulus blinding technique to help prevent against timing and side-channel attacks. Blinding countermeasures add randomness to private key operations, making determination of secrets from observations more difficult for the attacker.

In ECC, the base points are blinded. In ECDSA, the multiplication of d and the private key are blinded.

Terms and Abbreviations

AES	Advanced Encryption Specification
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CM	Cryptographic Module
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off The Shelf
CO	Crypto Officer
CSP	Critical Security Parameter
DES	Data Encryption Standard
ECIES	Elliptic Curve Integrated Scheme
FIPS	Federal Information Processing Standards Publication
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Science and Technology
OEM	Original Equipment Manufacturer
OTP	One-Time Programmable
SHA	Secure Hash Algorithm
SoC	System on Chip
TZ	Trust Zone

References

[1] OpenSSL man pages where crypto(3) provides the introduction and link to all OpenSSL APIs regarding the cryptographic operation and ssl(3) to all OpenSSL APIs regarding the SSL/TLS protocol family

[2] FIPS 140-2 Standard, https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards

[3] FIPS 140-2 Implementation Guidance, https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards

[4] FIPS 140-2 Derived Test Requirements, https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards

[5] FIPS 197 Advanced Encryption Standard, https://csrc.nist.gov/publications/fips

[6] FIPS 180-4 Secure Hash Standard, https://csrc.nist.gov/publications/fips

[7] FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC), https://csrc.nist.gov/publications/fips

[8] FIPS 186-4 Digital Signature Standard (DSS), https://csrc.nist.gov/publications/fips

[9] ANSI X9.52:1998 Triple Data Encryption Algorithm Modes of Operation, http://webstore.ansi.org/FindStandards.aspx?Action=displaydept&DeptID=80&Acro=X9&DpName=X9,%20Inc.

[10] NIST SP 800-67 Revision 1, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, https://csrc.nist.gov/publications/sp

[11] NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, https://csrc.nist.gov/publications/sp

[12] NIST SP 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, https://csrc.nist.gov/publications/sp

[13] NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, https://csrc.nist.gov/publications/sp

[14] NIST SP 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, https://csrc.nist.gov/publications/sp

[15] NIST SP 800-56A, Recommendation for Pair-Wise Key Establishment Schemes using Discrete Logarithm Cryptography (Revised), https://csrc.nist.gov/publications/sp

[16] NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, https://csrc.nist.gov/publications/sp