Qualcomm® Secure Processing Unit

Hardware Version 4.1

Firmware Version spss.a1.1.5_00039

FIPS 140-2 Non-Proprietary Security Policy

Version: 1.0

2022-03-21

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® Secure Processing Unit cryptographic module. The hardware version number of the Qualcomm Secure Processing Unit is 4.1 and the firmware version is spss.a1.1.5_00039. This document contains a specification of the rules under which the Qualcomm Secure Processing Unit must operate and describes how this Qualcomm Secure Processing Unit meets the requirements as specified in Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2) for a Security Level 2 module. It is intended for the FIPS 140-2 testing lab, Cryptographic Module Validation Program (CMVP), developers working on the release, administrators of the Qualcomm Secure Processing Unit and users of the Qualcomm Secure Processing Unit.

For more information about the FIPS 140-2 standard and validation program, refer to the NIST website at https://csrc.nist.gov/Projects/cryptographic-module-validation-program

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 implemented Qualcomm Secure Processing Unit 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 Secure Processing Unit meet their security requirements.

2. Cryptographic Module Specification

2.1.Module Description

The Qualcomm Secure Processing Unit is a single-chip hardware module implemented as a sub-chip in the Snapdragon®[1] 8cx Gen 3 Mobile Compute Platform SoC. From the validation perspective, the Qualcomm Secure Processing Unit is configured as a single chip hardware module.

The Qualcomm Secure Processing Unit is an isolated hardware security core implemented in the Snapdragon 8cx Gen 3 Mobile Compute Platform SoC. It's functionally similar to discrete smartcard Secure ICs used for high-assurance applications such as UICC and data user protection. As such, this security core incorporates standalone ROM, RAM, CPU, cryptographic acceleration units, countermeasure sensors, one-time programmable memory, etc. The cryptographic capabilities of this core include:

- Computation of hash values, e.g. SHA-1, SHA-256 to SHA-512
- Message authentication utilizing HMAC-SHA1, HMAC-SHA256, AES CMAC, hashing algorithms
- Hashing and ciphering operations using AES CCM
- Key generation, signing and verification utilizing RSA and ECC cryptosystems across a range of modes
- Symmetric encryption/decryption using AES-ECB, AES-CBC, AES-CTR cipher modes, as well as DES and 3DES

The Qualcomm Secure Processing Unit module uses the Qualcomm(R) Secure Processing Unit (SPU) Random Number Generator (RNG) (hereafter referred to as "Bound DRBG module") validated under certificate #3911 as a bound module. This bound DRBG module provides the random number generation service to the Qualcomm Secure Processing Unit module for the key generation purpose.

2.1.1.Hardware Description

The cryptographic module is implemented in the Qualcomm Secure Processing Unit with hardware version 4.1 and firmware version spss.a1.1.5_00039, which resides in Snapdragon 8cx Gen 3 Mobile Compute Platform processors (https://www.qualcomm.com/products/snapdragon-8cx-gen-3-compute-platform). The Qualcomm Secure Processing Unit provides a series of algorithms (as listed in Table 4-2) implemented in the device hardware.

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

2.1.2.Module Validation Level

The Qualcomm Secure Processing Unit is intended to meet requirements of FIPS 140-2 at an overall Security Level 2. 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	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	2
Overall Level		2

Table 2-2 describes the platform used to test the Qualcomm Secure Processing Unit.

Table 2-2: Tested Platforms

Module Name	Hardware version	Test Platform
Qualcomm Secure Processing Unit	4.1	Snapdragon 8cx Gen 3 Mobile Compute Platform

Table 2-3 describes the firmware that comprises the Qualcomm Secure Processing Unit while Table 2-5 describes the fuse setting that defines the FIPS validated module. The FIPS validated module for Qualcomm Secure Processing Unit comprises of a combination of the hardware version, firmware versions and fuse setting combined together.

Table 2-3: Firmware components

Firmware component	Artifacts	Version	Descriptions
Master Control Program (MCP)	Spss1p.mbn	spss.a1.1.5_00039	Qualcomm Secure Processing Unit kernel
Crypto app	Crypt1p.sig		System application that performs FIPS self test

Asym crypto app	Asym1p.sig		System application

Table 2-4: Fuse descriptions

Fuse	Descriptions
FIPS ENABLE	In order to place the Qualcomm Secure Processing Unit into FIPS certifiable mode, the OEM must enable it via blowing an OEM hardware fuse SP_FIPS_ENABLE which activates a mandatory self-test run inside the Qualcomm Secure Processing Unit every time it boots.
FIPS OVERRIDE	Once the Qualcomm Secure Processing Unit is in FIPS certifiable mode, it can be placed into non-FIPS certifiable mode by calling **spcom_sp_sysparam_write_ext**() API with system parameter ID SP_SYSPARAM_ID_FIPS_OVERRIDE. The API will internally trigger the blowing of a FIPS OVERRIDE fuse. Once the FIPS OVERRIDE fuse is blown, the Qualcomm Secure Processing Unit cannot be placed into FIPS certifiable mode again.

Table 2-5: Fuse setting

FIPS ENABLE	FIPS OVERRIDE	Mode
0	0	Non-FIPS certifiable
0	1	Non-FIPS certifiable
1	0	FIPS certifiable
1	1	Non-FIPS certifiable

2.2.Description of Modes of Operations

The Qualcomm Secure Processing Unit 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 Secure Processing Unit enters FIPS approved mode after successful completion of the power up self-tests. Invoking a non-approved service will result in the Qualcomm Secure Processing Unit implicitly switching to non-approved mode. After completion of the service the Qualcomm Secure Processing Unit 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 Secure Processing Unit is the physical boundary of the Snapdragon 8cx Gen 3 Mobile Compute Platform SoC which contains the Qualcomm Secure Processing Unit which is implemented as a sub-chip. Consequently, the embodiment of the Qualcomm Secure Processing Unit is a Single-chip cryptographic module. The logical boundary is the Qualcomm Secure Processing Unit.

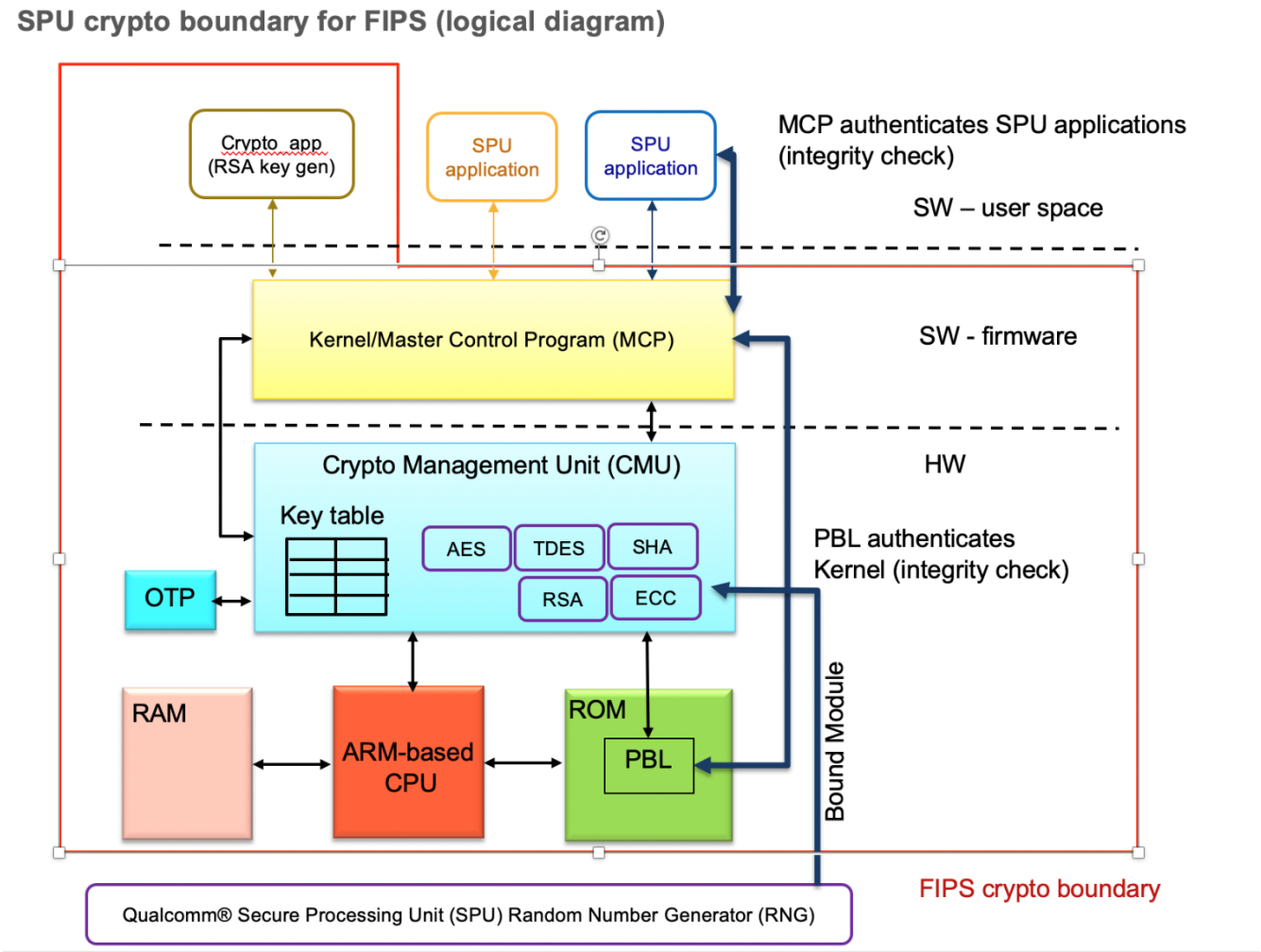

Figure 1: Qualcomm Secure Processing Unit Cryptographic Boundary for FIPS (logical diagram)

Crypto app and asym crytoapp are system applications that are within the FIPS boundary. Crypto app is responsible for executing FIPS self-test.

2.3.1.Hardware Block Diagram

In the hardware block diagram, the arrows depict the flow of the status, control and data. Parameters are passed to the Qualcomm Secure Processing Unit and results received from the Qualcomm Secure Processing Unit via Direct Memory Access (DMA) writing and through APIs.

The CSPs, such as the encryption key, are written directly to the OTP to be stored within the Qualcomm Secure Processing Unit. The remainder of the Snapdragon 8cx Gen 3 Mobile Compute Platform SoC, which is not part of the Qualcomm Secure Processing Unit passes the Critical Security Parameters (CSP) from the software executing on top of the SoC to the Qualcomm Secure Processing Unit.

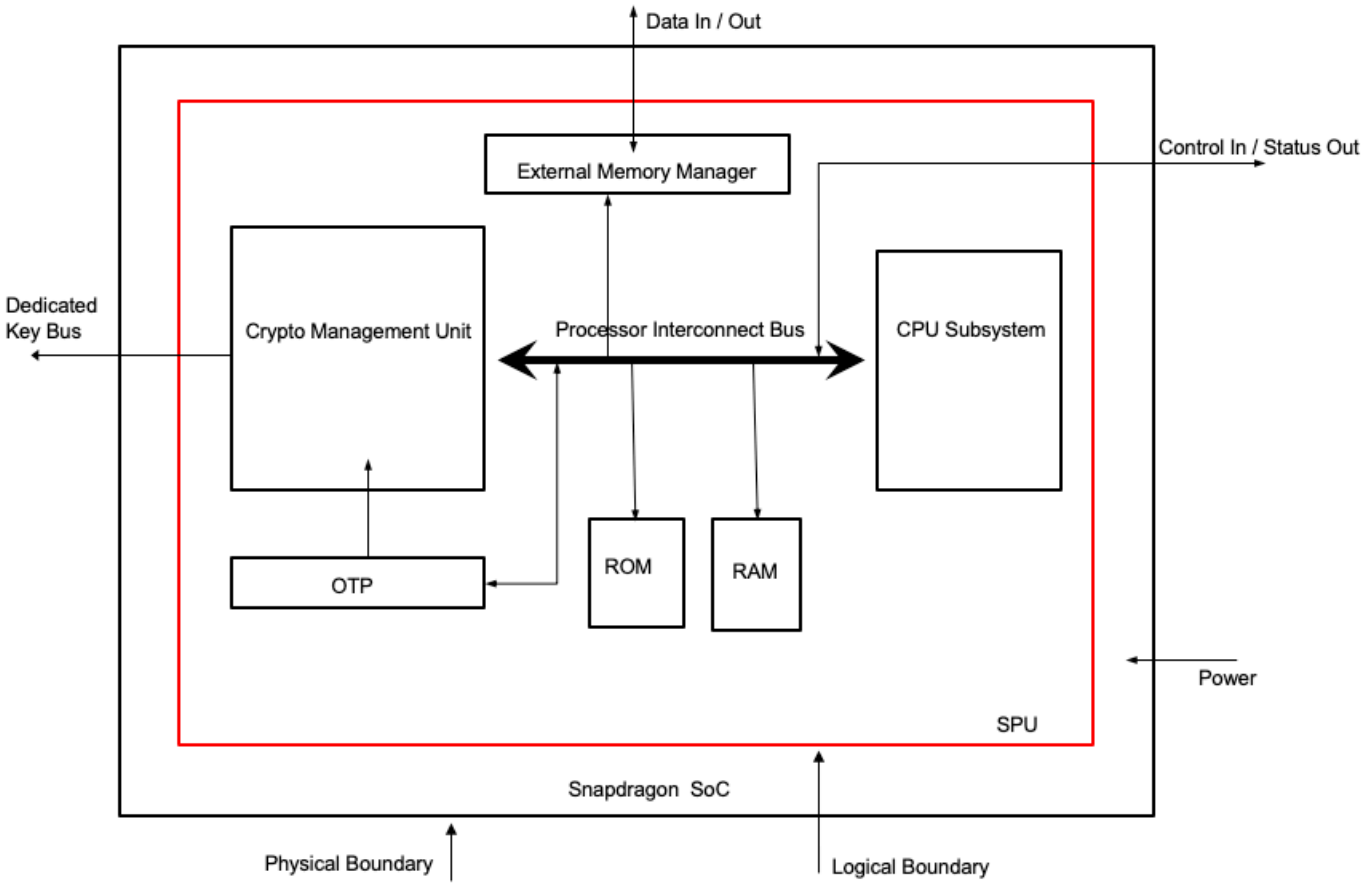

Figure 2: Block Diagram

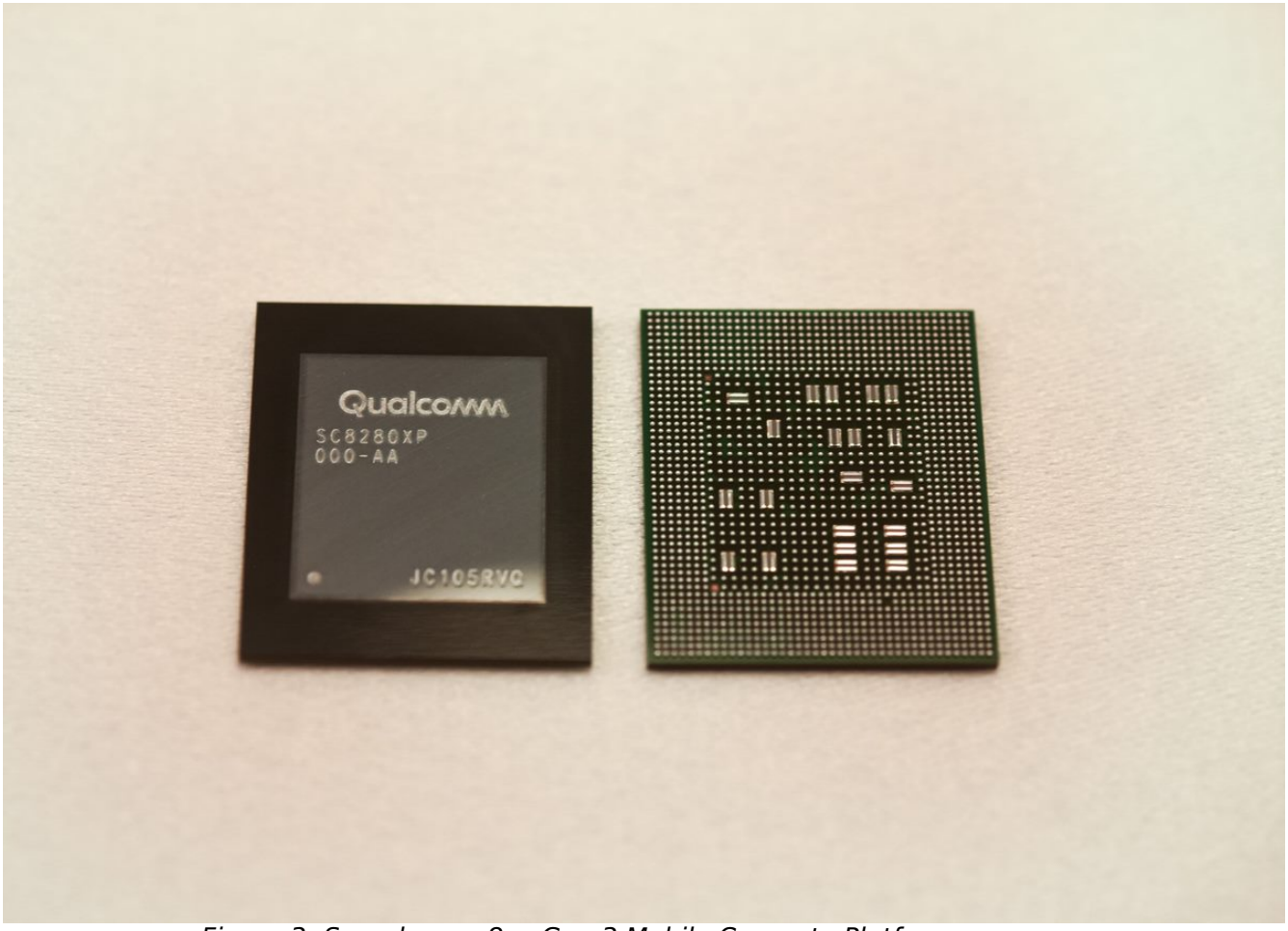

Figure 3: Snapdragon 8cx Gen 3 Mobile Compute Platform processor

3.Cryptographic Module Ports and Interfaces

Table 3-1 Ports and interfaces

FIPS Interface	Ports
Data Input	API calls, DMA
Data Output	API calls, DMA
Control Input	API calls, private key bus
Status Output	API calls, private key bus
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 Secure Processing Unit's logical boundary, which is the APIs and private key bus for control input. For data input and data output, the API calls and DMA implement the interface.

Caller-induced or internal errors do not reveal any sensitive material to callers. Cryptographic bypass capability is not supported by the Qualcomm Secure Processing Unit. The Qualcomm Secure Processing Unit ensures that there is no means to obtain CSP or key data from the Qualcomm Secure Processing Unit by placing the CSPs into write-only registers preventing any entity interacting with the Qualcomm Secure Processing Unit from being able to read the CSPs. Additionally, key zeroization can be performed by issuing a reset event to the Qualcomm Secure Processing Unit. There is no means to obtain sensitive information from the Qualcomm Secure Processing Unit.

4.Roles, Services and Authentication

4.1.Roles

The Qualcomm Secure Processing Unit implements role-based authentication with two roles: a Crypto Officer role and a User role.

The Qualcomm Secure Processing Unit supports concurrent application sessions (operators). 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 after Qualcomm Secure Processing Unit product delivery during configuration of the product by a customer (or OEM).

4.1.2.User Role

The software applications authenticate the User role when requesting any services provided by the Qualcomm Secure Processing Unit. The User role has access to all of the Qualcomm Secure Processing Unit's services except Qualcomm Secure Processing Unit configuration set up.

Table 4-1 Roles

Role	Services
User	Utilization of cryptographic services of the Qualcomm Secure Processing Unit
Crypto Officer	Qualcomm Secure Processing Unit configuration set up

4.2.Services

The Qualcomm Secure Processing Unit does not provide a bypass capability through which some cryptographic operations are not performed or where certain controls implemented during normal operation are not enforced.

The following tables (Table 4-2 and Table 4-3) illustrate the role and corresponding services for the Crypto Officer and User. When the services in Table 4-2 are performed, the Qualcomm Secure Processing Unit is in FIPS mode of operation. When the services in Table 4-3 are performed, the Qualcomm Secure Processing Unit is in non-FIPS mode of operation.

The following convention is used to specify access rights to a CSP:

1. **Read**: The service needs to read a key/CSP.
2. **Write**: The service needs to update or create a key/CSP.
3. **N/A**: The service does not access any CSP or key during its operation.

Table 4-2 Approved and Allowed Services in FIPS mode

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
	User	CO					
Symmetric Algorithms							
AES encryption and decryption	✓		AES Symmetric key (128, 256 bit)	CBC, ECB, CTR, CCM	HW – Cert. #A1007	Read	FIPS 197, SP800-38A, SP800-38C
Triple-DES encryption and decryption	✓		Triple DES Symmetric key (192 bits) (The key has 168 bits without parity)	CBC, ECB	HW – Cert. #A1007	Read	SP 800-67r1, SP800-38A
Hash Functions							
Hash operation using SHA-1	✓		None	N/A	HW – Cert. #A1007	N/A	FIPS 180-4
Hash operation using SHA-256	✓		None		HW – Cert. #A1007	N/A	FIPS 180-4
Hash operation using SHA-384	✓		None	N/A	HW – Cert. #A1007	N/A	FIPS 180-4
Hash operation using SHA-512	✓		None	N/A	HW – Cert. #A1007	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	HW – Cert. #A1007	Read	FIPS 198-1
HMAC SHA-256	✓		HMAC SHA-256 key (key length between 112 bits and 512 bits)	N/A	HW – Cert. #A1007	Read	FIPS 198-1

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
	User	CO					
HMAC SHA-384	✓		HMAC SHA-384 key (key length between 112 bits and 512 bits)	N/A	HW – Cert. #A1007 FW – Cert. #A1006	Read	FIPS 198-1
HMAC SHA-512	✓		HMAC SHA-512 key (key length between 112 bits and 512 bits)	N/A	HW – Cert. #A1007 FW – Cert. #A1006	Read	FIPS 198-1
AES-CMAC generation	✓		AES Symmetric key (128, 256 bit)	CMAC	HW – Cert. #A1007	Read	SP 800-38B
Key Generation							
Cryptographic Key Generation (CKG) for asymmetric keys	✓		RSA and ECDSA key generation	N/A	Vendor affirmed	Write	SP 800-133
RSA Key generation with 9.31	✓		RSA public and private key pair with 2048/3072/4096 -bit modulus size	B.3.3	FW – Cert. #A1006	Write	FIPS 186-4
			Hash-based SHA-256 DRBG from bound module		HW DRBG Cert. #A774 HW SHA Certs. #A773, #A774	Read	SP 800-90A
			NDRNG used from the bound module to seed its DRBG		N/A (Allowed in FIPS mode)	Read	N/A

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
	User	CO					
ECDSA Key-Pair generation	✓		ECDSA public/private key pair for P-224 through P-521 curves	B.4.2	FW – Cert. #A1006	Write	FIPS 186-4
			Hash-based SHA-256 DRBG from bound module		HW DRBG Cert. #A774 HW SHA Certs. #A773, #A774	Read	SP 800-90A
			NDRNG used from the bound module to seed its DRBG		N/A (Allowed in FIPS mode)	Read	N/A
Public Key Algorithms							
ECDSA Signature Generation	✓		ECDSA private key according to P-224 to P-521 curves	SHA-256, SHA-384, SHA-512	FW – Cert. #A1006	Read	FIPS 186-4
ECDSA Signature Verification	✓		ECDSA public key according to P-192 to P-521 curves	SHA-256, SHA-384, SHA-512	FW – Cert. #A1006	Read	FIPS 186-4
RSA Signature generation with PKCS1.5	✓		RSA private key pair with 2048/3072/4096 bit modulus size	SHA-256	FW – Cert. #A1006	Read	FIPS 186-4
RSA Signature Verification PKCS1.5	✓		RSA public key pair with 1024/2048/3072/4096bit modulus size	SHA-1, SHA-256	FW – Cert. #A1006	Read	FIPS 186-4
RSA Signature generation with PSS	✓		RSA private key pair with 2048/3072/4096 bit modulus size	SHA-256	FW – Cert. #A1006	Read	FIPS 186-4

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
	User	CO					
RSA Signature Verification PSS	✓		RSA public key pair with 1024/2048/3072/4096 bit modulus size	SHA-1, SHA-256	FW – Cert. #A1006	Read	FIPS 186-4
Key Derivation							
Key Derivation using 800-108 HMAC SHA-256	✓		Key derivation key and derived key	Counter Mode	FW – Cert. #A1006	Read/ Write	SP 800-108
Key Derivation using 800-108 CMAC AES-256	✓		Key derivation key and derived key	Counter mode	HW – Cert. #A1007 FW – Cert. #A1006	Read/ Write	SP 800-108
Key Wrap							
AES-CCM Key Wrapping Service (KTS)	✓		AES Symmetric key (128, 256 bit)	AES-CCM	HW – Cert. #A1007	Read	SP 800-38F
Miscellaneous							
Qualcomm Secure Processing Unit configuration set up		✓	None	N/A	N/A	N/A	N/A
Self Tests	N/A	N/A[2]	None	N/A	N/A	N/A	N/A
Show Status	✓		None	N/A	N/A	N/A	N/A
Zeroization	✓		All CSPs	N/A	N/A	Write	N/A

[2] The Self Tests due not require authentication so the Role has been marked as N/A

Table 4-3 Non-Approved Services in Non-FIPS mode

Service	Usage	Roles	
		User	CO
AES GMAC/GCM[3]	for authenticated encryption	✓	
AES-XTS[4]	for encryption/decryption	✓	
AEAD-SHA-1 AES	for authenticated encryption	✓	
AEAD-SHA-1 DES	for authenticated encryption	✓	
AEAD-SHA-1 Triple-DES	for authenticated encryption	✓	
ECC BrainpoolP256r1	for key pair generation, signature generation/verification	✓	
ECDH shared secret computation[5]	for shared secret computation	✓	
ECC curve-secp256k1	for key pair generation, signature generation/verification	✓	
HKDF[6]	for key derivation	✓	
DES	for encryption/decryption	✓	
FRP256v1	for key pair generation, signature generation/verification	✓	
HMAC SHA-1/SHA-256/SHA-384/SHA-512 with key size less than 112 bits	for hashed message authentication	✓	
RSA key wrapping with RSA OAEP	for key wrapping	✓	
RSA siggen/keygen with 1024-bit keys	for signature generation/verification	✓	
Firmware DES	for encryption/decryption	✓	

[3] GMAC/GCM is CAVP certified with Cert. #A1006. However, there are two requirements from FIPS below that contributed to the non-compliance: 1) the IV uniqueness must be enforced by the Qualcomm Secure Processing Unit; 2) FIPS required that only 2^32 cipher operations are performed with a given key. These are currently enforced by users of the Qualcomm Secure Processing Unit due to the usage model

[4] The required key check to ensure key1 does not equal key2 is not performed as required per IG A.9

[5] The ECDH shared secret computation is CAVP certified with Cert. #A1006. However, the required assurances from the section 5.6.2 of SP 800-56Arev3 are not implemented. There is a self-test for ECDH but is not listed since it is non-approved.

[6] HKDF does have a self-test but is non-approved and is not CAVP tested, so it is not listed.

Service	Usage	Roles	
		User	CO
Firmware Triple-DES for encryption/decryption (KAT is not performed)	SP 800-67r1	✓	

4.3.Authentication

The users of the Qualcomm Secure Processing Unit are the applications on the chip. Each application is signed by a unique ECDSA private key. Its signature is verified at the installation time as well as boot time. The application specific public key certificate is signed by an intermediate certificate which is in turn signed by the root private key stored on the device (3-level certificate chain), or the per-application certificate is directly signed by the root private key (2-level certificate). If the ECDSA signature verification succeeds, then the image is authenticated and hence can be loaded and executed on the Snapdragon 8cx Gen 3 Mobile Compute Platform SoC.

4.4.Strength of Authentication

The minimum ECDSA curve size that an application may use is 224 bits. According to table 1 in FIPS IG 7.5, an ECDSA curve size of 224 - 255 bits provides a minimum of 112 bits of strength and a curve size of 256 - 383 bits provides a minimum of 128 bits of strength. Therefore, the strength of the authentication mechanism in use is a minimum of $1 / 2^{112}$ or 1.925929944e-34. The ability to successfully authenticate the ECDSA signed image is dependent on the ability to guess the signing ECDSA private key that matches the verified public key. Even using a rate of 1µs per failed authentication, which would allow 60,000,000 consecutive attempts per minute (60s / 0.001s), only provides a probability of successfully authenticating that is less than or equal to $60,000,000 * 1 / 2^{112}$ (≤6.933347799e-19) which is much less than 1 / 100,000 or 0.00001.

4.5.Authentication Data Protection

The ECDSA public key stored in the read-only memory of the Qualcomm Secure Processing Unit is used as the means to verify the application. Since this memory is non-volatile read-only memory it cannot be modified.

5.Physical Security

The Qualcomm Secure Processing Unit is a sub-chip embedded in a single-chip standalone device which conforms to the Level 2 requirements for physical security. The device is a single integrated circuit in which the die is embedded in a printed-circuit board (PCB) which provides opaqueness in the visible spectrum. The Qualcomm Secure Processing Unit is contained in a tamper-evident enclosure which deters direct observation, probing, or manipulation and provides evidence of attempts to tamper with or remove the Qualcomm Secure Processing Unit. The Qualcomm Secure Processing Unit is made from production-grade components with a conformal coating that provides protection against environmental or other physical damage.

6.Operational Environment

The Qualcomm Secure Processing Unit is a single chip hardware module. The procurement, build and configuring procedure are controlled. Therefore, the operational environment is considered non-modifiable.

7.Cryptographic Key Management

7.1.Key Generation

The Secure Processing Unit bound DRBG module employs the SHA-256 Hash DRBG based on SP800-90A for the random number generation.

The Qualcomm Secure Processing Unit supports the following Approved keys/key material generation methods:

- The RSA and ECDSA keys are generated in compliance to FIPS 186-4. A seed (i.e. the random value) used in asymmetric key generation is directly obtained from SP 800-90A HASH-256 DRBG provided by the bound DRBG module. The unmodified DRBG output is used as a seed for asymmetric key generation per FIPS 186-4. It is compliant to NIST SP 800-133 and FIPS 140-2 IG D.12. None of the keys generated are output outside the physical boundary of the Qualcomm Secure Processing Unit.
- The keys are derived from the Hardware Unique Key and a Unique User ID (UUID) of the calling process using SP800-108 KDF.
- There is no dedicated symmetric key generation service.
- The Qualcomm Secure Processing Unit does not support manual key entry or intermediate key generation output.

7.2.Key Entry/Exit

The keys are input and output to and from the Qualcomm Secure Processing Unit within the same physical boundary only. The keys that are entered into the Qualcomm Secure Processing Unit can be in plain-text form or encrypted key blob form. All keys that are exported from the Qualcomm Secure Processing Unit are encrypted with AES CCM key wrapping.

7.3.Zeroization

The Secured Processor provides a means to zeroize the keys. The Secured Processor receives a request to clear the keys which will zero out the key material and free up the slot(s) occupied by the key.

7.4.Key Storage

The Cryptographic Management Unit (CMU) implements the key handling and key protection. All symmetric keys up to and including 32 bytes in length are present in its hardware-protected key store. Larger symmetric keys, and asymmetric keys are in the application space (user-space).

7.5.Key Establishment

The Qualcomm Secure Processing Unit provides key wrapping using the AES with CCM according to SP800-38F. The AES key wrapping provides 128 or 256 bits of encryption strength.

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

The Qualcomm Secure Processing Unit hardware component cannot be certified by the FCC as it is not a standalone device. It is a sub-chip imbedded in the Snapdragon8cx Gen 3 Mobile Compute Platform SoC which is also not a standalone device, but rather 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 Secure Processing Unit 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 Secure Processing Unit embedded prior to further marketing to a vendor or to a user.

9.Power up Tests

Power up self-tests consist of known-answer tests of algorithm implementations. The Qualcomm Secure Processing Unit power up tests are automatically performed without operator intervention during power up of the Qualcomm Secure Processing Unit. The power up tests are also run when a reset event is received. All self-tests are performed as a single atomic action that has two possible results: success or failure. If the result is success, the Qualcomm Secure Processing Unit becomes operational, if it is failure, the Qualcomm Secure Processing Unit enters an error state and cryptographic functions cannot be performed. To recover from the error state, re-initialization is possible by successful execution of the power up tests which can be triggered by either a power-off/power-on cycle or the receipt of a reset event.

“On demand” tests which are required by FIPS 140-2 can be performed by either of the following methods:

- A power-off/power-on cycle of the Qualcomm Secure Processing Unit
- Issuing a reset to the Qualcomm Secure Processing Unit

The Qualcomm Secure Processing Unit implements the following self-tests to ensure proper functioning of the implemented self-tests include power up self-tests of all approved algorithms.

All other cryptographic algorithm provided by the bound DRBG module are self-tested by the corresponding DRBG bound module.

9.1.Cryptographic algorithm tests (known answer tests)

Table 9-1 Power up Tests

Algorithm	Test
AES encryption (ECB)	KAT
AES decryption (ECB)	KAT
AES encryption (CCM)	KAT
AES decryption (CCM)	KAT
Triple-DES encryption (ECB)	KAT
Triple-DES decryption (ECB)	KAT
HMAC SHA-1	KAT
HMAC SHA-256	KAT
HMAC SHA-384	KAT
HMAC SHA-512	KAT
SHA-1, SHA-256, SHA-384, SHA-512	covered by respective HMAC KATs
AES-CMAC	KAT
ECDSA signature generation/verification using P-384 with SHA-384	KAT
RSA PKCSv15 and PSS. signature generation/verification with key size of 2048 using SHA-256	KAT

Algorithm	Test
KDF800-108	KAT
Error Detection Code using SHA-256 on firmware	Module Integrity
ROM Parity check on firmware in ROM	Module Integrity

9.2.Conditional Tests

The following table provides the lists of the conditional self- tests. The pair-wise consistency test is run whenever the Qualcomm Secure Processing Unit generates an asymmetric key pair. If any of the conditional test fails, the Qualcomm Secure Processing Unit enters the Error state. It returns the error code to the calling application to indicate the Error state. The Qualcomm Secure Processing Unit needs to be reinitialized in order to recover from the Error state.

Table 9-2 Conditional Tests

Algorithm	Test
RSA key generation	Pair-wise consistency test
ECDSA key generation	Pair-wise consistency test

10.Design Assurance

10.1.Configuration Management

10.1.1. Hardware

ClearCase, a version control system from IBM/Rational, is used to manage the revision control of the hardware code (Verilog code) and hardware documentation. The ClearCase version control system provides version control, workspace management, parallel development support, and build auditing. The Verilog code is maintained within the ClearCase database used by Qualcomm Technologies, Inc.

10.1.2.Software

GitLab, a version control system from GitLab Inc., is used to manage the revision control of the software code. The GitLab product provides version control, branching and merging of code lines, and concurrent development.

10.2.Crypto Officer Guidance

The Qualcomm Secure Processing Unit does not need FIPS 140-2 specific guidance. The FIPS 140-2 functional requirements are always invoked.

The Qualcomm Secure Processing Unit is determined to be a FIPS 140-2 validated module by using the validated hardware and firmware version listed in Table 2-2 and Table 2-3, as well as setting the related fuses according to Table 2-5. The fuse descriptions are defined in Table 2-4. The API **spcom_check_sp_health()** returns the struct **sp_health_status_data** below, which helps to determine if the fuses are set correctly according to Table 2-5. For more information, please refer to Qualcomm document 80-PF777-83: Qualcomm Secure Processing Unit User Guide.

typedef struct {

…

uint32_t fips_enabled;

uint32_t fips_self_test_passed;

…

.....

} **sp_health_status_data**;

The parameter **fips_enabled** will return the consolidated value of the ‘FIPS ENABLE’ and ‘FIPS OVERRIDE’ fuses (Table 2-5). The value returned will be '1' when "FIPS_ENABLE=1" and "FIPS_OVERRIDE=0". For all other cases the value returned will be '0'.:

0 - Device is not FIPS certifiable

1 – Device is FIPS certifiable

The parameter **fips_self_test_passed** will return the binary result of the self-test. The value will be returned only if device is FIPS certifiable:

0 – Power On Self Test failed

1 – Power On Self Test passed

In summary, the crypto officer should verify that the hardware version and the firmware version matches the information described in Table 2-2 and Table 2-5; and the **fips_enabled** parameter value returned from the **spcom_check_sp_health**() API is ‘1’.

10.3. User Guidance

The operation of the Qualcomm Secure Processing Unit does not need FIPS 140-2 specific guidance. The FIPS 140-2 functional requirements are always invoked.

For using the cryptographic services of the Qualcomm Secure Processing Unit, please refer to Qualcomm Technologies, Inc. document 80-PF777-83: Qualcomm Secure Processing Unit 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.

11. Mitigation of Other Attacks

Please refer to Table 11-1 for the list of counter-measure used in the Qualcomm Secure Processing Unit.

Table 11-1: List of counter-measure used

Algorithm	Implementation	Side-channel protection	Fault Detection
Triple-DES[7]	FW	Key masking (32-bit mask) Data masking (32-bit mask)	Full redundancy
AES	HW	Data masking	
RSA Decryption RSA Signature	HW+FW	Exponent blinding (in size) Message blinding (in size)	
RSA Verification	HW+FW		Double memcmp
RSA CRT	HW+FW	p and q blinding (32 bit) message blinding (in size)	
ECDSA signature	HW+FW	Key blinding (curve size) Base point blinding (curve size) Extended nonce (3n/2+32)	Consistency check on loop index Check P is on the curve
ECDSA verification	HW+FW		Double memcmp
ECDH	HW+FW	Private Key blinding (curve size) Public Key blinding (curve size)	
HMAC-SHA	HW(hash) FW(hmac scheme)	Full block (and therefore key) process in HW	

[7] Firmware DES and Triple-DES is not CAVP certified. Hardware TDES is FIPS certified but does not have counter-measure.

Terms and Abbreviations

AES	Advanced Encryption Specification
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CM	Cryptographic Module
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off The Shelf
CO	Crypto Officer
CSP	Critical Security Parameter
DES	Data Encryption Standard
DMA	Direct Memory Access
FIPS	Federal Information Processing Standards Publication
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Science and Technology
OTP	One-Time Programmable
SHA	Secure Hash Algorithm
SoC	System on Chip