Qualcomm® Secure Processing Unit (SPU)

Hardware Version 3.1

Firmware Version spss.a1.1.2_00078

FIPS 140-2 Non-Proprietary Security Policy

Version: 1.3

2019-10-07

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 3
1.1. Purpose of the Security Policy 3
2. Cryptographic Module Specification 4
2.1. Module Description 4
2.1.1. Hardware Description 4
2.1.2. Module Validation Level 5
2.2. Description of Modes of Operations 6
2.3. Cryptographic Module Boundary 6
2.3.1. Hardware Block Diagram 7
3. Cryptographic Module Ports and Interfaces 10
4. Roles, Services and Authentication 11
4.1. Roles 11
4.1.1. Crypto Officer Role 11
4.1.2. User Role 11
4.2. Services 11
4.3. Authentication 16
4.4. Strength of Authentication 16
4.5. Authentication Data Protection 17
5. Physical Security 18
6. Operational Environment 19
7. Cryptographic Key Management 20
7.1. Key Generation 20
7.2. Key Entry/Exit 20
7.3. Zeroization 20
7.4. Key Storage 20
7.5. Key Establishment 20
8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) 21
9. Power up Tests 22
9.1. Cryptographic algorithm tests (known answer tests) 22
9.2. Conditional Tests 23
10. Design Assurance 24
10.1. Configuration Management 24
10.1.1. Hardware 24
10.1.2. Software 24
10.2. Crypto Officer Guidance 24
10.3. User Guidance 25
11. Mitigation of Other Attacks 26

1.Introduction

This document is a FIPS 140-2 Security Policy for the Qualcomm Secure Processing Unit (SPU) cryptographic module. The hardware version number of the Qualcomm SPU is 3.1 and the firmware version is spss.a1.1.2_00078. This document contains a specification of the rules under which the Qualcomm SPU must operate and describes how this Qualcomm SPU 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 SPU and users of the Qualcomm SPU.

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 SPU 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 SPU meet their security requirements.

2. Cryptographic Module Specification

2.1.Module Description

The Qualcomm SPU is a single-chip hardware module implemented as a sub-chip in the Qualcomm® Snapdragon™ 855 SoC. From the validation perspective, the Qualcomm SPU is configured as a single chip hardware module.

The Qualcomm SPU is an isolated hardware security core implemented in the Qualcomm Snapdragon 855 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, RNG, 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

2.1.1.Hardware Description

The cryptographic module is implemented in the Qualcomm SPU with hardware version 3.1 and firmware version spss.a1.1.2_00078, which resides in Snapdragon 855 processors (https://www.qualcomm.com/products/snapdragon-855-mobile-platform). The Qualcomm SPU provides a series of algorithms (as listed in Table 4-2) implemented in the device hardware.

2.1.2.Module Validation Level

The Qualcomm SPU 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 SPU.

Table 2-2: Tested Platforms

Module Name	Hardware version	Test Platform
Qualcomm SPU	3.1	Snapdragon 855

Table 2-3 describes the firmware that comprises the Qualcomm SPU while Table 2-5 describes the fuse setting that defines the FIPS validated module. The FIPS validated module for Qualcomm SPU 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)	Spss2p.mbn	spss.a1.1.2_00078	Qualcomm SPU kernel
Crypto app	Crypt2p.sig		System application that performs FIPS self test
Asym crypto app	Asym2p.sig		System application

Table 2-4: Fuse descriptions

Fuse	Descriptions
FIPS ENABLE	In order to place the Qualcomm SPU 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 SPU every time it boots.
FIPS OVERRIDE	Once the Qualcomm SPU 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 SPU 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 SPU 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 SPU enters FIPS approved mode after successful completion of the power up self-tests. Invoking a non-approved service will result in the Qualcomm SPU implicitly switching to non-approved mode. After completion of the service the Qualcomm SPU 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 SPU is the physical boundary of the Snapdragon 855 SoC which contains the Qualcomm SPU which is implemented as a sub-chip. Consequently, the embodiment of the Qualcomm SPU is a Single-chip cryptographic module. The logical boundary is the Qualcomm SPU.

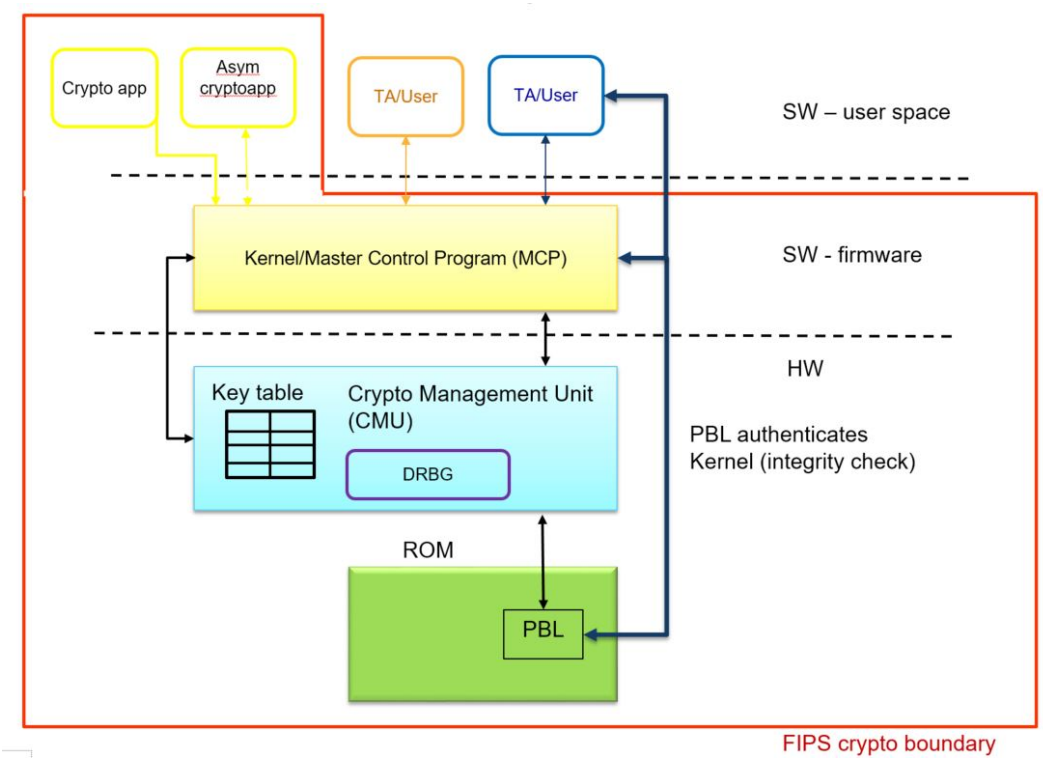


Figure 1: Qualcomm *SPU Cryptographic Boundary* for FIPS (logical diagram)

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 SPU and results received from the Qualcomm SPU 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 SPU. The remainder of the Snapdragon 855 SoC, which is not part of the Qualcomm SPU passes the Critical Security Parameters (CSP) from the software executing on top of the SoC to the Qualcomm SPU.

Figure 2: Block Diagram

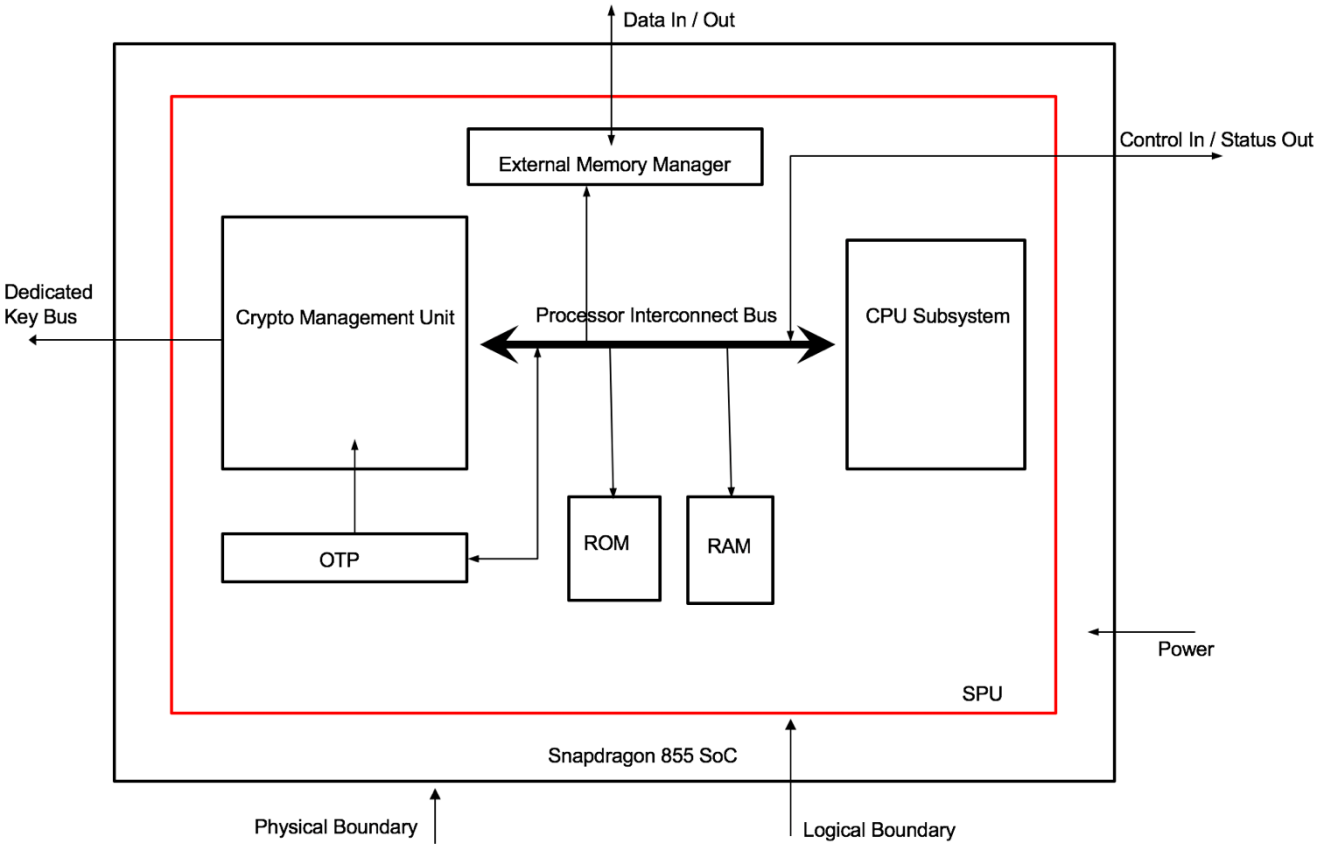
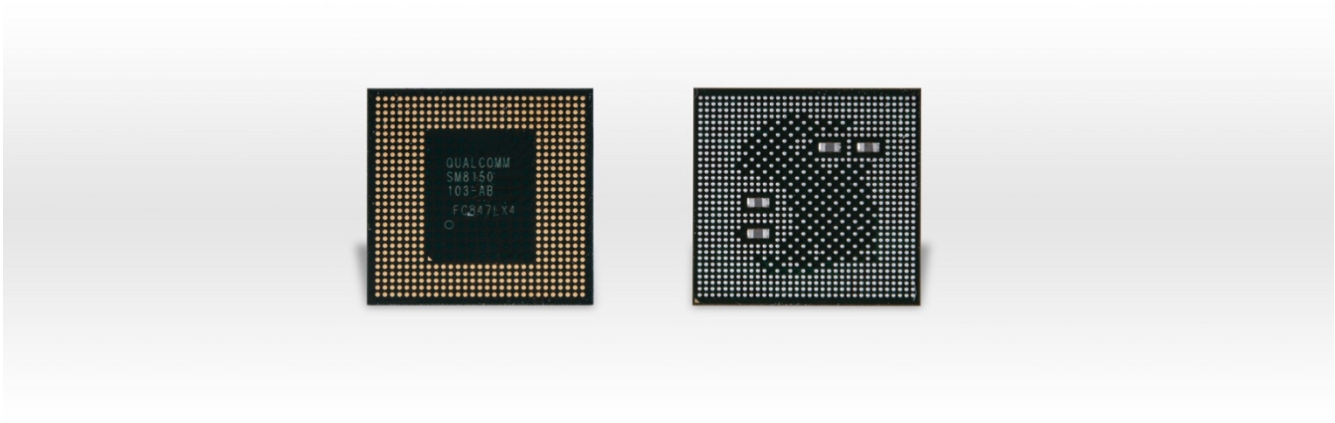


Figure 3: Snapdragon 855 processor



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 SPU'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 SPU. The Qualcomm SPU ensures that there is no means to obtain CSP or key data from the Qualcomm SPU by placing the CSPs into write-only registers preventing any entity interacting with the Qualcomm SPU from being able to read the CSPs. Additionally, key zeroization can be performed by issuing a reset event to the Qualcomm SPU. There is no means to obtain sensitive information from the Qualcomm SPU.

4.Roles, Services and Authentication

4.1.Roles

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

The Qualcomm SPU 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 SPU product delivery while 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 SPU. The User role has access to all of the Qualcomm SPU's services except Qualcomm SPU configuration set up.

Table 4-1 Roles

Role	Services
User	Utilization of cryptographic services of the Qualcomm SPU
Crypto Officer	Qualcomm SPU configuration set up

4.2.Services

The Qualcomm SPU 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 SPU is in FIPS mode of operation. When the services in Table 4-3 are performed, the Qualcomm SPU is in non-FIPS mode of 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. #C471	Read/ Write	FIPS 197, SP800-38A, SP800-38C

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
	User	CO					
Triple-DES encryption and decryption	✓		Triple DES Symmetric key (168 bits)	CBC, ECB	HW – Cert. #C454	Read/ Write	SP 800-67r1, SP800-38A
Hash Functions							
Hash operation using SHA-1	✓		None	N/A	HW – Cert. #C471	N/A	FIPS 180-4
Hash operation using SHA-256	✓		None		HW – Cert. #C471	N/A	FIPS 180-4
Hash operation using SHA-384	✓		None	N/A	HW – Cert. #C471	N/A	FIPS 180-4
Hash operation using SHA-512	✓		None	N/A	HW – Cert. #C471	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. #C471	Read/ Write	FIPS 198-1
HMAC SHA-256	✓		HMAC SHA-256 key (key length between 112 bits and 512 bits)	N/A	HW – Cert. #C471	Read/ Write	FIPS 198-1
HMAC SHA-384	✓		HMAC SHA-384 key (key length between 112 bits and 512 bits)	N/A	HW – Cert. #C471 FW – Cert. #C528	Read/ Write	FIPS 198-1

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
	User	CO					
HMAC SHA-512	✓		HMAC SHA-51 key (key length between 112 bits and 512 bits)	N/A	HW – Cert. #C471 FW – Cert. #C528	Read/ Write	FIPS 198-1
AES-CMAC generation	✓		AES Symmetric key (128, 256 bit)	CMAC	HW – Cert. #C471	Read/ Write	SP 800-38B
Random Number Generation							
Random number generation using Hash-based DRBG	✓		Entropy input string, seed, V, C	SHA-256	HW – Cert. #C433 Prerequisite[1] SHA – Certs. #C432 #C433	Read/ Write	SP 800-90A
				NDRNG used to seed Qualcomm SPU DRBG	N/A (Allowed in FIPS mode)	Read	N/A
Public Key Algorithms							
ECDH Key generation and shared secret generation	✓		ECDH public/private key pair for P-224 through P-521 curves, shared secret	6.1.2.2 Ephemeral Unified	FW – Cert. #C528	Write	FIPS 186-4, SP800-56A
ECDSA Key-Pair generation	✓		ECDSA public/private key pair for P-224 through P-521 curves	B.4.2	FW – Cert. #C528	Write	FIPS 186-4

[1] The SHA implementation tested by these certificates are used internally by the DRBG only and are not available externally to the Qualcomm SPU users.

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
	User	CO					
ECDSA Signature Generation	✓		ECDSA private key according to P-224 to P-521 curves	SHA-256, SHA-384, SHA-512	FW – Cert. #C528	Read/ Write	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. #C528	Read	FIPS 186-4
RSA Key generation with 9.31	✓		RSA public and private key pair with 2048-bit modulus size	B.3.3	FW – Cert. #C528	Write	FIPS 186-4
RSA Signature generation with PKCS1.5	✓		RSA private key pair with 2048-bit modulus size	SHA-256	FW – Cert. #C528	Read/ Write	FIPS 186-4
RSA Signature Verification PKCS1.5	✓		RSA public key pair with 1024/2048-bit modulus size	SHA-1, SHA-256	FW – Cert. #C528	Read	FIPS 186-4
RSA Signature generation with PSS	✓		RSA private key pair with 2048-bit modulus size	SHA-256	FW – Cert. #C528	Read/ Write	FIPS 186-4
RSA Signature Verification PSS	✓		RSA public key pair with 1024/2048-bit modulus size	SHA-256 SHA-1, SHA-256	HW – Cert. #C509 FW – Cert. #C528	Read	FIPS 186-4
Key Derivation							
Key Derivation using 800-108 HMAC SHA-256	✓		Key derivation key and derived key	Counter Mode	FW – Cert. #C528	Read/ Write	SP 800-108

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write)	Standard
	User	CO					
Key Derivation using 800-108 CMAC AES-256	✓		Key derivation key and derived key	Counter mode	HW – Cert. #C471 FW – Cert. #C528	Read/ Write	SP 800-108
Key Wrap							
AES-CCM Key Wrapping Service	✓		AES Symmetric key (128, 256 bit)	AES-CCM	HW – Cert. #C471	Read/ Write	SP 800-38F
Miscellaneous							
Qualcomm SPU configuration set up		✓	None	N/A	N/A	N/A	N/A
Self Tests	✓		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

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

Service	Roles	
	User	CO
AES GCM[2]	✓	
AEAD-SHA-1 AES	✓	
AEAD-SHA-1 DES	✓	
AEAD-SHA-1 Triple-DES	✓	
BrainpoolP256r1	✓	
DES	✓	
FRP256v1	✓	
HMAC SHA-1/SHA-256/SHA-384/SHA-512 with key size less than 112 bits	✓	
RSA key wrapping with RSA OAEP	✓	
RSA siggen/keygen with 1024 bit keys	✓	
Firmware DES	✓	
Firmware Triple-DES Cert. C#533 (KAT is not performed)	✓	

4.3.Authentication

The users of the Qualcomm SPU are the applications on the chip. Each application is signed by a unique RSA 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 RSA signature verification succeeds, then the image is authenticated and hence can be loaded and executed on the Snapdragon 855 SoC.

4.4.Strength of Authentication

The minimum RSA key size that an application may use is 2048-bits. According to table 1 in FIPS IG 7.5, an RSA key size of 2048 bits provides a minimum of 112 bits of strength and a key size of

[2] GCM is CAVP certified with Cert. #C528. However, there are two requirements from FIPS below that contributed to the non-compliance: 1) the IV uniqueness must be enforced by the Qualcomm SPU; 2) FIPS required that only 2^32 cipher operations are performed with a given key. These are currently enforced by users of the Qualcomm SPU due to the usage model.

3072 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 RSA signed image is dependent on the ability to guess the signing RSA 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 RSA public key stored in the read-only memory of the Qualcomm SPU 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 SPU 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 SPU 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 SPU. The Qualcomm SPU is made from production-grade components with a conformal coating that provides protection against environmental or other physical damage.

6.Operational Environment

The Qualcomm SPU 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 Qualcomm SPU employs the SHA-256 Hash DRBG based on SP800-90A for the random number generation. To seed the DRBG, the Qualcomm SPU uses a Non-Deterministic Random Number Generator (NDRNG) as the entropy source. The NDRNG is based on a series of ring oscillators. The NDRNG provides 256 bits of entropy to the DRBG. The Qualcomm SPU performs continuous random number generator test on the output of NDRNG to ensure that consecutive random numbers do not repeat, and implements the health tests for the DRBG as defined in section 11.3 of SP800- 90A.

The Qualcomm SPU supports the following Approved keys/key material generation methods:

- The RSA, ECDSA, and ECDH 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. 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 SPU.
- 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 SPU 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 SPU within the same physical boundary only. The keys that are entered into the Qualcomm SPU can be in plain-text form or encrypted key blob form. All keys that are exported from the Qualcomm SPU 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 SPU implements key agreement scheme based on SP800-56A without KDF. The Qualcomm SPU provides EC Diffie-Hellman shared secret computation with curves P-224 through P-521, providing 112 to 256 bit equivalent security strength.
The Qualcomm SPU also 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 SPU hardware component cannot be certified by the FCC as it is not a standalone device. It is a sub-chip imbedded in the Snapdragon 855 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 SPU 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 SPU 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 SPU power up tests are automatically performed without operator intervention during power up of the Qualcomm SPU. 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 SPU becomes operational, if it is failure, the Qualcomm SPU 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 SPU
- Issuing a reset to the Qualcomm SPU

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

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	KAT
ECDH	KAT
RSA	KAT
DRBG800-90A	KAT
KDF800-108	KAT
RSA signature verification 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 SPU generates an asymmetric key pair. If any of the conditional test fails, the Qualcomm SPU enters the Error state. It returns the error code to the calling application to indicate the Error state. The Qualcomm SPU 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
NDRNG	Continuous 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 SPU does not need FIPS 140-2 specific guidance. The FIPS 140-2 functional requirements are always invoked.

The Qualcomm SPU 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 in Android, 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 SPU User Guide.

typedef struct {

uint32_t ari_mode;

uint32_t ari_fuse_gauge;

uint32_t fips_enabled;

uint32_t fips_self_test_passed;

uint32_t sensors_calibrated;

.....

} **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 SPU 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 SPU, please refer to Qualcomm Technologies, Inc. document 80-PF777-83: Qualcomm SPU 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 SPU.

Table 11-1: List of counter-measure used

Algorithm	Implementation	Side-channel protection	Fault Detection
Triple-DES[3]	FW	Key masking (32 bit mask) Data masking (32 bit mask)	Full redundancy
AES	HW	Data masking	
RSA Decryption RSA Signature	HW+FW	Exponent binding (in size) Message binding (in size)	
RSA Verification	HW+FW		Double memcmp
RSA Encryption	HW+FW		
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	

[3] Firmware DES and Triple-DES is CAVP certified only. 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