Qualcomm® Secure Processing Unit (SPU) Random Number Generator (RNG)

Module Version 2.0

FIPS 140-2 Non-Proprietary Security Policy

Version 1.1

Last Update: 2021-04-13

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 the non-proprietary FIPS 140-2 Security Policy for the Qualcomm Secure Processing Unit (SPU) Random Number Generator (RNG) cryptographic module. The version number of the Qualcomm SPU RNG is 2.0. This document contains a specification of the rules under which the Qualcomm SPU RNG must operate. It also describes how the Qualcomm SPU RNG meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2) for Security Level 1 hardware cryptographic modules.

1.1 Purpose of the Security Policy

There are three major reasons that a security policy is needed:

- It is required for FIPS 140-2 validation.
- It allows individuals and organizations to determine whether the Qualcomm SPU RNG, as implemented, satisfies the stated security policy.
- It describes the capabilities, protections, and access rights provided by the Qualcomm SPU RNG. This essential information will help individuals and organizations determine whether Qualcomm SPU RNG will meet their security requirements.

2 Cryptographic Module Specification

2.1 Description of Module

The Qualcomm SPU RNG Is classified as a single chip hardware module for the purpose of FIPS 140-2 validation. It is designed to provide random numbers. The Qualcomm SPU RNG is a sub-chip hardware component contained within the Qualcomm® Snapdragon™ 888 5G Mobile Platform SoC. The Qualcomm SPU RNG implements a SHA-256 Hash DRBG as defined in SP 800-90A and a NDRNG used to seed the DRBG.

The hardware sub-chip cryptographic modules are specified in the following table:

Component	Type	Version Number
Qualcomm SPU RNG	hardware	2.0

Table 1: Components of the Hardware Cryptographic Module

The Qualcomm SPU RNG has been tested on the following platforms:

Module Name	Hardware version	Test Platform
Qualcomm SPU RNG	2.0	Snapdragon 888 5G Mobile Platform

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

FIPS 140-2 Sections	Security Level				
	N/A	1	2	3	4
Cryptographic Module Specification		X			
Cryptographic Module Ports and Interfaces		X			
Roles, Services and Authentication		X			
Finite State Model		X			
Physical Security		X			
Operational Environment	X				
Cryptographic Key Management		X			
EMI/EMC		X			
Self-Tests		X			
Design Assurance		X			

Mitigation of Other Attacks	X				

Table 2: Security Levels

2.2 Description of Approved Mode

The Qualcomm SPU RNG supports only a FIPS mode which is entered without any special configurations. All possible configurations entered via the registers are supported and do not violate the constraints of the FIPS mode.

When the Qualcomm SPU RNG is powered on, the power-up self-test is executed automatically without any operator intervention. The Qualcomm SPU RNG enters FIPS mode automatically if the power-up self-test completes successfully.

If any of self-tests fail during power-up, the Qualcomm SPU RNG goes into Error state. All cryptographic services are prohibited while in error state. When an error state is entered, the Qualcomm SPU RNG can be reset to reinitialize itself.

The status of the Qualcomm SPU RNG can be determined by its availability. If the Qualcomm SPU RNG is available, it has passed all self-tests. If it is unavailable, it is in the error state.

The Qualcomm SPU RNG provides the following CAVP validated algorithms (Note that the Qualcomm SPU RNG has two cores each implementing SHA-256) and the allowed algorithm:

Algorithms	Standards	CAVS Certs #
SHA-256 Hash DRBG	SP-800-90A	Cert.#: A774
SHA-256 (core 1)	FIPS 198-1	Cert.#: A774
SHA-256 (core 2)	FIPS 198-1	Cert.#: A773
NDRNG used to seed DRBG	N/A	N/A (Allowed)

Table 3: Approved and Allowed Algorithms

2.3 Cryptographic Module Boundary

The physical boundary of the Qualcomm SPU RNG is the physical boundary of the Snapdragon 888 5G Mobile Platform SoC, that contains the sub-chip which implements the Qualcomm SPU RNG version 2.0. Consequently, the embodiment of the Qualcomm SPU RNG is a single-chip standalone cryptographic module. The logical boundary is the Qualcomm SPU RNG, version 2.0.

The following figure illustrates the various data, status and control paths through the physical and logical boundary of the Qualcomm SPU RNG.

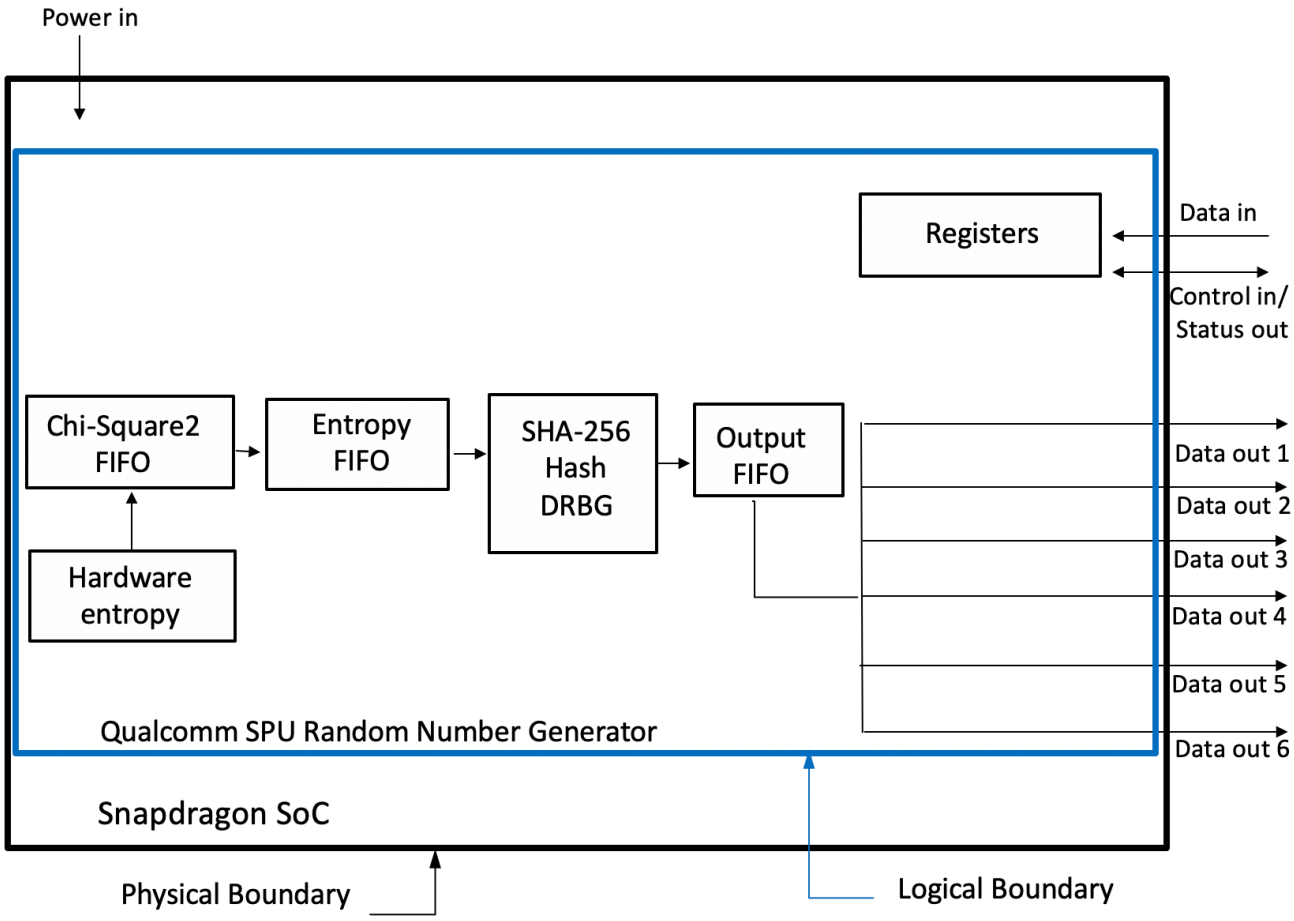

Figure 1: Cryptographic Boundary

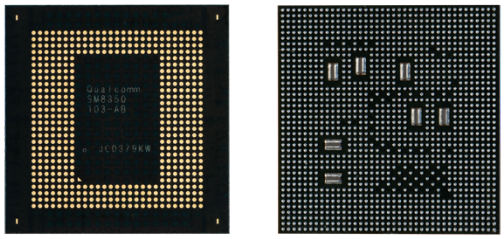

Figure 2: Snapdragon 888 5G Mobile Platform

3 Cryptographic Module Ports and Interfaces

FIPS Interface	Ports
Data Input	Registers
Data Output	FIFO
Control Input	Registers
Status Output	Registers
Power Input	Physical power connector

Table 4: Ports and Interfaces

As indicated in Table 4, all status output and control input are directed through the interface of the Qualcomm SPU RNG's logical boundary, which is the registers of the Qualcomm SPU RNG. For data input, the registers provide the interface. For data output, the FIFO provides random data to a set of defined interfaces.

4 Roles, Services and Authentication

4.1 Roles

Role	Description
User	Perform general security services, including cryptographic operations and other approved security functions.
Crypto Officer (CO)	Configuration of the Qualcomm SPU RNG.

Table 5: Roles

The Qualcomm SPU RNG meet all FIPS 140-2 Security Level 1 requirements for Roles and Services, implementing both User and Crypto Officer roles. It does not allow concurrent operators.

The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the Qualcomm SPU RNG.

4.2 Services

The Qualcomm SPU RNG does not support bypass capability. It provides random data from the SHA-256 Hash DRBG. The following table describes the services available in FIPS-mode:

Service	Roles		CSP	Access (Read, Write)
	User	CO		
Approved				
SHA-256-Hash-DRBG	✓		Seed, entropy input string, nonce, internal state values C and V	R,W
Self-Test (Self-Test is executed automatically when device is booted or restarted)	✓		N/A	N/A
Check Status/Get State	✓		N/A	N/A
Module Configuration		✓	N/A	N/A
Zeroization	✓		Seed, entropy input string, nonce, internal state values C and V	R,W
Non-approved but Allowed				
NDRNG	✓		Entropy input string, nonce	R

Table 6: Services

4.3 Operator Authentication

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

5 Physical Security

The Qualcomm SPU RNG is a sub-chip module implemented as part of the Snapdragon 888 5G Mobile Platform SoC, which is the physical boundary of the sub-chip module. The Snapdragon 888 5G Mobile 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 Qualcomm SPU RNG 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 Random Number Generation

Hardware is used to collect random bits as the entropy seed (i.e., the entropy input string and the nonce) for the Qualcomm SPU RNG to generate FIPS 140-2 compliant random numbers.

The DRBG used to generate random numbers is a SP 800-90A compliant SHA-256 Hash DRBG using a derivation function without prediction resistance. It processes a personalization string that is written by the calling application into a hardware register for use by the Qualcomm SPU RNG. The calling application has read/write access to the hardware register that holds the personalization string.

The implementation performs a continuous self-test, a health check, and a power-on self-test. A re-seed process is applied to the DRBG. The re-seed frequency is programmable, up to 2^32 blocks of data.

When the DRBG is instantiated, it runs a self-test with a set of test vectors. It also runs a health check test to verify that the instantiation function and generation function are able to handle any incorrect parameter inputs, such as, a negative number for the input data length, etc. The DRBG implements a continuous self-test that verifies the random number generation. The self-test compares the output bits with the generated bits from the previous round and ensures that they do not match.

The entropy source for the DRBG originates from two entropy sources that have 8 ring oscillators. The NDRNG consists of the combined data streams of the entropy sources which is fed into the DRBG. The DRBG also implements a derivation function to counter any slight imperfections in the entropy stream. Based on an analysis of the entropy output and the use of a 256 bit entropy value along with a 128 bit nonce, it has been determined that the input random data into the approved HASH DRBG contains at least 256 bits of security strength.

The output of the noise source is processed by a continuous self-test which compares the output bits with the generated bits from the previous round and ensures that they do not match.

7.2 Key and CSP List

The entropy input string and the nonce inputs to the DRBG are generated internal to the hardware Qualcomm SPU RNG and do not have an external interface.

The following table lists the CSP in the Qualcomm SPU RNG:

CSP	Generation	Storage	Zeroization
entropy input string and nonce	Hardware NDRNG	Internal registers	Reset event
DRBG Seed, internal state values (C and V)	During DRBG initialization	Internal registers	Reset event

Table 7: Keys and CSPs

7.3 Key/CSP Generation, Entry and Output

The Qualcomm SPU RNG does not provide any key generation service or perform key generation for any of its Approved algorithms. The caller of the DRBG can use the output for key generation.

The Qualcomm SPU RNG does not provide any asymmetrical algorithms or key establishment methods.

7.4 Key/CSP Storage and Zeroization

The entropy input string and nonce used by the DRBG are generated internally by the hardware and are not accessible externally to the Qualcomm SPU RNG. The personalization string is input by the caller of the DRBG into a register that is able to be read from and written to by the caller.

Zeroization of the DRBG CSPs is accomplished by either a reset event or a power-off/power-on cycle of the DRBG.

8 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The CM hardware component cannot be certified by the FCC as it is not a standalone device. It is a sub-chip embedded in the Snapdragon 888 5G Mobile Platform SoC, which is also not standalone devices. It 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 CM 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 CM embedded prior to further marketing to a vendor or user.

9 Power-Up Tests

Power-Up tests consist of Known-Answer-Tests (KAT) used for algorithm implementations. The power-up self-tests are automatically performed without any operator intervention during power-up of the Qualcomm SPU RNG. If any of the power-up self-tests fail, the Qualcomm SPU RNG will enter the error state. Data output is prohibited and no further cryptographic operation is allowed while in the error state. The Qualcomm SPU RNG can be reset to recover from the error state. Re-initialization is also possible by doing a power-cycle to set the Qualcomm SPU RNG to the power-on state.

FIPS 140-2 explicitly allows that the on-demand test can be fulfilled with a power cycle of the Qualcomm SPU RNG. Hence, a power cycle and its associated power-on self-test is the methodology used to perform the "on-demand" tests.

9.1 Cryptographic Algorithm Tests

Algorithm	Test
SP 800-90A DRBG	KAT for DRBG only
SHA-256	KAT performed for both SHA-256 cores independently

Table 8: Power-Up Cryptographic Algorithm Tests

9.2 Conditional Tests

The following table provides the lists of the conditional self- tests. If any of the conditional test fails, the Qualcomm SPU RNG will enter the error state. The Qualcomm SPU RNG needs to be reset in order to recover from the error state.

Algorithm	Test
SP 800-90A DRBG	Continuous Random Number Generator Test
Hardware NDRNG	Continuous Random Number Generator Test

Table 9: Conditional Tests

10 Design Assurance

The Qualcomm SPU RNG is implemented in hardware and is not modifiable; therefore, no integrity test is required.

10.1 Configuration Management

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.

11 Crypto Officer Guidance

The Crypto Officer needs to follow specific steps as part of the configuration of the module. The following is a list of high-level steps required. Please refer to the Secure Processor Hardware Programming Guide section 10.4.1 for details.

- Verify the clocks are running
- Enable the RNG LFSR
- Enable the RNG Health check
- Configure the DRBG initialization parameters as listed in section 10.4.1 of the Hardware Programming Guide
- Enable the DRBG

12 Mitigation of Other Attacks

No other attacks are mitigated.

13 Glossary and Abbreviations

ASG	Alternating Step Generator
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CMU	Cryptographic Management Unit
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standards Publication
KAT	Known Answer Test
NIST	National Institute of Science and Technology
PASG	Parallel Alternating Step Generator
SHA	Secure Hash Algorithm
SoC	System on Chip

14 References

[1] FIPS 140-2 Standard,
http://csrc.nist.gov/groups/STM/cmvp/standards.html

[2] FIPS 140-2 Implementation Guidance,
http://csrc.nist.gov/groups/STM/cmvp/standards.html

[3] FIPS 180-4 Secure Hash Standard,
http://csrc.nist.gov/publications/PubsFIPS.html

[4] NIST Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators
https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final