Qualcomm Technologies, Inc.

Qualcomm® Pseudo Random Number Generator

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1

Document Date: 2026-04-06

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

https://www.atsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

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

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

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	N/A
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

1.3 Additional Information

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

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Qualcomm Pseudo Random Number Generator is classified as a single chip hardware module for the purpose of FIPS 140-3 validation. It is designed to provide random numbers. The Qualcomm Pseudo Random Number Generator is a collection of hardware components contained within the Snapdragon® 8 Elite Mobile Platform SoC. The Qualcomm Pseudo Random Number Generator implements a SHA-256 Hash_DRBG as defined in SP 800-90Ar1.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: SubChip

Tested Operational Environment's Physical Perimeter (TOEPP): The physical perimeter of the Qualcomm Pseudo Random Number Generator is the physical perimeter of the Snapdragon 8 Elite Mobile Platform that contains the components which implement the Qualcomm Pseudo Random Number Generator. Consequently, the embodiment of the Qualcomm Pseudo Random Number Generator is a single-chip cryptographic module. Below is an illustrative diagram.

Cryptographic Boundary:

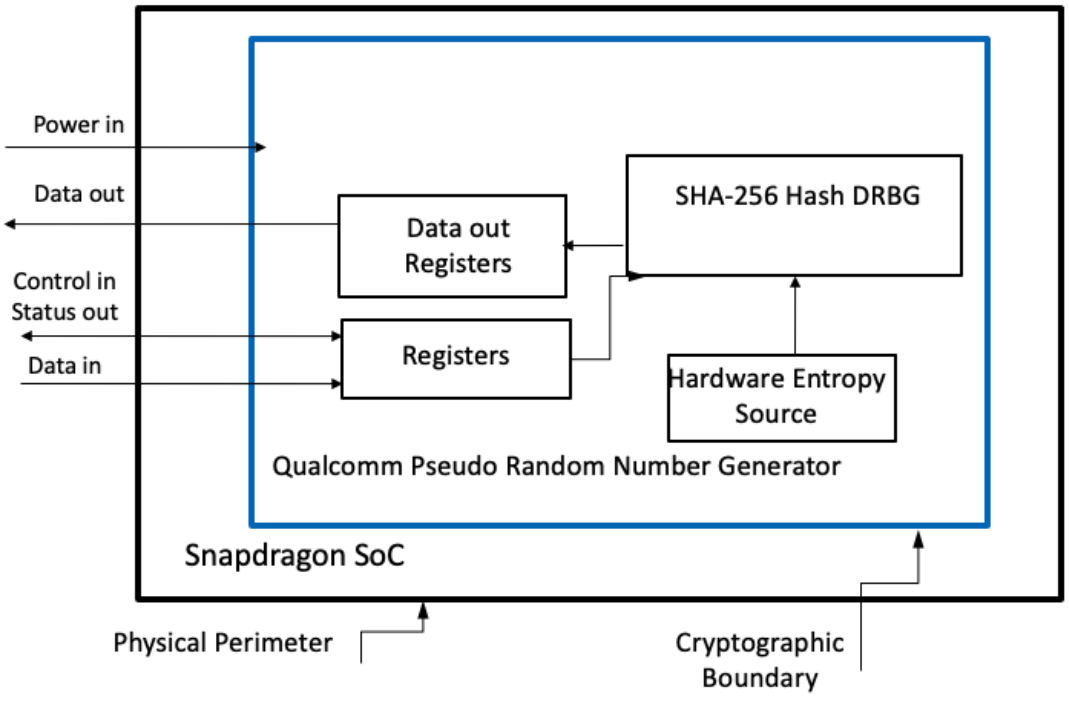

Figure 1: Block Diagram

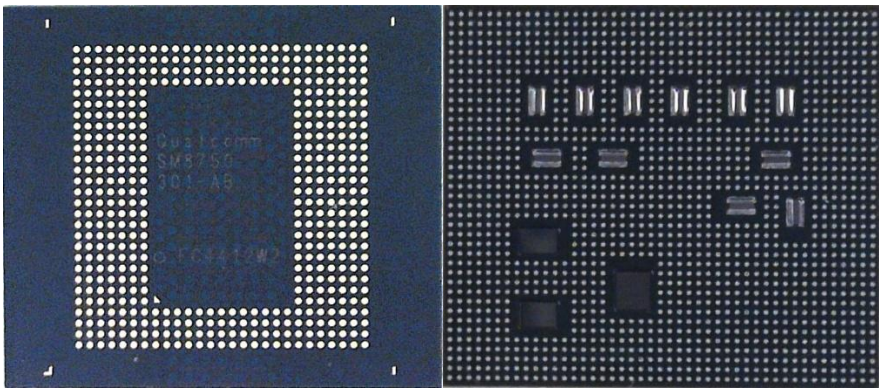

Figure 2: Snapdragon 8 Elite Mobile Platform

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Snapdragon® 8 Elite Mobile Platform	3.4.0	N/A	Snapdragon® 8 Elite Mobile Platform	N/A

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

N/A for this module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	Automatically entered whenever an approved service is requested	Approved	Equivalent to the indicator of the requested service

Table 3: Modes List and Description

The Qualcomm Pseudo Random Number Generator supports only an approved mode which is entered without any operator intervention.

When the Qualcomm Pseudo Random Number Generator is powered on, the pre-operational self-test and cryptographic algorithm self-tests are executed automatically without any operator intervention. The

Qualcomm Pseudo Random Number Generator enters the operational mode automatically if all self-tests complete successfully.

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

The status of the Qualcomm Pseudo Random Number Generator module can be determined by its availability. If the Qualcomm Pseudo Random Number Generator is available, it has passed all self-tests. If it is unavailable, it is in the error state.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
Hash DRBG	A6453	Prediction Resistance - No Mode - SHA2-256	SP 800-90A Rev. 1
SHA2-256	A6452	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-256	A6453	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Random number generator	DRBG	Random number generator		Hash DRBG: (A6453)

Name	Type	Description	Properties	Algorithms
Hash for DRBG	SHA	Hash for both DRBG core		SHA2-256: (A6452, A6453)

Table 5: Security Function Implementations

2.7 Algorithm Specific Information

Not applicable.

2.8 RBG and Entropy

Cert Number	Vendor Name
E207	Qualcomm Technologies, Inc.

Table 6: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Entropy Source of the Qualcomm® Pseudo Random Number Generator	Physical	Snapdragon® 8 Elite Mobile Platform	4	0.372050	

Table 7: Entropy Sources

The DRBG used to generate random bits is an SP 800-90Ar1 compliant SHA-256 Hash_DRBG without prediction resistance. It processes a personalization string that is written by the calling application into a hardware register for use by the module. The calling application has read/write access to the hardware register that holds the personalization string.

The DRBG obtains 640 samples from the entropy source to form its seed. Each sample consists of 4 bits. As these 640 samples provide 238 bits of entropy, the DRBG is limited to 238 bits of effective security strength in its output. Consequently, the module generates random strings whose strengths are modified by available entropy.

2.9 Key Generation

The module does not provide any SSP generation service or perform SSP generation for any of its approved algorithms. The caller of the DRBG could use the random strings output for SSP generation, but this service is not explicitly provided by the module.

2.10 Key Establishment

The module does not provide any kind of SSP establishment, entry, or output.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Registers	Data Input	Input parameters for data
Data Out Registers	Data Output	Output parameters for data
Registers	Control Input	Input parameters for control
Registers	Status Output	Return code, status values
Physical power connector	Power	Power port or pin for single-chip

Table 8: Ports and Interfaces

The module does not implement a control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The Qualcomm Pseudo Random Number Generator meets all FIPS 140-3 Security Level 1 requirements for Roles and Services, implementing the Crypto Officer role. It does not allow concurrent operators.

The Crypto Officer role is implicitly assumed by the entity accessing services implemented by the module. No authentication is required. The Crypto Officer can initialize the Qualcomm Pseudo Random Number Generator and perform the approved services.

4.2 Roles

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

Table 9: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
SHA-256 Hash_DRBG	Hash_DRBG that uses SHA-256	RNG_CM_PRNG_CHAR_STATUS register field bit 1 set to 0	Personalization string, requested output length	Random string	Random number generator Hash for DRBG	Crypto Officer (CO) - entropy input string: W,E - DRBG internal state V and C: G,E,W - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						seed: G,E
Self-test	Self-Test is executed automatically when device is booted or restarted	None	N/A	Pass/Fail	Hash for DRBG Random number generator	Crypto Officer (CO)
Show Status	Show status of the module state	None	N/A	status	None	Crypto Officer (CO)
Zeroization	Zeroizes all SSPs in the module	None	All SSPs	None	None	Crypto Officer (CO) - entropy input string: Z - DRBG internal state V and C: Z - DRBG seed: Z
Show version	Show the version of the module	None	N/A	module version	None	Crypto Officer (CO)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show identifier	Show the identifier of the module	None	N/A	Module identifier (value is 0x00000002)	None	Crypto Officer (CO)

Table 10: Approved Services

The following access rights are used in the table:

- **G** = **Generate**: The module generates or derives the SSP.
- **R** = **Read**: The SSP is read from the module (e.g. the SSP is output).
- **W** = **Write**: The SSP is updated, imported, or written to the module.
- **E** = **Execute**: The module uses the SSP in performing a cryptographic operation.
- **Z** = **Zeroise**: The module zeroises the SSP.

The Qualcomm Pseudo Random Number Generator does not support bypass capability.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

Not applicable.

5 Software/Firmware Security

5.1 Integrity Techniques

The Qualcomm Pseudo Random Number Generator does not support any software or firmware component. Therefore, this section is not applicable.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

How Requirements are Satisfied:

The Qualcomm Pseudo Random Number Generator is a single chip hardware module at security level 1. The operational environment is non-modifiable.

6.2 Configuration Settings and Restrictions

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

7 Physical Security

7.1 Mechanisms and Actions Required

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

Table 11: Mechanisms and Actions Required

The Qualcomm Pseudo Random Number Generator Cryptographic Module is a single-chip hardware module which conforms to the level 2 requirements for physical security. The Qualcomm Pseudo Random Number Generator is a single chip enclosed in a production grade component.

At the time of manufacturing, the die is embedded within a printed circuit board (PCB), which prevents visibility into the internal circuity of the Qualcomm Pseudo Random Number Generator. The layering process which is used to embed the die into the PCB also prevents tampering of the physical components without leaving tamper evidence.

The Qualcomm Pseudo Random Number Generator is further protected by being enclosed in commercial off the shelf mobile device utilizing production grade commercially available components and that the mobile device enclosure completely surrounds the Qualcomm Pseudo Random Number Generator.

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

8 Non-Invasive Security

The Qualcomm Pseudo Random Number Generator does not support any non-invasive security techniques, this section is not applicable.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Hardware Registers	Holds the SSP data for the module	Dynamic

Table 12: Storage Areas

9.2 SSP Input-Output Methods

N/A for this module.

There are no SSPs entered into or output from the Qualcomm Pseudo Random Number Generator. The entropy input string is obtained from entropy source within the cryptographic boundary.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power-off	All SSPs will be zeroized	The registers holding the SSPs are set to all zeroes	Operator can initiate this zeroization method by powering off the module

Table 13: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
entropy input string	entropy input string used for seeding the module's DRBG;	2560 bits - 238 bits	Entropy Data - CSP			Random number generator
DRBG seed	DRBG seed used for seeding the module's DRBG;	440 bits - 238 bits	Entropy Data - CSP	Random number generator		Random number generator
DRBG internal state V and C	DRBG internal state V and C used for random number generation;	V: 440 bits; C: 440 bits - 238 bits	DRBG internal state values - CSP	Random number generator		Random number generator

Table 14: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
entropy input string		Hardware Registers:Plaintext	Until module reset	Power-off	DRBG internal state V and C:Derives DRBG seed:Derives
DRBG seed		Hardware Registers:Plaintext	Until module reset	Power-off	DRBG internal state V and C:Derives
DRBG internal state V and C		Hardware Registers:Plaintext	Until module reset	Power-off	DRBG seed:Derived From

Table 15: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

N/A for this module.

The integrity test is not applicable since the Qualcomm Pseudo Random Number Generator is implemented in hardware and is non-modifiable. There are no bypass or critical function tests.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Hash DRBG	SHA2-256	KAT	CAST	Module becomes operational	SP800-90Arev1 section 11.3 Health test: instantiate, reseed,, generate functions	Test runs at Power-on
Entropy Source Health Tests - Startup	RCT with cutoff value of 51 and APT with cutoff value of 433.	Startup Test	CAST	Module becomes operational	RCT and APT performed on 1024 noise source samples (4096 bits).	Tests ran at startup as defined in SP800-90B
Entropy Source Health Tests - Continuous	RCT with cutoff value of 51 and APT with cutoff value of 433	Continuous Test	CAST	Module remains operational	RCT and APT performed	Continuous running of tests as defined in SP800-90B
SHA2-256	SHA2-256 for DRBG	KAT	CAST	Module becomes operational	Message digest	Test runs at Power-on

Table 16: Conditional Self-Tests

Conditional tests are performed automatically without any operator intervention during power-up of the Qualcomm Pseudo Random Number Generator; these tests ensure that the cryptographic algorithms work as expected. While the conditional tests are executing, services are not available, and input and output are inhibited.

The entropy continuous health tests are performed throughout the operation of the module.

10.3 Periodic Self-Test Information

N/A for this module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Hash DRBG	KAT	CAST	On Demand	Manually
Entropy Source Health Tests - Startup	Startup Test	CAST	On Demand	Manually
Entropy Source Health Tests - Continuous	Continuous Test	CAST	On Demand	Manually
SHA2-256	KAT	CAST	On Demand	Manually

Table 17: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	No cryptographic operation can be performed. No data input or output is possible.	CAST in Hardware failure Startup/continuous health test failure	Power cycling	BIST_FAILURE indicator is set or TZ_RNG_STATUS__PRNG_PERMANENT_FAILURE is set

Table 18: Error States

If any of the conditional self-tests fail, the Qualcomm Pseudo Random Number Generator will enter the error state. Data output is prohibited, and no further cryptographic operation is allowed in the error state. This is performed by the control logic and prevents external usage when an error is detected.

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. Once in the error state, the Qualcomm Pseudo Random Number Generator will only respond to a reset which will cause it to re-execute the power up tests. If the error persists, the Qualcomm Pseudo Random Number Generator will remain unavailable.

10.5 Operator Initiation of Self-Tests

A power cycle or reset event is the methodology used to perform the pre-operational and conditional self-tests.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Qualcomm Pseudo Random Number Generator is a single chip module in the Snapdragon 8 Elite Mobile Platform. The chips are delivered from the vendor via a trusted delivery courier. Upon delivery, the customer can detect any potential tampering by visually inspecting the chips. Any tampering will result in obvious damage or scratches and will likely render the chips non-functional. Once the product is received by the customer and powered up the self-tests defined in Section 10 will be executed.

11.2 Administrator Guidance

There is no specific crypto officer guidance required for the module.

11.3 Non-Administrator Guidance

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

11.4 Design and Rules

Not applicable.

11.5 Maintenance Requirements

Not applicable.

11.6 End of Life

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

12 Mitigation of Other Attacks

The module does not implement security mechanisms to mitigate other attacks.

Appendix A. Glossary and Abbreviations

CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standards Publication
KAT	Known Answer Test
SoC	System on Chip

Appendix B. References

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

FIPS140-3_IG **Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program**
March 2023
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements

FIPS180-4 **Secure Hash Standard (SHS)**
March 2012
https://doi.org/10.6028/NIST.FIPS.180-4

SP800-90Ar1 **NIST Special Publication 800-90A - Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators**
June 2015
http://dx.doi.org/10.6028/NIST.SP.800-90Ar1

SP800-90B **(Second DRAFT) NIST Special Publication 800-90B - Recommendation for the Entropy Sources Used for Random Bit Generation**
January 2018
https://doi.org/10.6028/NIST.SP.800-90B

SP800-140B **NIST Special Publication 800-140B - CMVP Security Policy Requirements**
March 2020
https://doi.org/10.6028/NIST.SP.800-140Br1