Qualcomm Technologies, Inc.

Qualcomm® Pseudo Random Number Generator

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0

Last update: 2026-03-31

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

https://www.atsec.com

Snapdragon and Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries.

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	1
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 firmware-hybrid 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 and firmware components contained within the Snapdragon® 4 Gen 2 Mobile Platform, Qualcomm® QCM4490 and Qualcomm® QCS4490 SoCs. The Qualcomm Pseudo Random Number Generator version 3.2.0 implements a SHA2-256 Hash_DRBG as defined in SP 800-90Ar1. The firmware component of the module controls the entropy and DRBG configuration parameters. The configuration is fixed for a given version of the firmware and cannot be altered by the operator of the module.

Module Type: Firmware-hybrid

Module Embodiment: SingleChip

Cryptographic Boundary:

The physical perimeter of the Qualcomm Pseudo Random Number Generator is the physical perimeter of the Snapdragon 4 Gen 2 Mobile Platform, QCM4490 and QCS4490 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.

Tested Operational Environment's Physical Perimeter (TOEPP):

The TOEPP of the module is the entire system-on-chip.

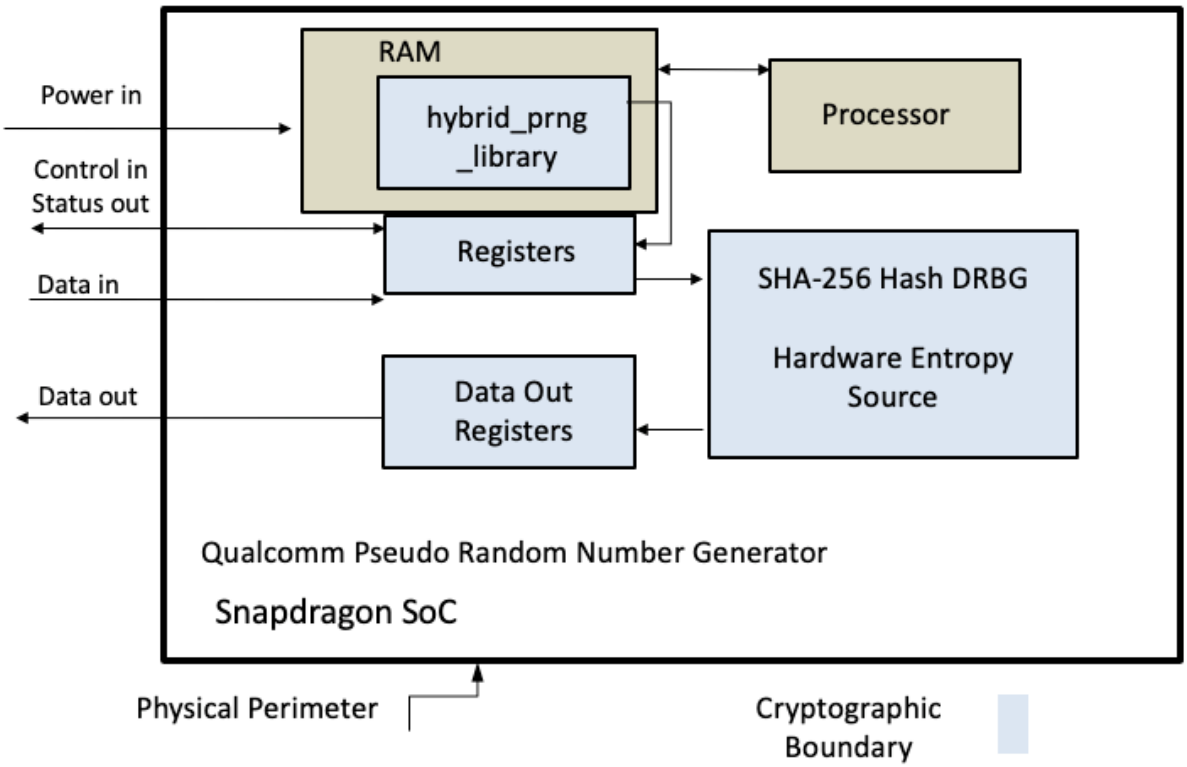

Figure 1: Block Diagram

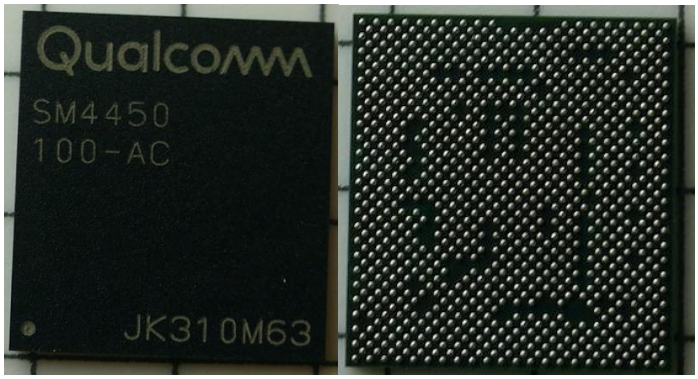

Figure 2: Snapdragon 4 Gen 2 Mobile Platform

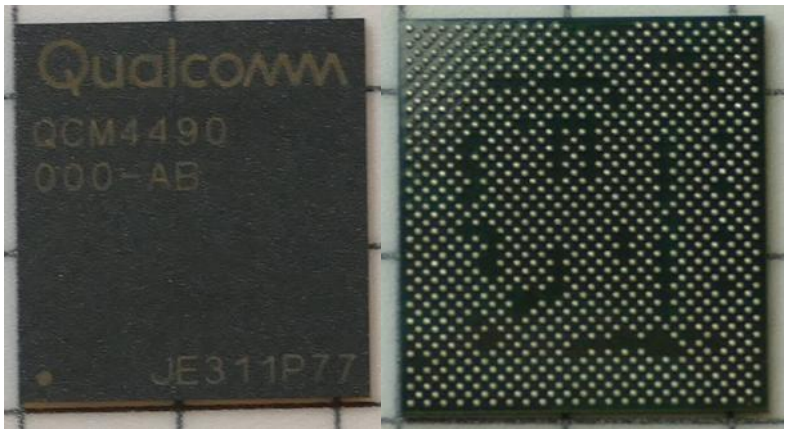

Figure 3: QCM4490

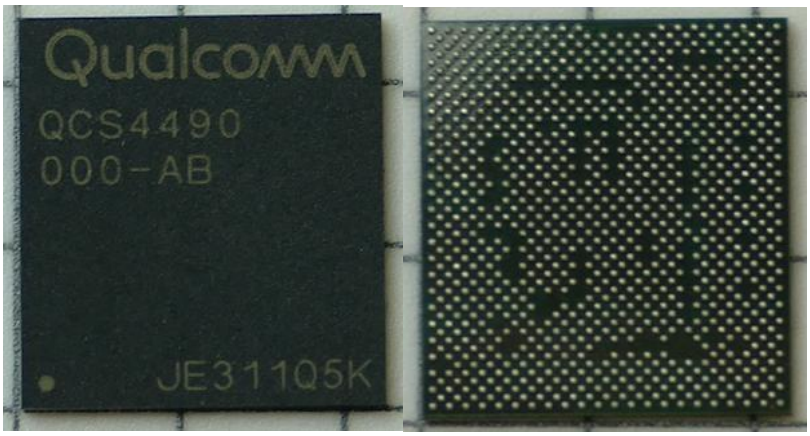

Figure 4: QCS4490

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Features	Integrity Test
hybrid_prng_library	43852ab90e520239a8b6177cd51fe534551e4987ffcce8e351d6b52ecdd92f22dd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d	N/A	SHA-256

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Single Chip: Qualcomm - Snapdragon 4 Gen 2 Mobile Platform Sub-Chip Disjoint Hardware: Hash-DRBG	3.2.0	N/A	Snapdragon 4 Gen 2 Mobile Platform	N/A
Single Chip: Qualcomm - QCM4490 Sub-Chip Disjoint Hardware: Hash-DRBG	3.2.0	N/A	QCM4490	N/A
Single Chip: Qualcomm - QCS4490 Sub-Chip Disjoint Hardware: Hash-DRBG	3.2.0	N/A	QCS4490	N/A

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
Qualcomm® Trusted Execution Environment (TEE) TZ.XF.5.18	Snapdragon 4 Gen 2 Mobile Platform	Snapdragon 4 Gen 2 Mobile Platform	No	N/A	43852ab90e520239a8b6177cd51fe534551e4987ffcce8e351d6b52ecdd92f22dd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d
Qualcomm TEE TZ.XF.5.18	QCM4490	QCM4490	No	N/A	43852ab90e520239a8b6177cd51fe534551e4987ffcce8e351d6b52ecdd92f22dd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d
Qualcomm TEE TZ.XF.5.18	QCS4490	QCS4490	No	N/A	43852ab90e520239a8b6177cd51fe534551e4987ffcce8e351d6b52ecdd92f22dd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d

Table 4: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

There are no excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode of operation	Automatically entered whenever an approved service is requested	Approved	The register 'RNG_CM_PRNG_CHAR_STATUS' has the bit 1 set to zero .

Table 5: Modes List and Description

The Qualcomm Pseudo Random Number Generator supports only an approved mode which is entered without any human assistance. 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	A3756	Prediction Resistance - No Mode - SHA2-256	SP 800-90A Rev. 1
SHA2-256	A3755	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-256	A3756	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-256	A4007	Message Length - Message Length: 256-65536 Increment 8	FIPS 180-4

Table 6: 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
HW Hash-DRBG	DRBG	provides random numbers		Hash DRBG: (A3756) SHA2-256: (A3756, A3755)
HW Hash	SHA	SHA-256		SHA2-256: (A4007)
FW Hash	SHA	SHA-256		SHA2-256: (A3755)
HW ESV	ENT-ESV	Entropy Source of the Qualcomm Pseudo random Number Generator		

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

Not applicable.

2.8 RBG and Entropy

Cert Number	Vendor Name
E153	Qualcomm Technologies, Inc.

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
NIST SP800-90B compliant	Physical	Snapdragon 4 Gen 2 Platform, QCM4490, QCS4490	4 bits	0.359603 bits	N/A

Table 9: Entropy Sources

The DRBG used to generate random bits is an SP 800-90Ar1 compliant SHA2-256 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 1536 samples of 4 bits each to form the seed, from the entropy source. As these 1536 samples provide 552 bits of entropy, the DRBG is seeded with sufficient entropy to provide the security strength of 256 bits.

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	status values
Physical power connector	Power	Power port or pin for single-chip

Table 10: Ports and Interfaces

All status output and control input are directed through the interface of the cryptographic boundary, which is the registers of the Qualcomm Pseudo Random Number Generator. For data input, the registers provide the interface. For data output, the data output is provided via data out registers.

Communication between the firmware component and the disjoint hardware component of the module is considered as controlled communication because QTEE (which is the module's operational environment) is designed to separate this communication from rest of the peripherals outside of the module's cryptographic boundary.

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	Role	CO	None

Table 11: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Hash-DRBG	The hardware component provides random numbers	The register 'RNG_CM_PRNG_CHAR_STATUS' has the bit 1 set to zero.	requested number of bits	Random numbers	HW Hash-DRBG HW ESV	Crypto Officer - DRBG entropy input string: W,E - DRBG seed: G,E - DRBG internal state V and C: G,W,E
Self-Test	This service is triggered by rebooting/restarting the module. This service is the on-demand	No explicit indicator	N/A	Pass/Fail	HW Hash-DRBG HW Hash FW Hash	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	initiation method of the pre-operational integrity test, SHA KATs, DRBG KAT, and start-up entropy source health tests, as these tests are executed automatically when the device is booted or restarted					
Show Status	Show status (provided by the hardware component) of the module state	No explicit indicator	N/A	Status	None	Crypto Officer
Show Version	Show the version (provided by both the hardware and firmware components) of the module	No explicit indicator	N/A	version information	None	Unauthenticated
Zeroization	Zeroizes all SSPs in the module (done by hardware component)	No explicit indicator	N/A	N/A	None	Crypto Officer - DRBG entropy input string: Z - DRBG seed: Z - DRBG internal state V and C: Z

Table 12: Approved Services

The Qualcomm Pseudo Random Number Generator does not support bypass capability. It provides random data from the SHA2-256 Hash_DRBG. The table above describes the services available in approved mode. 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.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

Not applicable.

4.6 Bypass Actions and Status

Not applicable.

4.7 Cryptographic Output Actions and Status

Not applicable.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the firmware component of the module is verified by using SHA2-256 value stored in the module that was computed at build time.

5.2 Initiate on Demand

Integrity tests are performed as part of the Pre-Operational Self-Tests. A reset of the cryptographic module can be used to perform the "on-demand" integrity test.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

The Qualcomm Pseudo Random Number Generator is a single chip firmware-hybrid module at security level 1. The operational environment is limited.

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 13: Mechanisms and Actions Required

The Qualcomm Pseudo Random Number Generator Cryptographic Module is a single-chip firmware-hybrid 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

8.1 Mitigation Techniques

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 14: Storage Areas

9.2 SSP Input-Output Methods

N/A for this module.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power-off (Reset)	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 15: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG entropy input string	Seed the module's DRBG	6144 bits - 552 bits	Entropy Data - CSP	HW ESV		HW Hash-DRBG
DRBG seed	Seed the module's DRBG	440 bits - 256 bits	Entropy Data - CSP	HW Hash-DRBG		HW Hash-DRBG
DRBG internal state V and C	Random number generation	V: 440 bits, C: 440 bits - 256 bits	DRBG internal state values - CSP	HW Hash-DRBG		HW Hash-DRBG

Table 16: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG entropy input string		Hardware Registers:Plaintext	Until module is powered off	Power-off (Reset)	DRBG internal state V and C:Used With DRBG seed:Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG seed		Hardware Registers:Plaintext	Until module is powered off	Power-off (Reset)	DRBG internal state V and C:Used With DRBG entropy input string:Derived From
DRBG internal state V and C		Hardware Registers:Plaintext	Until module is powered off	Power-off (Reset)	DRBG entropy input string:Used With

Table 17: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
SHA2-256 (A3755)	SHA2-256	Hash	SW/FW Integrity	Module becomes operational and services are available for use	Integrity Test

Table 18: Pre-Operational Self-Tests

The firmware integrity test is run at startup of the module automatically performed without any operator intervention. The CAST for SHA2-256 is performed before the integrity test.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A3755)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization
SHA2-256 (A4007)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Module becomes operational and services are available for use	Module initialization
SHA2-256 (A3756)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization
Hash DRBG (A3756)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	SP800-90Ar1 Section 11.3 Health Test: instantiate and generate functions	Module initialization
ESV	Startup health tests, performed on 1024 consecutive samples	APT and RCT	CAST	Module becomes operational and services are available for use	SP800-90B APT and RCT Health Test	Module initialization
ESV	continuous health tests	APT and RCT	CAST	Module becomes non-operational upon failure	SP800-90B APT and RCT Health Test	Module execution

Table 19: Conditional Self-Tests

While the module is executing the self-tests, services are not available, and input and output are inhibited.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A3755)	Hash	SW/FW Integrity	On-demand	Manually by invoking the Self-test service

Table 20: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A3755)	KAT	CAST	On-demand	Manually by invoking the Self-test service
SHA2-256 (A4007)	KAT	CAST	On-demand	Manually by invoking the Self-test service
SHA2-256 (A3756)	KAT	CAST	On-demand	Manually by invoking the Self-test service
Hash DRBG (A3756)	KAT	CAST	On-demand	Manually by invoking the Self-test service
ESV	APT and RCT	CAST	On-demand	Manually by invoking the Self-test service
ESV	APT and RCT	CAST	Continuous	Automatic

Table 21: 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.	Integrity or CAST failure in firmware CAST failure in Hardware Entropy health test failure	Power cycling	TZBSP_ERR_FATAL_PRNG_FIPS_HYBRID_ERR; BIST_FAILURE indicator is set; TZ_TNG_STATUS__PRNG_PERMANENT_FAILURE is set

Table 22: Error States

If any of the pre-operational self-tests or 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 locked, 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.

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 4 Gen 2 Mobile Platform, QCM4490 and QCS4490. 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

12.1 Attack List

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

Appendix A. Glossary and Abbreviations

CAVP	Cryptographic Algorithm Validation Program
CMT	Cryptographic Module Testing
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CVT	Component Verification Testing
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standards Publication
FSM	Finite State Model
KAT	Known Answer Test
NIST	National Institute of Science and Technology
PR	Prediction Resistance
RNG	Random Number Generator
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
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 26, 2024
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements

FIPS180-4 **Secure Hash Standard (SHS)**
March 2012
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

SP800-90Ar1 **NIST Special Publication 800-90A - Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators**
June 2015
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

SP800-90B **(Second DRAFT) NIST Special Publication 800-90B - Recommendation for the Entropy Sources Used for Random Bit Generation**
January 2018
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf

SP800-140B **NIST Special Publication 800-140B - CMVP Security Policy Requirements**
November 2023
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Br1.pdf