Qualcomm® Pseudo Random Number Generator

FIPS 140-3 Non-Proprietary Security Policy

Version 1.1

Last update: 2024-06-11

Prepared by:

atsec information security corporation

4516 Seton Center Parkway, Suite 250

Austin, TX 78759

www.atsec.com

Table of Contents

1 General

1.1 This Security Policy Document

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.
The Security Policy document is one document in a FIPS 140-3 Submission Package. In addition to this document, the Submission Package contains:

- The validation report prepared by the lab.

- The Entropy Assessment Report (EAR) if applicable.

- Other supporting documentation and additional references.

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 How this Security Policy was Prepared

The vendor has provided the non-proprietary Security Policy of the cryptographic module, which was further consolidated into this document by atsec information security together with other vendor-supplied documentation. 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.

This document is the non-proprietary FIPS 140-3 Security Policy for the Qualcomm Pseudo Random Number Generator. It has a one-to-one mapping to the [SP 800-140B] starting with section B.2.1 named "General" that maps to section 1 in this document and ending with section B.2.12 named "Mitigation of other attacks" that maps to section 12 in this document.

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 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

Table 1 - Security Levels

2   Cryptographic Module Specification

2.1   Description of Module

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® 8 Gen 1 Mobile Platform SoC, the Snapdragon 8+ Gen 1 Mobile Platform SoC, the Qualcomm QCM6490 SoC and the Qualcomm QCS6490 SoC. The Qualcomm Pseudo Random Number Generator implements a SHA-256 Hash_DRBG as defined in SP 800-90Ar1. The firmware component of the module controls the physical entropy source 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.

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	Qualcomm® Trusted Execution Environment (TEE) TZ.XF.5.16	Snapdragon 8 Gen 1 Mobile Platform	Snapdragon 8 Gen 1 Mobile Platform	N/A
2	Qualcomm TEE TZ.XF.5.18	Snapdragon 8+ Gen 1 Mobile Platform	Snapdragon 8+ Gen 1 Mobile Platform	N/A
3	Qualcomm TEE TZ.XF.5.11	Qualcomm QCM6490 and Qualcomm QCS6490	Qualcomm QCM6490 and Qualcomm QCS6490	N/A

Table 2 - Tested Operational Environments

The hardware components in this submission are identified by one hardware version (3.0.0). The firmware component ("hybrid_prng_library") has distinct versions (represented by a hash value), depending on the operational environment. The following firmware versions are included (in the same order as the operational environments listed in Table 2):

1. 79f3650da911b60d69384fc282c3d366a1a31bb1d1ad17855970b5655a491fadd258ddd441 63c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d
2. 3baa04170e303e524a1d7b47675098e13bb84f3158c559d0883ed6e8ab27fd5ddd258ddd44 163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d
3. b332427132413a158e4250ec1ad69a9ded5241353692905b39b9a3e981e6f9a4dd258ddd4 4163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d

The approved algorithms implemented by the module are listed in Table 3.

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A2064, #A2754	SHA / FIPS 180-4	SHA-256	SHA-256 digest computation (Implemented in hardware)	Hash for DRBG
#A2065, #A2753	SHA / FIPS 180-4	SHA-256	SHA-256 digest computation (Implemented in hardware)	Hash for DRBG

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A2065, #A2753	DRBG / SP-800-90Ar1	Hash_DRBG	SHA-256 (Implemented in hardware)	Random number generation
#A2218	SHA / FIPS 180-4	SHA-256	SHA from firmware component (version 1)	Hash for integrity test
#A2719	SHA / FIPS 180-4	SHA-256	SHA from firmware component (version 2)	Hash for integrity test
#A3327	SHA / FIPS 180-4	SHA-256	SHA from firmware component (version 3)	Hash for integrity test

Table 3 - Approved Algorithms

NOTE: the module does not implement any non-approved but allowed, non-approved but allowed with no security claimed, or non-approved algorithms.

2.2 Cryptographic Module Boundary

The physical perimeter of the Qualcomm Pseudo Random Number Generator is the physical perimeter of the Snapdragon 8 Gen 1 Mobile Platform, Snapdragon 8+ Gen 1 Mobile Platform, Qualcomm QCM6490 and Qualcomm QCS6490 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.
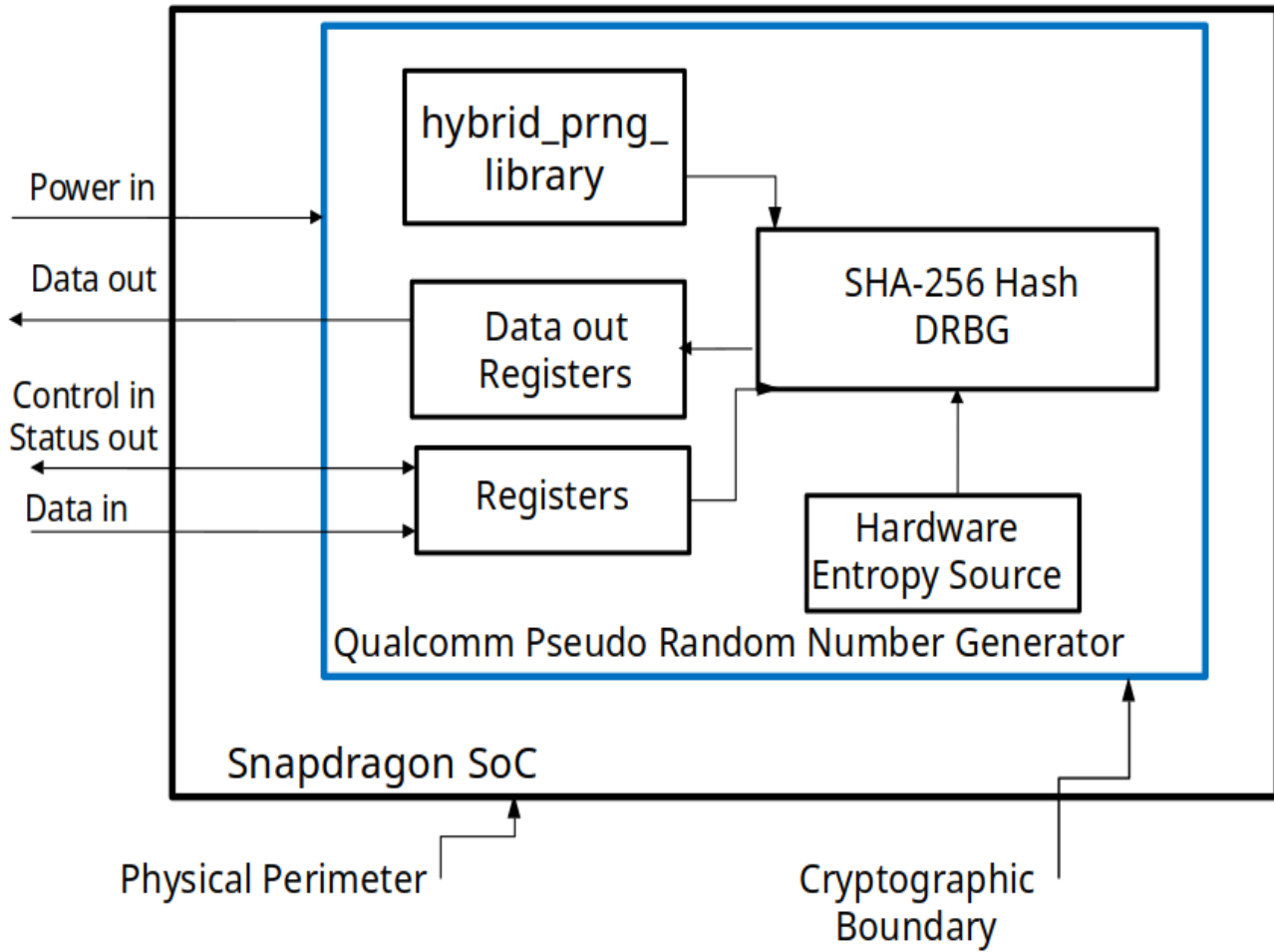
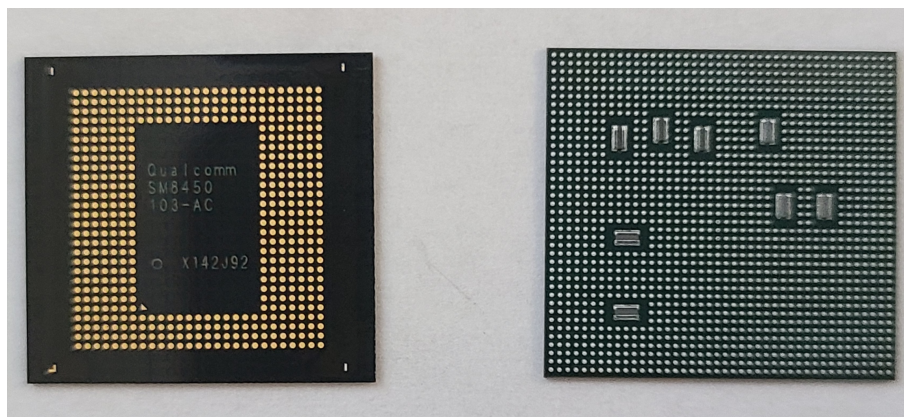*Figure 1: Block Diagram*

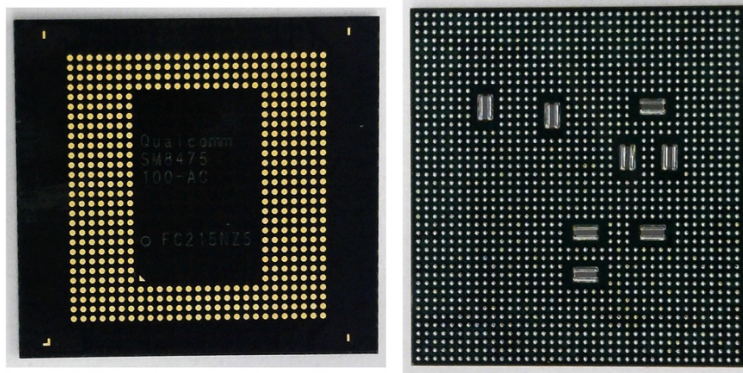Figure 2 - [Snapdragon 8 Gen 1 Mobile Platform]

Figure 3 - [Snapdragon 8+ Gen 1 Mobile Platform]
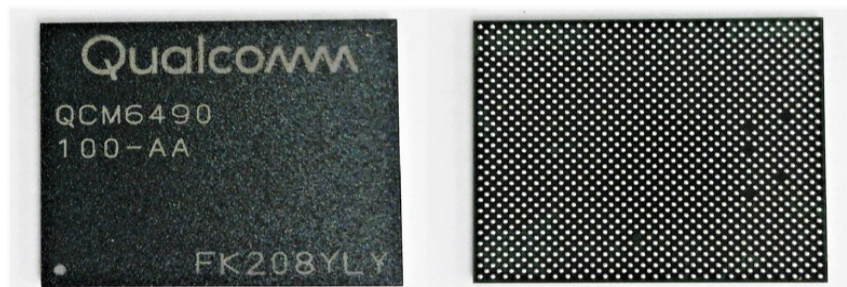
Figure 4 - [Qualcomm QCM6490]
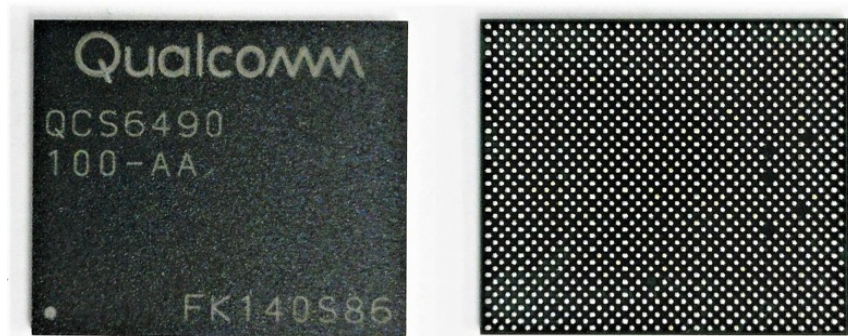
Figure 5 - [Qualcomm QCS6490]

2.3 Description of Approved Mode

The Qualcomm Pseudo Random Number Generator supports only an approved mode which is entered without any human assistance. All possible configurations entered via the registers are supported and do not violate the constraints of the approved mode.

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 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.

The table in section 4.2 lists all security functions of the module employed for approved services and implemented modes of operation.

3 Cryptographic Module Ports and Interfaces

Physical port	Logical Interface	Data that passes over port/interface
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 Input	Power port or pin for single-chip

Table 4 - Ports and Interfaces

As indicated in Table 4, 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. The module does not implement a control output interface.

4 Roles, services, and authentication

4.1 Roles

Role	Service	Input	Output
Crypto Officer (CO)	SHA-256 Hash_DRBG	Personalization string, requested output length	Random string
	Self-test	None	Pass/fail results of self-tests
	Status output	None	Current status in status output interface (as return codes and/or log messages).
	Show version	None	Version of the module
	Zeroization	All SSPs	None

Table 5 - Roles, Service Commands, Input and Output

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 Services

The Qualcomm Pseudo Random Number Generator does not support bypass capability. It provides random data from the SHA-256 Hash_DRBG. Table 6 describes the services available in operational 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.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
SHA-256 Hash_DRBG	Hash_DRBG that uses SHA-256	DRBG SHA-256	DRBG entropy input string	CO	W, E	Explicit (RNG_CM_P RNG_CHAR_ STATUS register field bit 1 set to 0)
			DRBG internal state V and C, DRBG seed		G, E	
Self-test	Self-Test is executed automatically when device is booted or restarted	DRBG SHA-256	N/A	CO	N/A	None

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Status output	Show status of the module state	None	N/A	CO	N/A	None
Show version	Show the version of the module	None	N/A	CO	N/A	None
Zeroization	Zeroizes all SSPs in the module	None	DRBG entropy input string; DRBG internal state V and C, DRBG seed	CO	Z	None

Table 6 - Approved Services

5 Software/Firmware security

5.1 Integrity Techniques

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

5.2 On-Demand Integrity Test

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.

5.3 Executable code

The module's firmware component consists of only executable code (a binary).

6 Operational Environment

6.1 Applicability

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

6.2 Tested Operational Environment

See the tested operational environments in Table 2.

6.3 Specifications for the Operational Environment

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

7 Physical Security

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

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

9 Sensitive Security Parameter Management

9.1 Random Number Generation

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 550 samples of 4 bits each as entropy input, from the entropy source. As the entropy source provides the min entropy rate of 0.420625 bits per sample, the 550 samples provide 231 bits of entropy, so the DRBG is limited to 231 bits of effective security strength in its output. Consequently, the module generates random strings whose strengths are modified by available entropy. The PUD for E67 can be found at https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/entropy/E67_PublicUse.pdf and the PUD for E95 can be found at . https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/entropy/E95_PublicUse.pdf.

Entropy Source	Minimum number of bits of entropy	Details
Entropy Source of the Qualcomm Pseudo Random Number Generator ESV certificates E67 and E95	231	The DRBG entropy input string is provided by the digitized entropy data from the physical noise source.

Table 7 - Non-Deterministic Random Number Generation Specification

9.2 SSP List

The entropy input string inputs to the DRBG are generated internal to the hardware and do not have an external interface. The DRBG internal state is never output from the module.

Key/SSP Name /Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establish-ment	Storage	Zero-ization	Use and related keys
DRBG entropy input string	231 bits	DRBG (A2065 and A2753)	Entropy Source of the Qualcomm Pseudo random Number Generator (ESV certs #E67 and #E95)	N/A	N/A	Hardware registers	Module reset	Used to compute the DRBG seed Related SSPs: DRBG internal state, DRBG seed
DRBG seed	231 bits	DRBG (A2065 and A2753)	Internally in the DRBG	N/A	N/A	Hardware registers	Module reset	Used to compute the DRBG internal

								state V and C Related SSPs: DRBG in-ternal state, DRBG en-tropy input string
DRBG in-ternal state V and C	231 bits	DRBG (A2065 and A2753)	Internally in the DRBG	N/A	N/A	Hardware registers	Module reset	Random number generation Related SSPs: DRBG en-tropy input string, DRBG seed

Table 8 - SSPs

9.3 SSP Generation, Entry and Output

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.

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

9.4 SSP Storage and Zeroization

The entropy input string and internal state used by the DRBG are generated internally by the hard-ware and are not accessible externally to the Qualcomm Pseudo Random Number Generator. Zeroization of the DRBG CSPs is accomplished by a reset event of the SoC. The registers for the CSPs will implicitly be set to zero upon the reset, indicating the zeroization was successful.

10 Self-tests

Self-tests implemented by the module consist of the pre-operational integrity test and cryptographic algorithm self-test used for algorithm implementations. All self-tests are automatically performed without any operator intervention during power-up of the module (with the exception of the physical entropy source continuous health tests). This includes the pre-operational integrity test and the cryptographic algorithm self-tests. While the module is executing the self-tests, services are not available, and input and output are inhibited.

For information about the error state, refer to Section 10.4.

10.1 Pre-operational tests

The firmware integrity test is run at startup of the module. The CAST for SHA-256 is executed before the integrity test is run.

Algorithm	Test
SHA-256	Integrity test for the firmware component

Table 9 - Pre-Operational Self-Tests

10.2 Conditional self-tests

The module performs self-tests on all FIPS approved cryptographic algorithms as part of the approved services using the tests shown in Table 10. The module transitions to the operational state only after the cryptographic algorithm self-tests are passed successfully. The physical entropy source continuous health tests are performed throughout the operation of the module.

Algorithm	Test
SHA-256	KAT performed for SHA-256 used for integrity test (firmware)
SHA-256	KAT performed for both SHA-256 cores independently (hardware)
SP 800-90Ar1 DRBG	KAT for DRBG only (hardware)
Physical entropy source	Startup health tests, performed on 1024 consecutive samples
	Continuous health tests (RCT and APT as defined in SP 800-90B)

Table 10 - Conditional Algorithm Self-Tests

10.3 Periodic/On-demand self-tests

A power cycle or reset event is the methodology used to perform the "on-demand" tests.

10.4 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.

Error State	Cause of Error	Status Indicator
Error	Integrity test or CAST failure (firmware)	Error status TZBSP_ERR_FATAL_PRNG_FIPS_HYBRID_ERR
	Continuous health test failure	Error status TZ_RNG_STATUS__PRNG_PERMANENT_FAILURE is set
	Cryptographic algorithm self-test failure (hardware)	BIST_FAILURE indicator is set

Table 11 *- Error States*

11 Life-cycle assurance

11.1 Delivery and Operation

The Qualcomm Pseudo Random Number Generator is a single chip module in the Snapdragon 8 Gen 1 Mobile Platform, Snapdragon 8+ Gen 1 Mobile Platform, Qualcomm QCM6490 and Qualcomm QCS6490. 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 End of Life

As stated in Section 9.4, 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 9.4). 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.

11.3 Crypto Officer Guidance

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

11.4 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. Perforce Visual Client(P4V), a version control system from Perforce, is used to manage the revision control of the Qualcomm firmware code. The Perforce Visual Client provides version control, branching and merging of code lines, and concurrent development.

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
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 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

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