

# Qualcomm Technologies, Inc.

# Qualcomm® Pseudo Random Number Generator

# FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0

Last update: 2025-07-11

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


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# Table of Contents

1 General ..... 6
1.1 Overview ..... 6
1.2 Security Levels ..... 6
1.3 Additional Information ..... 6
2 Cryptographic Module Specification ..... 7
2.1 Description ..... 7
2.2 Tested and Vendor Affirmed Module Version and Identification ..... 10
2.3 Excluded Components ..... 13
2.4 Modes of Operation ..... 13
2.5 Algorithms ..... 13
2.6 Security Function Implementations ..... 15
2.7 Algorithm Specific Information ..... 15
2.8 RBG and Entropy ..... 15
2.9 Key Generation ..... 16
2.10 Key Establishment ..... 16
2.11 Industry Protocols ..... 16
3 Cryptographic Module Interfaces ..... 17
3.1 Ports and Interfaces ..... 17
4 Roles, Services, and Authentication ..... 18
4.1 Authentication Methods ..... 18
4.2 Roles ..... 18
4.3 Approved Services ..... 18
4.4 Non-Approved Services ..... 19
4.5 External Software/Firmware Loaded ..... 19
5 Software/Firmware Security ..... 20
5.1 Integrity Techniques ..... 20
5.2 Initiate on Demand ..... 20
6 Operational Environment ..... 21
6.1 Operational Environment Type and Requirements ..... 21
6.2 Configuration Settings and Restrictions ..... 21
7 Physical Security ..... 22
7.1 Mechanisms and Actions Required ..... 22
8 Non-Invasive Security ..... 23
8.1 Mitigation Techniques ..... 23


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

9 Sensitive Security Parameters Management ....24
9.1 Storage Areas ....24
9.2 SSP Input-Output Methods ....24
9.3 SSP Zeroization Methods ....24
9.4 SSPs ....24
10 Self-Tests ....26
10.1 Pre-Operational Self-Tests ....26
10.2 Conditional Self-Tests ....26
10.3 Periodic Self-Test Information ....27
10.4 Error States ....28
10.5 Operator Initiation of Self-Tests ....29
11 Life-Cycle Assurance ....30
11.1 Installation, Initialization, and Startup Procedures ....30
11.2 Administrator Guidance ....30
11.3 Non-Administrator Guidance ....30
11.4 Design and Rules ....30
11.5 Maintenance Requirements ....30
11.6 End of Life ....30
12 Mitigation of Other Attacks ....31
12.1 Attack List ....31


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# List of Tables

Table 1: Security Levels ..... 6
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets) ..... 11
Table 3: Tested Module Identification – Hybrid Disjoint Hardware ..... 11
Table 4: Tested Operational Environments - Software, Firmware, Hybrid ..... 12
Table 5: Modes List and Description ..... 13
Table 6: Approved Algorithms ..... 14
Table 7: Security Function Implementations ..... 15
Table 8: Entropy Certificates ..... 15
Table 9: Entropy Sources ..... 15
Table 10: Ports and Interfaces ..... 17
Table 11: Roles ..... 18
Table 12: Approved Services ..... 19
Table 13: Mechanisms and Actions Required ..... 22
Table 14: Storage Areas ..... 24
Table 15: SSP Zeroization Methods ..... 24
Table 16: SSP Table 1 ..... 25
Table 17: SSP Table 2 ..... 25
Table 18: Pre-Operational Self-Tests ..... 26
Table 19: Conditional Self-Tests ..... 27
Table 20: Pre-Operational Periodic Information ..... 27
Table 21: Conditional Periodic Information ..... 28
Table 22: Error States ..... 28

# List of Figures

Figure 1: Block Diagram ..... 8
Figure 2 - [Snapdragon 8 Gen 1 Mobile Platform] ..... 8
Figure 3 - [Snapdragon 8+ Gen 1 Mobile Platform] ..... 9
Figure 4 - [Qualcomm QCM6490] ..... 9
Figure 5 - [Qualcomm QCS6490] ..... 10


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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® 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.

**Module Type**: Firmware-hybrid

**Module Embodiment**: Single Chip

**Module Characteristics**:

**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 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.

**Cryptographic Boundary:**


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

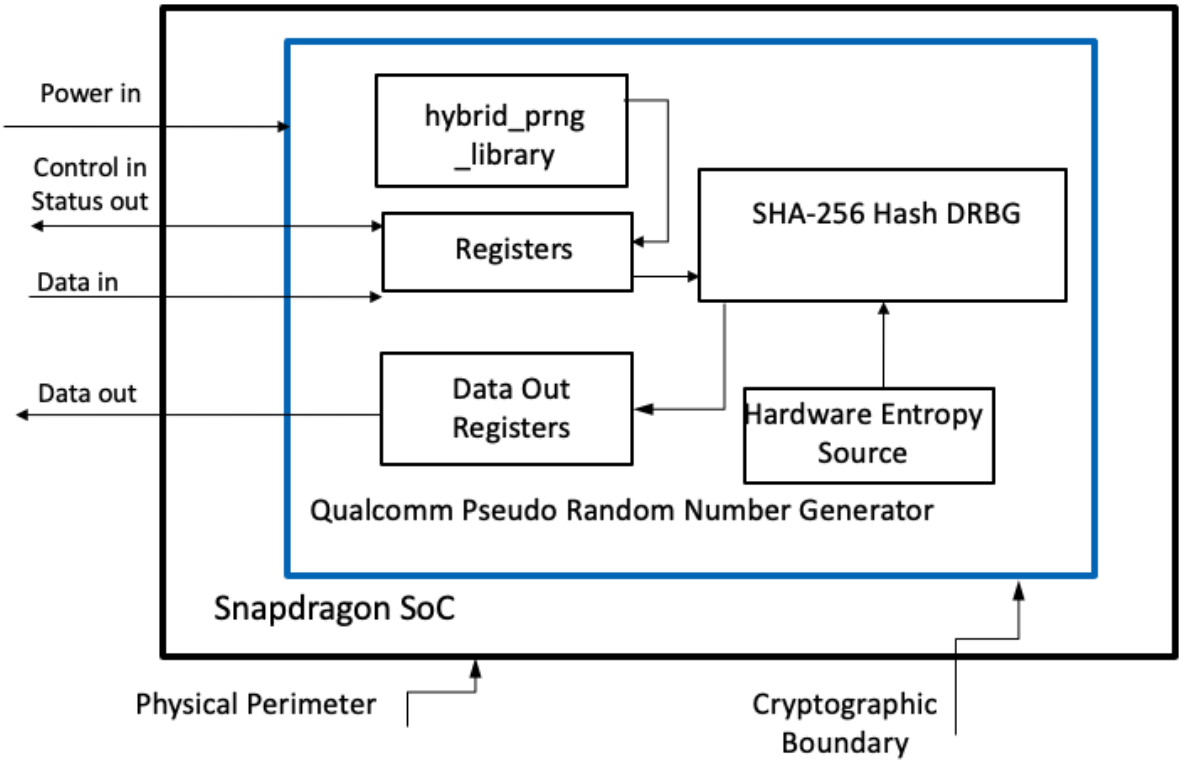



Figure 1: Block Diagram

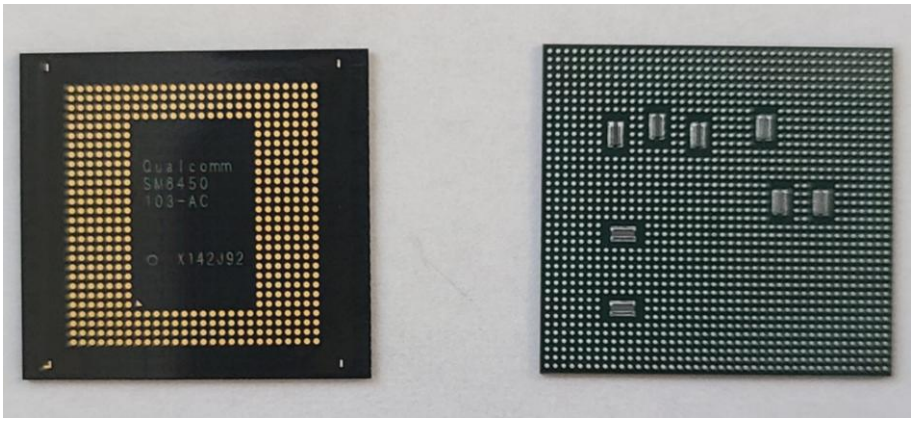



Figure 2 - [Snapdragon 8 Gen 1 Mobile Platform]


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

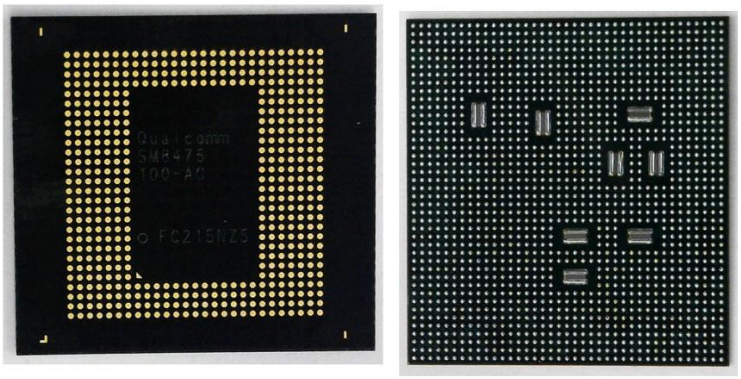



Figure 3 - [Snapdragon 8+ Gen 1 Mobile Platform]

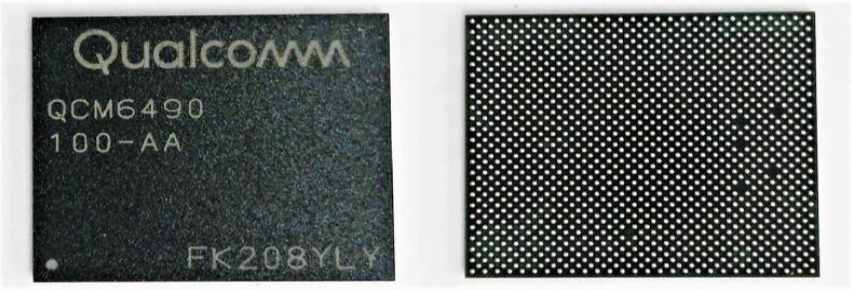



Figure 4 - [Qualcomm QCM6490]


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

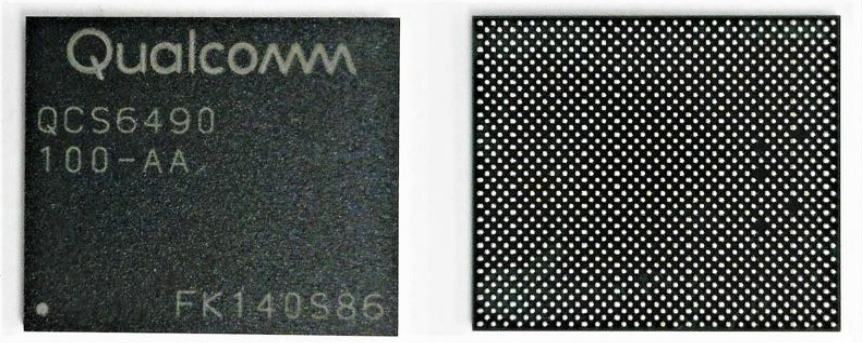



Figure 5 - [Qualcomm QCS6490]

## 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 on Qualcomm® Trusted Execution Environment (TEE) TZ.XF.5.16 | 79f3650da911b60d69384fc282c3d366a1a31bb1d1ad17855970b5655a491fadd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d | N/A | SHA-2-256 |
| hybrid_prng_library on | 3baa04170e303e524a1d7b47675098e13bb84f3158c559d0883ed6e8ab27fd5ddd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d | N/A | SHA-2-256 |


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

| Package or File Name | Software/ Firmware Version | Features | Integrity Test |
|---|---|---|---|
| Qualcomm TEE TZ.XF.5.18 | | | |
| hybrid_prng_library on Qualcomm TEE TZ.XF.5.11 (QCM6490) | b332427132413a158e4250ec1ad69a9ded5241353692905b39b9a3e981e6f9a4dd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d | N/A | SHA2-256 |
| hybrid_prng_library on Qualcomm TEE TZ.XF.5.11 (QCS6490) | b332427132413a158e4250ec1ad69a9ded5241353692905b39b9a3e981e6f9a4dd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d | N/A | SHA2-256 |

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 |
|---|---|---|---|---|
| Hash-DRBG on Snapdragon 8 Gen 1 Mobile Platform | 3.0.0 | N/A | Snapdragon 8 Gen 1 Mobile Platform | N/A |
| Hash-DRBG on Snapdragon 8+ Gen 1 Mobile Platform | 3.0.0 | N/A | Snapdragon 8+ Gen 1 Mobile Platform | N/A |
| Hash-DRBG on Qualcomm QCM6490 | 3.0.0 | N/A | Qualcomm QCM6490 | N/A |
| Hash-DRBG on Qualcomm QCS6490 | 3.0.0 | N/A | Qualcomm QCS6490 | N/A |

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

**Tested Operational Environments - Software, Firmware, Hybrid:**


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

| Operating System | Hardware Platform | Processors | PAA/PAI | Hypervisor or Host OS | Version(s) |
|---|---|---|---|---|---|
| Qualcomm® Trusted Execution Environment (TEE) TZ.XF.5.16 | Snapdragon 8 Gen 1 Mobile Platform | Snapdragon 8 Gen 1 Mobile Platform | No | N/A | 79f3650da911b60d69384fc282c3d366a1a31bb1d1ad17855970b5655a491fadd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d |
| Qualcomm TEE TZ.XF.5.18 | Snapdragon 8+ Gen 1 Mobile Platform | Snapdragon 8+ Gen 1 Mobile Platform | No | N/A | 3baa04170e303e524a1d7b47675098e13bb84f3158c559d0883ed6e8ab27fd5ddd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d |
| Qualcomm TEE TZ.XF.5.11 | Qualcomm QCM6490 | Qualcomm QCM6490 | No | N/A | b332427132413a158e4250ec1ad69a9ded5241353692905b39b9a3e981e6f9a4dd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d |
| Qualcomm TEE TZ.XF.5.11 | Qualcomm QCS6490 | Qualcomm QCS6490 | No | N/A | b332427132413a158e4250ec1ad69a9ded5241353692905b39b9a3e981e6f9a4dd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d |

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

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

N/A for this module.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

## 2.3 Excluded Components

There are no excluded components.

## 2.4 Modes of Operation

**Modes List and Description:**

| Mode Name | Description | Types of Services | Status Indicator |
|---|---|---|---|
| Approved mode | Automatically entered whenever an approved service is requested | Approved | Equivalent to the indicator of the requested service defined in section 4.3 |

Table 5: Modes List and Description

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.

**Mode Change Instructions and Status:**

Not applicable. The module only supports the approved mode of operation.

## 2.5 Algorithms

**Approved Algorithms:**


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| Hash DRBG | A2065 | Prediction Resistance - No<br>Supports Reseed - No<br>Mode - SHA2-256<br>Entropy Input - Entropy Input: 256<br>Nonce - Nonce: 128<br>Personalization String Length - Personalization String Length: 0, 32<br>Additional Input - Additional Input: 0, 0<br>Returned Bits - 1024 | SP 800-90A Rev. 1 |
| Hash DRBG | A2753 | Prediction Resistance - No<br>Supports Reseed - No<br>Mode - SHA2-256<br>Entropy Input - Entropy Input: 256<br>Nonce - Nonce: 128<br>Personalization String Length - Personalization String Length: 0, 32<br>Additional Input - Additional Input: 0, 0<br>Returned Bits - 1024 | SP 800-90A Rev. 1 |
| SHA2-256 | A2064 | Message Length - Message Length: 8-65536 Increment 8 | FIPS 180-4 |
| SHA2-256 | A2065 | Message Length - Message Length: 8-65536 Increment 8 | FIPS 180-4 |
| SHA2-256 | A2218 | Message Length - Message Length: 8-65536 Increment 8 | FIPS 180-4 |
| SHA2-256 | A2719 | Message Length - Message Length: 8-65536 Increment 8 | FIPS 180-4 |
| SHA2-256 | A2753 | Message Length - Message Length: 8-65536 Increment 8 | FIPS 180-4 |
| SHA2-256 | A2754 | Message Length - Message Length: 8-65536 Increment 8 | FIPS 180-4 |
| SHA2-256 | A3327 | Message Length - Message Length: 8-65536 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.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

**Non-Approved, Not Allowed Algorithms:**

N/A for this module.

## 2.6 Security Function Implementations

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| Hash for DRBG | SHA | Hash for DRBG | SHA2-256:SHA-256 digest computation (implemented in hardware) | SHA2-256: (A2064, A2065, A2753, A2754) |
| Hash for integrity test | SHA | Hash for integrity test | SHA2-256:SHA-256 digest computation (implemented in firmware) | SHA2-256: (A2719, A2218, A3327) |
| Hash DRBG | DRBG | Random number generator | Hash DRBG:SHA-256 (implemented in hardware)<br>SHA2-256:SHA-256 digest computation (implemented in hardware) | Hash DRBG: (A2065, A2753)<br>SHA2-256: (A2064, A2065, A2753, A2754) |

Table 7: Security Function Implementations

## 2.7 Algorithm Specific Information

Not applicable.

## 2.8 RBG and Entropy

| Cert Number | Vendor Name |
|---|---|
| E67 | Qualcomm |
| E95 | Qualcomm |

Table 8: Entropy Certificates

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|---|---|---|---|---|---|
| Entropy Source of the Qualcomm Pseudo Random Number Generator | Physical | See Tested Operational Environment Table | 4 | 0.420625 | |

Table 9: Entropy Sources


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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 to form the seed, from the entropy source. As these 550 samples provide 231 bits of entropy, 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.

## 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.

## 2.11 Industry Protocols

Not applicable. The module does not implement any industry protocols.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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 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. The module does not implement a control output interface.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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 11: 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 | Hash DRBG | Crypto Officer (CO)<br>- DRBG entropy input string: W,E<br>- DRBG internal state V and C: G,E,W<br>- DRBG seed: G,E |
| Self-test | Self-Test is executed automatically when device is booted or restarted | None | N/A | Pass/Fail | Hash for DRBG Hash DRBG | Crypto Officer (CO) |
| Integrity test | Test is executed automatica | None | N/A | Pass/Fail | Hash for | Crypto Officer (CO) |


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | lly when device is booted or restarted | | | | integrity test | |
| 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)<br>- DRBG entropy input string: Z<br>- DRBG internal state V and C: Z |
| Show version | Show the version of the module | None | N/A | module version | None | Unauthenticated |

Table 12: Approved Services

The Qualcomm Pseudo Random Number Generator does not support bypass capability. It provides random data from the SHA-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.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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 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.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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 firmware-hybrid 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.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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.

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

## 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 15: SSP Zeroization Methods

The entropy input string and internal state used by the DRBG are generated internally by the hardware 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.

## 9.4 SSPs

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| DRBG entropy input string | DRBG entropy input string used for seeding the module's DRBG; | 2200 bits - 231 bits | Entropy Data - CSP | | | Hash DRBG |
| DRBG seed | DRBG entropy input string used for seeding the module's DRBG; | 440 bits - 231 bits | Entropy Data - CSP | | | Hash DRBG |
| DRBG internal | DRBG internal state V and C used for random number generation; | V: 440 bits; C: 440 bits - 231 bits | DRBG internal state values - CSP | Hash DRBG | | Hash DRBG |


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| state V and C | | | | | | |

Table 16: SSP Table 1

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

Table 17: SSP Table 2


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 10 Self-Tests

## 10.1 Pre-Operational Self-Tests

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details |
|---|---|---|---|---|---|
| SHA2-256 (A2218) | SHA2-256 | Hash | SW/FW Integrity | Module is operational | N/A |

Table 18: Pre-Operational 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 entropy 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.

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

## 10.2 Conditional Self-Tests

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| Hash DRBG (A2065) | SHA2-256 | KAT | CAST | Module becomes operational | SP800-90Arev1 Health test | Test runs at Power-on before the integrity test |
| Hash DRBG (A2753) | SHA2-256 | KAT | CAST | Module becomes operational | SP800-90Arev1 Health test | Test runs at Power-on before the integrity test |
| Entropy Source Health Tests - Continuous (A2065) | N/A | RCT and APT | CAST | Module remains operational | Continuous Test | Continuous running of tests as defined in SP800-90B |
| Entropy Source Health Tests - Continuous (A2753) | N/A | RCT and APT | CAST | Module remains operational | Continuous Test | Continuous running of tests as defined in SP800-90B |
| Entropy Source Health Tests - Startup (A2065) | N/A | RCT and APT | CAST | Module becomes operational | Startup health Test | running of tests at startup as defined in SP800-90B |
| Entropy Source Health Tests - Startup (A2753) | N/A | RCT and APT | CAST | Module becomes operational | Startup health Test | running of tests at startup as defined in SP800-90B |
| SHA2-256 (A2218) | SHA2-256 for integrity | KAT | CAST | Module becomes operational | Message digest | Test runs at Power-on before the integrity test |


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| SHA2-256 (A3327) | SHA2-256 for integrity | KAT | CAST | Module becomes operational | Message digest | Test runs at Power-on before the integrity test |
| SHA2-256 (A2719) | SHA2-256 for integrity | KAT | CAST | Module becomes operational | Message digest | Test runs at Power-on before the integrity test |
| SHA2-256 (A2064) | SHA2-256 for DRBG | KAT | CAST | Module becomes operational | Message digest | Test runs at Power-on |
| SHA2-256 (A2065) | SHA2-256 for DRBG | KAT | CAST | Module becomes operational | Message digest | Test runs at Power-on |
| SHA2-256 (A2753) | SHA2-256 for DRBG | KAT | CAST | Module becomes operational | Message digest | Test runs at Power-on |
| SHA2-256 (A2754) | SHA2-256 for DRBG | KAT | CAST | Module becomes operational | Message digest | Test runs at Power-on |

Table 19: Conditional Self-Tests

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

## 10.3 Periodic Self-Test Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| SHA2-256 (A2218) | Hash | SW/FW Integrity | On Demand | Manually |

Table 20: Pre-Operational Periodic Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Hash DRBG (A2065) | KAT | CAST | On Demand | Manually |
| Hash DRBG (A2753) | KAT | CAST | On Demand | Manually |
| Entropy Source Health Tests - Continuous (A2065) | RCT and APT | CAST | On Demand | Manually |
| Entropy Source Health Tests - Continuous (A2753) | RCT and APT | CAST | On Demand | Manually |


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Entropy Source Health Tests - Startup (A2065) | RCT and APT | CAST | On Demand | Manually |
| Entropy Source Health Tests - Startup (A2753) | RCT and APT | CAST | On Demand | Manually |
| SHA2-256 (A2218) | KAT | CAST | On Demand | Manually |
| SHA2-256 (A3327) | KAT | CAST | On Demand | Manually |
| SHA2-256 (A2719) | KAT | CAST | On Demand | Manually |
| SHA2-256 (A2064) | KAT | CAST | On Demand | Manually |
| SHA2-256 (A2065) | KAT | CAST | On Demand | Manually |
| SHA2-256 (A2753) | KAT | CAST | On Demand | Manually |
| SHA2-256 (A2754) | KAT | CAST | On Demand | Manually |

Table 21: Conditional Periodic Information

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

## 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 test or CAST failure (firmware) Cryptographic algorithm self-test failure (hardware) Continuous health test failure | Power cycling | TZBSP_ERR_FATAL_PRNG_FIPS_HYBRID_ERR is set or BIST_FAILURE indicator is set or TZ_RNG_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


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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.

## 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.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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 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 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

N/A Therefore no specific design or rules to be followed.

## 11.5 Maintenance Requirements

N/A There are no maintenance requirements.

## 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.


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 12 Mitigation of Other Attacks

## 12.1 Attack List

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


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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 |


© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

# 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
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**
March 2020
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140B.pdf



© 2025 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.