Qualcomm Technologies, Inc.

Qualcomm® Pseudo Random Number Generator

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1

Last Update: 2026-07-27

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[1] 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.

[1] Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries.

This document has a one-to-one mapping to 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.

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 SoCs listed in Table 2. The Qualcomm Pseudo Random Number Generator version 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: Single Chip

Cryptographic Boundary:

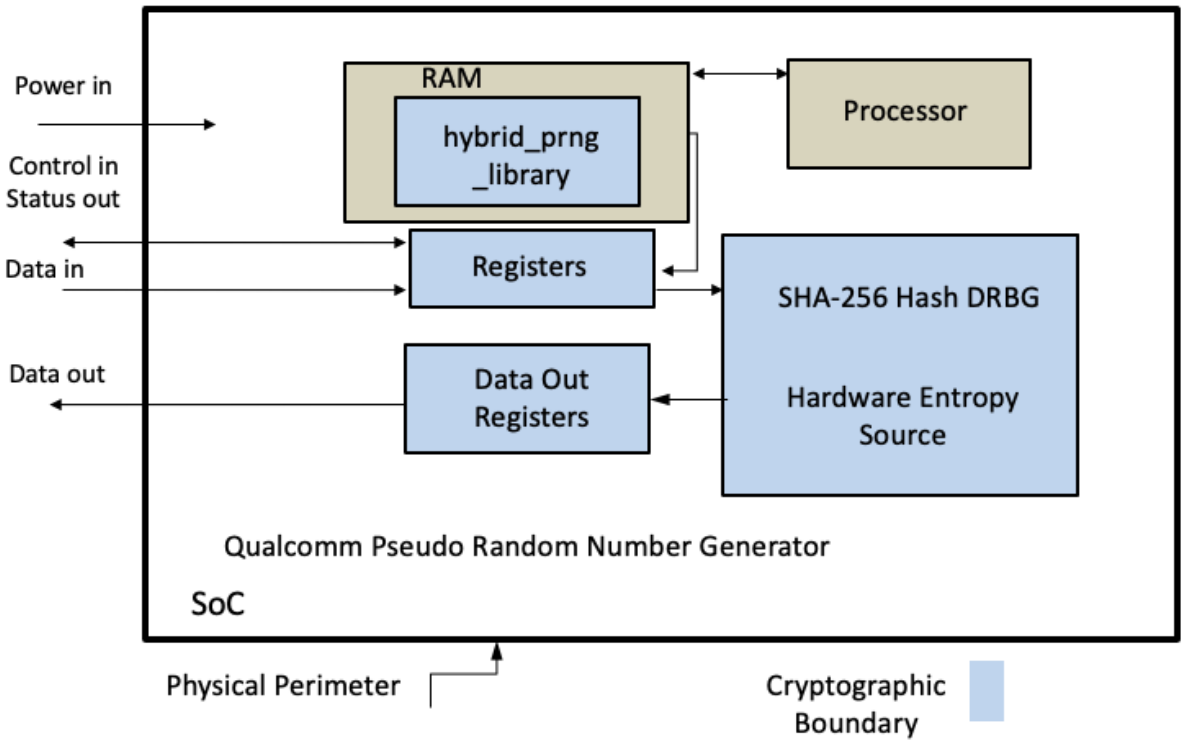

Figure 1: Cryptographic Boundary and Physical Perimeter

Tested Operational Environment's Physical Perimeter (TOEPP):

The tested operational environment's physical perimeter is the single chip. The tested operational environment contains an ESV-validated entropy source which is used by the module to obtain entropy.

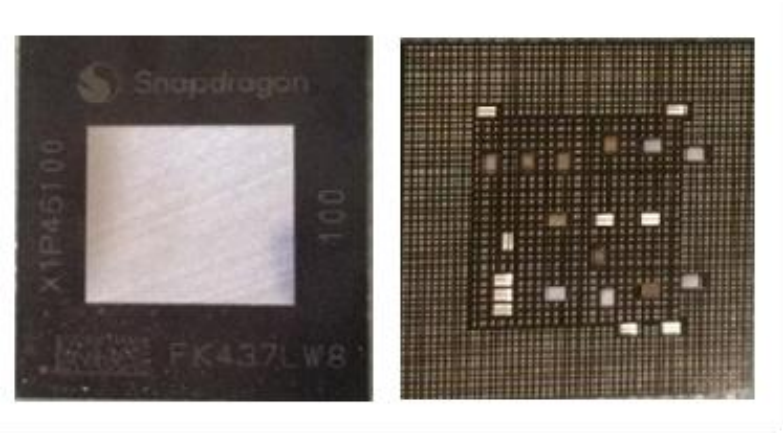

Figure 2: Snapdragon® X1 Plus

Figure 3: Snapdragon X Elite Compute Platform

2.2 Tested and Vendor Affirmed Module Version and Identification

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

Package or File Name	Software/ Firmware Version	Features	Integrity Test
hybrid_prng_library	78eb76d08487e42f2bbaeb3a6aceba28aa296673c319f3e8560e01cc8bc240f2dd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d	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 X Elite Compute Platform; Sub-Chip Disjoint Hardware: Hash-DRBG	3.2.0	N/A	Snapdragon X Elite Compute Platform	N/A
Single Chip: Qualcomm - Snapdragon X1 Plus; Sub-Chip Disjoint Hardware: Hash-DRBG	3.2.0	N/A	Snapdragon X1 Plus	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.5.28.1	Snapdragon X Elite Compute Platform	Snapdragon X Elite Compute Platform	No	N/A	78eb76d08487e42f2bbaeb3a6aceba28aa296673c319f3e8560e01cc8bc240f2dd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d
Qualcomm Trusted Execution Environment (TEE) TZ.XF.5.28.1	Snapdragon X1 Plus	Snapdragon X1 Plus	No	N/A	78eb76d08487e42f2bbaeb3a6aceba28aa296673c319f3e8560e01cc8bc240f2dd258ddd44163c90afe68b7a1766da625533f1f12e9819dade4cdf913dd7138d

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

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	Implicit approved mode of operation always assumed by the module.	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. 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.

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 and is operating in the approved mode. 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, A3756, A7688	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.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
HW Hash-DRBG	DRBG	Provide random numbers		Hash DRBG: (A3756)
HW Hash for DRBG	SHA	Hash for HW DRBG		SHA2-256: (A3756, A3755)
FW Hash	SHA	Hash for firmware integrity check		SHA2-256: (A7688)
HW ESV	ENT-ESV	Entropy Source of the Qualcomm Pseudo random Number Generator		

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

There is no algorithm specific compliance information.

2.8 RBG and Entropy

Cert Number	Vendor Name
E207	Qualcomm Technologies, Inc.
E282	Qualcomm Technologies, Inc.

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	Snapdragon X1 Plus	4 bits	0.4 bit	N/A
Entropy Source of the Qualcomm Pseudo Random Number Generator	Physical	Snapdragon X Elite Compute Platform	4 bits	0.407819 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 1024 samples from the entropy source to form its seed. Each sample consists of 4 bits. These 1024 samples provide at least 409 bits of entropy, sufficient to instantiate a DRBG with 256 bits of security strength.

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 key establishment services.

2.11 Industry Protocols

The module does not implement any industry protocols, or provide services designed to be used as part of any industry protocol.

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 information
Physical power connector	Power	N/A

Table 10: Ports and Interfaces

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 the 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

The module does not support authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 11: Roles

The Crypto Officer role is implicitly assumed by the entity requesting services from the module. The module does not allow concurrent operators.

4.3 Approved Services

The following access rights are used in the table below:

- **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.

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	Crypto Officer - Entropy input string: W,E - DRBG seed: G,E - DRBG

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						internal state V and C: G,W, E
Self-Test	Self-Test (for both hardware and firmware components) is executed automatically when device is booted or restarted	No explicit indicator	N/A	Pass/Fail	HW Hash-DRBG FW Hash HW Hash for DRBG HW ESV	Crypto Officer
Show Status	Show status of the module (status of KATs, FW integrity test, entropy source APT & RCT; overall module status; approved service indicator)	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	Crypto Officer
Zeroization	Zeroizes all SSPs in the module (done by hardware component)	No explicit indicator	N/A	N/A	None	Crypto Officer - Entropy input string: Z -

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						DRBG seed: Z - DRBG internal state V and C: Z
Show identifier	Output the module identifier (accessed through the register RNG_CM_PRNG_FIPS_ID)	No explicit indicator	N/A	0x2	None	Crypto Officer

Table 12: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

Not applicable. No external software or firmware is loaded.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the firmware component of the module is verified by comparing a SHA2-256 hash of the module computed during module initialization with the SHA2-256 value that was computed at build time and stored in the module.

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 which meets level 2 physical security requirements. 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 hardware component. 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 hardware component is further protected by being enclosed in a commercial off the shelf mobile device utilizing production grade commercially available components. The mobile device enclosure completely surrounds the Qualcomm Pseudo Random Number Generator hardware component.

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

All SSPs are stored in internal registers which can only be read and written to by the module. All internal storage is volatile.

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.

There are no SSPs entered into or output from the module. The entropy input string is obtained from the entropy source within the cryptographic boundary.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power-off (Reset)	All SSPs will be zeroized	The registers holding the SSPs lose state when power is removed	Operator can initiate this zeroization method by powering off the module

Table 15: SSP Zeroization Methods

A successful power-off indicates that all SSPs have been zeroized. Data output is inhibited during this zeroization process.

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	6144 bits - 614 bits	Entropy Data - CSP	HW ESV		HW Hash-DRBG
DRBG seed	DRBG seed used for seeding the module's DRBG	440 bits - 256 bits	Entropy Data - CSP	HW Hash-DRBG		HW Hash-DRBG

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG internal state V and C	DRBG internal state V and C used for 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
Entropy input string		Hardware Registers:Plaintext	Until module is powered off	Power-off (Reset)	DRBG seed:Derives
DRBG seed		Hardware Registers:Plaintext	Until module is powered off	Power-off (Reset)	Entropy input string:Derived From DRBG internal state V and C:Derives
DRBG internal state V and C		Hardware Registers:Plaintext	Until module is powered off	Power-off (Reset)	DRBG seed:Derived From

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 (A7688)	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 the startup of the module and is automatically performed without any operator intervention. The CAST for the firmware implementation of 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 (A3756)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization
SHA2-256 (A7688)	SHA2-256	KAT	CAST	Module becomes operational and services are available for use	Message digest	Module initialization
Hash DRBG (A3756)	SHA2-256, no pr	KAT	CAST	Module becomes operational and services are available for use	SP800-90Ar1 Section 11.3 Health Test for Instantiate() Reseed(), and Generate(), compliant with IG 10.3.A Resolution 6	Module initialization
ESV Startup RCT	Cutoff value: 51	RCT	CAST	Module becomes operational	RCT performed on 1024 noise source samples	Tests ran at startup as defined in SP800-90B

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ESV Startup APT	Cutoff value: 433	APT	CAST	Module becomes operational	APT performed on 1024 noise source samples	Tests ran at startup as defined in SP800-90B
ESV Continuous RCT	Cutoff value: 51	RCT	CAST	Module remains operational	RCT performed continuously on noise samples	Continuous running of tests as defined in SP800-90B
ESV Continuous APT	Cutoff value: 433	APT	CAST	Module remains operational	APT performed continuously on noise samples	Continuous running of tests as defined in SP800-90B

Table 19: Conditional Self-Tests

All self-tests are automatically performed without any operator intervention during power-up of the module. 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 (A7688)	Hash	SW/FW Integrity	On-demand	Manually

Table 20: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (A3755)	KAT	CAST	On-demand	Manually
SHA2-256 (A3756)	KAT	CAST	On-demand	Manually
SHA2-256 (A7688)	KAT	CAST	On-demand	Manually
Hash DRBG (A3756)	KAT	CAST	On-demand	Manually
ESV Startup RCT	RCT	CAST	On-demand	Manually
ESV Startup APT	APT	CAST	On-demand	Manually
ESV Continuous RCT	RCT	CAST	On-demand	Manually
ESV Continuous APT	APT	CAST	On-demand	Manually

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. In this state, data output is prohibited, and no further cryptographic operation is allowed. This is enforced by control logic which prevents external usage when an error is detected.

Once the Qualcomm Pseudo Random Number Generator is in the error state, it will only respond to a module reset command. This will cause it to re-execute all self-tests. If the error persists, the Qualcomm Pseudo Random Number Generator will remain unavailable.

10.5 Operator Initiation of Self-Tests

The operator can initiate the cryptographic algorithm self-tests by power cycling the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Qualcomm Pseudo Random Number Generator is a single chip module in the SoCs listed in Section 2.2.

The vendor uses a trusted delivery courier to transport the SoC to their customers. On the reception of the SoC, the operator shall first check all sides of the box to verify that it has not been tampered with during the shipment. Then, after opening the box the operator shall verify that the moisture barrier bag is still sealed and does not present any trace of tampering. Finally, after retrieving the SoC, the operator shall perform a visual inspection of the external package of the module; it should look like either Figure 2 or Figure 3 depending on the SoC model.

If one of these verifications fails, the operator shall contact their Qualcomm Technologies' representative who released the delivery before operating the module. Once the product is received by the customer and powered up, the tests defined in the Self-Tests section will be executed automatically and without operator intervention.

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

There is no specific design nor rules to be followed.

11.5 Maintenance Requirements

There are no maintenance requirements.

11.6 End of Life

Because the module does not have persistent storage, all SSPs are zeroized and the module is securely sanitized when powered down. Thus, the module may be distributed to other operators or disposed of after each power off.

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
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standards
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 a Chip

Appendix B: References

FIPS 140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** March 2019 https://doi.org/10.6028/NIST.FIPS.140-3
FIPS 140-3 IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program** February 2026 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS 180-4	**Secure Hash Standard (SHS)** August 2015 https://doi.org/10.6028/NIST.FIPS.180-4
SP 800-90A Rev. 1	**Recommendation for Random Number Generation Using Deterministic Random Bit Generators** June 2015 https://doi.org/10.6028/NIST.SP.800-90Ar1