Qualcomm
TECHNOLOGIES, INC

QTI Pseudo Random Number Generator

Version 2.0

FIPS 140-2 Non-Proprietary Security Policy

Version 1.2

Last Update: 2016-02-12

Prepared by:
atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
www.atsec.com

TABLE OF CONTENTS

1. INTRODUCTION 3

1.1 Purpose of the Security Policy 4
1.2 Target Audience 4
1.3 Document Organization / Copyright 4

2. CRYPTOGRAPHIC MODULE SPECIFICATION 5

2.1. Description of Module 5
2.2. Description of Approved Mode 5
2.3. Cryptographic Module Boundary 6

3. CRYPTOGRAPHIC MODULE PORTS AND INTERFACES 9

4. ROLES, SERVICES AND AUTHENTICATION 10

4.1. Roles 10
4.2. Services 10
4.3. Operator Authentication 11
4.4. Mechanism and Strength of Authentication 11

5. PHYSICAL SECURITY 11

6. OPERATIONAL ENVIRONMENT 12

6.1. Applicability 12

7. CRYPTOGRAPHIC KEY MANAGEMENT 13

7.1. Random Number Generation 13
7.2. Key and CSP List 13
7.3. Key/CSP Generation, Entry and Output 14
7.4. Key/CSP Storage and Zeroization 14

8. ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY (EMI/EMC) 15

9. POWER-UP TESTS 16

9.1. Cryptographic Algorithm Tests 16

10. DESIGN ASSURANCE 17

10.1. Configuration Management 17

11. MITIGATION OF OTHER ATTACKS 18

12. GLOSSARY AND ABBREVIATIONS 19

13. REFERENCES 20

Copyrights and Trademarks

1.Introduction

This document is the non-proprietary FIPS 140-2 Security Policy for the QTI Pseudo Random Number Generator cryptographic module. The version number of this cryptographic module is 2.0. This document contains a specification of the rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2) for a Security Level 1 hardware cryptographic module.

In this document, the terms “QTI Pseudo Random Number Generator”, “cryptographic module” or “module” are used interchangeably to refer to the QTI Pseudo Random Number Generator cryptographic module.

1.1 Purpose of the Security Policy

There are three major reasons that a security policy is needed:

- it is required for FIPS 140-2 validation,
- it allows individuals and organizations to determine whether the cryptographic module, as implemented, satisfies the stated security policy, and
- it describes the capabilities, protection, and access rights provided by the cryptographic module, allowing individuals and organizations to determine whether it will meet their security requirements.

1.2 Target Audience

This document is part of the package of documents that are submitted for FIPS 140-2 conformance validation of the module. It is intended for the following people:

- Developers working on the release
- FIPS 140-2 testing lab
- Cryptographic Module Validation Program (CMVP)
- Consumers

1.3 Document Organization / Copyright

This non-proprietary security policy document may be reproduced and distributed only in its original entirety without any revision, ©2016 Qualcomm Technologies, Inc.

2.Cryptographic Module Specification

2.1.Description of Module

The QTI Pseudo Random Number Generator is classified as a single chip hardware module for the purpose of FIPS 140-2 validation. It is designed to provide random numbers. The logical cryptographic boundary of the module is the QTI Pseudo Random Number Generator 2.0 which is a sub-chip hardware component contained within the Qualcomm Snapdragon 820 SoC. The sub-chip cryptographic module implements a SHA-256 Hash DRBG as defined in SP 800-90A.

The hardware sub-chip cryptographic module is specified in the following table:

Component	Type	Version Number
QTI Pseudo Random Number Generator	hardware	2.0

Table 1: Components of the Hardware Cryptographic Module

The module has been tested on the following platform:

Qualcomm Snapdragon 820

The module is intended to meet the requirements of FIPS 140-2 at an overall Security Level 1. The table below shows the security level claimed for each of the eleven sections that comprise the validation:

FIPS 140-2 Sections	Security Level				
	N/A	1	2	3	4
Cryptographic Module Specification		X			
Cryptographic Module Ports and Interfaces		X			
Roles, Services and Authentication		X			
Finite State Model		X			
Physical Security		X			
Operational Environment	X				
Cryptographic Key Management		X			
EMI/EMC		X			
Self Tests		X			
Design Assurance		X			
Mitigation of Other Attacks	X				

Table 2: Security Levels

2.2.Description of Approved Mode

The module supports only FIPS mode which is entered without any special configurations. All configurations possible via the registers are supported and do not violate the constraints of the FIPS mode.

When the module is powered on, the power-up self-test is executed automatically without any operator intervention. The module enters FIPS mode automatically if the power-up self-test completes successfully.

If any of self-tests fail during power-up, the module goes into Error state. All cryptographic services are prohibited in error state. When an error state is entered the module can be reset to reinitialize the module.

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

The module provides the following CAVP validated algorithm (Note that the module has two cores each implementing SHA-256):

Algorithms	Standards	CAVS Certs #
SHA-256 Hash DRBG	SP-800-90A	Cert.#: 885
SHA-256 (core 1)	FIPS 198-1	Cert.#: 2908
SHA-256 (core 2)	FIPS 198-1	Cert.#: 2930

Table 3: Approved Algorithms

2.3.Cryptographic Module Boundary

The physical boundary of the module is the physical boundary of the Qualcomm Snapdragon 820 SoC that contains the sub-chip which implements the module. Consequently, the embodiment of the module is a single-chip standalone cryptographic module. The logical boundary of the module is the Pseudo Random Number Generator sub-chip.

The following figure illustrates the various data, status and control paths through the physical and logical boundary of the cryptographic module.

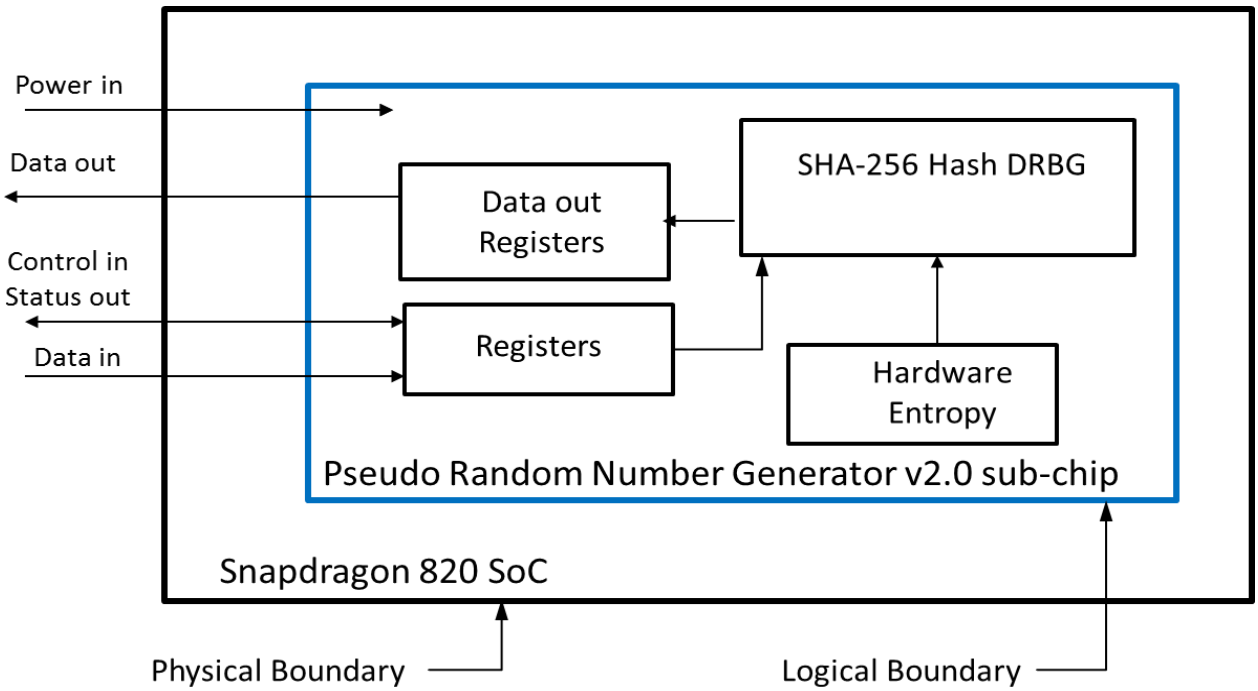
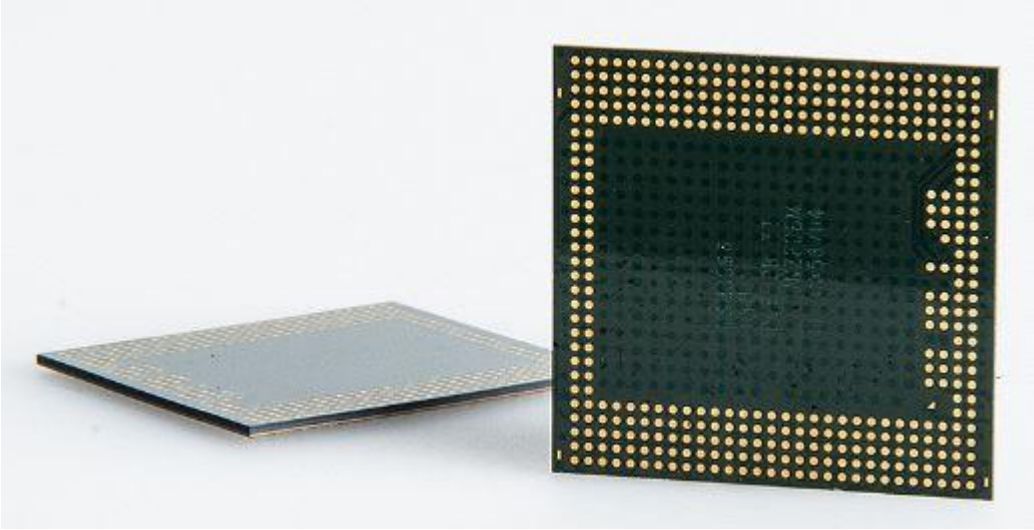
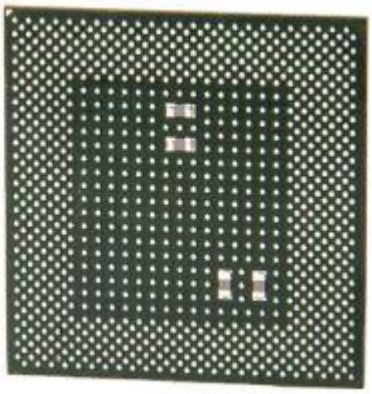


Figure 1: Cryptographic Boundary



Back view



Front view

Figure 2: Qualcomm Snapdragon 820

3.Cryptographic Module Ports and Interfaces

FIPS Interface	Ports
Data Input	Registers
Data Output	Data Out Registers
Control Input	Registers
Status Output	Registers
Power Input	Physical power connector

Table 4: Ports and Interfaces

As indicated in Table 4, all status output and control input are directed through the interface of the module’s logical boundary, which is the registers of the module. For data input, the registers also provide the interface. The data output is provided via data out registers.

4.Roles, Services and Authentication

4.1.Roles

Role	Description
User	Perform general security services, including cryptographic operations and other Approved security functions.
Crypto Officer (CO)	Configuration of the module.

Table 5: Roles

The module meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing both User and Crypto Officer roles. The module does not allow concurrent operators.

The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the module. No further authentication is required. The Crypto Officer can initialize the module.

4.2.Services

The module does not support bypass capability. The module provides random data from the SHA-256 Hash DRBG.

The following table describes the services available in FIPS-mode:

Service	Roles		CSP	Access (Read, Write, Execute)
	User	CO		
Approved				
SHA-256-Hash-DRBG	✓		Seed, (i.e., entropy input string and nonce), Personalization string	R, X
Self-Test (Self-test is executed automatically when device is booted or restarted)	✓		N/A	R, X
Check Status/Get State	✓		N/A	R
Module Configuration		✓	N/A	N/A
Zeroization	✓		Seed, (i.e., entropy input string and nonce), Personalization string	N/A
Non-approved but Allowed				
NDRNG	✓		Entropy input string, nonce	R

Table 6: Services

4.3.Operator Authentication

There is no operator authentication; assumption of role is implicit by action.

4.4.Mechanism and Strength of Authentication

No authentication is required at security level 1; authentication is implicit by assumption of the role.

5.Physical Security

The QTI Pseudo Random Number Generator 2.0 is a sub-chip module implemented as part of the Qualcomm Snapdragon 820 SoC, which is the physical boundary of the sub-chip module. The Qualcomm Snapdragon 820 SoC is a single chip with a production grade enclosure and hence conforms to the Level 1 requirements for physical security.

6.Operational Environment

6.1.Applicability

The module is a single chip hardware module. The procurement, build and configuring procedure are controlled. Therefore the operational environment is considered non-modifiable.

7.Cryptographic Key Management

7.1.Random Number Generation

Hardware is used to collect random bits as the entropy seed (i.e., the entropy input string and the nonce) for the module to generate FIPS 140-2 compliant random numbers.

The DRBG used to generate pseudo random numbers is an SP 800-90A compliant SHA-256 Hash DRBG using a derivation function without prediction resistance. It processes a personalization string that can be provided by the caller. The implementation performs a continuous self-test, a health check, and a power-on self-test.

A re-seed process is applied to the DRBG, the re-seed frequency is programmable, up to 2^32 blocks of data.

When the DRBG is instantiated, it runs a self-test with a set of test vectors, and also runs a health check test to verify that the instantiation function and generation function are able to handle any incorrect parameter inputs, such as the input data length being a negative number, etc. The DRBG implements a continuous self-test verifying the random number generation. The self-test compares the output bits with the generated bits from the previous round and ensures that they do not match.

The entropy source for the DRBG originates from a series of ring oscillators. The NDRNG consists of the combined data streams of the oscillators which is fed into the DRBG. Statistical tools have been used to measure the entropy generated by each ring oscillator and also the combined output of the oscillators. The combined output has been determined to contain one bit of entropy per bit of output.

The DRBG also implements a derivation function to counter any slight imperfections in the entropy stream. Based on an analysis of the entropy output and the use of a 256 bit entropy value along with a 128 bit nonce, it has been determined that the input random data into the approved HASH DRBG contains at least 256 bits of security strength.

The output of the noise source is processed by a continuous self-test which compares the output bits with the generated bits from the previous round and ensures that they do not match.

7.2.Key and CSP List

The entropy input string and the nonce inputs to the DRBG are generated internal to the hardware module and do not have an external interface. The personalization string 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 following table lists the CSP in the module:

CSP	Generation	Storage	Zeroization
DRBG Seed (i.e., entropy input string and nonce)	Hardware NDRNG	Internal registers	Reset event
Personalization string	User	Hardware register (Read/write by application)	Reset event

Table 7: Keys and CSPs

7.3.Key/CSP Generation, Entry and Output

The module does not provide any key generation service or perform key generation for any of its Approved algorithms. The caller of the DRBG can use the output for key generation.

The cryptographic module does not provide any asymmetrical algorithms or key establishment methods.

7.4.Key/CSP Storage and Zeroization

The entropy input string and nonce used by the DRBG are generated internally by the hardware and are not accessible external to the module. The personalization string is input by the caller of the DRBG into a register that is able to be read and written by the caller.

Zeroization of the DRBG CSPs is accomplished by either a reset event or a power-off/power-on cycle of the DRBG.

8.Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The CM hardware component cannot be certified by the FCC as it is not a standalone device. It is a sub-chip imbedded in the Qualcomm Snapdragon 820 SoC which is also not a standalone device, but rather intended to be used within a COTS device which would undergo standard FCC certification for EMI/EMC.

According to 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, the CM is not subject to EMI/EMC regulations because it is a subassembly that is sold to an equipment manufacturer for further fabrication. That manufacturer is responsible for obtaining the necessary authorization for the equipment with the CM embedded prior to further marketing to a vendor or to a user.

9.Power-Up Tests

Power-Up tests consist of known-answer tests (KAT) of algorithm implementations. The power-up self-tests are automatically performed without any operator intervention during power-up of the module. If any of the power-up self-tests fail, the module will enter the error state. Data output is prohibited and no further cryptographic operation is allowed in the error state. The module can be reset to recover from the error state. Re-initialization is also possible by doing a power-cycle to set the module to the power-on state.

FIPS 140-2 explicitly allows that the on-demand test can be fulfilled with a power cycle of the module. Hence, a power cycle and its associated power-on self-test is the methodology used to perform the "on-demand" tests.

9.1.Cryptographic Algorithm Tests

Algorithm	**Test**
SP 800-90A DRBG	Continuous Random Number Generator Test KAT for DRBG only (not the hash)
SHA-256	KAT performed for both SHA-256 cores independently
Hardware NDRNG	Continuous Random Number Generator Test

Table 8: Power-Up Cryptographic Algorithm Tests

10.Design Assurance

The module is implemented in hardware and is not modifiable; therefore no integrity test is required.

10.1.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 QTI ClearCase database.

11.Mitigation of Other Attacks

No other attacks are mitigated.

12. Glossary and Abbreviations

CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off The Shelf
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standards Publication
KAT	Known Answer Test
NIST	National Institute of Science and Technology
SHA	Secure Hash Algorithm
SoC	System on Chip

13.References

[1] FIPS 140-2 Standard,
http://csrc.nist.gov/groups/STM/cmvp/standards.html

[2] FIPS 140-2 Implementation Guidance,
http://csrc.nist.gov/groups/STM/cmvp/standards.html

[3] FIPS 180-4 Secure Hash Standard,
http://csrc.nist.gov/publications/PubsFIPS.html

[4] NIST Special Publication 800-90A, Reccomendation for Random Number Generation Using Deterministic Random Bit Generators
http://csrc.nist.gov/publications/nistpubs/800-90A/SP900-90A.pdf