Google, LLC

B227 True Random Number Generator (TRNG) Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

Introduction

Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140-3 program. NVLAP accredits independent testing labs to perform FIPS 140-3 testing; the CMVP validates modules meeting FIPS 140-3 validation. Validated is the term given to a module that is documented and tested against the FIPS 140-3 criteria. More information is also available on the CMVP website at: http://csrc.nist.gov/groups/STM/cmvp/index.html

About this Document

This non-proprietary Cryptographic Module Security Policy for the B227 True Random Number Generator (TRNG) Cryptographic Module from Google LLC. provides an overview of the product and a high-level description of how it meets the overall Level 1 security requirements of FIPS 140-3. The B227 True Random Number Generator (TRNG) Cryptographic Module can also be referred to as “B227 TRNG” or the “module” in this document.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Google LLC. shall have no liability for any error or damages of any kind resulting from the use of this document.

Notices

This document may be freely reproduced and distributed in its entirety without modification.

This document describes the cryptographic module security policy for Google LLC. B227 True Random Number Generator (TRNG) Cryptographic Module. It contains specifications of the security rules under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-3 standard.

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	N/A
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

1.3 Additional Information

The module claims an overall Security Level of 1 with all individual sections at a Security Level 1. The module does not implement any non-invasive security mitigations or mitigations of other attacks and does not contain any firmware. Thus, the requirements per the Non-Invasive Security, Mitigation Of Other Attacks and Software/Firmware Security sections are inapplicable.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The purpose of the module is to provide random bits to the Integrated Compute Complex (ICC) module and other sub-systems within the Google IN763 SoC. Specifically, the B227 True Random Number Generator (TRNG) Cryptographic Module provides seed values to the firmware DRBG implemented in the ICC module for key generation functions.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: SubChip

Cryptographic Boundary:

The B227 True Random Number Generator (TRNG) Cryptographic Module is a sub-chip cryptographic subsystem hardware module within a single chip embodiment.

The module does not contain any persistent storage.

Tested Operational Environment's Physical Perimeter (TOEPP):

The module is of type hardware and the physical perimeter is the entirety of the IN763 SoC.

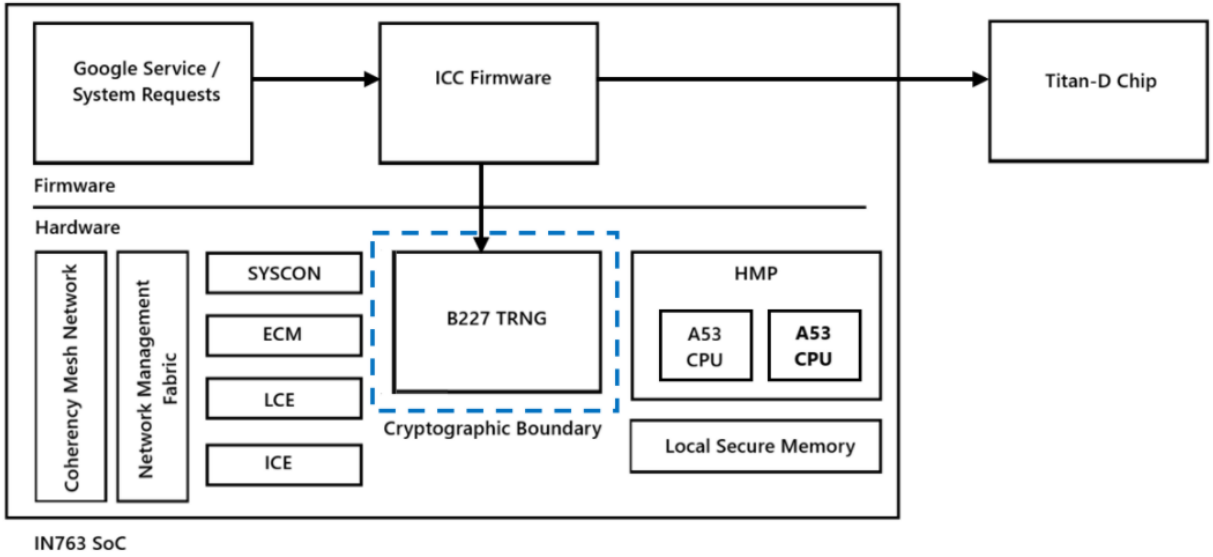

Figure 1: Block Diagram

Figure 2: Single-chip picture

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
IN763 SoC A0	3.00b	N/A	N/A	N/A

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

No components have been excluded from the cryptographic boundary of the module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	No configuration of the module or installation steps are required by the operator. When the module is powered on its self-tests are executed without any operator intervention; The module enters the Approved mode of operation automatically if the self-tests at boot complete successfully	Approved	PSP initialized, self-test pass

Table 3: Modes List and Description

The module only supports one mode of operation where only Approved cryptographic functions and services are available.

Mode Change Instructions and Status:

The module only supports an Approved mode of operation.

Degraded Mode Description:

The module does not support a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
Conditioning Component Block Cipher Derivation Function SP800-90B	A2272	-	SP 800-90B
Counter DRBG	A2721	Prediction Resistance - No, Yes Mode - AES-128, AES-256 Derivation Function Enabled - No	SP 800-90A Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The module does not support any Vendor-Affirmed Algorithms.

Non-Approved, Allowed Algorithms:

The module does not support any Non-Approved, Allowed Algorithms.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not support any Non-Approved, Allowed Algorithms with no Security claimed.

Non-Approved, Not Allowed Algorithms:

The module does not support any Non-Approved, Not Allowed Algorithms.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Random Bit Generation	DRBG	Generation of random bits		Counter DRBG: (A2721)
Entropy	ENT-ESV	Entropy source (TRNG) within the module		Conditioning Component Block Cipher Derivation Function SP800-90B: (A2272)

Table 5: Security Function Implementations

2.7 Algorithm Specific Information

Per IG D.L, the CSPs for the approved DRBG have been defined in Section 9.4 SSP Table 1 and SSP Table 2.

2.8 RBG and Entropy

Cert Number	Vendor Name
E137	Google

Table 6: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
TRNG Entropy Source	Physical	IN763 SoC A0	128 bits	128 bits (full entropy)	BlockCipher_DF (A2272)

Table 7: Entropy Sources

The module is a sub-chip cryptographic subsystem hardware module containing a hardware-based DRBG conformant to NIST SP 800-90Ar1, which is seeded by an NIST SP 800-90B compliant entropy source with the required 384 bits. The module's entropy source is consistent with Scenario 1 (a) described in FIPS 140-3 IG 9.3.A.

2.9 Key Generation

The module does not generate any SSPs (Sensitive Security Parameters) but provides random bits to other sub-systems (specifically, the ICC) within the IN763 SoC.

2.10 Key Establishment

The module does not support SSP establishment.

2.11 Industry Protocols

The module does not support any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
AMBA (On-chip system bus) Serial Peripheral Interface (SPI)	Data Input	Requests for random bits
AMBA (On-chip system bus)	Data Output	Random bits
AMBA (On-chip system bus)	Control Input	Reset signal
Physical power connector	Power	Provides power to the module
AMBA (On-chip system bus)	Status Output	Status of the Approved Mode of operation and self-tests i.e. success/failure indicator for the NIST SP 800-90Ar1 DRBG health tests

Table 8: Ports and Interfaces

The module does not support control output.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The module does not support operator authentication; assumption of the Crypto Officer (CO) role is implicit based on the selected service(s). The CO role has access to all module services, and the module does not support a User/Maintenance role.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	Crypto Officer	None

Table 9: Roles

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

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Random Bit Generation	Provides random bits to the ICC module	Approved mode indicator combined with successful completion of the service	Request for ranbom bits from the ICC	Random bits	Random Bit Generation Entropy	CO - B227 DRBG Entropy Input String: G,E - B227 DRBG Seed: G,E - B227 DRBG V: G,E - B227 DRBG Key: G,E - B227 DRBG Output: G,R
Show Status	Current state of the module	Approved mode indicator/Hard Error State indicator combined with successful completion of the service	Reboot to trigger CAST execution	Status	None	CO
Show module's versioning information	Retrieval of the module ID and hardware version	Approved mode indicator combined with successful completion of the service	command "mem read32 0x200780001c"	Hardware version: 3.00b; Module ID: 0	None	CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Perform self-tests	On demand self-test execution on rebooting the module	0	Power cycle	Status	None	CO
Perform zeroisation	Reboot/power-cycle of the module zeroises all SSPs as they are stored ephemerally	Approved mode indicator combined with successful completion of the service	Power cycle/reboot	Status	None	CO - B227 DRBG Entropy Input String: Z - B227 DRBG Seed: Z - B227 DRBG V: Z - B227 DRBG Key: Z - B227 DRBG Output: Z

Table 10: Approved Services

4.4 Non-Approved Services

The module does not support any Non-Approved Services.

4.5 External Software/Firmware Loaded

The module does not support loading of any firmware.

4.6 Bypass Actions and Status

The module does not support a bypass capability.

4.7 Cryptographic Output Actions and Status

The module does not support a self-initiated cryptographic output capability.

5 Software/Firmware Security

5.1 Integrity Techniques

The module is implemented entirely in hardware and is non-modifiable. Therefore, the integrity test requirements do not apply in accordance with IG 5.A. Per the allowance in the IG, instead, the module implements the NIST SP 800-90Ar1 DRBG Cryptographic Algorithm Self-Tests (CAST) and is designed to execute the same on every boot.

5.2 Initiate on Demand

The Cryptographic Algorithm Self-Test (CAST) can be initiated on demand by rebooting the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

How Requirements are Satisfied:

The module is a sub-chip cryptographic subsystem hardware module. The procurement, build, and configuration procedure are controlled by the manufacturer. Therefore, the operational environment is considered non-modifiable.

6.2 Configuration Settings and Restrictions

Additional restrictions do not apply.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Standard passivation applied on the IN763 SoC	None	None

Table 11: Mechanisms and Actions Required

The B227 True Random Number Generator (TRNG) Cryptographic Module is a sub-chip cryptographic subsystem hardware module implemented as part of the IN763 SoC, which is the physical perimeter of the sub-chip module. The IN763 SoC is a single chip with a production grade IC packaging and hence conforms to the Level 1 requirements for physical security.

8 Non-Invasive Security

8.1 Mitigation Techniques

The module does not support any non-invasive attack mitigations.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Internal registers	Ephemeral storage of SSPs in plaintext	Dynamic

Table 12: Storage Areas

The module does not maintain any persistent SSP storage.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Random bits	Internal registers	ICC module	Plaintext	Manual	Electronic	

Table 13: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroised on reset	SSPs stored ephemerally are zeroised on resetting the module	SSPs stored ephemerally are zeroised on resetting the module	Operator Initiated

Table 14: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
B227 DRBG Entropy Input String	Entropy Input provided by the entropy source; Defined as a CSP per IG D.L Resolution 3. for CTR_DRBG	384 bits - 256 bits	Entropy Input - CSP	Entropy		Random Bit Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
B227 DRBG Seed	Seed provided to the NIST SP 800-90Ar1 DRBG; Defined as a CSP per IG D.L Resolution 3. for CTR_DRBG	384 bits - 256 bits	DRBG Seed - CSP	Random Bit Generation		Random Bit Generation
B227 DRBG V	NIST SP 800-90Ar1 DRBG state V value; Defined as a CSP per IG D.L Resolution 3. for CTR_DRBG	128 bits - 128 bits	Internal state of DRBG - CSP	Random Bit Generation		Random Bit Generation
B227 DRBG Key	NIST SP 800-90Ar1 DRBG state Key value; Defined as a CSP per IG D.L Resolution 3. for CTR_DRBG	256 bits - 256 bits	Internal state of DRBG - CSP	Random Bit Generation		Random Bit Generation
B227 DRBG Output	NIST SP 800-90Ar1 DRBG random bit output	128 bits - 128 bits	Random bits - CSP	Random Bit Generation		

Table 15: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
B227 DRBG Entropy Input String		Internal registers:Plaintext	Until reset	Zeroised on reset	B227 DRBG Seed:Derives
B227 DRBG Seed		Internal registers:Plaintext	Until reset	Zeroised on reset	B227 DRBG Entropy Input String:Derived From B227 DRBG Output:Derives
B227 DRBG V		Internal registers:Plaintext	Until reset	Zeroised on reset	B227 DRBG Seed:Derived From B227 DRBG Key:Paired With
B227 DRBG Key		Internal registers:Plaintext	Until reset	Zeroised on reset	B227 DRBG Seed:Derived From B227 DRBG V:Paired With
B227 DRBG Output	Random bits	Internal registers:Plaintext	Until reset	Zeroised on reset	B227 DRBG Seed:Derived From

Table 16: SSP Table 2

-- CSP: Critical Security Parameter
-- PSP: Public Security Parameter

Please Note: The module's entropy source has been validated under NIST SP 800-90B per the ESV Cert. #E137. The Public Use Document for the same can be found at: https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/entropy/E137_PublicUse.pdf.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Counter DRBG (A2721)	CTR_DRBG (AES-CTR, 256 bits)	KAT	SW/FW Integrity	0	Used as approved DRBG for generation of random bits according to SP800-90Ar1

Table 17: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A2721)	CTR_DRBG (AES-CTR, 256 bits)	KAT	CAST	0	-	During boot
NIST SP 800-90B Entropy Source Repetition Count Test (RCT)	Cutoff value (C) = 41; False positive error rate (alpha) = 2^-20	RCT	CAST	the core is ready to be used	-	During boot and continuously
NIST SP 800-90B Entropy Source Adaptive Proportion Test (APT)	Cutoff value (C) = 793; Window Size (w)=1024 False positive error rate (alpha) = 2^-20	APT	CAST	the core is ready to be used	-	During boot and continuously

Table 18: Conditional Self-Tests

In the event that any of the above conditional tests fail, the cryptographic module will be halted, and data output will be inhibited.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A2721)	KAT	SW/FW Integrity	On Demand	Manually, via a reboot

Table 19: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Counter DRBG (A2721)	KAT	CAST	On Demand	Manually, via a reboot
NIST SP 800-90B Entropy Source Repetition Count Test (RCT)	RCT	CAST	On Demand	Manually, via a reboot
NIST SP 800-90B Entropy Source Adaptive Proportion Test (APT)	APT	CAST	On Demand	Manually, via a reboot

Table 20: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Hard Error state	No cryptographic functions can be executed and all data output is inhibited; An operator can attempt to reset the state by cycling the power	Failure of a CAST	The module would have to be re-initialized via a power-cycle of the IN763 SoC i.e., by rebooting the module	FAILED_TEST_ID_0 has non-zero value in case of a failure in the DRBG CAST
Soft Error state	The Soft Error state is cleared automatically by the entropy source (the source raises an alarm, zeroises itself and becomes operational again)	Failure of a NIST SP 800-90B Health Test	The entropy source (and thus the module as a whole) recovers automatically	Failure of a NIST SP 800-90B Health Test causes the entropy source to raise an alarm and zeroise itself

Table 21: Error States

10.5 Operator Initiation of Self-Tests

An operator can initiate pre-operational and conditional cryptographic algorithm self-tests on demand by rebooting the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

No specific instructions are required for initialization of the module in an Approved mode apart from powering on the underlying SoC/chip.

11.2 Administrator Guidance

Please see Sections 2, 3, 4 and 11 in this document.

11.3 Non-Administrator Guidance

Please see Sections 2, 3, 4 and 11 in this document. The module only supports the role of a Crypto Officer (Administrator).

11.4 Maintenance Requirements

No specific maintenance requirements apply.

11.5 End of Life

The module can be zeroised to perform secure sanitization.

12 Mitigation of Other Attacks

12.1 Attack List

The module does not support mitigation of any other attacks and thus the requirements of this section do not apply.