Non-Proprietary FIPS 140-2 Security Policy

Google LLC.

Integrated Management Complex (IMC) & B227 True Random Number Generator (TRNG) Firmware-Hybrid Cryptographic Module

Hardware version: 3.00b

Firmware version: 20230126

Date: 2/3/2023

Prepared By:

intertek acumen security

2400 Research Blvd

Suite 395

Rockville, MD 20850

Introduction

Federal Information Processing Standards Publication 140-2 — 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 program. NVLAP accredits independent testing labs to perform FIPS 140-2 testing; the CMVP validates modules meeting FIPS 140-2 validation. Validated is the term given to a module that is documented and tested against the FIPS 140-2 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 Integrated Management Complex (IMC) & B227 True Random Number Generator (TRNG) Firmware-Hybrid 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 140-2.

The Integrated Management Complex (IMC) & B227 True Random Number Generator (TRNG) Firmware-Hybrid Cryptographic Module also be referred to as “IMC & 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

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Scope

This document describes the cryptographic module security policy for the Google LLC. Integrated Management Complex (IMC) & B227 True Random Number Generator (TRNG) Firmware-Hybrid Cryptographic Module (also referred to as the "module" hereafter). It contains specification of the security rules under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-2 standard.

1.2 Overview

The IMC Secure Firmware represents the firmware portion of the module, which manages functions such as power-on, reset, clock and power control, configuration, and security functions including encryption and decryption, key derivation, key generation, and hashing. The IMC implements these functions as ARM Trusted Execution Environment (TEE) firmware executing on two ARM-A53 processors. The hardware portion of the module comprises the B227 TRNG, which is a NIST SP 800-90 A/B compliant TRNG employed by the IMC Secure Firmware for generating cryptographic keys.

2. Security Level

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
Electromagnetic Interference / Electromagnetic Compatibility	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Overall Level	1

Table 1 - Security Level

3. Cryptographic Module Specification

3.1 Cryptographic Boundary

The IMC & B227 TRNG Firmware-Hybrid Cryptographic Module is a sub-chip firmware-hybrid module within a single chip embodiment. The IMC Secure Firmware portion of the module executes on two ARM Cortex A53 management processors within the Integrated Management Complex (IMC) hardware block of the IN762 system-on-a-chip (SoC). The IMC Secure Firmware is the controlling component of the B227 True Random Number Generator (TRNG), which comprises the hardware portion of the module. The module's cryptographic boundary consists of only the IMC Secure Firmware and the B227 TRNG. The cryptographic boundary of the module and the relationship among the various internal components of the module are depicted in Figure 1 below.

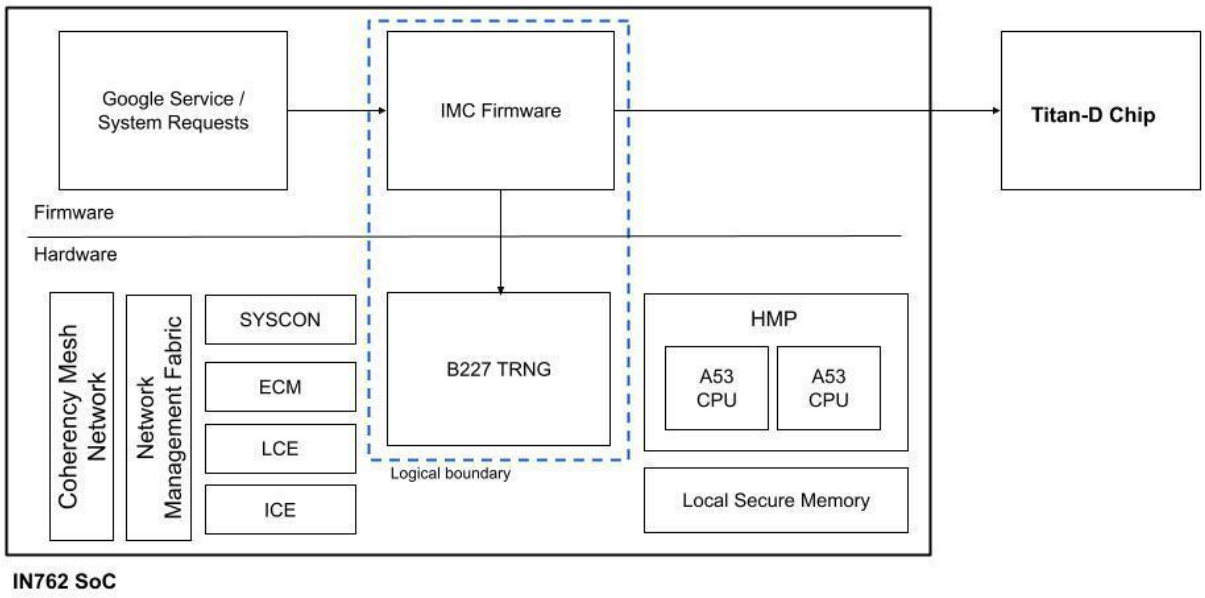

Figure 1 - IMC/B227 Block Diagram

The Google IN762 SoC contains the Host Management Processor (HMP) consisting of the two ARM-A53 CPUs on which the module's firmware executes, Local Secure Memory (LSM), System Controller (SYSCON), eFUSE Controller Module (ECM), the B227 TRNG (hardware portion of the module), and the Network Management Fabric and Coherency Mesh Network connecting these components and other subsystems. The components within the IN762 SoC are interconnected via an AMBA[1] on-chip system bus. The module does not contain any persistent storage; however, it mediates access between the secure and non-secure memory structures within the HMP.

The IMC Secure Firmware is comprised of a single binary image. The hardware portion is the B227 TRNG which provides seed values to a firmware DRBG for key generation functions.

[1] ARM Microcontroller Bus Architecture

The module's primary role is to generate, maintain, control, and manage the Critical Security Parameters (CSPs) and keys required for the operation of other cryptographic services within the IN762 SoC. In particular, the module:

- Implements a secure interface to one or more True Random Number Generators (TRNGs) which serve as trusted sources of entropy, which can be used as the basis for generation of keys and nonces. The firmware may use the B227 TRNG or the external Titan-D Chip (FIPS 140-2 Cert# 4367) as an approved entropy source.
- Implements an instance of a firmware-based Deterministic Random Bit Generator, seeded by the above entropy source(s), to generate cryptographic keys in support of the PSP Security Protocol (PSP) and ICE Secure Association Database (SADB). Note: The module does not perform encryption for PSP or SADB nor are these components included in the logical boundary.
- Implements a second instance of the same Deterministic Random Bit Generator (seeded independently from the same entropy source(s) as the first) which outputs a random bit stream upon request to external applications.
- Supports PSP by implementing a secure Security Parameter Index (SPI) management function, tied to a secure Key Derivation Function (KDF). The module maintains associations between SPIs and PSP Master Keys, and the SPI-specific AES-GCM keys derived from them.
- Performs a firmware load test for the Lookaside Compression and Cryptographic Engine (LCE).
- Maintains access control to Critical Security Parameters (CSPs) which are isolated to secure memory locations.
- Implements basic board- and processor-specific control and maintenance functions, such as "start CPU".

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

4. Cryptographic Module Ports and Interfaces

The physical interfaces provided by the module are mapped to the FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following table:

Physical Port	Ports	Description
Data Input	AMBA (On-chip system bus) Serial Peripheral Interface (SPI)	• Secure EL1 command parameters • Fast Secure Monitor API parameters • Google service request API parameters • SPI interface to Titan-D
Data Output	AMBA (On-chip system bus)	• Secure EL1 return data • Fast Secure Monitor API return data • Google service request API return data

Physical Port	Ports	Description
Control Input	AMBA (On-chip system bus)	• Secure EL1 commands • Fast Secure Monitor API commands • Google service request API commands
Status Output	AMBA (On-chip system bus)	• Secure EL1 command response codes • Fast Secure Monitor API response codes • Google service request API response codes
Power Input	Physical power connector	Provides power to the module

Table 2 - Physical Port and Logical Interface Mapping

All control input data is directed through the firmware portion of the module.

5. Roles, Services and Authentication

5.1 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. The module does not support authentication.

5.2 Services

The module provides the following Approved services which utilize algorithms listed in Table 5. The module's firmware provides APIs operating at three levels. Execution requests come in at higher levels and are translated into lower-level service calls:

- Secure EL1 (Lowest level)
- Fast Secure Monitor (Mid-level)
- Google service requests (Mid- and High-Level)

:

Service	Roles		CSP	CSP Access
	User	CO		R = Read W = Write X = Execute
Initialize (Module and PSP functions including generate PSP Master Key)	✓	✓	Master PSP Key	W
Perform self-tests (executed automatically when powered on)	✓	✓	N/A	N/A
Show status	✓	✓	N/A	N/A

Service	Roles		CSP	CSP Access
	User	CO		R = Read W = Write X = Execute
Zeroization	✓	✓	All	W
Secure EL1				
CPU state management (CPU on)	✓	✓	N/A	N/A
Fast Secure Monitor				
Get information (print buffer, command buffer)	✓	✓	N/A	N/A
Print buffer management (start, stop)	✓	✓	N/A	N/A
Submit request data	✓	✓	N/A	N/A
Retrieve response data	✓	✓	N/A	N/A
Execute Google service request	✓	✓	N/A	N/A
Google Service Requests				
Generate New PSP Master Key (Post-initialization) a.k.a. "Rotate key generation"	✓	✓	Master PSP Key	W
Derive PSP Session Key(s)	✓	✓	PSP Session Key	W
			Master PSP Key	R, X
Generate DRBG output	✓	✓	IMC DRBG Seed B227 DRBG Seed IMC DRBG Key B227 DRBG Key IMC DRBG V B227 DRBG V	R, W, X
			SADB Protection Key	W
Generate DRBG output for Linux	✓	✓	N/A	N/A
Perform Firmware Load Test (LCE)	✓	✓	N/A	N/A

Table 3 - Approved Services and Role Allocation

5.3 Authentication

There is no operator authentication; assumption of role is implicit based on the selected service(s). The User and CO roles have access to all module services; there is no separation of role access.

6. Physical Security

The IMC and B227 TRNG is a firmware-hybrid module implemented as part of the IN762 SoC, which is the physical boundary of the sub-chip module. The IN762 SoC is a single chip with production grade IC packaging and hence conforms to the Level 1 requirements for physical security.

7. Operational Environment

The module is a single-chip firmware-hybrid module. The procurement build and configuration procedure are controlled by the manufacturer. Therefore, the operational environment is considered non-modifiable.

8. Cryptographic Algorithms and Key Management

8.1 Cryptographic Algorithms

There are algorithms, modes and key sizes tested via CAVP but not implemented by the module. The module implements the following approved algorithms:

IMC Secure Firmware Algorithm Implementation					
ACVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
A2469	AES-ECB	128, 192, 256 bits	SP 800-38A	ECB	Encryption
A2469	AES-CMAC	128, 192, 256 bits	SP 800-38B	AES-CMAC	Message Authentication
Vendor Affirmed	CKG	256 bits	SP 800-133rev2	Section 4 Option 1	Symmetric Cryptographic Key Generation
A2469	DRBG	256 bits	SP 800-90A	CTR_DRBG	Random Bit Generation
A2469	KBKDF (Counter Mode)	256 bits	SP 800-108	CMAC	Key Derivation
A2469	SHS	SHA-256	FIPS 180-4	N/A	Hashing
B227 TRNG					
ACVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
A2721	AES-CTR	256 bits	SP 800-38A	AES-CTR	Random Bit Generation
A2721	DRBG	256 bits	SP 800-90A	CTR_DRBG	Random Bit Generation
A2932	ENT (P)	N/A	SP 800-90B	Conditioning Component - Block Cipher Derivation Function	Entropy Source

Table 4 - Approved Algorithms

8.2 Cryptographic Key Management

The module supports the following CSPs listed below in Table 5. The CSP access policy is denoted in Table 3 above.

Keys and CSPs	Key Description	Algorithm and Key Size	Generation	Input / Output Method	Storage / Zeroization
IMC Entropy Input String	SP 800-90A DRBG	256-bits	Generated via an approved entropy source (B227 DRBG and/or Titan-D Chip).	Internally generated (B227) or Input via direct physical interface (Titan-D). Never exits the module.	LSM; zeroized on reset.
IMC DRBG Seed	SP 800-90A DRBG	384-bits	Generated via an approved entropy source (B227 DRBG and/or Titan-D Chip).	Internally generated (B227) or Input via direct physical interface (Titan-D). Never exits the module.	LSM; zeroized on reset.
IMC DRBG V	SP 800-90A DRBG	128-bits	Calculated according to SP 800-90A algorithm specifications, with backtracking resistance.	N/A	LSM; zeroized on reset.
IMC DRBG Key	SP 800-90A DRBG	128-bits	Calculated according to SP 800-90A algorithm specifications, with backtracking resistance.	N/A	LSM; zeroized on reset.
B227 DRBG Entropy Input String	SP 800-90A DRBG	256-bits	Generated via B227 entropy source.	Internally generated. Never exits the module.	Internal registers; zeroized on reset.
B227 DRBG Seed	SP 800-90A DRBG	384-bits	Generated via B227 entropy source.	Internally generated. Never exits the module.	Internal registers; zeroized on reset.

Keys and CSPs	Key Description	Algorithm and Key Size	Generation	Input / Output Method	Storage / Zeroization
B227 DRBG V	SP 800-90A DRBG	128-bits	Calculated according to SP 800-90A algorithm specifications, with backtracking resistance.	N/A	Internal registers; zeroized on reset.
B227 DRBG Key	SP 800-90A DRBG	256-bits	Calculated according to SP 800-90A algorithm specifications, with backtracking resistance.	N/A	Internal registers; zeroized on reset.
Master PSP Keys	Used to derive per-SPI PSP Session keys.	256-bit, AES-ECB, SP-800-108 KDF	Generated via SP 800-90A DRBG.	N/A	LSM; zeroized on reset.
Security Association Database (SADB) Protection keys	Used to encrypt SADB.	256-bit, AES-GCM	Generated via SP 800-90A DRBG.	N/A	LSM; zeroized after writing to the calling application/subsystem or on reset.
PSP Session Keys	Used to encrypt/decrypt PSP traffic.	128-bit and 256-bit, AES-GCM	Generated via SP-800-108 KDF.	N/A	LSM; zeroized after writing to the calling application/subsystem or on reset.

Table 5 - Approved Keys and CSPs

8.3 Key Generation and Entropy

The module is a firmware-hybrid module which includes one firmware and one hardware-based DRBG conformant to SP 800-90A, which is seeded by an SP 800-90B compliant entropy source. The IMC Secure Firmware DRBG and the B227 DRBG are seeded with 384 bits.

The IMC Secure Firmware DRBG may be seeded by the B227 TRNG or the external Titan-D Chip (FIPS 140-2 Cert# 4367). When the Titan-D entropy source is used, the entropy seed is loaded directly over a Serial Peripheral Interface (SPI) bus.

The module's entropy source is consistent with Scenario 1 (a) described in FIPS 140-2 IG 7.14. The module generates symmetric keys in accordance with IG D.12 and SP 800-133rev2, Section 4.

8.4 Key Storage and Zeroization

All CSPs are stored in LSM and are cleared upon power cycle or after having been written to the calling application or subsystem internal to the IN762 SoC. Zeroization may be triggered by the IMC firmware via the SYSCON block, which resets the ARM-A53 cores. In addition to this, the TRNG state stored in hardware registers of the B227 is zeroized on reset.

The module does not maintain any persistent CSP storage.

9. Self-tests

FIPS 140-2 requires self-tests to ensure the correctness of the cryptographic functionality at start-up. Some functions require conditional tests during normal operation of the module.

If any of the tests fail, the module will return an error code and transition to an error state. Upon reaching a hard error state, no cryptographic functions are able to be executed and all data output is inhibited. An operator can attempt to reset the state by cycling the power. However, the failure of a self-test may require the module to be replaced. In the event of a transition to a soft error state, the module will return an error and resume operation. These error conditions are further explained in the sections below.

9.1 Power-On Self-Tests

Power-on self-tests are run upon the initialization of the module and do not require operator intervention to run. If any of the tests fail, the module will not initialize, and any data output is inhibited.

The module implements the following power-on self-tests:

Type	Test Description
IMC Secure Firmware	
Known Answer Tests	• AES-ECB 128, 192, 256 Encrypt forward cipher Known Answer Test.
	• AES-CMAC 128-bit Known Answer Test.
	• SHA-256 Known Answer Test
	• SP 800-108 KBKDF Known Answer Test
	• CTR_DRBG KAT (Instantiate, Generate, Reseed)
Firmware Integrity Test	• AES-CMAC 256-bit integrity test
B227 TRNG	
Known Answer Tests	• CTR_DRBG KAT (Instantiate, Generate, Reseed)
	• Block Cipher Derivation Function

Table 6 - Power-up Self-Tests

The module performs all power-on self-tests automatically when it is initialized. Power-on self-tests must pass before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module.

9.2 Conditional Self-Tests

Conditional self-tests are run under specific conditions, such as during TRNG instantiation or continuously, as well as during firmware loading.

Type	Test Description
Firmware Load Test	• AES-CMAC 256-bit firmware load test
LCE Firmware Integrity Test / Firmware Load Test	• AES-CMAC 256-bit integrity test and firmware load test for LCE module
SP 800-90B Health Tests	• B227 Adaptive Proportion Test
	• B227 Repetition Count Test

Table 7 - 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, with the exception of the LCE Firmware Integrity Test / Firmware Load Test. In this case, the test is performed on behalf of the LCE module. Upon failure, the IMC/B227 module will reject the LCE firmware and the LCE module will remain in an uninitialized state. However, the IMC/B227 module will resume its operations.

9.3 Critical Function Tests

The module implements a critical function test which validates whether the proper production fuses have been set in the eFUSE Controller Module (ECM) located within the IN762 SoC. If any of the production fuses are found to be set incorrectly, or have not been set, the IMC Secure Firmware will halt initialization of other IN762 subsystems external to the cryptographic boundary.

10. Mitigation of Other Attacks

No specific claims for this section.

11. Crypto Officer and User Guidance

No specific instructions are required for initialization of the module in a FIPS Approved mode. The module is only considered valid if operated with the firmware and hardware versions as specified on the validation certificate.

12. Glossary

Term	Description
AES	Advanced Encryption Standard
AMBA	ARM Microcontroller Bus Architecture
AXI	Advanced Extensible Interface
CAVP	Cryptographic Algorithm Validation Program
CMAC	Cipher-based Message Authentication Code
CMN	Coherency Mesh Network
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CTR	Counter Mode
DRBG	Deterministic Random Number Generator
ECM	eFUSE Controller Module
FIPS	Federal Information Processing Standards
HMP	Host Management Processor
ICE	Inline Cryptographic Engine
IG	Implementation Guidance
IMC	Integrated Management Complex
KAT	Known answer test
KDF	Key Derivation Function
LCE	Lookaside Compression and Cryptography Engine
LSM	Local Secure Memory
NDRNG	Non-deterministic Random Number Generator
NMF	Network Management Fabric
PSP	PSP Security Protocol
SADB	Security Association Database
SHA	Secure Hash Algorithm
SoC	System On Chip
SPI	Security Parameter Index
SPI	Serial Peripheral Interface
SYSCON	System Controller
TEE	Trusted Execution Environment
TRNG	True Random Number Generator

Table 8 - Glossary of Terms

End of Document