

Titan-BPN TRNG Entropy Source

Hardware Version: H1BxP
Firmware Version: gqfips-1.3

SP 800-90B Non-Proprietary Public Use Document

Document Version 1.4

April 2025

Prepared for:

Google LLC

Prepared by:



www.lightshipsec.com

Table of Contents

1 Introduction 3
1.1 Description 3
1.2 Security Boundary 3
2 Configuration 5
2.1 Operating Conditions 5
2.2 Configuration Settings 5
2.3 Physical Security Mechanisms 5
2.4 Maintenance 5
3 Entropy Source 6
3.1 Interfaces 6
3.2 Min-Entropy 6
3.3 Health Tests 6
3.4 Statistical Testing 6

1 Introduction

1.1 Description

1 The Google Titan chip is a custom, secure microcontroller. It can implement a variety of security, encryption, and cryptography protocols. The protocols are running on a secure processor on-chip, interfacing with a host using an API across a trusted SPI peripheral. It provides secure EEPROM Boot, using SPI pass-through technology that allows Titan to confirm authorship of Boot Code, ensuring code-signing before code swap is completed.

2 The Titan-BPN TRNG Entropy Source (ES) is composed of a physical noise source that operates on the principle of frequency collapse in a Three-Edge Ring Oscillator (TERO), a vetted conditioning component, and health tests.

3 The ES was tested on the hardware platforms listed in Table 1 under the assumption that its output is non-IID.

Table 1: Hardware Platforms

Part Number	H1
Hardware Revision	BxP (B1P, B3P)[1]
Firmware Version	gqfips-1.3
Software Version	N/A

1.2 Security Boundary

4 The security boundary of the ES is the entire Titan chip as shown in Figure 1.

[1] The SHA block (Titan SHA Module 1.0) is identical across Titan Chip H1B revisions. The hardware OE "H1B3P" denotes a SKU number for a specific Titan Chip package. The number "1" is a minor revision of the package.

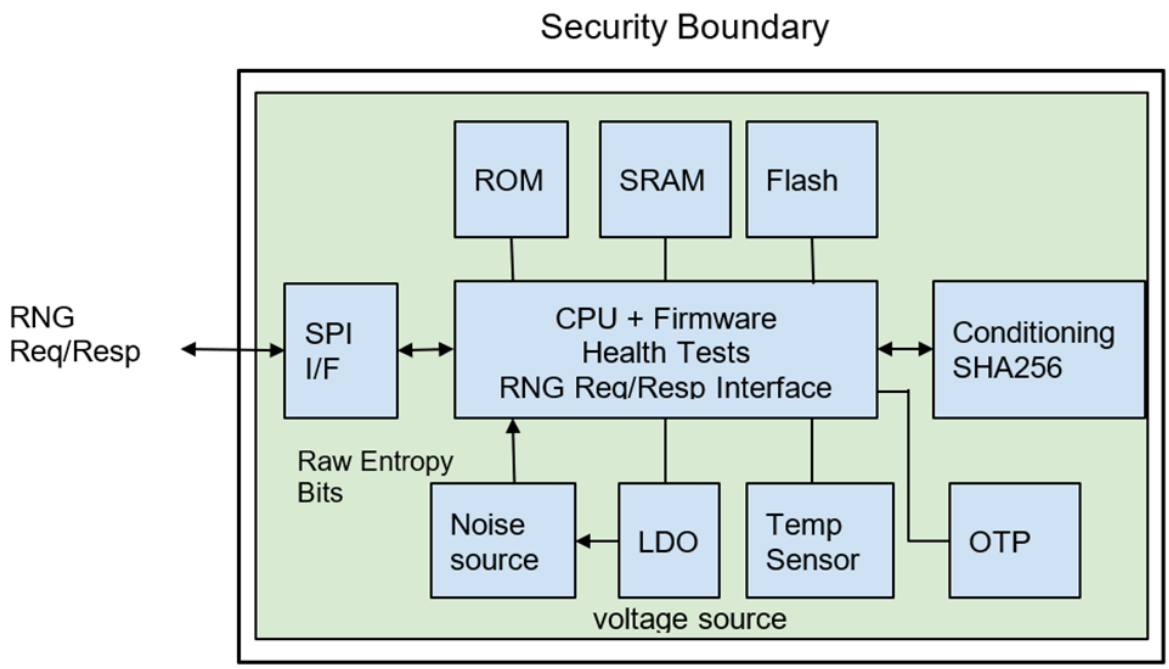


Figure 1: Security Boundary

The security boundary includes the following components:

a) **Noise Source.** SP800-90B compliant noise source.

b) **Health Tests.** SP800-90B compliant health tests.

c) **Conditioning component.** CAVP certified (CAVP #A5420) vetted conditioning component SHA2-256.

2 Configuration

2.1 Operating Conditions

6 The ES operates correctly under the inherent operating conditions of the hardware platform:

Table 2: Operating Conditions

Parameter	Value	Description
Temperature	0C to 85C	Full PVT (Process, Voltage and Temperature) characterization has been performed and covered the temperature range of 0C to 85C per datasheet specifications.
Voltage	2.5V and 3.6V	The external VDDIO voltage between 2.5V and 3.6V
Clock speed	24 MHz	

2.2 Configuration Settings

7 For the ES tested in the OEs listed in Table 1, the customer does not have the ability to modify the ES configuration settings.

2.3 Physical Security Mechanisms

8 The noise source is a physical noise source that resides on the Google Titan chip. The tamper-resistant chip provides secure storage, secure identity, hardened cryptography, and Google proprietary features to consumer devices. High level security features are the security-hardened RISC-V processor, voltage, frequency, temperature, and parity attack detectors, and configurable alert responders.

2.4 Maintenance

9 There are no maintenance requirements.

3 Entropy Source

3.1 Interfaces

10 There is a dedicated host and peripheral SPI interface, which can be used to provide access to raw data of the noise source.

3.2 Min-Entropy

11 The min-entropy rate at the output of source (H_out for the output of the vetted conditioning function per section 3.1.5 of 90B) is 256-bits per 256-bit output sample.

3.3 Health Tests

12 Google has designed health tests to detect failures of the Noise Source, or to detect a deviation from the expected entropy rate during the correct operation of the Noise Source before the raw data is conditioned. Following the NIST SP 800-90B requirements, the vendor has implemented three types of health tests in this product:

a) **Start-up Test.** On startup, 4096 raw 1-bit samples are run through a Repetition Count Test(RCT) and an Adaptive Proportion Test(APT). If either of these tests fail, the firmware resets the chip.

b) **Continuous Test.** The approved health tests Repetition Count Test (RCT), and the Adaptive Proportion Test (APT) are implemented. All the raw data pulled off the noise source FIFO is fed into the RCT and APT. The initial state of these tests is from the earlier startup tests. Only if RCT and APT pass, the data is made available to the conditioning component.

c) **On-Demand Test.** The host can send a command to restart the firmware at any time, which will cause the startup tests to be performed.

13 The entropy source continuously runs the SP 800-90B health tests and will produce an error upon failure. In particular, if the continuous tests have failed more than 10 times, the ES goes into a permanent error state, and all calls for entropy will fail until the chip is reset. If the continuous tests are currently failing, but have failed less than 10 times, the ES returns an error code.

14 If the start-up tests have failed, the firmware resets the chip.

3.4 Statistical Testing

15 The ES is configured in the platforms listed in Table 1 to comply with SP800-90B at the first start of the respective device. There is no testing required.

16 To test the entropy source one million consecutive raw physical noise samples must be collected from the noise source interface of the entropy source.

17 The results obtained from the NIST SP800-90B tool must be at least as high as the H_submitter. The H_submitter is 0.79 bits of entropy per bit.

18 1000 raw physical noise samples after 1000 restarts for assessment that (1) the sanity test passes and (2) the minimum of the row-wise and column-wise entropy rate shall not be less than half of the entropy rate from 1 above.