

Titan TRNG Entropy Source

Hardware Version: Google H1B2
Firmware Version: OpenSK 4.0.2

SP 800-90B Non-Proprietary Public Use Document

Document Version 1.0

May 2024

Prepared for:

Google LLC

Prepared by:



www.lightshipsec.com

Document History

Version	Date	Description
1.0	27 May 2024	Updated firmware and ES name.

Table of Contents

1 Introduction 4
1.1 Description 4
1.2 Security Boundary 4
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 Titan 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.

2 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	B2
Firmware Version	OpenSK 4.0.2

1.2 Security Boundary

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

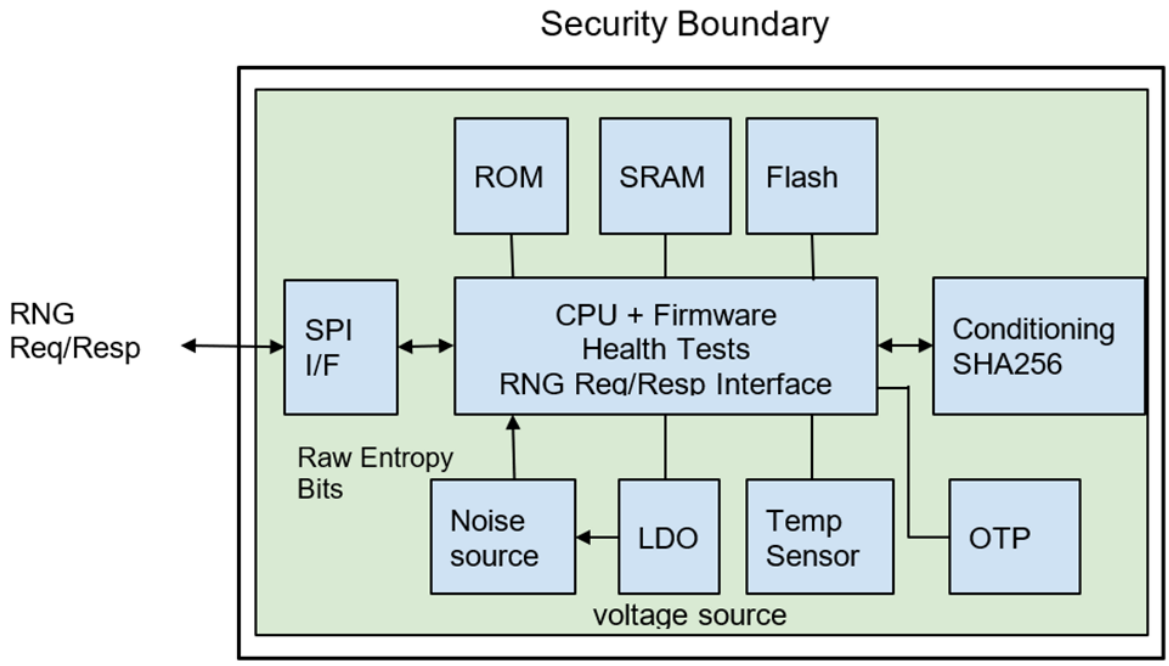


Figure 1: Security Boundary

4 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 #A2352) vetted conditioning component SHA2-256.

2 Configuration

2.1 Operating Conditions

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

a) **Temperature Range:** between 0°C and 85°C.

b) **Voltage Range:** between 2.5V and 3.6V.

2.2 Configuration Settings

6 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

7 The noise source is a physical noise source that resides on the Google Titan chip. The Google Titan chip is a secure microcontroller for use in mobile devices.

8 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 interfaces, 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, 1024 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. If start-up tests fail, the firmware resets the chip.

3.4 Statistical Testing

14 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.

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

16 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.

17 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.