SP 800-90B Non-Proprietary Public Use Document

Phison PS5020-E20/PS5302 Entropy Source

Hardware version: NOISEGEN_T12FFC

Date: Nov 8, 2024
Document Version 0.6



47488 Kato Road
Fremont, CA 94538



Phison Electronics Corporation
No.1, Qun-Yi Road, Jhunan, Miaoli County,
Taiwan 350

Template Revision History

Version	Date	Change
V0.1	05-12-2023	Initial release
V0.2	05-31-2023	Update information
V0.3	11-20-2023	Update information
V0.4	01-25-2024	Update information
V0.5	01-31-2024	Update information
V0.6	11-08-2024	Add PS5302 as new OE

This document may freely be reproduced and distributed in its entirety only.

Table of Contents

Description 4

Security Boundary 4

Operating Conditions 4

Configuration Settings 5

Physical Security Mechanisms 5

Conceptual Interfaces 5

Min-Entropy Rate 5

Health Tests 5

Maintenance 5

Required Testing 5

[Note: Some sections in this document may be pared down or excluded when the entropy source is validated as reuse restricted to vendor.]

This document may freely be reproduced and distributed in its entirety only.

Description

The PS5020-E20/PS5302 ASIC hardware includes a true non-deterministic random number generator called “NOISEGEN_T12FFC”. This NOISEGEN_T12FFC is a physical entropy source that meets the requirements of SP 800-90B. It is used to seed a deterministic random bit generator (DRBG) that complies with SP 800-90A. The claimed non-IID output of the entropy source has been tested on the PS5020-E20/PS5302 ASIC microcontroller which is contained within an NVMe self-encrypting drive.

Security Boundary

Figure 1 shows the entropy source block diagram within the PS5020-E20/PS5302 ASIC. The entropy source boundary contains its own health tests, which are performed on all random bits generated by the noise source. If no failures occur, the random bit can be used for DRBG mechanisms.

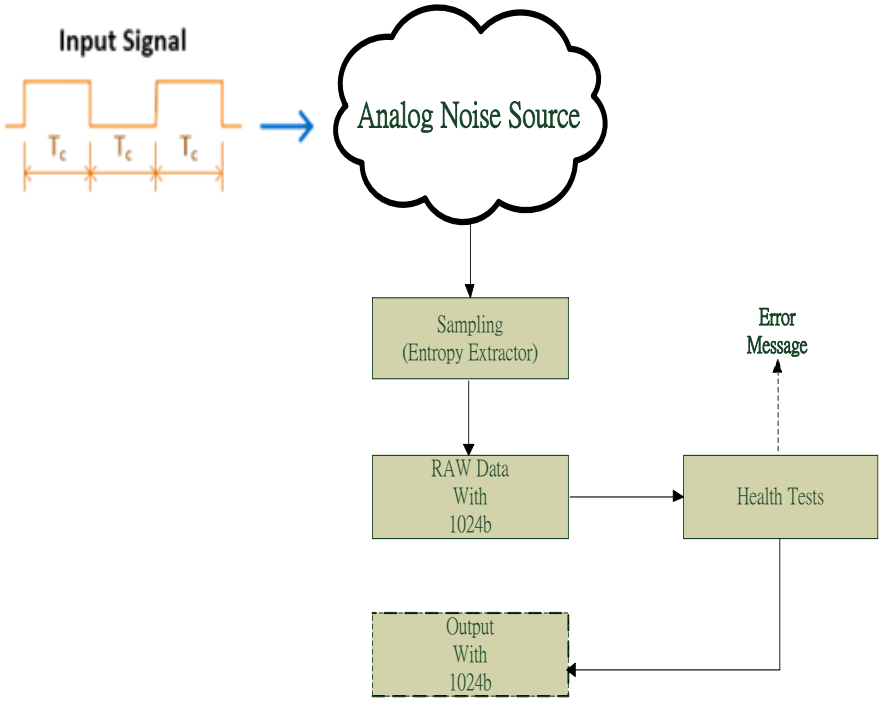


Figure 1: Entropy Source Security Boundary

Operating Conditions

The entropy source is expected to generate random data under normal operating conditions for the built-in PS5020-E20 ASIC SSD module, which are detailed in the following table.

Parameter	Value	Description
Temperature	Min. 0˚C Typ. 25 ˚C Max. 70 ˚C	operational temperature
Voltage	~0.82V/~0.80V	VCCK

This document may freely be reproduced and distributed in its entirety only.

Parameter	Value	Description
Clock speed	10MHz	Frequency of clock

Configuration Settings

Customers would not have the ability to configure the settings of the entropy source.

Physical Security Mechanisms

The entropy source operates within PS5020-E20/PS5302 ASIC which is protected by Seagate® Secure NVMe Self-Encrypting Drives (SED) device package. The SED is capable of meeting FIPS 140-3 level 2 physical security requirement and provides tamper-evidence protection.

Conceptual Interfaces

A user can access the following conceptual method: TCG Random

Min-Entropy Rate

Based on the Entropy Assessment Report, the most pessimistic result from the output of the NOISEGEN_T12FFC is 0.594772 bits of min-entropy per output bit.

Health Tests

The entropy source performs a modified Repetition Count Test (RCT) and an Adaptive Proportion Test (APT) for start-up, continuous, and on-demand requirements. These tests are run over consecutive 1024 bits collected from the noise source before they are available for use The PS5020-E20 ASIC checks the counts of failures while performing continuous health tests. If the counts exceed 1, the fault will be considered as a permanent/persistent failure. The RNG interface will report an error status, and the PS5020-E20/PS5302 ASIC will be stuck. In the case where a persistent failure is detected, the entropy source will not produce any outputs.

Maintenance

There are no maintenance requirements related to the Entropy Source.

Required Testing

The Entropy Source compliance to SP 800-90B was validated using the special testing interface by the SP 800-90B entropy assessment Tool version 1.1.7 provided by NIST.

The raw noise data samples, including 1,000,000 consecutive samples, were obtained directly from the noise source. Both the theoretical assessment and the test results predicted a higher min-entropy than the expected conservative min-entropy of 0.594772.

This document may freely be reproduced and distributed in its entirety only.

The built-in health test includes the modified Repetition Count Test (RCT) and the Adaptive Proportion Test (APT). These health tests will run every time entropy data is requested. If either test fails, the entropy source raises an error. This built-in health test is used to check the validity of the noise source, so no further testing is required.

This document may freely be reproduced and distributed in its entirety only.