

SP 800-90B Non-Proprietary Public Use Document
Kanguru Defender Series Entropy Source
Document Version 1.0

Kanguru Solutions

July 26th, 2024

Revision History

Version	Date	Change
V1.0	7/26/2024	Initial Release

Table of Contents

Description 4
Security Boundary 4
Operating Conditions 4
Configuration Settings 4
Physical Security Mechanisms 5
Conceptual Interfaces 5
Min-Entropy Rate 5
Health Tests 5
Maintenance 5
Required Testing 5

Description

The Kanguru Defender Series Entropy Source is a physical (P) entropy source. It is certified under the January 2018 version of Special Publication 800-90B and the March 26th, 2024 version of the FIPS Implementation Guidance.

This entropy source is restricted to the vendor.

The Kanguru Defender Series Entropy Source was tested on the Kanguru Defender3000 Crypto Processor.

Security Boundary

The security boundary of the entropy source includes the noise source, the sampling hardware, and the health tests which are performed on raw data. The security boundary is shown in **Figure 1**.

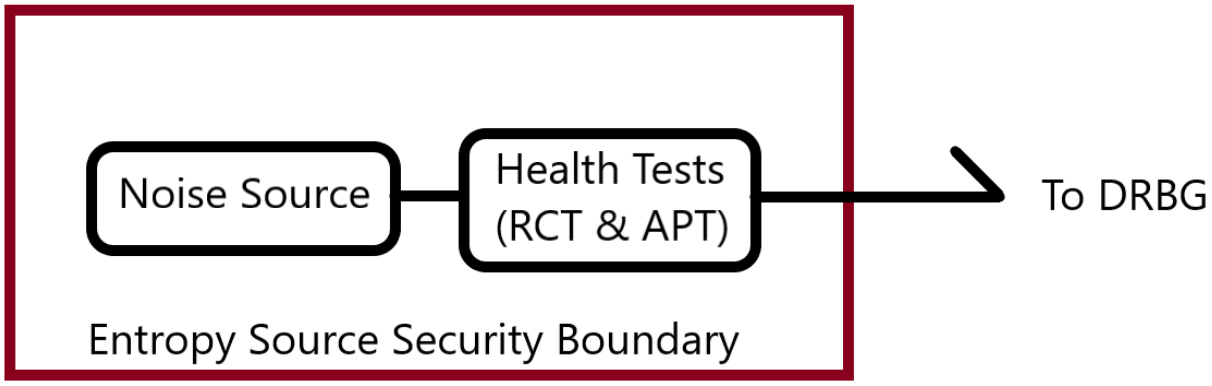


Figure 1: Security Boundary Block Diagram

Operating Conditions

The entropy source operates correctly within the operating conditions shown in **Table 1** below.

Table 1: Entropy-Relevant Parameters

Environmental Parameters	Value	Description
Temperature	0-70°C	The expected entropy rate will be met or exceeded over this temperature range.
Voltage	3.3-5.0V	The expected entropy rate will be met or exceeded over this voltage range.

Configuration Settings

There are no configuration settings that impact the entropy source.

Physical Security Mechanisms

The Kanguru Defender Series is designed to meet FIPS 140-3 Level 3 Physical Security requirements.

The module is housed within a strong, non-removable, tamper-evident, opaque enclosure. In addition, all components are protected with a hard epoxy coating that protects each component from being viewed or probed. Attempts at removing the epoxy will render the module inoperable.

Conceptual Interfaces

A user can access the following conceptual interfaces: GetEntropy, HealthTest.

Min-Entropy Rate

The Min-entropy rate of the Kanguru Entropy Source is 25%.

Health Tests

The entropy source utilizes the Repetition Count Test and Adaptive Proportion Test as described in SP 800-90B. These tests are used for startup testing, on demand testing, and continuously monitor the entropy source during operation. During startup, at least 1024 samples are health tested before any entropy data is released to consuming applications. On demand health tests can be called by power cycling the entropy source. In the event of an error, the entropy source must be power cycled. The anticipated failure modes are that the entropy source gets stuck on a single value, which is detected by the Repetition Count Test, or that the entropy source experiences a drop in entropy, which is detected by the Adaptive Proportion Test. In case of an error state, the device can be power cycled to reinitiate the health tests.

Maintenance

The module does not support any entropy maintenance roles or services.

Required Testing

This entropy source is restricted to the vendor.

Note: End users do not have access to raw data and must rely on the included health tests to detect any drops in entropy.