SP 800-90B Non-Proprietary
Public Use Document

# Accelerometer Based Entropy Source

| | |
|---|---|
| **Hardware Versions:** | GO9 Accelerometer - LSM6DS3USTR<br>GO9B Accelerometer - LSM6DSOTR |
| **Entropy Source Revision:** | 1.0 |
| **Document Version:** | 1.0 |
| **Vendor Info:** | GEOTAB<br>2440 Winston Park Dr, Oakville, ON, Canada |

Date: May 31, 2023

**Template Revision History**

| Version | Date | Change |
|---|---|---|
| V1.0 | | Initial release |
| | | |

# Table of Contents

## Description

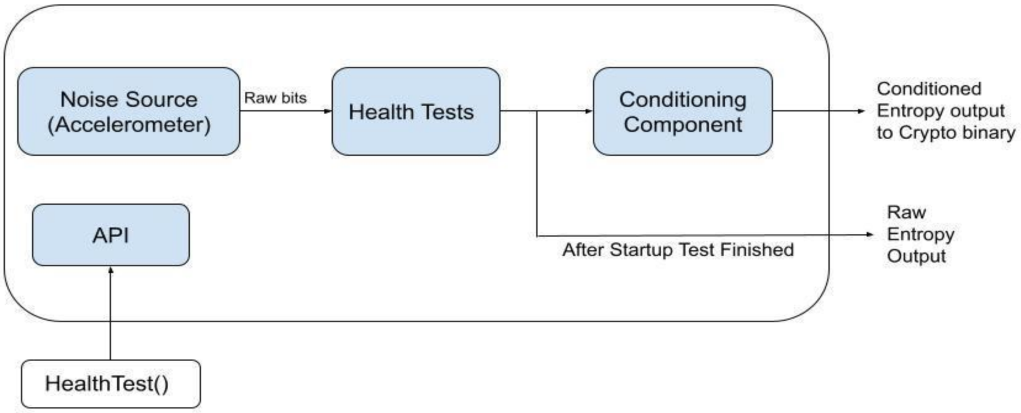
The two platform variations on which the entropy source was tested uses the following accelerometers to acquire entropy:

- GO9 device uses IMU model - LSM6DS3USTR
- GO9B uses IMU model - LSM6DSOTR

Firmware that interfaces with entropy source hardware and identified by its version (1.0).The entropy source category is physical (P) and has been tested with the non-IID tests suite.

## Security Boundary

Figure 1: Security Boundary


Noise Source (Accelerometer)
Raw bits
Health Tests
Conditioning Component
Conditioned Entropy output to Crypto binary
API
After Startup Test Finished
Raw Entropy Output
HealthTest()

The Security boundary composed of:

- A primary noise source which is accelerometer
- Health tests
- A SHA256 vetted conditioning component (CAVP Cert. #A4203)

Referring to figure 1, the boundary shown is the security boundary of the entropy source. All entropy source related activity occurs within this security boundary. The only outputs are the raw entropy output, which is collected only for data validation testing, and the conditioning component output, which goes directly into the cryptographic binary security boundary.

## Configuration Settings

The entropy source is not configurable.

## Conceptual Interfaces

APIs exposed:

- HealthTest()

The entropy source does not expose the GetEntropy() API to read entropy in operational mode, but rather calls the hard-coded cryptographic module API to supply the collected entropy.
The entropy source does not expose the GetNoise() API to obtain a raw digitized output in operational mode, but rather calls a hard-coded API to export samples for collection if sources are compiled for raw entropy evaluation with a special flag (test mode flag).

## Min-Entropy Rate

The entropy source produces 256-bits of entropy per 256-bit output.

## Health Tests

Health tests consist of the approved APT and RCT tests (NIST SP 800-90B) that are executed on raw entropy samples. There are no known entropy source modes or patterns of failure that require additional health tests. These tests are executed in all three modes:

- Start-up. Executes on 1024 samples after device reset or power-cycling.
- Continuous, which is implemented as a continuation of the start-up test.
- On-demand. Implemented but never executed by the application.

Our entropy source is designed to produce a predefined limited amount of entropy in a way that the entropy collection and testing commences when start-up test begins and executes until enough is collected and tested. After collecting sufficient entropy, health test executes up to the sample where the already collected entropy is healthy and cannot be affected by future entropy source deterioration:

- The APT window (1024 samples due to the source binarity), during which entropy was collected, is completed without failure.
- The RCT test did not fail while processing C (Cut-off) samples after the last sample that was collected for entropy.

The collected entropy becomes available for cryptographic module operation only after health tests are successfully completed.

After the collected entropy is supplied to the cryptographic module, the entropy processing and production is ceased, thus no more entropy is produced and no health tests are run until the device is power-cycled.

In case of health test failure, the entropy collection process is designed to self-reset to the start-up health test and the previously collected entropy samples discarded. The entropy source does not produce any signals to indicate failures. Instead, it does not supply the collected entropy to the cryptographic module, which blocks its DRBG functionality until healthy entropy is supplied.

## Maintenance

The entropy source does not require maintenance.

## Required Testing

The noise source samples obtained for raw data collection and restart test. Using SP 800-90B entropy assessment tool (https://github.com/usnistgov/SP800- 90B_EntropyAssessment).

- For the Target GO9B, The entropy source output has been assessed at $H_{original}$ = 0.843393 for Raw data collection Test. For the restart test, the sanity test result is passed and calculated H = 0.831374.
- For the Target GO9, The entropy source output has been assessed at $H_{original}$ = 0.834176 for Raw data collection Test. For the restart test, the sanity test result is passed and calculated H = 0.845056.