SP 800-90B Non-Proprietary Public Use Document

Entropy Source: DataLocker JENT

Document Version 1.0
Firmware Version 1.0

November 2nd, 2023

Revision History

Version	Change
1.0	Initial Release

Table of Contents

Description

The DataLocker JENT 1.0 is a non-physical (NP) entropy source. It is certified under the January 2018 version of Special Publication 800-90B and the August 1, 2023 version of the FIPS Implementation Guidance.

Table 1 describes the tested configuration.

Table 1: Evaluated Version

Identifier	Version
Software Version	DataLocker JENT 1.0
Hardware	Microcontroller: STM32L452ve USB-SATA bridge chip: Fujitsu MB86C31

Security Boundary

The DataLocker JENT 1.0 entropy source is shown below in ***Figure 1***. The noise source is based on processor execution time variance. The security boundary is shown in red in ***Figure 1***.

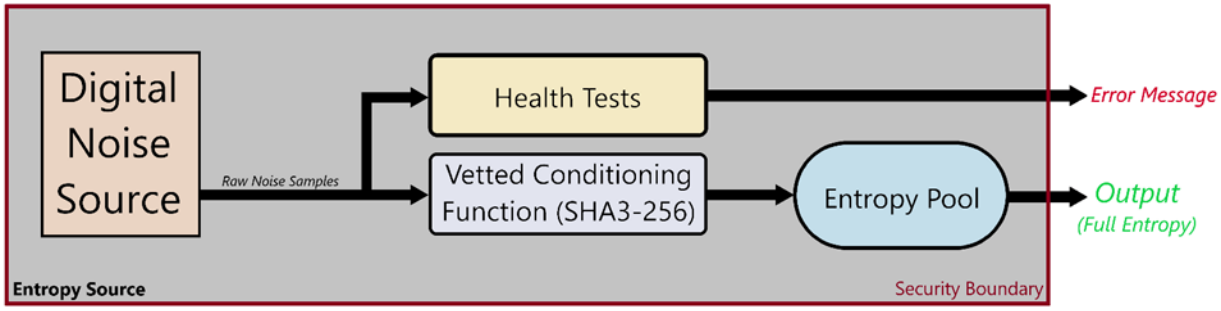

Figure 1: Entropy Source with Security Boundary

Operating Conditions

This section has been omitted, as the entropy source is restricted to the vendor.

Configuration Settings

The configuration settings for the DataLocker JENT entropy source are shown in **Table 2** below.

Table 2: Configuration Settings

Parameter	Value	Description
JENT_CONF_DISABLE_LOOP_SHUFFLE	Disabled	Loop Shuffle disabled
JENT_HEALTH_LAG_PREDICTOR	Enabled	Lag Predictor health test enabled

Physical Security Mechanisms

This section has been omitted, as the entropy source is non-physical.

Conceptual Interfaces

The DataLocker JENT entropy source provides a GetEntropy interface called by *jent_read_entropy*, which allows a caller to request an amount of output entropy. A Health Test interface is available through on-demand health tests which can be initiated by allocating a new instance of the entropy source.

Min-Entropy Rate

The DataLocker JENT entropy source provides full entropy output.

Health Tests

The DataLocker JENT entropy source provides the following health tests.

Start-up Health Tests:

- Adaptive Proportion Test (APT) as described in SP 800-90B.
- Enhanced Repetition Count Test (eRCT) which is an enhanced version of the Repetition Count Test specified in SP 800-90B.
- Hardware Test which ensures that none of the noise samples are zero, indicating that the time stamps collected provide enough precision to capture execution time variance.

Continuous Health Tests:

- APT and eRCT
- Stuck Test
  - Detects patterns in time stamps measured by calculating the first, second and third discrete derivative of the time stamps captured during entropy collection. The test passes if exactly all three values are non-zero.
- Lag Predictor Test
  - The Lag Predictor Test, built upon the prediction mechanism described in SP 800-90B Section 6.3.8, attempts to predict the next time delta value using past time delta values. This test ensures that deterministic behavior detected using past time delta values cannot occur without triggering an error.

On-demand Health Tests:

- Identical to start-up health tests

Health Test Operation

Start-up health tests occur when an instance of the entropy source is initialized and run on 1024 consecutive raw noise samples which are subsequently discarded.

Continuous health tests run continuously while the entropy source operates.

On-demand health tests can be initiated by allocating a new instance of the entropy source.

Anticipated Failure Modes

Anticipated failure modes include the entropy source becoming stuck, the entropy rate degrading below an acceptable value, or the inability to capture time stamps fine enough to capture execution time variance. If the noise source becomes stuck on a single value, it will be detected by the eRCT. If the underlying time stamps get stuck on a single value, increase linearly, or increase at a constantly increasing or decreasing rate, the Stuck Test and eRCT will detect this. If the entropy rate degrades, it will change the ratio of symbols produced by the noise source, and this failure will be detected by the APT. If the noise source enters a known failure mode where output is mostly deterministic and can be predicted based on previous output, the Lag Predictor Test will detect this degradation in entropy. If the time stamps used to compute time delta samples do not contain the precision necessary to detect execution time variance, this will be detected at startup by the Hardware Test.

Error Handling

All health test failures trigger a permanent error state in which the entropy source will not provide entropy output[1]. To recover, a module may reallocate a new instance of the entropy source.

There are no known failure modes which will not be detected by the APT, eRCT, Stuck Test, Lag Predictor Test, and Hardware Test.

Maintenance

The DataLocker JENT entropy source does not require maintenance.

Required Testing

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

[1] The Stuck Test is an exception to this statement. Failure of the stuck test is much less significant than a failure of the eRCT or APT. Instead of triggering a permanent error state, Stuck Test failure simply enforces that intended entropy added to the entropy pool by the failing data does not count towards the total entropy in the pool.