Ciena User CPU Jitter RNG

Entropy Source Version 3.4.1

SP 800-90B Non-Proprietary Public Use Document

Document Version: 1.3

Document Date: 2026-10-05

Prepared for:

Ciena Corporation
7035 Ridge Road
Hanover, MD 21076

Prepared by:

atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759

© 2026 Ciena Corporation / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Table of Contents

1 Description 3
2 Security Boundary 3
3 Operating Conditions 4
4 Configuration Settings 5
5 Physical Security Mechanisms 5
6 Conceptual Interfaces 5
7 Min-Entropy Rate 5
8 Health Tests 5
9 Maintenance 6
10 User Verification 6
11 Vendor Permissions and Relationship 7

© 2026 Ciena Corporation / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1 Description

The Ciena User CPU Jitter RNG version 3.4.1 is a non-physical entropy source implemented in multi-chip embodiment. The noise generation of this entropy source is based on the tiny variations in the execution time of the same piece of code. The execution time of this piece of code is made unpredictable by the complexity of the different hardware components that comprise modern CPUs and the different internal states that the operating system can have at a certain point in time.

The entropy source information is summarized in Table 1 was tested on the operational environments (without additional configurations) listed in Table 2. The noise source was tested under the assumption that its output is non-IID.

Table 1: Entropy source summary.

Characteristic	Description
Vendor	Ciena Corporation
Entropy source name	Ciena User CPU Jitter RNG
Standard, IGs	SP800-90B (2018) IG D.J (2021-11-05) IG D.K (2026-04-16) IG D.O (2021-05-04): N/A
Entropy category	Non-Physical (NP)
Entropy source version	3.4.1
Embodiment and type	Multi-Chip Standalone, hardware

Table 2: Operational environments.

OE #	Operating System	Processor	Cache	Conditioning Component CAVP Cert.
1	Waveserver OS 3.3, Linux kernel 5.15	Marvell OCTEON TX2 ARMv8 CN913x	L1 Cache (Per Core): 48 KB I-cache (Instruction), 32 KB D-cache (Data). L2 Cache (Shared): 1 MB total shared cache, organized as 512 KB per cluster of 2 cores. L3 Cache (System/Coherent): 1 MB	A8283

2 Security Boundary

The boundary for this non-physical, software-based entropy source is the executable binary compiled from the C code that implements it.

Figure 1 depicts the overall design of the entropy source and its core operations.

© 2026 Ciena Corporation / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

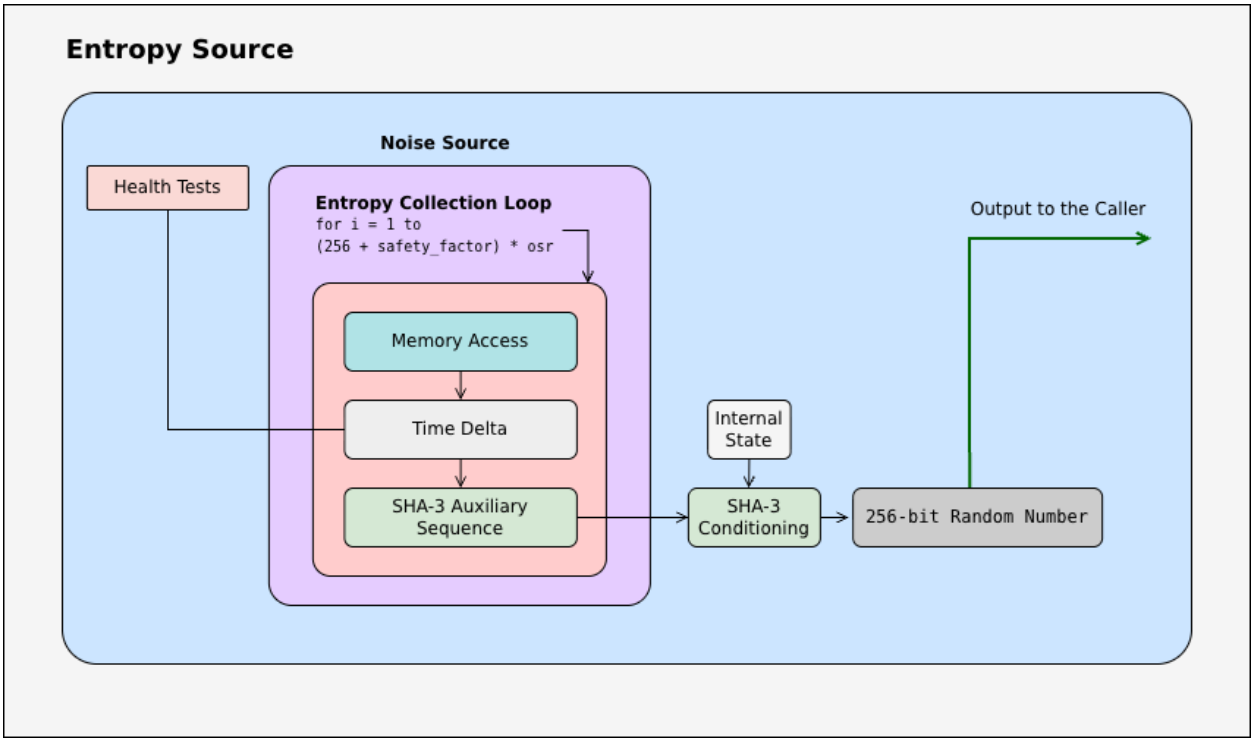


Figure 1: Entropy source block diagram.

The noise source is implemented by collecting and accumulating variances of the execution time of a defined set of instructions. The time jitter of the execution time is measured over time variances of variable memory accesses and variances in the execution time of a defined set of instructions, which includes an implementation of SHA3-256.

If the Repetition Count Test (RCT) or the Adaptive Proportion Test (APT) health tests fail, the noise data is discarded, the entropy source halts without outputting any data, and a failure code is returned to the caller.

3 Operating Conditions

The noise source is non-physical, and thus the operating conditions are inherited from the operational environment in which the entropy source is installed, as shown in Table 3.

Table 3: Operating conditions for the operational environments.

OE#	Temperature Range	Voltage Range / Power	Humidity
1	Normal operating temperature: 5°C to 40°C; 41°F to 104°F Short-term operating temperature: -5°C to 5°C and 40°C to 45°C (23°F to 41°F and 104°F to 113°F)	AC PSU input power range: - 2 kW: input 90 VAC to 180 VAC - 3 kW: input 180 VAC to 305 VAC - 3 kW: input 180 VDC to 300 VDC	93% maximum

© 2026 Ciena Corporation / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

OE#	Temperature Range	Voltage Range / Power	Humidity
		DC PSU: - 2.3 kW: input -40 VDC to -72 VDC	

4 Configuration Settings

The DENABLE_FIPS_ENTROPY_CPU_JITTER=1 flag must be used to enable the entropy source and receive entropy data.

5 Physical Security Mechanisms

Being a non-physical entropy source, there are no specific physical security mechanisms except those provided by the module's and/or operational environment embodiment.

6 Conceptual Interfaces

The entropy source provides the following interfaces:

- jent_read_entropy(): Obtains conditioned entropy for the caller. This interface corresponds to the GetEntropy() conceptual interface from SP800-90B.
- jent_measure_jitter(): Obtains raw noise data for testing purposes. This interface corresponds to the GetNoise() conceptual interface from SP800-90B. This interface is not accessible by an operator of the entropy source in production.

7 Min-Entropy Rate

The entropy source provides 256 bits of entropy per 256-bit conditioned output block (i.e., full entropy).

8 Health Tests

The entropy source implements the following continuous health tests:

- Repetition Count Test conforming to SP 800-90B section 4.4.1.
  - $H = \frac{1}{3}$ bits of entropy per 64-bit sample.
  - Permanent failure alpha value of $\alpha = 2^{-30}$
  - Permanent cutoff value $C = 91$
- Adaptive Proportion test conforming to SP 800-90B section 4.4.2.
  - $W = 512$
  - $H = \frac{1}{3}$ bits of entropy per 64-bit sample
  - Permanent failure alpha value of $\alpha = 2^{-30}$
  - Permanent cutoff value $C = 459$
- Stuck (Non-Permanent) Test: The Stuck Test computes the first, second and third discrete derivatives of the time value that will be processed by SHA3-256. If any of these

© 2026 Ciena Corporation / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

derivatives are zero, then the received time delta is considered stuck. In this case the input state to SHA3-256 is not updated, and the entropy value is not counted. The stuck test then triggers the RCT for further processing. The second derivative is in fact the RCT itself.

- Lag Predictor Test: The goal of this test is to detect a failure mode in which the outputs may become mostly deterministic. In essence, this test constructs a scoreboard and tracks the number of times that a subpredictor was correct. The subpredictor that scored the most correct predictions is used to predict the next value of a series. The lag predictor test is configured in this entropy source with the following parameters:
  - $\alpha = 2^{-22}$
  - Window size: 131072
  - Lag history size: 8
  - Global cutoff = 104761
  - Local cutoff = 111

The continuous-health tests are applied to each new sample obtained from the noise source. Whenever a failure is detected during the health testing specifically for the RCT and APT, entropy data is not returned to the caller; instead, a failure code is returned to enable the caller to acknowledge the failure. In the case of permanent failures, the entropy source then halts and will refuse new requests for entropy. Upon return of the permanent failure code, the caller shall attempt to reset or reboot the entropy source or return an error to its own operator. The stuck test is considered non-permanent, as positive stuck tests will be registered but will not immediately halt the entropy source.

Startup tests conduct the same set and parameters of the continuous health tests on 1024 samples of noise data. The data is discarded after the startup tests have completed successfully.

On-demand health tests of the noise source may be performed by rebooting the operational environment, which results in the immediate execution of the start-up tests. Typically, this entropy source designed for user space cannot be reloaded without restarting the executable. Similarly, the data used for the on-demand health tests are discarded after successful completion.

9 Maintenance

There are no maintenance requirements.

10 User Verification

The entropy source ships with the system by default and no operator action is required to enable it. The entropy source cannot be disabled.

To verify the version of the entropy source, the operator may issue the following command using the command-line interface of the module that implements the entropy source:

```
# software show
```

The version information of the operational environment and operating system of that module that implements the entropy source is then displayed on the console port. That information can then be mapped to the entropy source version through documentation provided by the vendor and through the Security Policy document of the module.

© 2026 Ciena Corporation / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

The system automatically monitors the health of the entropy source. Any failure results in a system reboot to allow the entropy source to recover. A hard error condition results in the system being inoperable and must be returned to the supplier.

11 Vendor Permissions and Relationship

This entropy source validation is “Reuse restricted to vendor”.

© 2026 Ciena Corporation / atsec information security corporation.
This document can be reproduced and distributed only whole and intact, including this copyright notice.