SP 800-90B Non-Proprietary Public Use Document
Octeon III Entropy Source (CN7xxx)
Document Version 0.2
Entropy Source Version 1.0

Palo Alto Networks, Inc.
3000 Tannery Way
Santa Clara, CA 95054
February 22, 2024

Revision History

Version	Change
0.1	Initial draft

Table of Contents

1. Description

The Octeon III Entropy Source (CN7xxx) is a physical entropy source, which includes the following devices:

- CN71XX Family: Cavium Octeon III CN7130 (cnMIPS64); FW version: 3.1.2-p5 and Conditioning FW version: 1.0
  - This family includes CN70XX and CN71XX processors
- CN73XX Family: Cavium Octeon III CN7350 (cnMIPS64); FW version: 3.1.2-p5 and Conditioning FW version: 1.0
  - This family includes CN72XX and CN73XX processors
- CN78XX Family: Cavium Octeon III CN7885 (cnMIPS64); FW version: 3.1.2-p5 and Conditioning FW version: 1.0
  - This family includes CN76XX and CN78XX processors

2. Security Boundary

The entropy source is demonstrated in the figure below. The noise source is based on a set of ring oscillators, whose output goes through applicable health tests before going through conditioning.

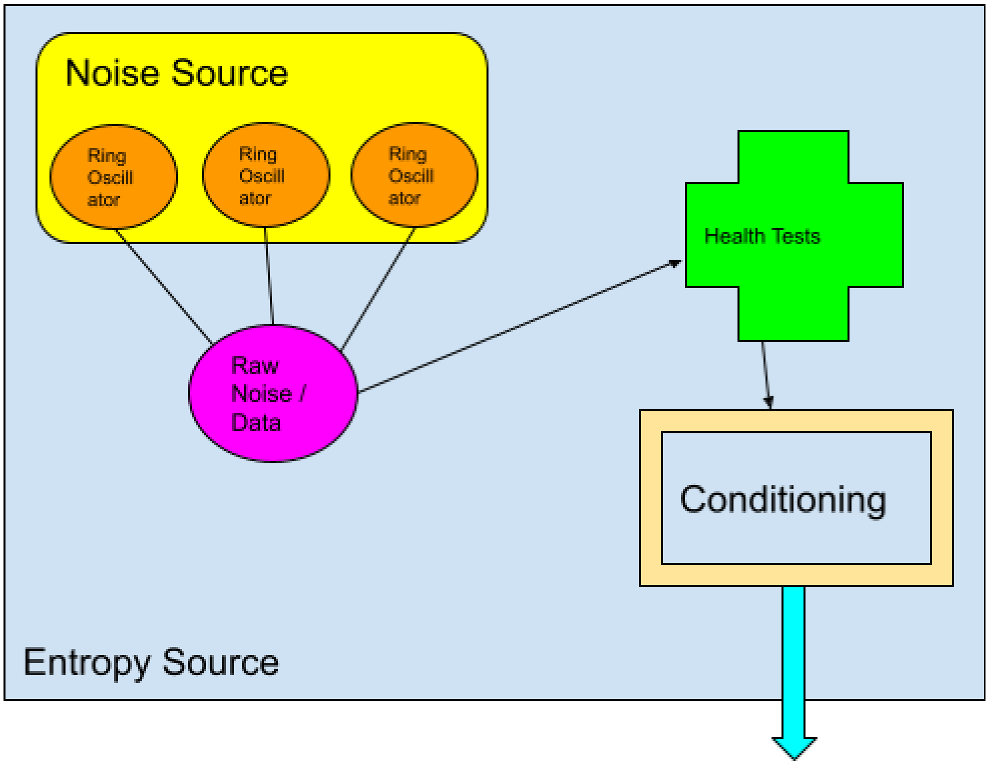

Figure 1 - Entropy Source Boundary

3. Operating Conditions

The entropy operating conditions include the following:

Parameter	Device Family	Value
Temperature	CN71xx	0 to 100 C
	CN73xx	0 to 95 C
	CN78xx	0 to 90 C
Voltage	CN71xx	0.82 to 0.88 V
	CN73xx	0.82 to 0.88 V
	CN78xx	0.87 to 0.93 V

4. Configuration Settings

The entropy source is required to have the following configurations set in order to operate in the SP 800-90B mode. The mode is selected by RNG_CTL_STATUS [EXP_ENT]. When set, the device provides unconditioned raw entropy.

- RNG_CTL_STATUS [EXP_ENT] = 1

5. Physical Security Mechanisms

The CN7XXX entropy source operates within the physical protection mechanisms provided by the device that hosts it. These include production grade components, opacity shield(s), and tamper evident labels that all meet FIPS 140-3 Level 2 requirements.

6. Conceptual Interfaces

The interfaces available for various functions such as GetEntropy are not available to the user, but are done internally by the Palo Alto Networks modules.

7. Min-Entropy Rate

Table 2 summarizes the minimum entropy rate for the device family groups.

Device Family	**Min Entropy (per bit)**
CN71xx	0.50668693116
CN73xx	
CN78xx	

Table 2 - Minimum Entropy Rate

8. Health Tests

The CN7XXX entropy source implements the following health tests:

- Adaptive Proportion Test (APT) - performed on start-up and as continuous tests
- Repetition Count Test (RCT) - performed on start-up and as continuous tests
- On-demand test - performed by restarting the entropy source and re-running the startup tests

If any of the tests above fail, the entropy source returns an error and the unit is disabled such that it does not provide any output to any applications.

9. Maintenance

There are no maintenance actions needed for the entropy source.

10. Required Testing

Raw noise data is not available to the user to test. The user must rely on the health tests to obtain assurance that the device is operating correctly. No further testing is required.