SP 800-90B Non-Proprietary Public Use Document
Palo Alto Networks DRNG RDSEED Entropy Source
Document Version 0.1
Entropy Source Version 1.0

Palo Alto Networks, Inc.
3000 Tannery Way
Santa Clara, CA 95054
March 8, 2024

Revision History

Version	Change
0.1	Initial draft

Table of Contents

1. Description

The Palo Alto Networks DRNG RDSEED Entropy Source is a physical entropy source, which includes the following applicable devices:

Package	Processors
FCBGA1310	Intel Atom C3436L
	Intel Atom C3558R
	Intel Atom C3758R
FCBGA1667 (8-Core Die)	Intel Pentium D1517
	Intel Xeon D-1548
FCBGA1667 (16-Core Die)	Intel Xeon D-1567
FCBGA2518	Intel Xeon D-2187NT
FCLGA2011 (10-Core Die)	Intel Xeon E5-2620 V4
FCLGA2011 (15-Core Die)	Intel Xeon E5-2680 V4
FCLGA3647	Intel Gold 6248

2. Security Boundary

The entropy source is demonstrated in the figure below. The noise source output first goes through applicable health tests before passing through Palo Alto Networks' conditioning component, which is then used by the system on which it resides.

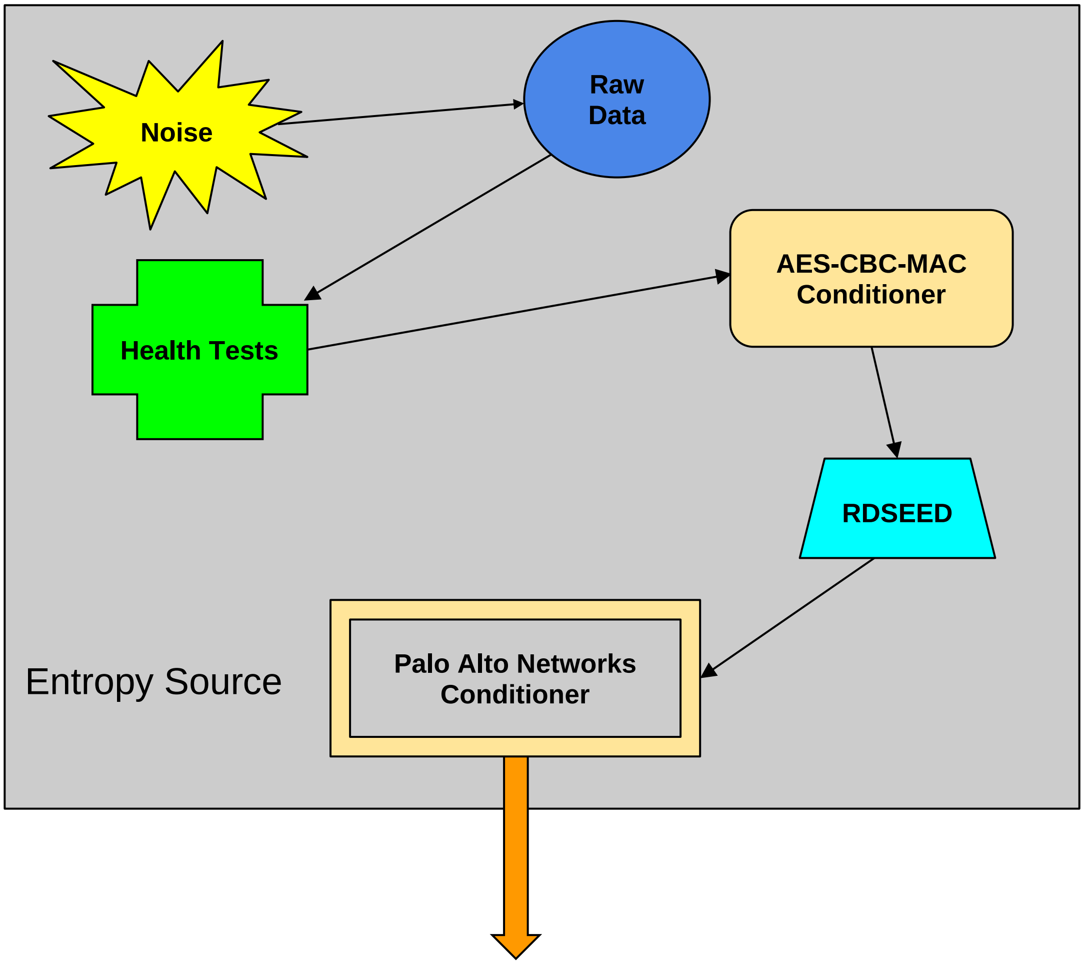

Figure 1 - Entropy Source Boundary

3. Operating Conditions

The entropy operating conditions include the following:

Parameter	Package	Minimum	Maximum
Temperature	FCBGA1310	0 °C	83 °C
Temperature	FCBGA1667 (8-Core Die)	0°C	80°C
Temperature	FCBGA1667 (16-Core Die)	0°C	91°C
Temperature	FCBGA2518	0°C	80°C
Temperature	FCLGA2011 (10-Core Die)	0°C	74°C
Temperature	FCLGA2011 (15-Core Die)	0°C	89°C
Temperature	FCLGA3647	0°C	89°C

4. Configuration Settings

There are no configuration settings needed for this source.

5. Physical Security Mechanisms

The packaging of the chip is within a tamper evident enclosure, and further protected by the host platform that it is included in.

6. Conceptual Interfaces

The interfaces available for various functions such as GetEntropy are not available to the user, but are handled by the module using the entropy source.

7. Min-Entropy Rate

The entropy source provides a minimum entropy of 0.50694 bits per bit of data.

8. Health Tests

The entropy source includes the following:

- Continuous Health Tests (CHT)
- Startup Noise Source Health Tests
- Startup Logic Integrity BIST (Built in Self-Test)

In the failure state, no more random numbers are issued, and the failure state is reflected in the BIST status register result bits.

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.