SP 800-90B Non-Proprietary Public Use Document

Entropy Source [ES] Name

Document Version

Hardware/Firmware/Software Versions

Vendor Info (Name, Address, etc.)

Date

**Revision History**

|  |  |
| --- | --- |
| Version | Change |
|  |  |
|  |  |

Table of Contents

[Description 4](#_gjdgxs)

[Security Boundary 4](#_30j0zll)

[Operating Conditions 4](#_1fob9te)

[Configuration Settings 4](#_3znysh7)

[Physical Security Mechanisms 4](#_2et92p0)

[Conceptual Interfaces 4](#_tyjcwt)

[Min-Entropy Rate 4](#_3dy6vkm)

[Health Tests 4](#_1t3h5sf)

[Maintenance 4](#_4d34og8)

[Required Testing 4](#_2s8eyo1)

[Note: Some sections in this document may be pared down or excluded when the entropy source is validated as bound to a specific module or set of modules. In those cases, sections that outline proper behavior of the entropy source should be included i.e., Operating Conditions, Configuration Settings, Physical Security Mechanisms, Maintenance. Other sections may be optionally included.]

# Description

Description of source including source name, standard version, entropy category [physical (P) or non-physical (NP)], version/identification of the source and all components (hardware, software, or firmware), platform(s) on which it was tested on, IID or Non-IID, etc. Most of this information will appear on the certificate listing as well.

# Security Boundary

Security boundary shall be well-defined with a supporting block diagram. Outline all noise sources. A diagram like Figure 1 of 90B with more information is ideal.

# Operating Conditions

Operating Conditions (e.g., temperature range, voltages, system activity, etc.) under which the entropy source is claimed to operate correctly.

# Configuration Settings

Configuration settings including setting register parameters (e.g., sample interval, startup delay, conditioning function to use, [n\_in, n\_out] compression ratio for conditioning, noise source to use [if several options are present, must identify the 90B validated source], health-tests enable, limits for health-tests where configurable, clock multiplier, etc.), compiler options, other initialization requirements, security rules, or rules of operation.

# Physical Security Mechanisms

Physical security mechanisms in place (if any), e.g., opacity, tamper seals, tamper response, and alarms. Also, any additional physical security requirements to meet specific security levels of FIPS 140.

# Conceptual Interfaces

Conceptual interfaces (i.e., GetEntropy, GetNoise and HealthTest of 90B Section 2.3.1). Not all are required to be available.

# Min-Entropy Rate

Min-entropy rate at output of source (either H as defined in section 3.1.4.2 of 90B if there is no conditioning function, or H\_out for the output of the conditioning function per section 3.1.5 of 90B). Should also include H\_submitter and the bits per request sample.

# Health Tests

Health tests including start-up, continuous, on-demand, and known failure modes. List conditions under which the tests are performed. Describe all error states and status indicators, anything a module may need to respond to and act.

# Maintenance

Specify any maintenance requirements. For example, the entropy source must be powered off and on after every 1024 samples.

# Required Testing

The target platform shall test for [a checklist for the module to ensure the entropy source is running properly, example provided below]:

1. Raw noise data through the raw noise source interface and processed by the SP800-90B tool to obtain an entropy rate which must be near equal to or the defined min-entropy rate.
2. Obtain the restart noise data through the raw noise source interface and processed by the SP800-90B tool.
   1. the sanity test to apply to the noise restart data must pass, and
   2. the minimum of the row-wise and column-wise entropy rate shall not be less than half of the entropy rate from 1 above.