SP 800-90B Non-Proprietary Public Use Document

Entropy Source [ES] Name

Document Version

Hardware/Firmware/Software Versions

Vendor Info (Name, Address, etc.)

Date

**Template Revision History**

|  |  |  |
| --- | --- | --- |
| Version | Date | Change |
| V1.0 |  | Initial release |
| V1.1 | March 9, 2023 | Updated Required Testing section to match CMVP expectations. Removed some the IID or non-IID classification on the Description section. Stated that the Operating Conditions and Physical Security Mechanisms are not always required based on the entropy source. Added Vendor Permissions and Relationship section. |

Table of Contents

[Description 4](#_Toc129261133)

[Security Boundary 4](#_Toc129261134)

[Operating Conditions 4](#_Toc129261135)

[Configuration Settings 4](#_Toc129261136)

[Physical Security Mechanisms 4](#_Toc129261137)

[Conceptual Interfaces 4](#_Toc129261138)

[Min-Entropy Rate 4](#_Toc129261139)

[Health Tests 4](#_Toc129261140)

[Maintenance 5](#_Toc129261141)

[Required Testing 5](#_Toc129261142)

[Vendor Permissions and Relationship 5](#_Toc129261143)

[Note: Some sections in this document may be pared down or excluded when the entropy source is validated as reuse restricted to vendor.]

# 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.

# 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. This section may be omitted when the entropy source is restricted to the vendor as this information would match the module security policy.

# 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. This section may be omitted for non-physical entropy sources, or when the entropy source is restricted to the vendor, at which point the physical security mechanisms will be provided by the module security policy.

# Conceptual Interfaces

Conceptual interfaces (i.e., GetEntropy, GetNoise and HealthTest of 90B Section 2.3.1) that are available to the user. 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).

# 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

Guidance for a user or module developer to confirm that the entropy source is configured properly. If the raw noise data is available to be collected for statistical tests, include instructions on how to obtain the data. If the raw noise data is not available, state that the user must rely on the health tests to detect any drops in entropy.

For example:

A checklist for the module to ensure the entropy source is running properly:

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.

# Vendor Permissions and Relationship

If the ESV indicates “Reuse restricted to vendor”, someone other than the vendor can only use the certificate with written and signed permission from the vendor’s point of contact (as indicated on the ESV certificate). This optional section of the PUD can be used to include this signed permission with any associated details.

This section can also be used when two or more vendors are part of the same company (e.g., different divisions with slightly different names, or a company is a subsidiary of another company that has a validation) to clarify this relationship and include the supporting evidence.

For more information, see the [FIPS 140-3 Management Manual](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual) *Entropy Source Validation (ESV) Processes*.