

SP 800-90B Non-Proprietary Public Use Document
Micron® MSA11-P5 Entropy Source

Document Version 1.0

Hardware Versions

Micron® MSA11-P5 SSD Controller

Micron Technology, Inc.
8000 S Federal Way, Boise Idaho 83716, USA

Date: August 30, 2024

Revision History

Version	Date	Author	Change
V1.0	August 30, 2024	Joan Tseng	Initial release

Contents

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

Tables

Table 1. Security Parameters 4

Figures

Figure 1. Entropy Source Blocks 3
Figure 2. TRNG Security Boundary 3

1. Description

The TRNG core is compliant with SP 800-90B. The TRNG core is a physical entropy source. The noise source in the TRNG is a ring oscillator-based noise source that creates random bits. The vetted conditioning function Block_Cipher_df from SP 800-90B Section 3.1.5.1.1 is used. The health test block continuously tests the output of the entropy source, refer to Figure 1 below. SP 800-90B compliance testing was performed on the Micron® MSA11-P5 SSD drive.

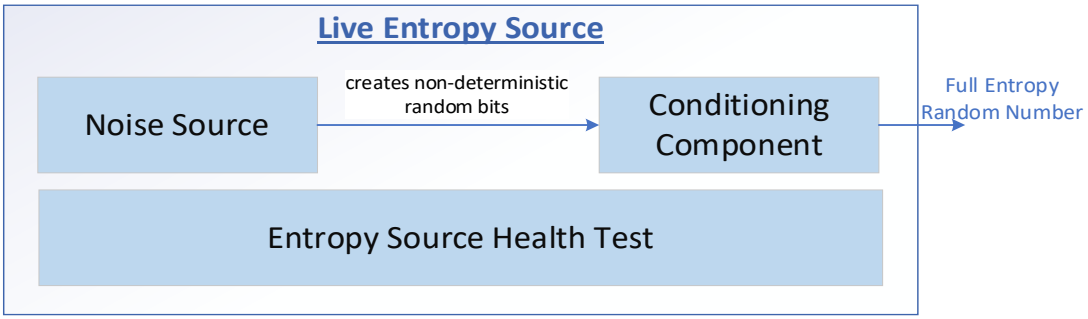


Figure 1. Entropy Source Blocks

2. Security Boundary

The Security Boundary is defined below in Figure 2. The TRNG core is constructed of the following components: live entropy source, DRBG, health test blocks, registers, and the control unit, all are protected under one security boundary. Communication between the core and the host is done through the bus interface and no secure information is exposed outside the security boundary.

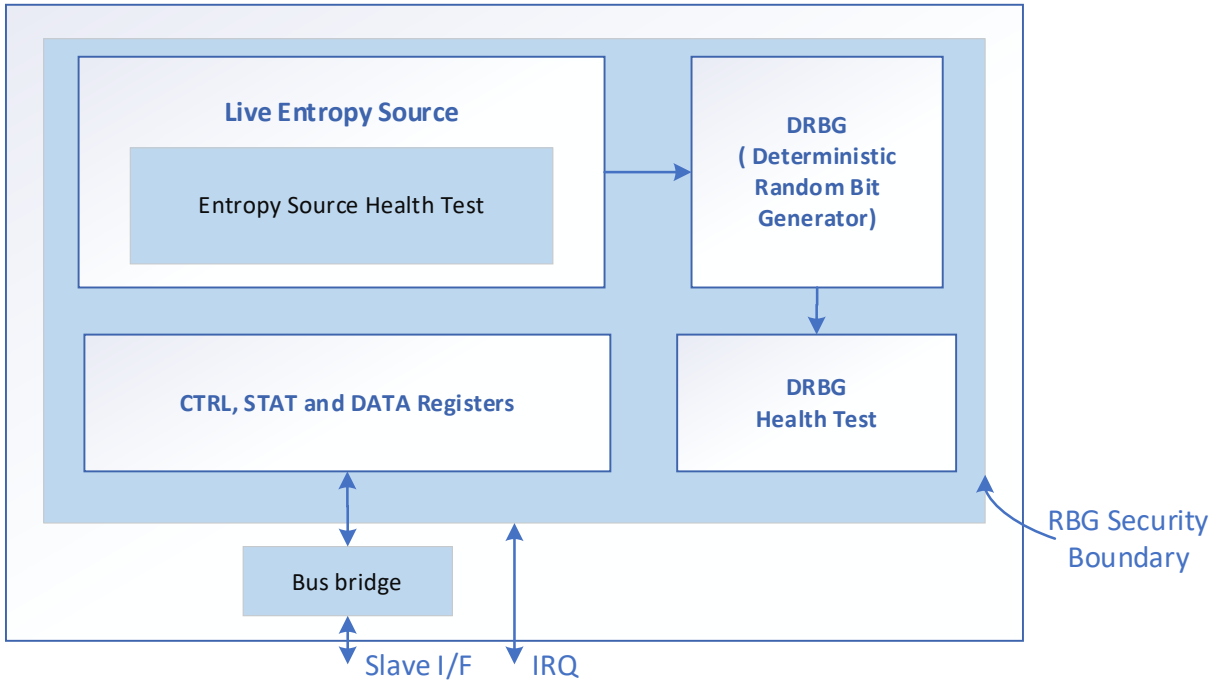


Figure 2. TRNG Security Boundary

3. Operating Conditions

The entropy source is claimed to operate correctly under the inherent operating conditions of the System-on-Chip (SoC):

Table 1. Security Parameters

Parameter	Value
Temperature	0~125℃
Voltage	0.675V~0.825V
Clock Rate	500M Hz

4. Configuration Settings

The TRNG does not require any additional configuration of entropy-relevant parameters.

5. Physical Security Mechanisms

The TRNG core is embedded in the System on Chip (SoC)s. The SoCs are single-chip embodiments of production-grade components. The SoCs are covered with either an opaque lid or compartment or black-coated material or metal coating. They are soldered on the logic board from the ball grid array (BGA).

6. Conceptual Interfaces

The GEN_NOISE command lets the entropy source in the TRNG core provide seeds for the DRBG. The output is saved in NPA_DATA# registers. When the raw noise output is ready, the TRNG core will issue the NOISE_RDY interrupt. Reading the raw noise source output is only available in test mode.

7. Min-Entropy Rate

The min-entropy (H) claimed from the noise source is 0.5 bit/bit, but the entropy source is claimed to be 1 bit/bit.

8. Health Tests

The TRNG core ‘s entropy source health tests include:

1. Start-up Tests
   Upon start up, the TRNG performs the Continuous Tests on a block of 1024 bits. A conditioner Known Answer Test (KAT) is also performed. The KAT provides a known input to the conditioner and the result is checked.

2. Continuous Tests
   - Repetition Count Test.
   - Adaptive Proportion Test

3. On-demand Test
   - On-demand Tests are performed by rebooting the core, thus executing the Start-up Tests.
   - The Conditioner KAT is also available upon request through the CTRL register.

When any health test fails, the core stops generating random bits, issues an alarm on a non-maskable IRQ pin, zeroizes all internal secret information, the system enters a nonoperational state, and no services beside getting status are allowed. The cause of failure can be read from the ALARMS register. The system remains in a nonoperational state until the reset.

9. Maintenance

No specific maintenance is required.

10. Required Testing

Built-in Health Tests described in the Health Tests section constantly check the validity of the noise source. No additional testing is required.

11. Vendor Permissions and Relationship

Reuse restricted to the vendor.