SP 800-90B Non-Proprietary Public Use Document

Trusted Platform Module 2.0 SLB 9672 Entropy Source

Document Version 0.4

Hardware Versions:

SLB 9672VU20 (Package PG-UQFN-32-1 or PG-UQFN-32-2),

SLB 9672XU20 (Package PG-UQFN-32-1 or PG-UQFN-32-2)

Firmware Versions:

15.20.15686,

15.21.16430,

15.22.16832

Infineon Technologies AG

Am Campeon 1-15

Neubiberg, BY 85579, Germany

December 23, 2022

**Revision History**

|  |  |
| --- | --- |
| Version | Change |
| 0.1 | Initial draft |
| 0.2 | Included review comments |
| 0.3 | Added health test conditions |
| 0.4 | Added information on testing |
|  |  |

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)

# Description

The Trusted Platform Module 2.0 SLB 9672 Entropy Source is a physical entropy source. The entropy source is a Non-IID source and was tested for the platform and firmware versions listed on the title page.

# Security Boundary

The Trusted Platform Module 2.0 SLB 9672 Entropy Source is entirely contained within a single-chip module.



Figure . The Trusted Platform Module 2.0 SLB 9672 Entropy Source

# Operating Conditions

The following table lists the relevant operating conditions for which the Trusted Platform Module 2.0 SLB 9672 Entropy Source was characterized.

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Value** | **Description** |
| Temperature | -40°C to 110°C | Operating ambient temperature range |
| VDD | 1.62 V to 3.60 V | Operating supply voltage |

# Configuration Settings

To select the SP 800-90B validated source the Trusted Platform Module 2.0 SLB 9672 Entropy Source must be set to **TRNG Mode**.

To start the entropy source, the mode must be set from **Configuration Mode** into **Operational Mode**. There are no further configuration settings available to the operator.

# Physical Security Mechanisms

The Trusted Platform Module 2.0 SLB 9672 Entropy Source is part of a single-chip module that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The module employs standard passivation techniques. The module is intended for deployment on standard PCBs or similar assemblies.

The module comes with a hard and opaque coating. Any attempt of physical tampering by mechanical means will leave evidence in form of scratches, broken edges of the coating or similar.

# Conceptual Interfaces

*GetEntropy* interface is a read operation on the ***Data*** register of the Trusted Platform Module 2.0 SLB 9672 Entropy Source. Once the ready flag is set in the ***Status*** register, 32 bit of entropy data can be read from the ***Data*** register.

There is no dedicated *HealthTest* interface. Data is only released once the health testing is passed. In case health testing fails, a flag is set in the ***Status*** register. To restart the entropy source the ***Mode*** must be set to **Operational Mode**.

*GetNoise* is an internal interface only available in a dedicated privileged mode.

# Min-Entropy Rate

H\_submitter = 0.73 bits per symbol for a symbol size of one bit after digitization.

We claim an output (H\_out) of at least 7.51729 bits per byte, or 30.069 bits of min entropy per 32-bit block.

# Health Tests

The Transition Count health test, a developer-defined health test, is applied both on startup and as a continuous test and assesses the health of the noise source using blocks of 128 RAW bits. The false positive rate for the Transition Count health test is quite small.

False Positive Rate ≈ 2-176.

As a developer-defined health test it complies with the requirements of SP 800-90B Section 4.5.

**Continuous health testing** is performed for each generated output symbol during normal operation. An output symbol is only released to the ***Data*** register if continuous health testing was passed.

**Start-up health testing** is performed by applying the Transition Count health test to 1024 RAW bits. This is initiated by reading 8 bytes of conditioned data from the Trusted Platform Module 2.0 SLB 9672 Entropy Source ***Data*** register. If no alarm was indicated in the ***Status*** register after 8 bytes were read, the start-up health testing result is “pass” for the 1024 RAW bits.

**On demand health testing** is possible by reading entropy data from the Trusted Platform Module 2.0 SLB 9672 Entropy Source ***Data*** register and monitoring the health test error bit in the ***Status*** register.

# Maintenance

There is no special maintenance necessary to operate the Trusted Platform Module 2.0 SLB 9672 Entropy Source.

# Required Testing

There is no additional testing required by the target platform. Since *GetNoise* is an internal interface only available in a dedicated privileged mode, the user must rely on the health test to ensure the entropy source is configured correctly and is working as expected.