SP 800-90B Non-Proprietary Public Use Document
Infineon Trusted Platform Module 2.0 Entropy Source
Document Version 1.1

Hardware Versions:

SLB 9672
SLB 9673

Infineon Technologies AG
Am Campeon 1-15
Neubiberg, BY 85579, Germany
March 21, 2024

Revision History

Version	Change
1.0	Initial version
1.1	Version information

Table of Contents

Description 4

Security Boundary 4

Operating Conditions 4

Configuration Settings 4

Physical Security Mechanisms 4

Conceptual Interfaces 5

Min-Entropy Rate 5

Health Tests 5

Maintenance 5

Required Testing 6

Description

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

Security Boundary

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

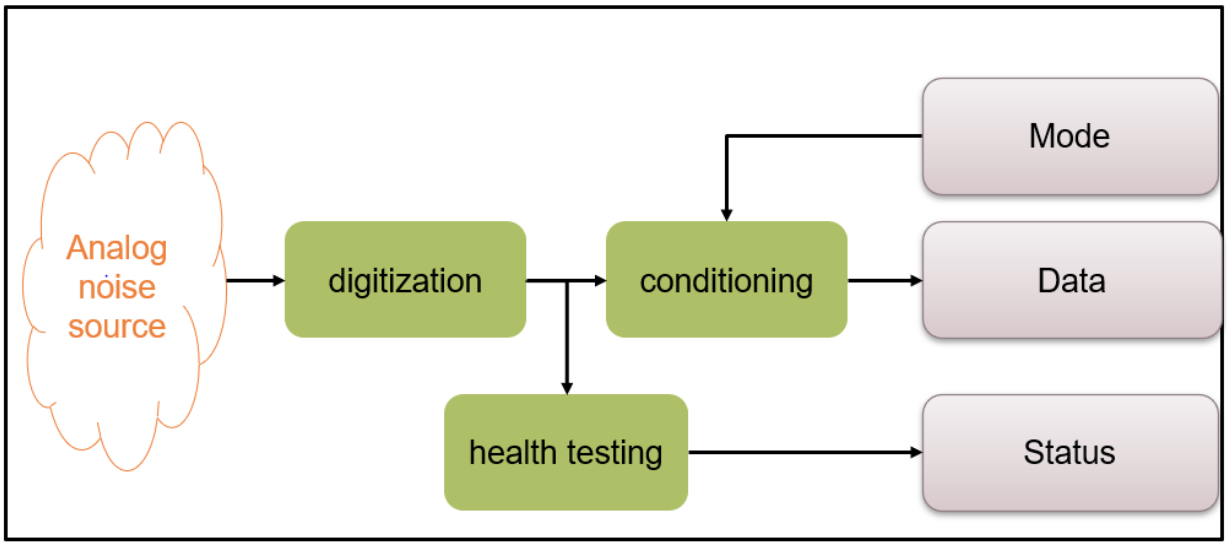


Figure 1. The Trusted Platform Module 2.0 Entropy Source

Operating Conditions

The following table lists the relevant operating conditions for which the Infineon Trusted Platform Module 2.0 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 Infineon Trusted Platform Module 2.0 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 Infineon Trusted Platform Module 2.0 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.

Conceptual Interfaces

GetEntropy interface is a read operation on the ***Data*** register of the Infineon Trusted Platform Module 2.0 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 $\approx 2^{-176}$.

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 Infineon Trusted Platform Module 2.0 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 Infineon Trusted Platform Module 2.0 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 Infineon Trusted Platform Module 2.0 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.