SP 800-90B Non-Proprietary Public Use Document
Infineon 32-bit Security Controller Entropy Source
Document Version 1.0

Hardware Versions:

SLC 36 32-bit Security Controller V16
SLC 38 32-bit Security Controller V22
SLC 39 32-bit Security Controller V23

Infineon Technologies AG
Am Campeon 1-15
Neubiberg, BY 85579, Germany
July 18, 2024

Revision History

Version	Change
1.0	Initial version

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 5

Description

The Infineon 32-bit Security Controller 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 32-bit Security Controller Entropy Source is entirely contained within a single-chip module.

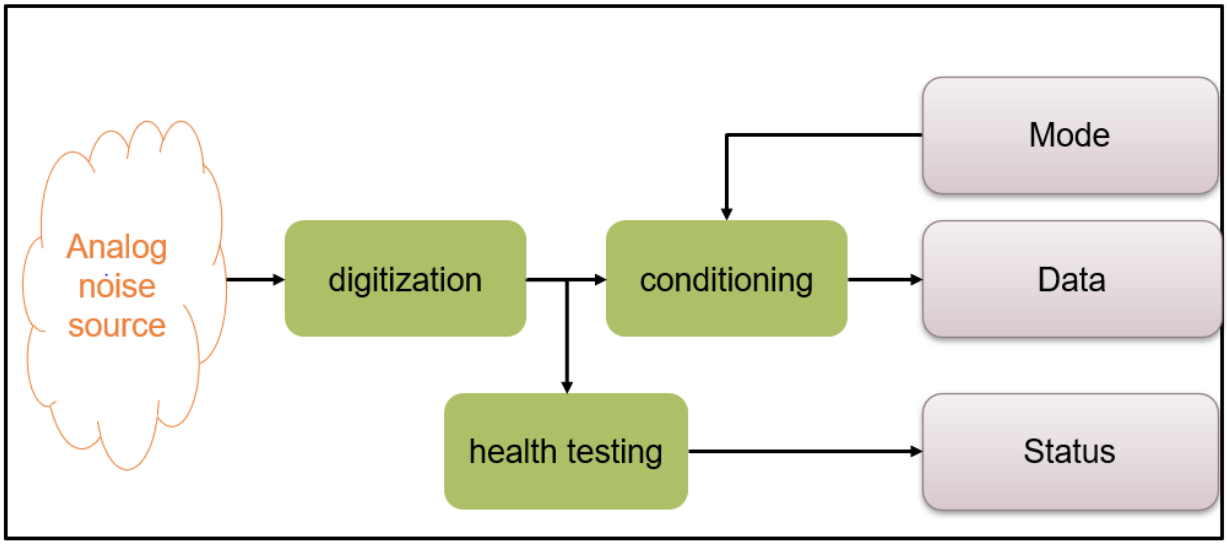


Figure 1. The Infineon 32-bit Security Controller Entropy Source

Operating Conditions

The following table lists the relevant operating conditions for which the Infineon 32-bit Security Controller Entropy Source was characterized.

Parameter	Value	Description
Temperature	-40°C to 115°C	Operating ambient temperature range
VCC	1.62 V to 5.50 V	Operating supply voltage

Configuration Settings

To select the SP 800-90B validated source, the Infineon 32-bit Security Controller 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 32-bit Security Controller Entropy Source is part of a single-chip module that meets commercial-grade specifications for power, temperature and reliability. The module employs standard passivation techniques.

Conceptual Interfaces

GetEntropy interface is a read operation on the ***Data*** register of the Infineon 32-bit Security Controller 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

We claim an output (H_out) of at least 0.709 bits per bit, or 22.688 bits of min entropy per 32-bit block.

Health Tests

The RAW data after digitization is tested by the Adaptive Proportion Test (APT) and the Repetition Count Test (RCT). For the RCT, the selected cutoff is C=64 and for the APT, the selected cutoff is C=451.

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 implemented health tests to 1024 RAW samples. This is initiated by reading 8 times 32-bit of conditioned data from the Infineon 32-bit Security Controller Entropy Source ***Data*** register. If no alarm was indicated in the ***Status*** register after 8 32-bit words were read, the start-up health testing result is “pass” for the 1024 RAW symbols.

On demand health testing is possible by reading 8 times 32-bits of entropy data from the Infineon 32-bit Security Controller Entropy Source ***Data*** register and monitoring the health test alarm bit in the ***Status*** register.

Maintenance

There is no special maintenance necessary to operate the Infineon 32-bit Security Controller 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.