SP 800-90B Non-Proprietary Public Use Document
EFR32MG21B010PZ045IM32 Entropy Source

Document Version 0.6

Hardware Version:
B with SE Firmware Version 1.2.13

Infinera,
6373 San Ignacio Avenue,
San Jose, CA, 95119, USA

July 3, 2024

Revision History

Version	Date	Change
0.1	01-Nov-2023	Initial release
0.4	06-Dec-2023	Updates from Silabs • Updated Repetition Count Test parameters • Updated Adaptive Proportion Test parameters • Added additional Adaptive Proportion Test (64-sample window
0.6	03-July-2024	Updates in response to the CMVP ESV comments

Table of Contents

Description 4

Security Boundary 4

Operating Conditions 4

Configuration Settings 4

Physical Security Mechanisms 5

Conceptual Interfaces 5

Min-Entropy Rate 5

Health Tests 5

Maintenance 6

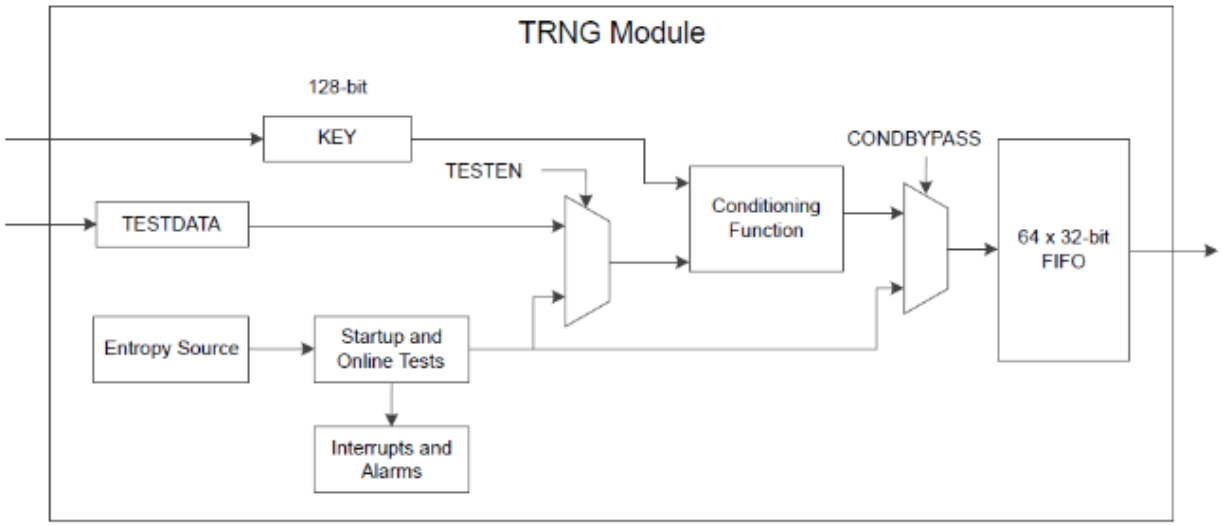
Required Testing 6

Description

EFR32MG21B010PZ045IM32 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

EFR32MG21B010PZ045IM32 Entropy Source is entirely contained within a single-chip TRNG module. In additional, within the chip, the TRNG and Entropy Source is isolated within the security subsystem (SE) and TRNG module is accessible only to the SE CPU core within SE. Other modules within the chip external to the SE do not get access to TRNG module. The software running on SE CPU core is responsible for the setup and control of TRNG module.



Operating Conditions

The following table lists the relevant operating conditions for which the EFR32MG21B010PZ045IM32 Entropy Source was characterized.

Parameter	Value	Description
Temperature	-40 to 135°C	Operating ambient temperature range
VDD	1.03 to 1.21 V	Operating supply voltage

Configuration Settings

The system always select SP 800-90B validated EFR32MG21B010PZ045IM32 Entropy Source.

Physical Security Mechanisms

The EFR32MG21B010PZ045IM32 Entropy Source is part of a single-chip module that meets commercial-grade specifications for power, temperature and reliability. The module is intended for deployment on standard PCBs or similar assemblies.

Conceptual Interfaces

sl_se_get_random() interface requests data from SE, and SE reads the data FiFO of the EFR32MG21B010PZ045IM32 Entropy Source. There is no dedicated health test interface. Data is only released to sl_se_get_random() once the health testing is passed. In case health testing fails, sl_se_get_random() returns failure and the entropy source is re-initialized.

Min-Entropy Rate

Minimum entropy estimate per raw noise sample, following non-IID track and using NIST SP 800-90B test suite, is $H_out \approx 0.84$ bits per 1-bit sample.

After vetted conditioning, the overall entropy source produces 128-bit outputs with full entropy.

Health Tests

The EFR32MG21B010PZ045IM32 Entropy Source performs the required NIST SP 800-90B health tests as follow:

Continuous health testing is performed for each generated output symbol during normal operation. A failure detected by continuous health testing will cause the TRNG to stop generating data. The entropy source implements the following continuous health tests:

- Repetition Count Test conforming to SP 800-90B section 4.4.1
- Adaptive Proportion Test (4096-sample window) conforming to SP 800-90B section 4.4.2
- Adaptive Proportion Test (64-sample window) conforming to SP 800-90B section 4.4.2

Start-up health testing is performed in startup state by applying standard repetition count and adaptive proportion test to 1024 raw, 1-bit noise sample. SE releases data to sl_se_get_random() only after start-up health testing has passed.

On demand health testing is possible by invoking by sl_se_get_random() and monitoring the status register.

When a test fails, the TRNG falls into error state and stops outputting data. The only way to recover from this state is to perform a reset.

Maintenance

There is no special maintenance necessary to operate the Entropy Source.

Required Testing

There is no additional testing required by the target platform. User must rely on the health test to ensure the entropy source is configured correctly and is working as expected.