Ranix TRNG

Hardware Version 1.0
Firmware Version 1.0

SP 800-90B Non-Proprietary Public Use Document

Document Version 1.5
July 2026

Ranix Inc.

2F, Ranix Bldg., 25, Eonju-ro 135-gil, Gangnam-gu, Seoul, Korea, 06053
Phone: 82-2-584-5516
FAX: 82-2-584-5528
www.ranix.co.kr

Document prepared by:

Lightship Security
Applus

https://www.lightshipsec.com/

Table of Contents

Description 3
Security Boundary 3
Operating Conditions 3
Configuration Settings 4
Physical Security Mechanisms 4
Conceptual Interfaces 4
Min-Entropy Rate 5
Health Tests 5
Maintenance 5
User Verification 5
Vendor Permissions and Relationship 5

Description

Ranix TRNG uses a hardware physical entropy source, and it has selected the non-IID track for validation. The noise source utilizes a digitally implemented free-running ring oscillator.

The tested operating environment (OE) is as follows:

Table 1: Operating Environments

Identifier	Version
Operating Environment	ARM SecurCore SC300 running on Xilinx XCVU095 FPGA Family IMFAS Platform

Ranix TRNG is compliant with NIST Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation (Last Modified Date: January 2018), IG D.J (Last Modified Date: November 5, 2021) and IG D.K (Last Modified Date: March 17, 2023).

Security Boundary

Ranix TRNG consists of a TRNG Core, which generates hardware noise and performs health tests, and TRNG firmware, which contains a SHA 256 vetted conditioning component (CAVP #A6819).

To generate random numbers using Ranix TRNG, all 256 bits of the Ranix TRNG output are used as the seed input to the CTR-DRBG in the hardware structure.

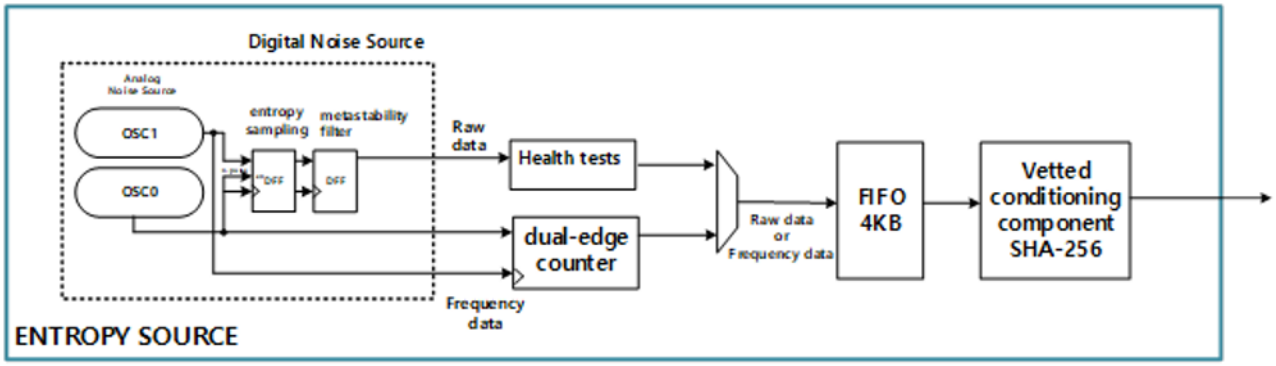


Figure 1: Security boundary

Inputs and outputs related to the evaluation of the Ranix TRNG are only available during the installation process. During the operational phase, it only outputs the results based on random number generation requests.

Operating Conditions

The stable operating environments supported by Ranix TRNG are as follows:

Table 2. Entropy-Relevant Parameters

Parameter	Value
Temperature	0°C ~ 100°C

Parameter	Value
Voltage	0.922V ~ 0.979V

Configuration Settings

The configuration settings are summarized in the table below.

Table 3: Configuration Settings

Configuration parameter	Description	Value
WARMUP_N	Specifies the number of warm-up cycles(waiting jitter acculturation time) required for the oscillator to stabilize before producing the first valid clock.	3500
REG_MODE	Specifies noise source collection and health test enablement.	0x12
ENTROPY_CUT_RCT	Specifies the RCT cutoff value according to the measured entropy,	35
ENTROPY_CUT_APT	Specifies the APT cutoff value according to the measured entropy,	748
FIFO_IN_SEL_RNG	Specifies the FIFO buffer to output the noise source.	1
FREERUN_ON	Specifies to continuously extract noise sources corresponding to the requested number of noise sources.	Enabled
ROSC_EN_1	Specify the oscillator value to be used for the noise source.	0x200
FSM_START	Specifies the noise source start signal.	Enabled

Physical Security Mechanisms

Ranix TRNG is embedded in a single-chip embodiment, making it opaque to visible inspection.

Conceptual Interfaces

With Ranix TRNG, the user requests random numbers, and if the generation is successful, the requested length of random numbers and the results are output. The API used for random number generation is as follows:

- RNX_HSM_GenerateRandom

The RNX_HSM_GenerateRandom corresponds to the conditioned TRNG output. During the installation process of Ranix TRNG, the following API is provided for raw entropy evaluation and TRNG configuration:

- GetTRNG
- SetTRNG

Min-Entropy Rate

Ranix TRNG generates an output that is considered to have full entropy. A request for 256 bits of entropy results in 256 bits of entropy per output sample, or full entropy.

Health Tests

Ranix TRNG has implemented the Repetition Count Test (RCT) and Adaptive Proportion Test (APT) for health testing. The health tests are conducted on start-up, continuously, and on demand.

- Calculation of SP800-90B Repetition Count:
  - Min-entropy (H): 0.6
  - Acceptable false-positive probability (α) = 2^ (-20)
  - Cutoff value (C): 1+(-LOG(α,2))/H = 35

- Calculation of SP800-90B Adaptive Proportion Count:
  - Min-entropy (H): 0.6
  - Window size (W): 1024 (binary data)
  - Acceptable false-positive probability (α) = 2^ (-20)
  - Cutoff value (C): 1+CRITBINOM (W, 2^(-H), 1- α) = 748

Maintenance

Ranix TRNG does not have any maintenance requirements.

User Verification

In the OE operating environment, entropy is evaluated, and RCT and APT health tests are performed according to SP800-90B testing standards, so no additional testing is required.

However, if it is not the OE operating environment, the entropy of the raw noise source output from the GetTRNG API should be evaluated from at least three random samples to ensure a minimum entropy of 0.6 or higher, or the RCT and APT cutoff values are adjusted.

Ranix TRNG was tested on the Xilinx XCVU095 FPGA. To use Ranix TRNG in an ASIC environment, the oscillator ring shall be configured by selecting appropriate standard cell types and cell counts to meet the required oscillation characteristics and timing constraints.

Vendor Permissions and Relationship

The ESV certificate is open for reuse with a written permission from the vendor.