SAMSUNG

SP 800-90B Non-Proprietary Public Use Document

[Samsung TRNG Exynos 1480]
Document Version 1.02

Hard macro Version:
sf_crypt_samsung_trng_ln04lpe_3108000_v2.10
Soft macro Version: sf_crypt_samsung_trng_system_v9.00

Samsung Electronics Co., Ltd.
1 Samsung-ro
Yongin-si Gyeonggi-do 17113
KOREA

June 17, 2026

Revision History

Version	Change
1.00	Initial Draft
1.01	Change name of Samsung TRNG to “Samsung TRNG Exynos 1480”
1.02	Content update to reflect v1.2 template requirements

Table of Contents

1. Description 4
2. Security Boundary 4
3. Operating Conditions 5
4. Configuration Settings 5
5. Physical Security Mechanisms 5
6. Conceptual Interfaces 5
7. Min-Entropy Rate 5
8. Health Tests 6
9. Maintenance 7
10. User Verification 7
11. Vendor Permissions and Relationship 7

1. Description

The Samsung TRNG Exynos 1480 is a physical (P) entropy source based on Meta-RO (metastable ring oscillator). Table 1 provides details of the operational environment of the entropy source. The entropy source was assessed against SP800-90B, IG D.J, IG D.K and IG D.O. The tests were performed using the NIST SP800-90B Entropy Assessment Test Suite in version 1.1.8.

Characteristic	Description
Vendor	Samsung Electronics Co., Ltd.
Entropy source name	Samsung TRNG Exynos 1480
Standard, IGs	SP800-90B (2018) IG D.J (2021-11-05) IG D.K (2023-03-17)
Entropy category	Physical (P)
Entropy source version	Hard macro version: sf_crypt_samsung_trng_ln04lpe_3108000_v2.10 Soft macro version: sf_crypt_samsung_trng_system_v9.00
Tested Platform	Exynos 1480
Embodiment and type	Single chip

Table 1: Entropy source and operational environment information.

2. Security Boundary

The Security Boundary of the entropy source is depicted in Figure 1.

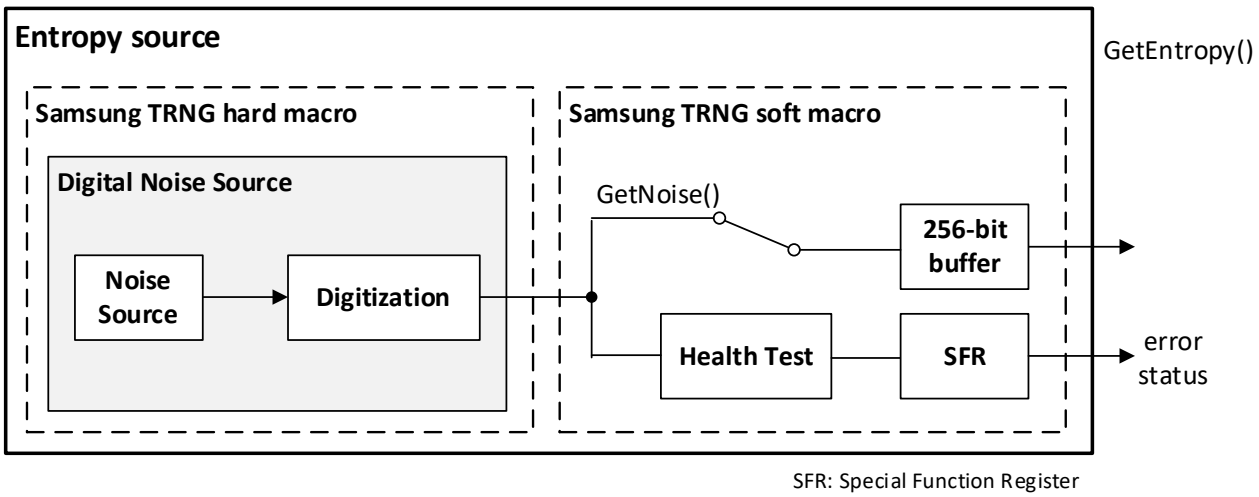


Figure 1: Security Boundary.

The digital noise source includes the noise source (Meta-RO) and digitization circuitry. Health tests are applied to the output of the digitization circuitry and an error status is returned in case of failure of a health test.

3. Operating Conditions

The entropy source operating conditions are provided in Table 2:

Parameter	Value
Operating temperature range	-25℃ ~ 85℃
Operating voltage range	0.75V ± 5 %

Table 2: Operating Conditions

4. Configuration Settings

The operator of the entropy source does not have the ability to modify the entropy source configuration settings.

5. Physical Security Mechanisms

Samsung TRNG Exynos 1480 is embedded in the single-chip embodiment which encases in opaque package within the visible spectrum. And strong removal resistant and penetration resistant IC packaging technique is applied to the single-chip to prevent and detect the physical access.

6. Conceptual Interfaces

The GetEntropy() interface is implemented by GenerateRandomNumber() function in the cryptographic module FW which controls the Samsung TRNG Exynos 1480 to provide 512 bits of entropy input and 256 bits of nonce to construct a seed for DRBG.
The GetNoise() interface has been used for ESV purpose only. There is no implementation to use the raw data of the noise source directly in the cryptographic module FW.
The HealthTest() interface is implemented to monitor the SFR at every calling of GenerateRandomNumber() function in the cryptographic module FW whether there is a healthtests failure or not.

7. Min-Entropy Rate

The claimed $H_{\text{submitter}}$ is 0.5 bits of min-entropy per bits.
Samsung TRNG Exynos 1480 generates 1 bit per sample and the confirmed min-entropy per bit $H = 0.5$
refers to the initial entropy estimation and confirmation by restart testing.
The GetEntropy request receives 768 (512 + 256) bits of RRN (raw random number) from Samsung TRNG Exynos 1480, which corresponds to 768*0.5 = 384 of entropy bits per request.

8. Health Tests

The entropy source implements both the approved Repetition Count Test (RCT) and Adaptive Proportion Test (APT).
The startup health tests are executed automatically after a reset or power-up. During startup, the health test unit collects 1024 samples of raw data and performs RCT and APT on this data. The collected data samples are discarded and not used for random number generation.
The continuous tests implement both the RCT and APT.
The on-demand health tests are activated by a request of the user or caller by setting the flag TRNG_STARTUP_CTRL.STARTUP_HTPASS to 1'b1 and the control bit TRNG_RAND_OUT_CTRL.RAND_OUT_PTR to 1'b1. This triggers the execution of the startup health tests. The samples for those tests are discarded upon successful completion.

8.1. Repetition Count Test (RCT)

The entropy source implements the RCT as specified in SP 800-90B.
To comply with the recommendation in IG D.K (National Institute of Standards and Technology, 2021), the RCT uses $\alpha = 2^{-40}$, which lies within the required range of $2^{-20} \leq \alpha \leq 2^{-40}$. The cut-off value is given by the equation in Section 4.4.1 in SP 800-90B:

$$C = 1 + \left\lceil \frac{-log_2 \alpha}{H} \right\rceil = 81$$

where,

$$\alpha = 2^{-40};$$
$$H = 0.5$$

8.2. Adaptive Proportion Test (APT)

The entropy source implements the APT as specified in SP 800-90B. The APT is computed over a window size of 1024 samples. The cut-off value is defined as $C = 824$ per the computation of the inverse cumulative binomial distribution and significance level $\alpha = 2^{-40}$ (Section 4.4.2 in SP 800-90B).

8.3. Status and Error Codes

The health test unit provides the following status codes.

Flag	Value	
TRNG_TEST_STATUS.HTDONE	1'b0	Startup health test not yet completed.
TRNG_TEST_STATUS.HTDONE	1'b1	Startup health test completed.
TRNG_ERROR_STATUS.HT_ERROR	1'b0	No failure found in health tests.
TRNG_ERROR_STATUS.HT_ERROR	1'b1	Failure found in health tests.

Table 3: Status and Error Codes

9. Maintenance

There are no maintenance requirements.

10. User Verification

In order to test the entropy source, raw data samples must be collected when the entropy source is in test mode, in which case the health tests are disabled so that the noise data can be collected as is from the GetNoise() interface, with or without failures. This test mode is not available in the user mode of the entropy source.
In order to monitor the health of the entropy source, the error status is available from the Health Test.
The pre-collected raw noise data is available for the end used on request.

11. Vendor Permissions and Relationship

This entropy source validation is "Open for reuse", meaning that any vendor can use the certificate within their module without any specific permission.