THALES
Building a future we can all trust

SP 800-90B Non-Proprietary Public Use Document
Thales G7 Hardware Platform TRNG

NOVEMBER 16, 2023, Rev. D

HARDWARE VERSION / PART NUMBERS: 808-000064-005, 808-000065-005, 808-000080-001 and 808-000080-002.

FIRMWARE VERSION: N/A.

Revision History

Version	Change
November 7, 2023, Rev A.	Initial release.
November 7, 2023, Rev B.	Update following comments.
November 7, 2023, Rev C.	Added vendor permissions and relationship section.
November 16, 2023, Rev D.	Addressed test lab comments.

Table of Contents

1. Description

The entropy source is the TRNG supported by the Thales G7 Hardware Platform. The entropy source is contained entirely in hardware on the System-On-Chip (SoC) used by the platform.

The hardware identifiers for the Thales G7 hardware platform[1] are:

- 808-000064-005, 808-000065-005, 808-000080-001 and 808-000080-002.

The TRNG does not use firmware. To be used in the approved configuration, the system utilizing the TRNG must program the configuration settings recorded in section 4 ahead of attempting to extract entropy. Settings are recorded in hardware registers provided by the SoC.

The operating environment for the SoC containing the TRNG is based on the limits enforced for Environment Failure Protection (EFP) by the hardware platform.

This is a non-IID source.

2. Security Boundary

Figure 2-1 presents the entropy source architecture.

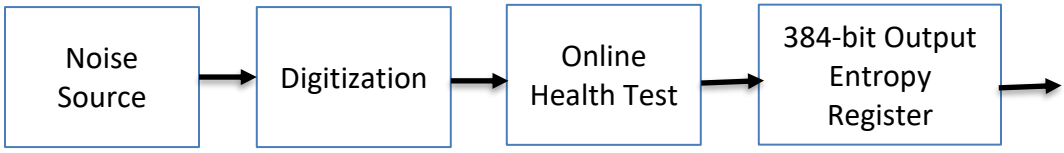

Figure 2-1: Entropy Source Architectural Representation

The entropy source is contained entirely within the SoC embedded in the Thales G7 Hardware Platform. The Thales G7 Hardware Platform is a potted module that protects against physical access to the SoC.

The security boundary for the TRNG is identified as the entropy source boundary internal to the SoC that is contained inside the Thales G7 Hardware Platform.

3. Operating Conditions

The Thales G7 Hardware Platform supports the operation conditions enforced by the platform environmental failure protection (EFP) as seen in Table 3-1 and Table 3-2.

Table 3-1: Nominal Voltage EFP Thresholds

Power Net	Under Voltage	Over Voltage
5V	3.9V ± 0.11V	5.71 ± 0.145V

[1] all hardware parts include the same SoC containing the entropy source.

Table 3-2: Nominal Temperature EFP Thresholds

Under Temperature	Over Temperature
-0°C ± 2°C	+70°C ± 2°C

4. Configuration Settings

The TRNG must be configured using the settings in Table 4-1 and Table 4-2 from firmware running on the embedded SoC but outside the entropy source boundary:

Table 4-1: Entropy Source Configuration

Parameter	Purpose	Setting for approved use of the TRNG
Von Neumann sampling enabled	Used to enable/disable the optional conditioning function.	Disabled
Entropy Delay	In clock cycles, the length of time the oscillator is allowed to run between sampling the output of the counter.	3200 clock cycles (@ 300 MHz)
Continuous Health Test Limits	Cut-off values for statistical tests.	See Table 4-2.
Entropy Source Clock Divider	Allows software to slow down the clocking of the source in the case it is running too fast and where entropy delay cannot be made sufficiently large.	No-divide
Enable Entropy Access Mode	Allows access to raw entropy using special validation interfaces.	Disabled
Entropy Sample Size	Number of bits provided to the statistical checker for each block of entropy output by the noise source.	2500
Entropy Source Retry Count	Number of times to retry entropy generation following a continuous test failure	3

Table 4-2: Health Test Bounds

Health Test	Min Limit	Max Limit
Monobit	1116	1384
Poker	24445	26912
Runs of length 1	227	485
Runs of length 2	98	220
Runs of length 3	37	125
Runs of length 4	11	75
Runs of length 5	1	47
Runs of length 6+	1	47
Long Runs	N/A	34

The noise source shall be restarted following update of the configuration settings ahead of attempting to extract entropy.

5. Physical Security Mechanisms

The physical protection of the entropy source consists of those features provided by the hardware platform.

The Thales G7 Hardware Platform includes a hard coating or strong plastic enclosure that provides tamper-evidence if opened following manufacture. Any tampering that might compromise a module's security is detectable by visual inspection of the module.

The module's enclosure is opaque in order to resist visual inspection of the device design, physical probing of the device, and attempts to access sensitive data on individual components of the device.

Any attempts to remove the internal potting of the module to gain access to the SoC will result in sufficient physical damage to the device to render it inoperable.

6. Conceptual Interfaces

Output from the noise source is fed directly to the DRBG embedded in the same SoC. The output of the TRNG is not available when operational to firmware or other hardware components other than the SoC, DRBG component.

7. Min-Entropy Rate

The noise source produces 1-bit samples, which are assessed at 0.838411 bits of min-entropy per sample. The entropy source provides entropy in blocks of 384 bits to the DRBG, which provides the DRBG with 321.9 bits of min-entropy.

8. Health Tests

The entropy source includes the SP 800-90B's required continuous, start-up and on-demand health tests.

The continuous health tests include statistical tests based on those used with FIPS 140-1. These tests have limits selected to support a false positive of 1 in 10^6. The source enters its error state if three (3) consecutive failures on different tested samples are detected.

These tests have been demonstrated to meet the criteria in section 4.5. 'Developer-Defined Alternatives to the Continuous Health Tests' from SP 800-90B.

9. Maintenance

No maintenance activities are prescribed for this entropy source.

10. Required Testing

The TRNG was tested in accordance with SP 800-90B requirements. Input data was collected from the module using special validation interfaces that allow access to raw entropy. These interfaces are not available in user implementations during operation; therefore, the user must rely on health tests to ensure that the entropy source is configured correctly and is working as expected.

No further testing is required.

11. Vendor Permissions and Relationship

This certificate is re-usable by any company within the Thales group of companies. In particular this includes the fully owned subsidiary, Thales Trusted Cyber Technologies.