THALES
Building a future we can all trust

SP 800-90B Non-Proprietary Public Use Document
Thales K7 Hardware Platform TRNG

002-000534-001, Rev. C
NOVEMBER 16, 2023

HARDWARE VERSION / PART NUMBERS: 808-000048-002, 808-000048-003, 808-000066-001, 808-000073-001 and 808-000073-002.

FIRMWARE VERSION: 1.0.

Revision History

Date	Version	Change
October 26, 2023	Rev. A	Initial release.
November 11, 2023	Rev. B	Updated target part identifiers.
November 16, 2023	Rev. C	Addressed test lab comments.

Table of Contents

1. Description

The entropy source is the TRNG supported by the Andretta 2.0 System on Chip (SoC) included on the Thales K7 Hardware Platform.

The hardware identifiers for the Thales K7 Hardware Platform[1] are:

- 808-000048-002, 808-000048-003, 808-000066-001, 808-000073-001 or 808-000073-002.

All hardware parts include the Andretta 2.0 SoC that embodies the noise source in hardware. Conditioning, statistical testing, and control of the entropy source are performed using a firmware library, Andretta_TRNG_FW, version 1.0.

This is a non-IID source.

2. Security Boundary

Figure 2-1 presents the entropy source architecture.

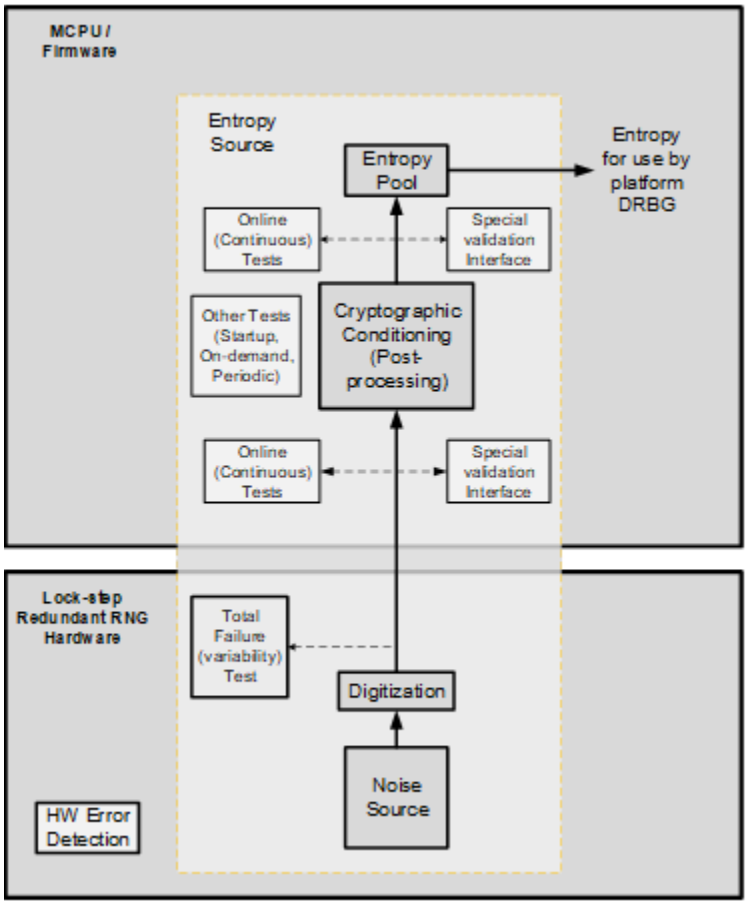

Figure 2-1: Entropy Source Architectural Representation

The entropy source spans the Andretta 2.0 ASIC hardware and firmware running on the embedded MCPU within the same ASIC.

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

Entropy is provided by an Andretta 2.0 ASIC implemented as a set of Free Running Oscillators (FROs) running at different frequencies and asynchronously to one another. The FROs are sampled to produce a single bit of new raw entropy every sampling interval. This bit stream is tested in hardware for total failure.

The raw entropy is made available to the firmware running on the MCPU as a 512-byte block of raw entropy in response to a Direct Memory Access (DMA) request. A combination of hardware and firmware mechanisms guarantees that every output block represents a consecutive, total failure free bit-stream of raw entropy.

The raw entropy flows through a vetted conditioning function which compresses it to produce a smaller block of full entropy as output. Once the conditioned entropy passes the continuous tests, it is moved into the entropy pool. Entropy is retrieved from the pool using the function `RN_EntropyPool_FillBuffer(…)` which acts as the interface to the noise source for the tested entropy.

3. Operating Conditions

The Andretta ASIC noise source operates within the bounds enforced by the platform environmental failure protection (EFP).

Table 3-1: Nominal Voltage EFP Thresholds

Power Net	Under Voltage	Over Voltage
5V	4.76v	5.26v
3.3V	3.07v	3.61v
1.8V	1.62v	2.00v

Table 3-2: Nominal Temperature EFP and Tamper Thresholds

Under Temperature	Over Temperature
-2°C ± 2°C	+80°C ± 2°C

4. Configuration Settings

There are no configuration settings for the entropy source that are available to the operator.

5. Physical Security Mechanisms

The physical protection of the entropy source consists of those features provided by the cryptographic module. Modules embedding the chip typically include either a hard coating or strong metal enclosure that provides tamper-evidence. Any tampering that might compromise a module's security is detectable by visual inspection of the module.

The module's enclosure is opaque 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.

6. Conceptual Interfaces

Output from the noise sources is available exclusively through the `RN_EntropyPool_FillBuffer(…)` function provided by the Andretta_TRNG_FW library.

7. Min-Entropy Rate

The source provides full entropy output.

The noise source produces 1-bit samples that are assessed at **0.4682** bits of min-entropy per bit. 2048 bits of noise samples are conditioned into 512 bits of full entropy output by a SHA2-512 conditioning component whose CAVP certificate is #C1707.

8. Health Tests

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

The source conducts Individual FRO Startup Tests on initialization of the Random Number Generator (RNG) subsystem. A Startup Statistical Test is also run on initialization of this subsystem. A Total Failure (variability) Test is run on the raw entropy, and Continuous Tests of Raw Entropy detect weak raw entropy. A Known Answer Test (KAT) is run for the Conditioning Function and a Continuous Test of Conditioned Entropy is run to detect weak conditioned entropy.

Detection of a noise source failure results in the module being halted.

9. Maintenance

No maintenance activities are prescribed for this entropy source.

10. Required Testing

The Andretta 2.0 entropy source 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 and conditioned entropy, and permit failure injection. These interfaces are not available in user implementations; 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.