SP 800-90B Non-Proprietary Public Use Document

Entropy Source Name : Aquarius PTRNG

Document Version : 1.2

Hardware Versions: Rev C

THALES DIS FRANCE SAS
Arteparc Meyreuil Bâtiment D
Route de la Côte d'Azur
13590 MEYREUIL – France

February 22nd, 2024

Template Revision History

Version	Date	Change
1.0	December 20Th 2023	Initial release
1.1	February 16th 2024	• Typo correction: REVA => REVC • Upated health-tests section
1.2	February 22nd 2024	• Change classification

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 5

Required Testing 5

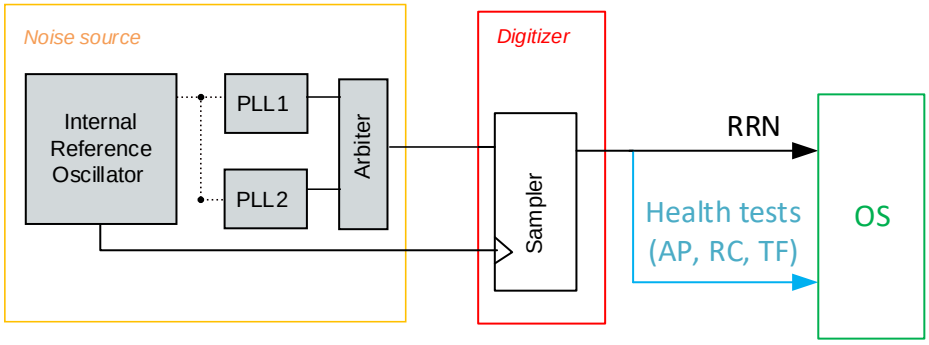
References 5

Description

Thales TRNG is a Physical True Random Number Generator (PTRNG) based on the comparison of two identical Phase-Locked Loops (PLL) outputs affected by thermal noise. It has been tested on Aquarius.

Security Boundary

The simplified PTRNG architecture and its security boundaries is represented in the figure below. There is a unique noise source. The digitizer consists in sampling the information of which PLL is in advance at each falling edge of the clock reference. There are also health tests. The regular SP800-90B Adaptative Proportion (AP), and Repetition Count (RC) together with an additional total failure. The result of those tests is made available to the upper layers such as for instance the Operating System (OS). No conditioning is provided.



Operating Conditions

The PTRNG is suited for applications that shall be compliant with the following operating conditions defined in the ISO 7816 and in the ISO/IEC 14443:

- Contact VCC= [1.62:5.5] V
- Contactless H=[1.5: 7.5]A/m
- Temperature in the range of [-25, 85]°C

In practice PTRNG is still functional in the following wider operating conditions:

- Contact Vcc= [1.55:5.5] V
- Contactless H=[1: 12]A/m
- Temperature in the range of [-40, 125]°C

Configuration Settings

There are no configurable settings.

Physical Security Mechanisms

The PTRNG is embedded in the Aquarius chip that has been evaluated through Common Criteria and reached the level EAL6+ [1,2] that proves strong resistance against physical attacks with respect to its target [3,4]. The PTRNG benefits from the chip resistance.

Conceptual Interfaces

Only the GetEntropy and the HealthTest interfaces are available to the user.

Min-Entropy Rate

The min-entropy rate is 0.25 per bit.

Health Tests

The implemented health tests are the one described in [5] and are processed on raw data. An additional total failure test is provided which is also processed on raw data.
Hence Adaptive Proportion and Repetitive Count are implemented following the description given in [5] while an additional proprietary total failure test in also implemented.
When at least one of these tests fails during start-up test or before or after using random bits, the application shall discard retrieved random bits and can restart the analog source at most once. After restarting, if the tests remain failed, the platform shall be reset.

Maintenance

No maintenance is required.

Required Testing

The Aquarius PTRNG was tested accordingly with requirements in [5]. No further testing is required.

References

[1] Rapport de certification ANSSI-CC-2023/01 AQUARIUS_BA_09 AQUARIUS_v1 Paris, le 11 Janvier 2023, https://www.commoncriteriaportal.org/files/epfiles/anssi-cc-2023_01_0.pdf
[2] Rapport de maintenance ANSSI-CC-2023/01-M01 AQUARIUS_BA_09 & CA_09 AQUARIUS_v2 Certificat de référence : ANSSI-CC-2023/01 Paris le 21 Juin 2023, https://www.commoncriteriaportal.org/files/epfiles/ANSSI-CC-2023_01-M01.pdf
[3] AQUARIUS_BA_09_ST_Security_Target, Reference: AQUARIUS_B_ST_Lite Revision: 002 Date of revision: 19 October 2022, https://www.commoncriteriaportal.org/files/epfiles/anssi-cible-2023_01en_0.pdf
[4] AQUARIUS_ST_Security_Target, Reference: AQUARIUS_ST_Lite Revision: 003 Date of revision: 02 June 2023, https://www.commoncriteriaportal.org/files/epfiles/ANSSI-cible-CC-2023_01-M01.pdf
[5] Meltem Sönmez Turan, Elaine Barker, John Kelsey, Kerry A. McKay, Mary L. Baish and Mike Boyle. Recommendation for the Entropy Sources Used for Random Bit Generation. January 2018.