STMICROELECTRONICS

ST31N600 entropy source

SP 800-90B Non-Proprietary Public Use Document

Firmware revision: RNGLIB v1.0.1
HW version: ST31N600 rev B & rev C

Date: 2023-11-14
Document Version: 01-01

NON-PROPRIETARY DOCUMENT

Table of Contents

1 DESCRIPTION

The ST31N600 contains an entropy source that is composed of:

- A HW True Random Number Generator module identified by its version ST31N600 rev B and rev C.

  The application software must call the interface USER_GetProductInformation() and must check that the fields :

  - MPIN (Master Product identification) value is 0x0200
  - HWInternalRevision (Product internal Revision) value is 0x42 (‘B’) for rev B and 0x43 (‘C’) for rev C

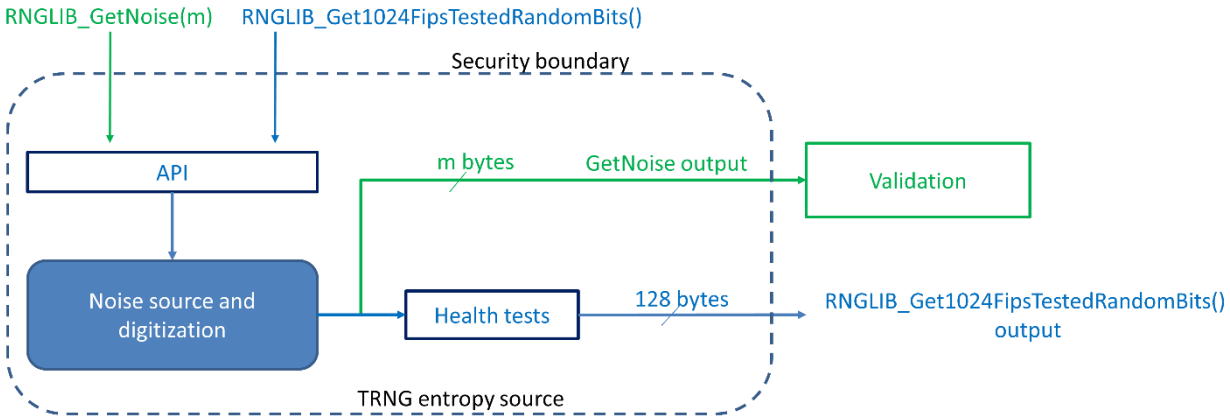
- A library RNGLIB that interfaces with HW and identified by its version. The application software must call the RNGLib_GetVersion() method and must check that the value is 0x01000102. The use of RNGLIB is licensed-based.

It is recommended to provide this traceability information at application level to identify the product and the library used.

The entropy source category is physical (P) and has been tested with the non-IID tests suite.

2 SECURITY BOUNDARY

The security boundary is represented by the dotted line in the figure below.



The TRNG (inside its security boundary) is composed of:

- A noise source and digitization block.
- Software APIs to request generation of consecutive random bits.
- Implementation of SP 800-90B health tests. If tests are failed, output of random bits are not available, and an error flag indicates the failure to the application.

3 OPERATING CONDITIONS

The noise source operates correctly and uniformly at the following conditions:

- A temperature range of the security module comprised between -25°C and +85°C
- A supply voltage from 2.7V to 5.5V (±10%).

Beyond these ranges, any misuse of TRNG can be guaranteed by the activation of the temperature and power supply detectors.

4 CONFIGURATION SETTINGS

The entropy source is not configurable.

5 PHYSICAL SECURITY MECHANISMS

The entropy source is part of a single silicon chip encapsulated in a hard, opaque, production grade integrated circuit (IC) package.

6 CONCEPTUAL INTERFACES

The RNGLIB provides the following interfaces:

- *RNGLIB_Init* to set the maximum number of retry.
- *RNGLIB_GetNoise(m)* to get noise samples concatenated on m bytes at the output of the noise source to be used for statistical testing
- *RNGLIB_Get1024FipsTestedRandomBits()* to get health-tested noise samples concatenated on 128 bytes to be used by the application

Health tests are implicitly used by the *RNGLIB_Get1024FipsTestedRandomBits()* method.

7 MIN ENTROPY RATE

The min-entropy rate reached by the design is H = 0.75 per sample bit. The entropy source produces 192 bits of entropy per 256-bit output.

8 HEALTH TESTS

8.1 Description

Health tests are systematically executed before output of any random value, on each new batch of non-conditioned 1024-bits from the *RNGLIB_Get1024FipsTestedRandomBits()* method. RNGLIB implements two health tests from SP800-90B approved tests.
The noise source design and verification (statistical tests) did not exhibit any proprietary noise source failure mode that would request dedicated continuous health tests for its detection other than the two health tests implemented. The two health-tests are run as continuous tests, performed automatically at each new random request from the *RNGLIB_Get1024FipsTestedRandomBits()* method.

8.2 Approved Continuous Health Tests

The implemented approved tests are the repetition count test (RCT) and the adaptive proportional test (APT) as detailed in §4 of [SP800-90B]. APT is performed on a window of W=1024 samples parametrized to accommodate a false positive rate of $\alpha=2^{-20}$.

8.3 Additional Health Tests

An additional health tests is performed:

- A HW continuous detection test that flags a succession of 48 steady ‘0’ or ‘1’ raw samples. The false positive rate ($\alpha=2^{-18}$ per hour) is relative to the absolute time of operation (i.e. not directly related to the consuming application's requests).

8.4 Failure management

In case of failure of one of the two health-tests:

- A retry counter is incremented
- The current batch of 1024-bits is discarded and a new batch is generated.

When the retry counter reaches the maximum value parameterized with the *RNGLIB_Init* method (corresponding to x consecutive health tests failed), this is interpreted as a permanent failure for the application software.

If one of the health tests fails, there is no random value output from the RNGLIB.

9 MAINTENANCE

There is no maintenance requirement.

10 REQUIRED TESTING

The entropy source output obtained with the *RNGLIB_GetNoise()* DRGB have been tested with the SP800-90B entropy assessment tool (*https://github.com/usnistgov/SP800-90B_EntropyAssessment*) and has been assessed at H = 0.75.

No further testing required.

Acronyms

Term	Definition
APT	Adaptive proportional test
RCT	Repetition count test
TRNG	True Random Number Generator

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

This document may be reproduced only in its original entirety without revision.

www.st.com