STMICROELECTRONICS

Trusted Platform Module
ST33KTPM2X, ST33KTPM2XSPI, ST33KTPM2XI2C, ST33KTPM2A, ST33KTPM2I
Entropy Source

SP 800-90B Non-Proprietary
Public Use Document

Entropy Source Revision: 1.0
HW Version: ST33K1M5A revB /
ST33K1M5T revC /
ST33K1M5T revD

Date: 2023-05-09
Document Version: 01-02

NON-PROPRIETARY DOCUMENT

Table of Contents

1 DESCRIPTION

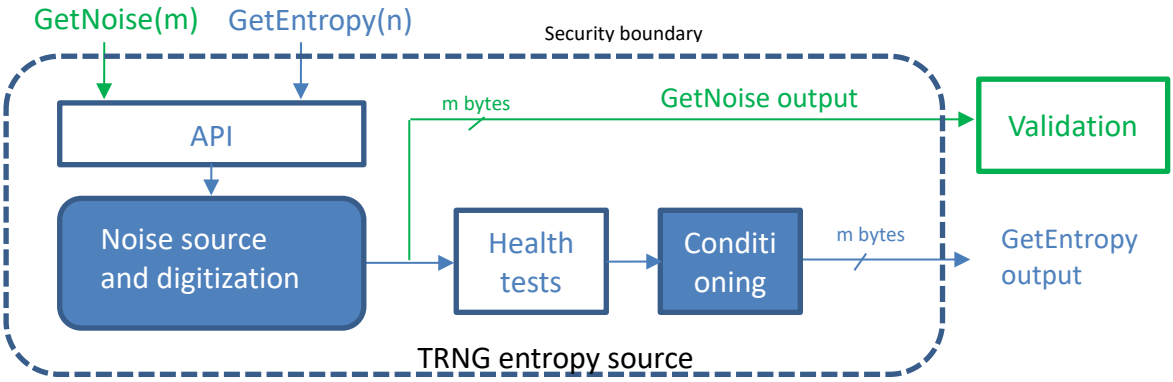
The Trusted Platform Modules ST33KTPM2X, ST33KTPM2XSPI, ST33KTPM2XI2C, ST33KTPM2A, ST33KTPM2I contain an entropy source that is composed of:

- A HW True Random Number Generator module identified by its version (ST33K1M5A revB, ST33K1M5T revC or ST33K1M5T revD)
- FW that interfaces with HW and identified by its version (1.0[1])

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 and AIS31 health tests. If tests are failed, output of random bits is inhibited, and an error flag indicates the failure to the application.
- A conditioning component relying on a SHA256 hash function.

3 OPERATING CONDITIONS

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

- A temperature range of the security module comprised between -40°C and +105°C.
- A voltage range at 1.8V or 3.3V (±10%).

4 CONFIGURATION SETTINGS

The entropy source is not configurable.

[1] Decimal representation

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 entropy source provides the following interfaces:

- GetNoise(m) to get noise samples concatenated on m bytes at the output of the noise source to be used for statistical testing
- GetEntropy(n) to get conditioned and health-tested noise samples concatenated on n bytes to be used by the application

Health tests are implicitly used by the GetEntropy() method.

7 MIN ENTROPY RATE

The min-entropy rate reached by the design is H = 0.81926 per sample bit. The entropy source produces 209 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. TRNG implements four health tests:

- Two SP 800-90B approved tests
- Two additional 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 four health tests implemented. The four health-tests are run as:

- Start-up tests, performed automatically on DRBG seeding, during start-up of the module
- Continuous tests, performed automatically at each new random request
- On-demand testing, that can be performed by restarting the security module with the consequence of executing the start-up tests again

In addition to the APT and RCT tests whose purpose are described in SP 800-90B, the AIS31 test described below aims at detecting possible periodic outputs.

8.2 Start-Up Tests

The startup tests automatically run the continuous heath tests (refer to the 4 tests described below) during the security module start-up over 1024 samples. The samples are not available for normal operations until the tests are completed.

8.3 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 $\alpha=2^{-20}$.

8.4 Additional Health Tests

Two additional health tests are performed:

- A HW continuous detection test that flags a succession of 48 steady ‘0’ or ‘1’ raw samples. It is equivalent to a RCT test with $\alpha = 2^{-44}$.

- A standard 3 degree-of-freedom χ^2 statistical test with a false positive rate of $\alpha = 10^{-5}$, derived from the AIS31 standard. This test is included for AIS31 standard compliance and would allow detecting repetition patterns of two consecutive bits in addition to RCT and APT.

8.5 Failure Management

In case of failure of one of the four health-test:

- A retry counter is incremented.
- The current batch of 1024-bits is discarded and interpreted as an intermittent failure. A new batch of 1024-bits is collected and tested.

The retry counter requires consecutive failures to increment beyond one. A batch of 1024 bits that does not fail the health tests will reset the retry increment counter to zero. The security module enters a failure mode that only enables performing a diagnosis and/or resetting the module when the retry counter reaches a maximum value of 4 retries. If one of the health tests fails, no random value output from the TRNG is made available to the user.

9 MAINTENANCE

There is no maintenance requirement.

10 REQUIRED TESTING

The entropy source output obtained with the GetNoise() API have been tested with the SP 800-90B entropy assessment tool (*https://github.com/usnistgov/SP800-90B_EntropyAssessment*), and has been assessed at H = 0.81926.

No further testing required.

11 ACRONYMS

Term	Definition
DRBG	Deterministic Random Bit Generator
SHA	Secure Hash Algorithm
TCG	Trusted Computed Group
TPM	Trusted Platform Module
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.

© 2023 STMicroelectronics - All rights reserved
www.st.com