

SP 800-90B Non-Proprietary Public Use Document
NPCT7xx TPM2.0 Entropy Source
Version 1.0

Hardware version: LAG019
Firmware versions: 7.2.3.0, 7.2.3.1, 7.2.4.1, 7.2.5.1

Nuvoton Technology Corporation

No. 4, Creation Road III
Hsinchu Science Park
Taiwan

November 13, 2025

Revision History

Version	Date	Description
1.0	December 21, 2022	First version.
1.1	January 23, 2023	Added more information to Section 10.
1.2	December 11, 2023	Added Firmware version 7.2.4.0 and refined the Firmware and Hardware description in Section 1 (Description).
1.3	October 1, 2024	Added Firmware version 7.2.5.0.
1.4	December 18, 2024	Added a new certificate number to section 6 (for Firmware version 7.2.5.0).
1.5	June 17, 2025	Added Firmware version 7.2.4.1.
1.6	August 10, 2025	Removed version 7.2.4.0 and updated min-entropy rate description in Section 7.
1.7	November 13, 2025	Replaced version 7.2.5.0 with 7.2.5.1

Table of Contents

1.	Description	4
2.	Security Boundary	4
3.	Operating Conditions	5
4.	Configuration Settings	5
5.	Physical Security Mechanisms	5
6.	Conceptual Interfaces	6
7.	Min-Entropy Rate	6
8.	Health Tests	6
9.	Maintenance	6
10.	Required Testing	6

1. Description

The NPCT7xx chip is a Trusted Platform Module (TPM) consisting of both Hardware and Firmware (version 7.2.3.0, 7.2.3.1, 7.2.4.1 or 7.2.5.1) as follows:

Component	Identification Field ¹	Value
Hardware (LAG019)	Device ID (DID)	00FCh
Firmware 7.2.3.0	TPM_PT_FIRMWARE_VERSION_1	00070002h
	TPM_PT_FIRMWARE_VERSION_2	00030000h
Firmware 7.2.3.1	TPM_PT_FIRMWARE_VERSION_1	00070002h
	TPM_PT_FIRMWARE_VERSION_2	00030001h
Firmware 7.2.4.1	TPM_PT_FIRMWARE_VERSION_1	00070002h
	TPM_PT_FIRMWARE_VERSION_2	00040001h
Firmware 7.2.5.1	TPM_PT_FIRMWARE_VERSION_1	00070002h
	TPM_PT_FIRMWARE_VERSION_2	00050001h

The NPCT7xx chip is certified as part of the NPCT7xx Common Criteria EAL4+ certification (Firmware versions 7.2.3.0/1 Certificate IDs: ANSSI-CC-2022/24 - ANSSI-CC-2022/31, Firmware version 7.2.4.1 and version 7.2.5.1 are pending approval).

The physical (P) Entropy Source module is part of NPCT7xx; it is compliant with SP 800-90B and seeds a Deterministic Random Bit Generator (DRBG) compliant with SP 800-90A.

The noise source was tested under the assumption that its output is non-IID.

2. Security Boundary

The following block diagram describes the building blocks and security boundary of the Entropy Source.

¹ For more information, see *TCG PC Client Platform TPM Profile (PTP) Specification, Family 2.0 Version 1.05 Revision 14, September 4, 2020*, or later.

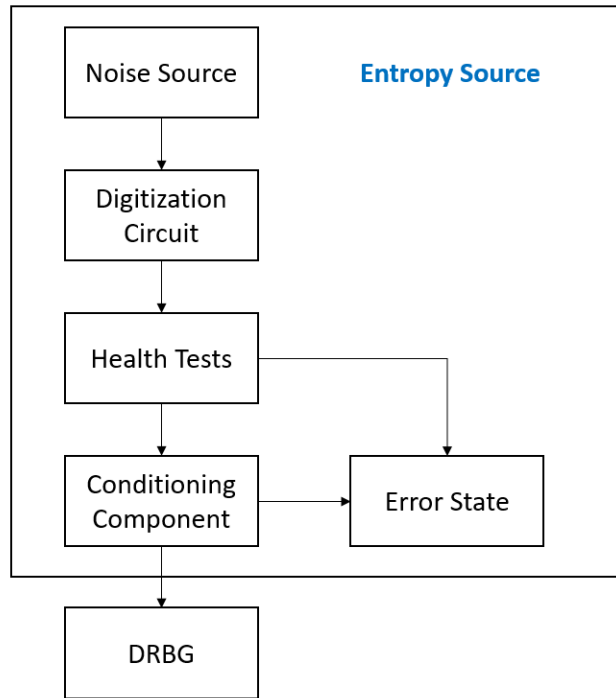


Figure 1: Entropy Source Building Blocks and Security Boundary

3. Operating Conditions

The operating conditions of the Entropy Source are derived from the NPCT7xx operating conditions and summarized in the following table:

Parameter \ Value	Min	Max	Unit
Supply Voltage, option 1	3.135	3.465	V
Supply Voltage, option 2	1.71	1.89	V
Operating Temperature	-40	+85	°C

4. Configuration Settings

There are no configuration settings for the Entropy Source.

5. Physical Security Mechanisms

The Entropy Source is part of the NPCT7xx, which meets the FIPS 140-2/3 Physical Security Level 3 requirements and provides hardness, opacity and tamper-evidence protection.

6. Conceptual Interfaces

The Entropy Source provides an interface to seed the DRBG. In addition, for testing purposes, it provides two interfaces, which are not available in the production state of the NPCT7xx, as follows:

1. Extraction of bits from the Digitization Circuit; this is used for the Validation of the Entropy Source according to Section 3 in SP 800-90B.
2. Insertion/Extraction of bits to/from the Conditioning Component; this is used for FIPS Cryptographic Algorithm Validation Program (CAVP) testing (Certificate numbers A1961, A4792 and A6386).

7. Min-Entropy Rate

The vetted conditioning component `Block_Cipher_df`, defined in SP800-90B is fed directly by the Digitization Circuit (see Figure 1). The vetted conditioning component input is 1024 bits containing 512 bits of entropy (based on a min-entropy of 0.5 bits per bit). The output of the vetted conditioning component provides 384 bits with full entropy.

8. Health Tests

The Entropy Source implements the Repetition Count Test (RCT) and Adaptive Proportion Test (APT) from SP 800-90B. The estimated false positive of the Health Tests is 2^{-20} .

9. Maintenance

There are no maintenance requirements related to the Entropy Source.

10. Required Testing

The Entropy Source compliance to SP 800-90B was validated using the testing interface (not available outside of test units, as mentioned in Section 6), the CAVP and the SP 800-90B entropy assessment tool. Both the theoretical assessment and the test results predicted a higher min-entropy than the conservative min-entropy claimed (0.5).

To validate the theoretical assumptions about the noise source, the following tests were performed. Data was collected from the device in its designated operational range; the tests were performed according to Section 3 of SP 800-90B:

- Raw Noise samples comprising of at least 1,000,000 bits were collected via the raw noise source interface and processed by the NIST SP800-90B tool. The entropy rate must be at least the min-entropy rate defined in Section 7.
- Restart data must be collected in accordance with the procedure specified in SP800-90B (in the format of 1,000 samples from 1,000 restarts) through the raw noise source interface and processed by the NIST SP800-90B tool. The restart sanity tests must all pass and the minimum of the row-wise and column-wise entropy rate should not be less than half of the entropy rate obtained from the raw noise data test, described above.

No further testing is required on the Entropy Source.