SP 800-90B Non-Proprietary Public Use Document for Nuvoton NTCES01

Entropy Source Version: 1.0

Document Version: 1.0

Document Date: 2023-09-14

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

Table of Contents

1. Description

The Nuvoton NTCES01 is a physical entropy source that resides on a single chip. The noise generation of this entropy source is based upon the principle of Ring Oscillators.

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

The entropy source was tested on the operational environments listed in Table 1.

Table 1: Operational Environment.

Entropy Source Name	Operational Environment
Nuvoton NTCES01	Nuvoton Arbel BMC NPCM8mnx single chip

2. Security Boundary

Figure 1 depicts the security boundary of the entropy source and its components.

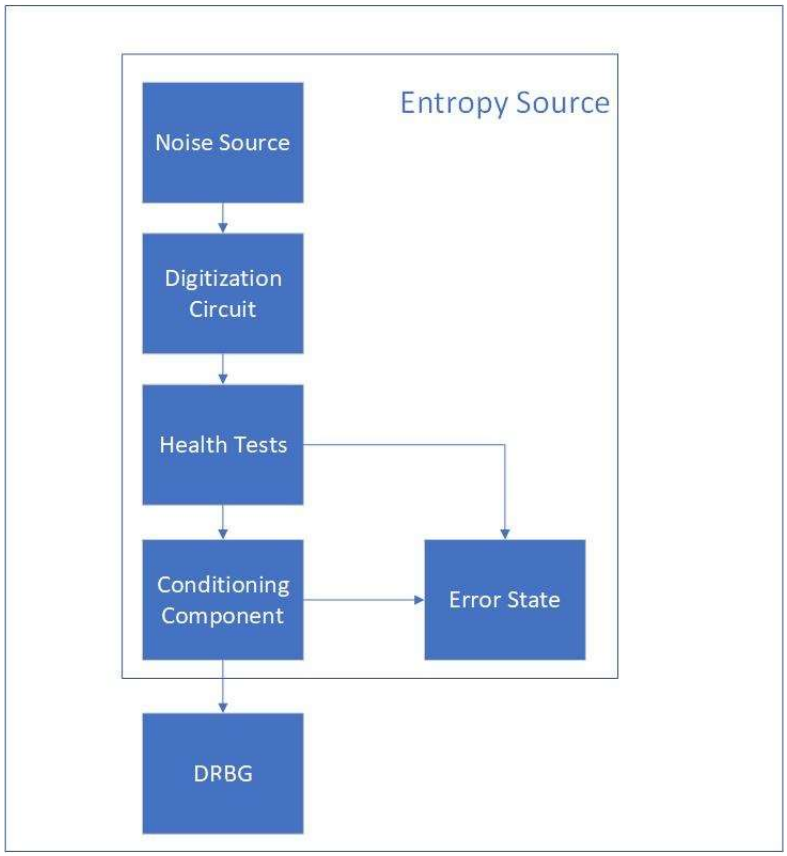

Figure 1: Security boundary of the entropy source.

3. Operating Conditions

The operating conditions of the entropy source are the same as those of the chip on which it resides:

Temperature range: -5°C to 115°C

Voltage range: 1.035V to 1.105V

4. Configuration Settings

The entropy source is a physical source and does not have any configurable parameters or settings.

5. Physical Security Mechanisms

The noise source is physical in nature and so it inherits the physical security mechanisms of the chip that it resides in. Physical security is provided by the silicon die which is housed in an opaque package.

6. Conceptual Interfaces

The output of the entropy source is 512-bits in length and has full entropy. The output is provided from the entropy source to the calling DRBG.

7. Min-Entropy Rate

$H_{submitter}$ = 0.6 bits per 1-bit symbol.

8. Health Tests

The entropy source implements the following continuous health tests:

- Repetition Count Test conforming to SP 800-90B section 4.4.1.
  - $H = 0.6$ bits of entropy per 1-bit sample.
  - alpha value of $\alpha = 2^{-20}$.
  - Cutoff value $C = 35$.
- Adaptive Proportion test conforming to SP 800-90B section 4.4.2.
  - $W = 1024$
  - $H = 0.6$ bits of entropy per 1-bit sample
  - alpha value of $\alpha = 2^{-20}$.
  - Cutoff value $C = 748$.

The startup tests conduct the same set of continuous health tests to 1024-bit samples of noise source output. If any health tests fails, the initial 1024-bit samples are discarded and a new set of 1024-bits are obtained. If the health tests fail again, the entropy source transitions to a permanent error state. Whenever the health tests pass, the 1024-bits are fed into the SHA2-512 conditioning function.

The entropy source can only produce 1024 bits and then is disabled.

On-demand health tests are run by powering the chip off and on. This operation will then trigger the startup tests.

Whenever health tests fail, an error code is returned to the caller who is requesting the entropy.

9. Maintenance

There are no maintenance requirements applicable to this entropy source.

10. Required Testing

To test the entropy source, raw data samples must be collected using a special Nuvoton test tool that is capable of accessing the raw noise interface of the entropy source.

Raw noise data samples consisting of at least 1,000,000 bits must be collected from the operational environment at its normal operating conditions and processed by the SP 800-90B entropy tool that is provided by NIST. The expected min-entropy rate must approach the one in Section 7.

Restart data must be collected at normal operating conditions through the raw noise source interface following the restart procedure specified in SP 800-90B (i.e., 1,000 samples from 1,000 restarts each) and processed by the NIST SP 800-90B entropy tool. The minimum of the row-wise and column-wise entropy rate must be more than half that of the raw noise entropy rate.

11. Vendor Permissions and Relationship

The ESV certificate is “Reuse restricted to vendor”. Someone other than the vendor can only use the certificate with written and signed permission from the vendor’s point of contact (as indicated on the ESV certificate).