Century Longmai Technology Co., Ltd.

Longmai mToken CryptoID Entropy Source

ESV Public Use Document

Document Version 0.4

May 3, 2023

Table of Contents

References

Ref.	Full Specification Name	Date
[90A]	NIST, SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators	24-Jun-2015
[90B]	NIST, SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation	10-Jan-2018
[140]	NIST, FIPS PUB 140-3, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES	22-Mar-2019
[140IG]	NIST, Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program	7-Oct-2022

1 Description

This document provides the information required by the NIST Entropy Source Validation (ESV) program.

This assessment was conducted using data and parameters measured in the evaluated version and configurations described in Table 1. The Century Longmai Technology mToken CryptoID Entropy Source design is described in Section 2.

Table 1: Evaluated Entropy Source Specification

Identifier	Description
Entropy Source Name	Longmai mToken CryptoID Entropy Source
Hardware Revision	SCC-XE
Firmware Version	3.12
Entropy Category	Physical (P)
Entropy Estimation Track (per SP 800-90B §3.1.2)	Non-IID

2 Security Boundary

The Longmai mToken CryptoID Entropy Source is definitionally all the components and functionality within the Entropy Source “security boundary" (depicted in Figure 1 as the dotted line). The Entropy Source is comprised by the following:

- A hardware noise source based on a single ring oscillator
- A firmware health test

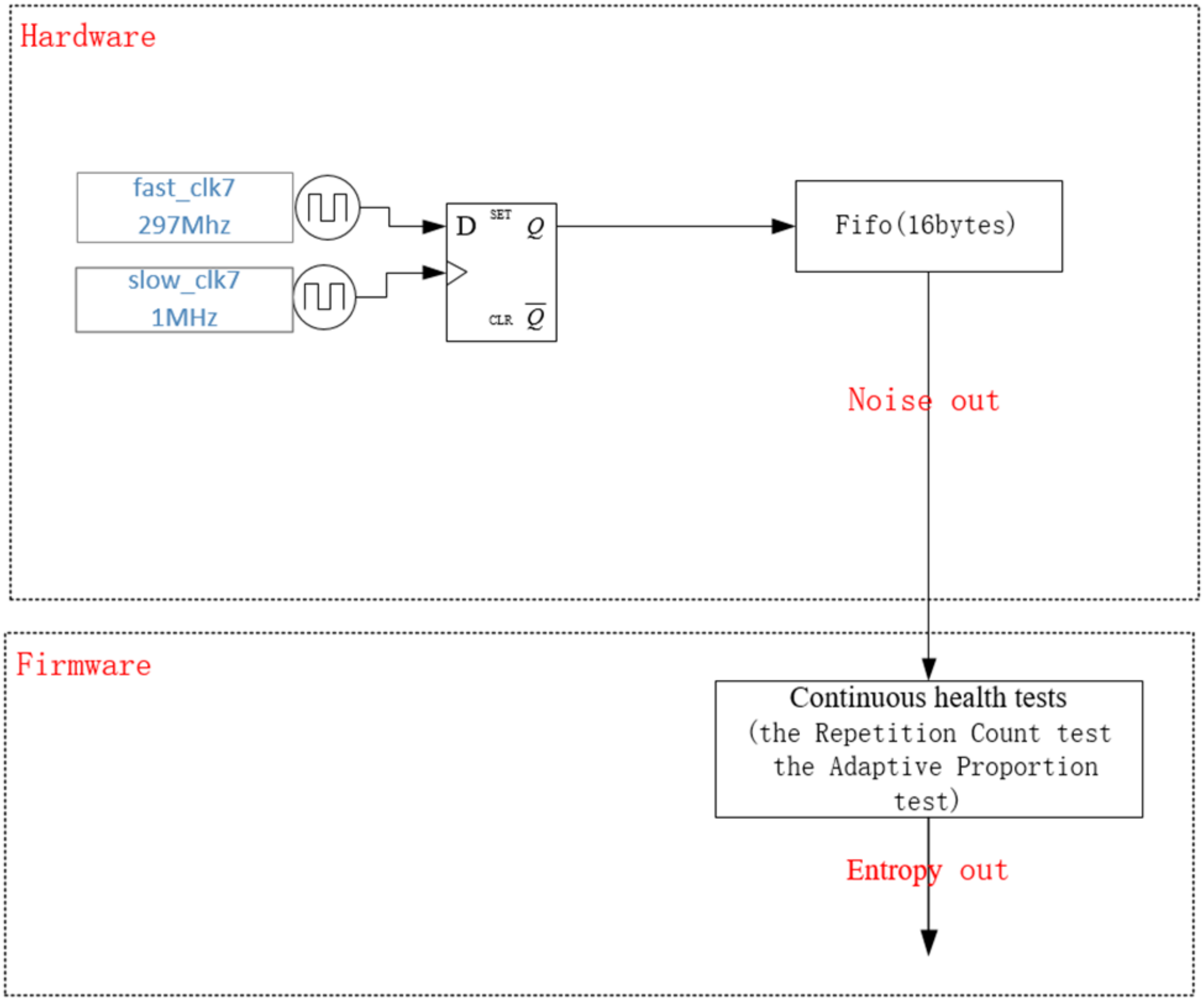

Figure 1: mToken CryptoID Entropy Source

3 Operating Conditions

The entropy-relevant operating conditions for all entropy source variants listed in Table 1 are given in Table 2.

Table 2: Entropy-Relevant Operating Conditions

Parameter	Value
Temperature	-45°C to 90°C
Voltage	2.4V to 6.1V

4 Configuration Settings

The Longmai mToken CryptoID Entropy Source does not require configuration of entropy-relevant parameters. However, the use of the Longmai mToken CryptoID Entropy Source to seed SP 800-90A compliant DRBGs is expected to adhere to the recommendations of Sections 6 and 7 of this document.

5 Physical Security Mechanisms

The Longmai mToken CryptoID Entropy Source does not impose any physical security requirements beyond the nominal FIPS 140-3 requirements. Modules undergoing FIPS 140-3 validation that incorporate the Longmai mToken CryptoID Entropy Source into their boundary must fulfill the physical security requirements appropriate to the targeted module type and security level.

6 Conceptual Interfaces

The only available interface is DRBGNoiseEntropy. A minimum of 1 byte can be extracted from the interface at a time. If the minimum amount is not currently available, the requesting application must wait for a byte to become available.

7 Min-Entropy Rate

Table 3 summarizes the results of the entropy assessment performed for the output of the Longmai mToken CryptoID Entropy Source.

Table 3: Min Entropy Per 1-bit Raw Output

Min Entropy
0.222745

If the output of this entropy source is used to seed a compliant DRBG, then the seeding requirements summarized in Table 4 must be met.

Table 4: Seeding Requirements for Security Strengths

DRBG Security Strength	1-bit Blocks Required (Nonce Provided)	Bytes Required (Nonce Provided)	1-bit Blocks Required (Random Nonce)	Bytes Required (Random Nonce)
112	503	63	755	95
128	575	72	862	108
192	862	108	1293	162
256	1150	144	1724	216

8 Health Tests

The Longmai mToken CryptoID Entropy Source implements the following health tests:

- APT (Adaptive Proportion Test) and RCT (Repetition Count Test) are performed on start-up and as continuous tests.
- On-demand health tests are fulfilled by the start-up health tests triggered by a reset.

On start-up (as in its normal operating mode) data is made available only after start-up health tests pass. The start-up health tests are run on the first 1024 symbols; a failure of the start-up health tests causes an error condition, and no data is output. Samples used during start-up tests are discarded.

If a health test fails, the entropy source provides indication of the error, and must be reset in order to continue operation.

9 Maintenance

No maintenance is required.

10 Required Testing

An end user can confirm that the noise source is working by gathering a sample set of 1,000,000 1-bit samples (125,000 bytes) from the entropy source (which is raw data) in a file we'll call `required-testing.bin`. The most straightforward way to assess this data is using the NIST `ea_non_iid` tool in its conditioning mode. Such a command is as follows:

```
ea_non_iid -c -a -vv required-testing.bin 8
```

If the assessed entropy is less than 6, then this result is inconsistent with the analysis present in the current entropy assessment.