SP 800-90B Non-Proprietary Public Use Document

TC58NC1142GTC-0001 Entropy Source

Document Version 1.0.0

Hardware Version: 0001
Firmware Version: EntropyDriver-a2d29b37

KIOXIA Corporation
1-21, Shibaura 3-chome
Minato-ku, Tokyo 108-0023
Japan

12 23, 2025

Revision History

Version	Change
1.0.0	first version

Table of Contents

Description 4
Security Boundary 4
Operating Conditions 5
Configuration Settings 5
Physical Security Mechanisms 5
Conceptual Interfaces 5
Min-Entropy Rate 6
Health Tests 6
Maintenance 6
Required Testing 6
User Verification 6
Vendor Permissions and Relationship 7

Description

TC58NC1142GTC-0001 Entropy Source(Hardware Version: 0001, Firmware Version: a2d29b37) is consist of a hardware component for physical noise source and a firmware component for health tests. The physical noise source is consist of a fast ring oscillator and a slow ring oscillator which provides with no conditioned raw data. TC58NC1142GTC-0001 is a controller embedded in a Solid State Drive (SSD) and has a module that provide various security functions including random number generation (TC58NC1142GTC CRPT module). The entropy source was tested by collecting data from multiple process, voltage, and temperature (PVT) operational conditions from implementation on a silicon substrate. The hardware noise source is claimed to produce non-IID outputs. Health tests are executed by firmware component of the TC58NC1142GTC CRPT module which is loaded into the module. The firmware component provides the entropy output which passed the health tests to the DRBG algorithm. TC58NC1142GTC-0001 Entropy Source is used embedded in SSDs and is not intended to be implemented in any other execution environment. TC58NC1142GTC-0001 Entropy Source is designed to compliant to the SP 800-90B(January 2018) and the FIPS 140-3 IG(April 18, 2025).

Security Boundary

Block diagram of the entropy source is shown below.

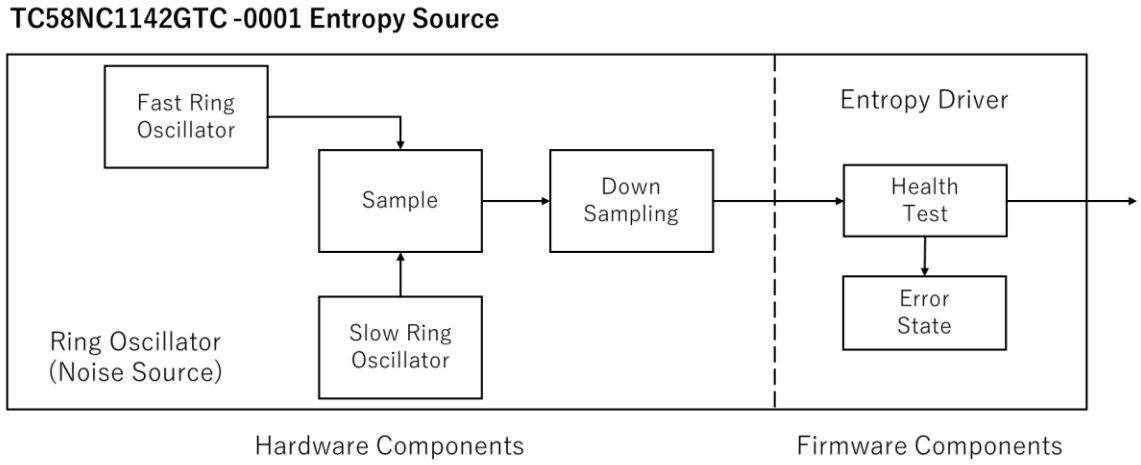


Figure 1. Block diagram of the Hardware Noise Source + Firmware components

The security boundary includes Hardware components such as ring oscillators and registers, as well as Firmware component which perform health tests in accordance with SP800-90B and access registers to change configuration (Entropy Driver). Direct access to the entropy source is only permitted to the firmware of the TC58NC1142GTC CRPT module.
The fast ring oscillator and the slow ring oscillator are standalone and oscillate independently. The rising edge of slow ring oscillator is used to randomly sample the fast ring oscillator, whose samples are the random number source output, and the sampled result is reduced by Down Sampling block.

The sampling data is input directly into the firmware components of Health test, which means that the Health tests is performed to the entropy output sampled from a ring oscillator which is not conditioned.

Operating Conditions

The entropy source was tested under several different PVT corners. Table 1 shows the environmental conditions range within which the entropy source operate correctly is guaranteed.

Table 1. Operational Conditions

Parameter	Condition	Description
Temperature (C)	Min: 0, Typical: 25, Max: 80	Composite temperature - reported by the SMART of the embedded SSD
Voltage (V)	Min: 0.72, Typical: 0.80, Max: 0.88	Operating voltage

Configuration Settings

TC58NC1142GTC-0001 Entropy Source does not require configuration of entropy-relevant parameters.

Physical Security Mechanisms

The entropy source is hardware implemented to the TC58NC1142GTC CRPT module. This module is enclosed in a single chip that is covered with opaque package which is used standard passivation techniques. Physical access to the internal components is impossible without forcing the package to open. In this case, it can be confirmed package damage as a tamper-evidence.

Conceptual Interfaces

In the Entropy Source, entropy output acquisition is performed at module's startup or random number generation (only when a reseeding is required). At these timings, the module's firmware requests entropy output (GetEntropy) and the Entropy Source stores the sampled data in the Data Out Reg (GetNoise). The firmware obtains these data up to 1024 bits for running the Health Tests. Entropy output is export to the firmware implemented DRBG algorithm, only if the Health Tests are passed.

Min-Entropy Rate

The Entropy Source provides 0.65 bit of entropy per 1 bit.

Health Tests

Table 3. Health Tests execution

Health tests Type	Testing condition
Start-up	Module's power-on
Continuous	Required to reseed from DRBG algorithm
On-demand	Any Module's power-off and reboot

When Health Tests are failed, the Entropy Source reports the error to the TC58NC1142GTC CRPT module. The module receiving the result will transition to error state and cannot execute any security relevant command including entropy output acquisition. To recover from the error state, the module needs to be rebooted and pass the Health Tests to be performed again.

Maintenance

No maintenance requirements for the entropy source.

Required Testing

TC58NC1142GTC-0001 Entropy Source has been tested for case of continuous sampling and case of sampling across the module restarts to confirm an entropy rate must be near equal to or the defined min-entropy. In these tests, special test command is used to obtain entropy output that would normally be input to firmware implemented DRBG algorithm. An obtained entropy output data is processed with the SP800-90B tool and calculated Min-Entropy rate. Moreover, in the restart sampling case the sanity test which confirm the restart sampling data is not be less than half of the entropy rate from continuous one is also performed.

User Verification

The module has the interface to get raw data in the Data Out Reg (GetNoise) but does not have the interface to modify proper configuration of entropy source. So, the module's developer relies on the health test described in "Health Tests" to detect anomaly of entropy source.

Vendor Permissions and Relationship

TC58NC1142GTC-0001 Entropy Source is “Reuse restricted to vendor”.