TOSHIBA

SP 800-90B Non-Proprietary Public Use Document

Toshiba Hardware Security Module Entropy Source

Hardware Version : 3.21

Document Version : 1.3
Release Date : August 19, 2026

Prepared for: Toshiba Corporation

TOSHIBA

Table of Contents

Description 3

Security Boundary 3

Operating Conditions 4

Configuration Settings 4

Physical Security Mechanisms 4

Conceptual Interfaces 5

Min-Entropy Rate 5

Health Tests 5

Maintenance 6

User Verification 6

Vendor Permissions and Relationship 6

Description

The Toshiba Hardware Security Module Entropy Source is a physical entropy source implemented in a multi-chip embedded Hardware Security Module (HSM).
The entropy source is entirely composed of circuits within the SoC (SoC FPGA) mounted on the HSM.

Table 1 Version identifier

Identifier	Version
Standard Version	NIST SP 800-90B (January 2018)
Applied IG	FIPS 140-3 IG 2026/4/16 D.J, D.K
Entropy Category	Physical (P)
Hardware Version	3.21
platform	XCZU15EG

The entropy source does not use firmware.
Users of the HSM cannot modify the operational configuration of the entropy source.
The output of the entropy source is classified as non-independent and identically distributed (non-IID).

Security Boundary

A block diagram of the entropy source is shown in Figure 1.
The noise source consists of a circuit in which the output of a high-speed oscillating ring oscillator is sampled by a flip-flop using a low-speed system clock within the SoC.
Eight noise sources are implemented, and their outputs form an 8-bit noise source output (raw data) that is input to the conditioning component.
The conditioning component generates a 1-bit Entropy Source Output, which is stored in a shift register.
In addition, the entropy source includes components that perform health tests on the 8-bit raw data and randomness tests on the Entropy Source Output.
All components of the entropy source consist of logic circuits located within the SoC security boundary.

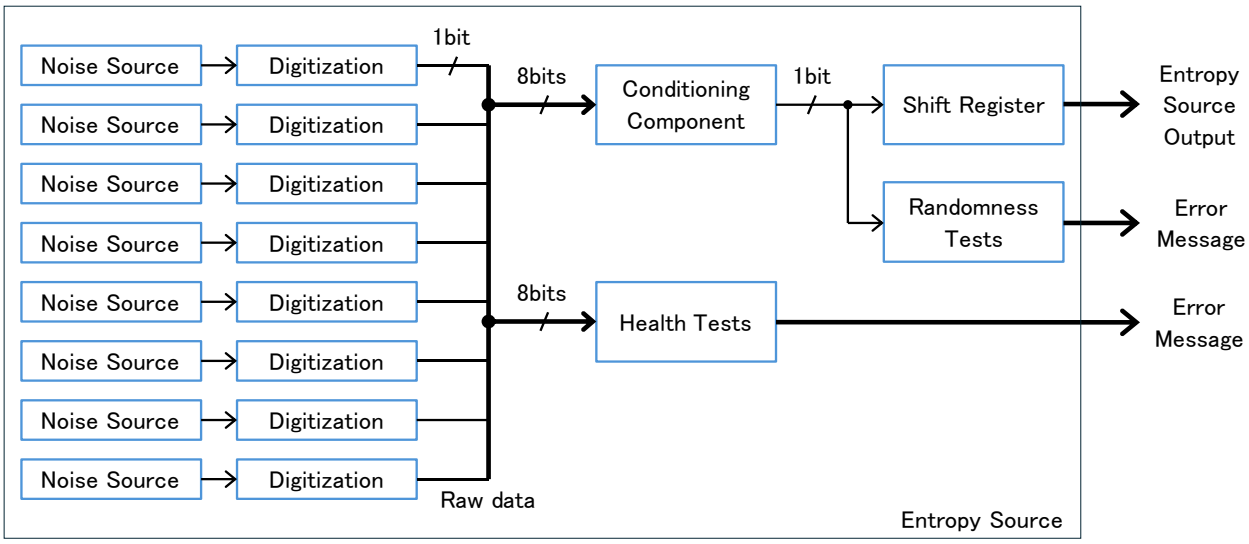


Figure 1 Entropy Source

Operating Conditions

Table 2 Operating conditions

Parameter	Condition	Description
Temperature (°C)	−30 - 80 °C	Operating temperature
Voltage (V)	11 – 13 V	Operating voltage PCIe input voltage supplied to the cryptographic module in which the SoC is mounted

Configuration Settings

There are no configuration settings that HSM users need to set for entropy source operation.

Physical Security Mechanisms

The entropy source is implemented within the SoC and is physically encapsulated in resin.
The module is robust and resistant to physical destruction; any attempt to destroy the module results in the cryptographic and random number generation functions within the SoC becoming non-operational.
The resin is opaque and sufficiently hard to prevent probing.

Conceptual Interfaces

The entropy source is implemented within the SoC, and the output of the entropy source cannot be obtained from outside the SoC.
The output of the entropy source is provided as input to the DRBG implemented within the SoC; therefore, users of the cryptographic module cannot access it directly.

Min-Entropy Rate

The min-entropy rate is derived from an evaluation performed in compliance with NIST SP 800-90B and is determined to be 0.822 per bit of Entropy Source Output.

Health Tests

RCT and APT, as defined in Section 4.4 of NIST SP 800-90B, are applied to the raw data.
The test conditions are summarized in Table 3.

Table 3 Health test

	RCT	APT
Symbol size (k)	8 bits	8 bits
Number of samples under test (W)	1024 samples	512 samples
Entropy estimate (H)	5.0	5.0
False positive rate (α)	2^{-30}	2^{-20}
Number of test executions per 1,024-bit Entropy Source Output generation	4	8

For the Entropy Source Output, the Repetition Count Test (RCT) and Adaptive Proportion Test (APT) specified in Section 4.4 of NIST SP 800-90B, as well as the Online Test exemplified in Section 5.5.1 of AIS20/31 (Version 2.0, September 18, 2011), are performed.
These three tests are used as randomness tests to strengthen the health testing of the entropy source.
The test conditions are shown in Table 4.

Table 4 Randomness test

	RCT	APT	Online Test
Symbol size (k)	1 bit	1 bit	1 bit
Number of samples under test (W)	1024 samples	1024 samples	128 samples
Entropy estimate (H)	1.0	1.0	—
False positive rate (α)	2^{-29}	2^{-20}	3.8×10^{-7}
Number of test executions per 1,024-bit Entropy Source Output generation	1	1	8

Upon detection of a failure in either the health tests or the randomness tests, the entropy source retries the generation of the 1,024-bit Entropy Source Output.
A maximum of three consecutive retries is allowed.
If a failure is detected during the third retry, the entropy source ceases Entropy Source Output generation and issues an error message.

Maintenance

No maintenance is required for the entropy source.

User Verification

The entropy source is tested in accordance with NIST SP 800-90B.
Test data is collected via a dedicated test interface.
This dedicated test interface is not available during normal operation and enables the detection of anomalies through health tests.
No additional testing is required.

Vendor Permissions and Relationship

Reuse restricted to vendor.