FEITIAN Technologies Co., Ltd.

HSEC_ES Entropy Source

ESV Public Use Document

Document Version 1.0

January 18, 2024

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 information required for the NIST Entropy Source Validation (ESV) program.

This evaluation was performed using the data and parameters measured in the evaluation version and configuration described in Table 1.

Table 1*: *Evaluated Entropy Source Specification

Identifier	Description
Entropy Source Name	HSEC_ES
Hardware Revision	V1.0
Firmware version	V1.0
Entropy Category	Physical (P)
Entropy Estimation Track (per SP 800-90B §3.1.2)	Non-IID

2. Security Boundary

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 of the following:

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

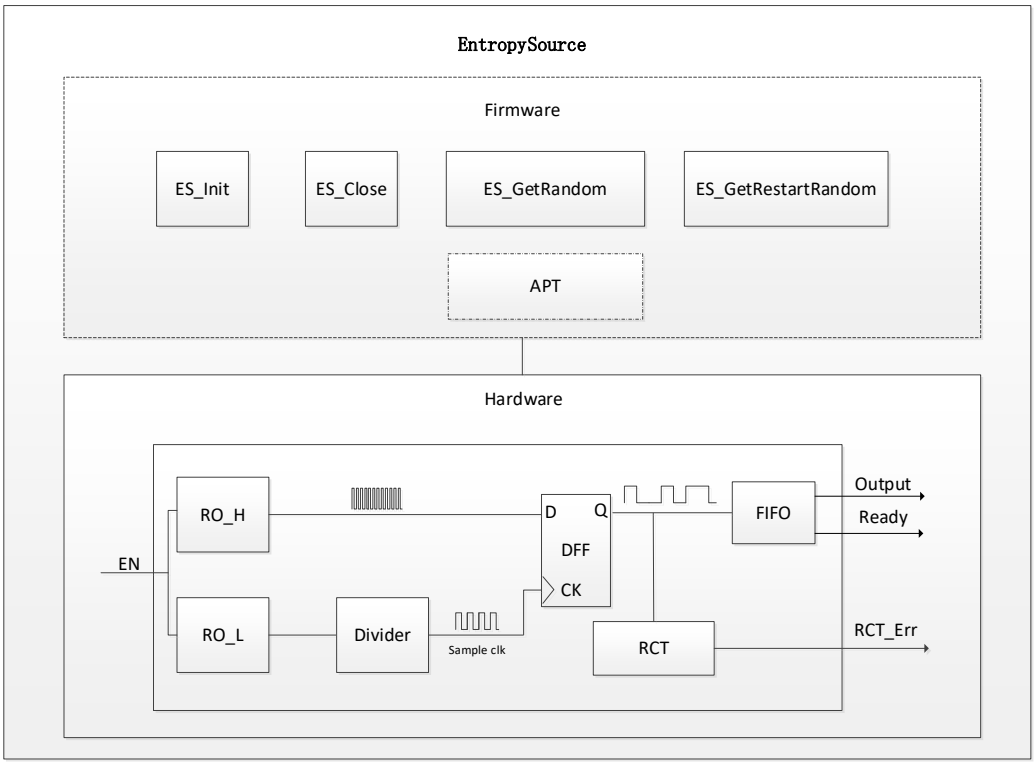

Figure 1. Entropy Source

3. Operating Conditions

The operating conditions of the entropy source are shown in Table 2.

Table 2: Entropy-Relevant Parameters

Parameter	Value	Description
Temperature	-40℃ ~ 85 ℃	Normal operating temperature range.
Voltage	2.8V ~ 5.5V	Normal operating voltage range.

4. Configuration Settings

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

5. Physical Security Mechanisms

The HSEC_ES 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 HSEC_ES Entropy Source into their boundary must fulfill the physical security requirements appropriate to the targeted module type and security level.

6. Conceptual Interfaces

Four functions are available to interface with the entropy source providing the capability to retrieve entropy data, enable and disable the device, and retrieve data suitable for testing under SP 800-90B requirements.

- The “ES_GetRandom“ function is used for obtaining the random number output from the entropy source.
- The “GetEntropy” call returns requested data in groups of words, with one word being 32 bits. The minimum unit of random number output by this interface is 1 word.
- The ES_Init function is used to enable the entropy source while the ES_close function disables the source.
- The ES_GetRestartRandom collects data suitable for testing restart formatted data following SP 800-90B.

7. Min-Entropy Rate

Min-entropy rate for the output of the entropy source is a per bit entropy rate for raw digitized data.

Table 3 summarizes the results of the entropy assessment performed for the output of the HSEC_ES Entropy Source.

Table 3: Min Entropy Per 1-bit Raw Output

Hmin (bits/bit)
0.3308

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

Table 4: Seeding Requirements for Security Strengths

DRBG Security Strength (bits)	Blocks Required (Nonce Provided)	Blocks Required (Random Nonce)
112	339	508
128	387	581
192	581	871
256	774	1161

8. Health Tests

The HSEC_ES Entropy Source implements the following categories of health tests:

- Start-up
- On-demand
- Continuous

All health test categories include the use of the approved SP 800-90B continuous tests the RCT and APT. Start-up and on-demand tests are performed by calling the ES_Init function. Calls for data from the device run the continuous health tests on all data before samples are provided by the device.

The startup health test is executed immediately after the startup of the entropy source. The start-up health tests are run on the first 1024 samples(bits) produced by the source; samples used during start-up health tests are discarded regardless of health tests results. If the start-up health tests fail, no random numbers are output, and the entropy source produces an error flag.

9. Maintenance

No maintenance is required.

10. Required Testing

The HSEC_ES entropy source does not require any testing before operation. The entropy source has been assessed using the NIST SP 800-90B tool. This testing can be optionally duplicated by users of this source for further assurance of proper functionality.

The ES_GetRandom function call can be used to collect sequential data samples, in groupings of at least 1,000 to form a sample set of at least 1 million bits. After formatting the data to the requirements of the testing tool the ea_non_iid command can be used to test the sequential dataset. An entropy estimate of greater than 0.330805 should be achieved.

The ES_GetRestartRandom function can be used to collect restart data samples. This sample set will need to be formatted to the requirements of restart data structure and the testing tool. After formatting the data can be tested using the ea_restart command. An entropy estimate of greater than 0.330805 should be achieved.

If the assessed entropy is less than 0.330805, then this result is inconsistent with the analysis present in the current entropy assessment.

11. Vendor Permissions and Relationship

This source has been submitted as reuse restricted to vendor.