



SP 800-90B Non-Proprietary Public Use Document

Capri ASIC Entropy Source with EP11 CLIC

Hardware Version/Part Number: 02WP146, 02WP147

Firmware Version:

**df9ba5c427b0156e60154cb256532cdc3b4555d711cc543
cdd78eae7a87d84ce**

Document Version: 1.1

Document Date: 2026-08-27

Prepared by:

atsec information security Corporation
4516 Seton Center Pkwy, Suite 250
Austin, TX 78759, USA

Prepared for:

IBM
2455 South Rd
Poughkeepsie, NY 12601, USA

Table of Contents

1.	Description	3
2.	Security Boundary	3
3.	Operating Conditions	4
4.	Configuration Settings	4
5.	Physical Security Mechanisms	4
6.	Conceptual Interfaces	4
7.	Min-Entropy Rate	5
8.	Health Tests	5
9.	Maintenance	5
10.	User Verification	5
11.	Vendor Permissions and Relationship	6

1. Description

The Capri ASIC Entropy Source with EP11 CLIC is a physical entropy source comprising components listed in Table 1.

The entropy source embodiment is a multi-chip.

The creation of entropy in the noise source within this entropy source is based upon the principles of variations of the oscillating period of ring oscillators.

The entropy source meets all the requirements of SP 800-90B and the associated FIPS 140-3 IGs D.J, D.K., D.O. (as N/A).

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

Table 1: Entropy source and operational environment information.

Characteristic	Description
Vendor	IBM
Entropy source name	Capri ASIC Entropy Source with EP11 CLIC
Standard, IGs	SP800-90B (2018) IG D.J (2021-11-05) IG D.K (2026-04-16) IG D.O (2021-05-04): N/A
Entropy category	Physical (P)
Entropy source version	Hardware Versions/Part Numbers: 02WP146 and 02WP147 Firmware: df9ba5c427b0156e60154cb256532cdc3b4555d711cc543cdd78eae7a87d84ce
Operational environment	02WP146 Capri ASIC (IBM PowerPC 470) 02WP147 Capri ASIC (IBM PowerPC 470)
Embodiment and type	Multi-chip standalone, Hardware

The ASIC part number can be identified by invoking the Coprocessor Load Utility (CLU) in the module that uses the entropy source, or by consulting the documentation provided by the vendor to the customer with the proper mapping between module part number and ASIC part number. The noise source was tested under the assumption that its output is non-IID.

2. Security Boundary

Figure 1 shows the high-level design of the entropy source. The entropy source boundary is defined by the bold black box.

The entropy source consists of a noise source of 96 ring oscillators, the SP 800-90B health tests performed in the EP11 CLIC and a SHA2-512 vetted conditioning function implemented in the ASIC.

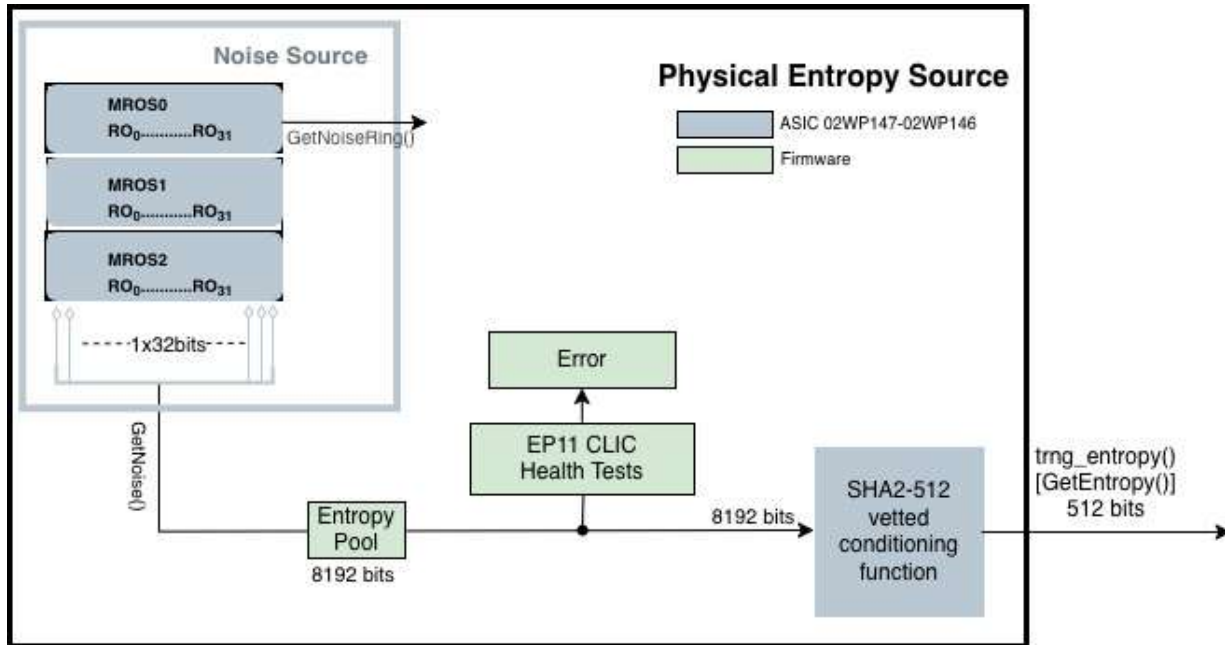


Figure 1: Block Diagram of the entropy source.

3. Operating Conditions

The ASIC operating temperature is in the 0°C to 78°C range.

The ASIC operating VDD is in the 0.833 V to 0.930 V range.

The operating conditions apply to all operational environments.

Within these operating condition ranges, the entropy source will operate normally.

4. Configuration Settings

There are no configuration settings for the entropy source that are available to the operator.

5. Physical Security Mechanisms

The physical security of the entropy source is provided by the module's physical security, in which the entropy source is implemented.

6. Conceptual Interfaces

The entropy source provides the following entropy interfaces as shown in Figure 1.

- interface available in production: `trng_entropy()` requests entropy from the entropy source and returns status from the entropy source and result code from the call.
- interfaces are only enabled by the vendor for testing purposed and are not available by the operator of the entropy source:
- `GetNoiseRing()` collects noise data directly from each MROS.
- `GetNoise()` collects noise data directly from the output of the noise source, which is the XOR of the MROS units.

The `trng_entropy()` interface returns codes (Table 2) to indicate whether the request for entropy was successful, and error status codes otherwise, also depending on the the test being performed at the moment.

Table 2: Return codes.

Return Code Macro	Return Code Value	Reason	Entropy Source Behavior
### APT Fail ###	-2	Adaptive Proportion Test Limit hit	Immediate halt
### RCT Fail ###	-1	Repetition Count Test Limit hit	Immediate halt

7. Min-Entropy Rate

The entropy source provides an output of 512 bits with full entropy (1 bit/bit).

8. Health Tests

IBM has implemented the following continuous health tests in the EP11 CLIC firmware module component at restart (startup tests) and at runtime (continuous tests).

- Repetition Count Test conforming to SP 800-90B section 4.4.1.
 - Cutoff value $C = 21$.
- Adaptive Proportion test conforming to SP 800-90B section 4.4.2.
 - $W = 512$.
 - Cutoff value $C = 311$.

The noise source sample size is 8 bits for health test purposes.

The continuous health tests are applied to each new sample obtained from the noise source. Whenever a failure is detected during the health test, entropy data is not returned to the caller; instead, a failure code is returned to enable the caller to determine the reason for the failure (Table 2). The entropy source then behaves as indicated in Table 2 and will refuse new requests for entropy. Upon return of the failure code, the caller shall attempt to reset or reload the entropy source or return an error to its own operator.

Startup tests conduct the same set and parameters of the continuous health tests on 8 times the 8192 (65536 bits) bits of noise data. The data is discarded after the startup tests complete successfully.

On-demand health tests of the noise source may be performed by reloading the cryptographic module containing the entropy source, which results in the immediate execution of the start-up tests. Similarly, the data used for the on-demand health tests are discarded after successful completion.

9. Maintenance

There are no specific maintenance requirements.

10. User Verification

To test the entropy source, raw data samples is collected using a special characterization mode of the ASIC that allows access to the entropy samples via the enabled `GetNoise()`

interface, before the conditioning function. This configuration of the ASIC is only available to IBM and is not available to the customer.

Raw noise data samples consisting of at least 1,000,000 bits are collected at the source normal operating conditions. The samples are processed by the SP 800-90B entropy tool provided by NIST.

Restart data is collected at the noise source normal operating conditions 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.

The ASIC is not visually accessible by an operator. There is a label on top of the card with the card part number, and the vendor provides a mapping from that card part number to the ASIC part number within it.

11. Vendor Permissions and Relationship

This entropy source validation is classified as “Reuse restricted to vendor.”