SP 800-90B Non-Proprietary Public Use Document
Wavelogic 5e Encryption Modem
EIP-76 TRNG
Document Version 1.0

Ciena Corporation
7035 Ridge Road
Hanover, MD 21076
USA

April 12, 2023

Revision History

Version	Change
1.0	Initial version
1.1	Updated per first round of CMVP comments
1.2	Updated per second round of CMVP comments

Table of Contents

Description

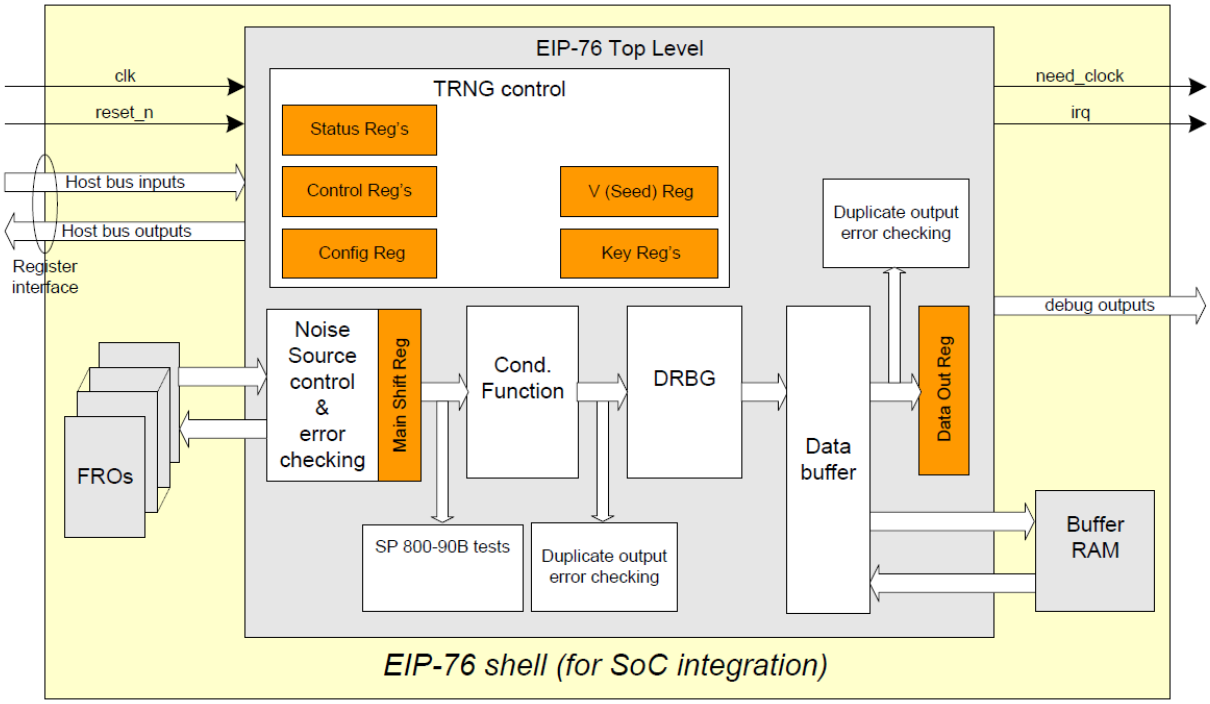
The EIP-76 TRNG is a physical (P) SP 800-90B compliant non-IID entropy source used in the Ciena Corporation WaveLogic 5 Extreme Encryption Modem module.

The entropy source has been tested on the following hardware platform:

Platform	Processor	H/W Version
WaveLogic 5 Extreme Encryption Modem	Ciena WL5e	174-0506-841 Hardware Version: 012 With Mech Kit 500-0506-020 Version 001. 174-0506-842 Hardware Version:012 With Mech Kit 500-0506-020 Version 001. 174-0506-843 Hardware Version 014 With Mech Kit 500-0506-020 Version 001. 174-0506-844 Hardware Version 007 With Mech Kit 500-0506-020 Version 001.

Security Boundary

The following figure depicts the security boundary of the EIP-76. The noise source within the entropy source is based on Free Ring Oscillators (FROs). The output of entropy source seeds a SP 800-90A DRBG.



Operating Conditions

The operating conditions under which the entropy source is claimed to operate correctly are:

Supply Voltage (V)	Min	Typical	Max
	0.56	0.6	0.62
Operating Temperature Range (°C)	Min	Typical	Max
	-20	85	105

Configuration Settings

Since the entropy source is pre-configured and used in the Ciena WaveLogic 5 Extreme Encryption Modem FIPS 140-3 hardware module, there are no configuration settings available to the end user.

Physical Security Mechanisms

The WaveLogic 5 Extreme Encryption Modem hardware module in which the entropy source resides meets the physical security requirements of FIPS 140-3 Level 2 through the usage of tamper detection seals.

Conceptual Interfaces

Since the entropy source is pre-configured and used in the Ciena WaveLogic 5 Extreme Encryption Modem FIPS 140-3 hardware module, there are no conceptual interfaces available

to the user. The following are conceptual interfaces per SP 800-90B and the equivalents provided by the entropy source:

SP 800-90B	EIP-76
GetNoise	By reading the TRNG_RAW_L and TRNG_RAW_H registers 64bits of captured data can be retrieved from the device.
HealthTest	Health tests are performed at startup of entropy source and are run continuously.

Min-Entropy Rate

The measured lower bound for the min entropy per bit, as given by the non-IID tests in SP800-90B for 1-bit symbols is 0.851246 and H_submitter = 0.5/bit or 4/8-bit symbol, thus the overall min entropy per bit = min (0.851246, 0.50) = 0.5/bit. The entropy source produces 256-bit output samples with full i.e., 256 bits of entropy.

Health Tests

SP 800-90B health tests are performed using the Adaptive Proportion Test (APT) and Repetition Count Test (RCT) and are run at startup and continuously under the normal operating conditions listed above. In case of a health test failure, the entropy source will enter a fatal error state and shutdown. The entropy source has also been designed with a developer defined health test to detect an additional failure. If all FROs are stopped, the noise source fails and the RCT and APT tests will detect this failure. Stopping of one or more FROs will deteriorate the noise source's performance but this may not be detected by the RCT or APT. Therefore, each FRO has a lock detector to monitor correct operation of the FRO and issue an alarm when this is not the case.

Maintenance

There are no maintenance requirements specific to the entropy source.

Required Testing

The target platform testing included gathering 1,000,000 raw data samples as well as 1,000 samples of raw data after each of 1,000 restarts. No additional testing is required. To verify that the entropy source is configured and operating correctly, the health tests can be initiated on demand. The tests can be run on-demand using the TRNG Test Register TRNG_TEST. Setting the bit [14] to '1' = Enable testing of the [SP 800-90B] 'Repetition Count' and 'Adaptive Proportion' tests by allowing the 'show_counters' and 'show_values' bits in the TRNG_SPB_TESTS register to be set non-zero. To perform Known Answer Tests on those functions, the 'test_known_noise' bit in this register must be set to '1' too.