SP 800-90B Non-Proprietary Public Use Document

Senetas TRNG Entropy Source

Hardware Version: 1.0
Firmware Version: 1.0

Senetas Security
312 Kings Way
South Melbourne, Vic 3205

Document Version 2.3

May 15, 2023

Revision History

Version	Change
2.0	Initial Draft
2.1	Second draft for ESV submission.
2.2	Final version for ESV submission.
2.3	Revised for CMVP comments.

Table of Contents

1. Description

The Senetas TRNG Entropy Source is a proprietary physical entropy source. The entropy source has been designed solely for use in the Senetas CN Series of Ethernet encryptors. Senetas makes no IID claim for the entropy source.

2. Operating Environments and Conditions

Table 1 summarizes the operating conditions for each of the tested platforms.

Platform	Processor	Clock Speed	Platform Temperature	Platform Voltage (AC)	FPGA
CN4010	ARM® Cortex A9	2.00GHz	0°C – 40°C	90V – 264V	Xilinx XC7Z020
CN4020	ARM® Cortex A9	2.00GHz	0°C – 40°C	90V – 264V	Xilinx XC7Z020
CN6010	ARM® Cortex A9	2.00GHz	0°C – 40°C	90V – 264V	Xilinx XC7Z020
CN6110	ARM® Cortex A9	2.00GHz	0°C – 40°C	90V – 264V	Xilinx XC7Z030
CN6140	ARM® Cortex A9	2.00GHz	0°C – 40°C	90V – 264V	Xilinx XC7Z045
CN9100	ARM® Cortex A9	2.00GHz	0°C – 40°C	90V – 264V	Xilinx XC7Z015
CN9120	ARM® Cortex A9	2.00GHz	0°C – 40°C	90V – 264V	Xilinx XC7Z015

Table 1 - Operating Environments and Conditions

3. Configuration Settings

There are no specific configuration settings for the entropy source.

4. Physical Security Mechanisms

The Senetas TRNG Entropy Source is enclosed entirely within the module’s cryptographic boundary which is protected by tamper evident seals, anti-probing barriers and electronic tamper detection and is assessed for FIPS level 3 Physical Security compliance. The noise source is further protected by physical RF shielding, electronic filtering on power supplies and constant temperature monitoring.

5. Min-Entropy Rate

The Senetas TRNG Entropy Source provides 256 bits of entropy per 256 bits of output or full entropy.

6. Health Tests

The NIST SP 800-90B (section 4) Repetition Count Test (RCT) and Adaptive Proportion Test (APT) health tests are run at start up and continuously during operation. In addition, the Senetas TRNG Entropy Source continuously runs a developer test to identify noise source hardware faults. If any of these tests fail persistently, the entropy source raises a critical error. The operator must reboot to attempt to correct the operation of the entropy source.

7. Maintenance

The Entropy Source does not require maintenance.

8. Required Testing

Validation testing was carried out on the Senetas TRNG Entropy Source in accordance with section 3 of SP 800-90B on data sets containing raw data samples, post non-vetted conditioning samples and restart samples.

To test the entropy source, raw data samples must be collected using a test harness capable of accessing the noise interface from the entropy source. The test harness and accessory kernel tools must be supplied by the vendor.

Raw noise data samples consisting of at least 1,000,000 bytes must be collected from the operational environment at its normal operating conditions and processed by the SP 800-90B entropy tool that is provided by NIST. The expected min-entropy rate must approach the one in Section 5.

Restart data must be collected at 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.

Conditioned entropy data samples consisting of at least 1,000,000 bytes must be collected at normal operating conditions from the output of the non-vetted conditioner and processed by the SP 800-90B entropy tool that is provided by NIST. The expected min-entropy rate must approach the one in Section 5.