Ultra Intelligence & Communications

Edge Security Module

SP 800-90B Non-Proprietary Public Use Document

Document Version: v1.1
Release Date: <December 15, 2023>

Prepared by:

<Ultra Intelligence & Communications>

<12410 Milestone Center Drive #650>

<Germantown, MD 20876>

<USA>

Change History

Version	Change Description	Date	Author
0.1	Initial draft	10-18-2023	M.Murphy
1.0	Certification submission	10-23-2023	M.Murphy
1.1	Updated PUB based on CMVP comment	12-15-2023	M.Murphy

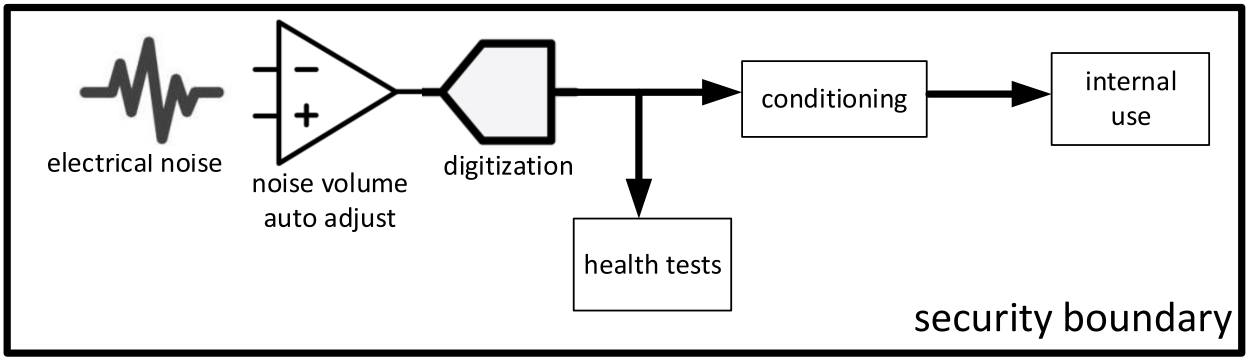
Table of Contents

1 Description

The Edge Security Module includes a physical entropy source, implemented as amplified and sampled electronic noise. The raw entropy samples are then fed through a NIST vetted conditioning algorithm (SHA2-256).

2 Security Boundary

The entropy hardware and sampling and conditioning software is entirely within the physical boundary of the Edge Security Module enclosure. The noise source is a dedicated circuit, not subject to other activity within the module, and shielded from variations in the external power input. The entropy is for internal use of the module in cryptographic operations; entropy alone is not provided as a service of the module, except for the purpose of certification testing. In normal operation, no access to the raw or conditioned entropy is permitted by the module.



3 Operating Conditions

The Edge Security Module is intended for use in a temperature range of -40C to +70C. The module is powered by a nominal 5 Volts DC, +/-5%.

4 Configuration Settings

The entropy source used in the Edge Security Module is not configurable.

5 Physical Security Mechanisms

The Edge Security Module has an opaque aluminum enclosure on 5 sides, with no entry points and tamper evidence security tape covering all fasteners. The module has exposed circuit board on the bottom face for the external interface, intended to plug into a larger system. The entropy circuit components reside on the inside face of the circuit board, and no electrical nets for this circuit are exposed on the outside face. The processor, memory, and flash memory are also entirely enclosed.

6 Conceptual Interfaces

The Edge Security Module has the SP 800-90B GetNoise and GetEntropy interfaces defined, but these are not accessible to the user in normal operation, as the module does not function as a stand-alone entropy service device. The GetNoise and GetEntropy interfaces are only exposed by special software build for certification testing.

The on-demand health test of the Edge Security Module occurs by any restart of the module to execute the startup health test. Thus, the HealthTest interface consists of any restart of the module, from the web user interface, the restart signal at the electrical interface, or a power cycle of the module.

7 Min-Entropy Rate

The Edge Security Module entropy source provides min-entropy rate of 6.638 bits per entropy sample with the sample Size: 8 bits.

The min-entropy rate at the output of the entropy source for the output of the conditioning function per section 3.1.5 of SP800-90B, is 256 bits per 256-bit output sample.

8 Health Tests

The startup self-test for the Edge Security Module entropy circuit draws and discards a set of samples, checks the raw noise signal variance, and adjusts the circuit. After this process a additional sample set is drawn for the test, and the mean and variance values are verified to be within acceptable limits.

The Edge Security Module performs the Repetition Count Test and Adaptive Proportion Test, as defined in SP 800-90B, on all entropy samples used after the completion of the startup testing. The probability of a false positive in the Repetition Count Test is approximately $2^{-39.8}$. The probability of a false positive in the Adaptive Proportion Test is approximately 2^{-29}.

9 Maintenance

The entropy circuit is self-adjusted to optimize the raw noise signal during any startup of the Edge Security Module. The user does not perform any other maintenance.

10 Required Testing

For certification, test data was collected from multiple samples of the Edge Security Module, including at the operating temperature limits. The sample data sets were processed by the SP 800-90B software non-iid test and restarts test. The startup and continuous health tests were also exercised and induced to fail to verify the fail state behavior of the module.

Verification of the entropy sources is also incorporated in the manufacturing test for the Edge Security Modules.

In the event of failure of the entropy source in the live operation continuous health testing, the event will be logged on the Edge Security Module, and the module will restart. If the module restarts successfully, the entropy error event will be accessible in the log, obtained from the module's web user interface. If the entropy source is completely inoperable, the module will not start operation, and instead provide the FIPS startup tests error indication output signal to the external interface. Should this occur, the module should be sent for repair or replaced. No other testing is required by the user.