SP 800-90B Non-Proprietary Public Use Document
Motorola Advanced
Crypto Engine (MACE) Entropy Source
Document Version 1.2
Firmware: R01.01.01 running on Hardware IC: 5185912

Motorola Solutions
March 26, 2024

Revision History

Version	Date	Change
V1.0	9/28/2023	Initial release
V1.1	11/21/2023	Updates after review
V1.2	03/26/2024	Updated Required Testing section to rely on health tests.

Table of Contents

Description

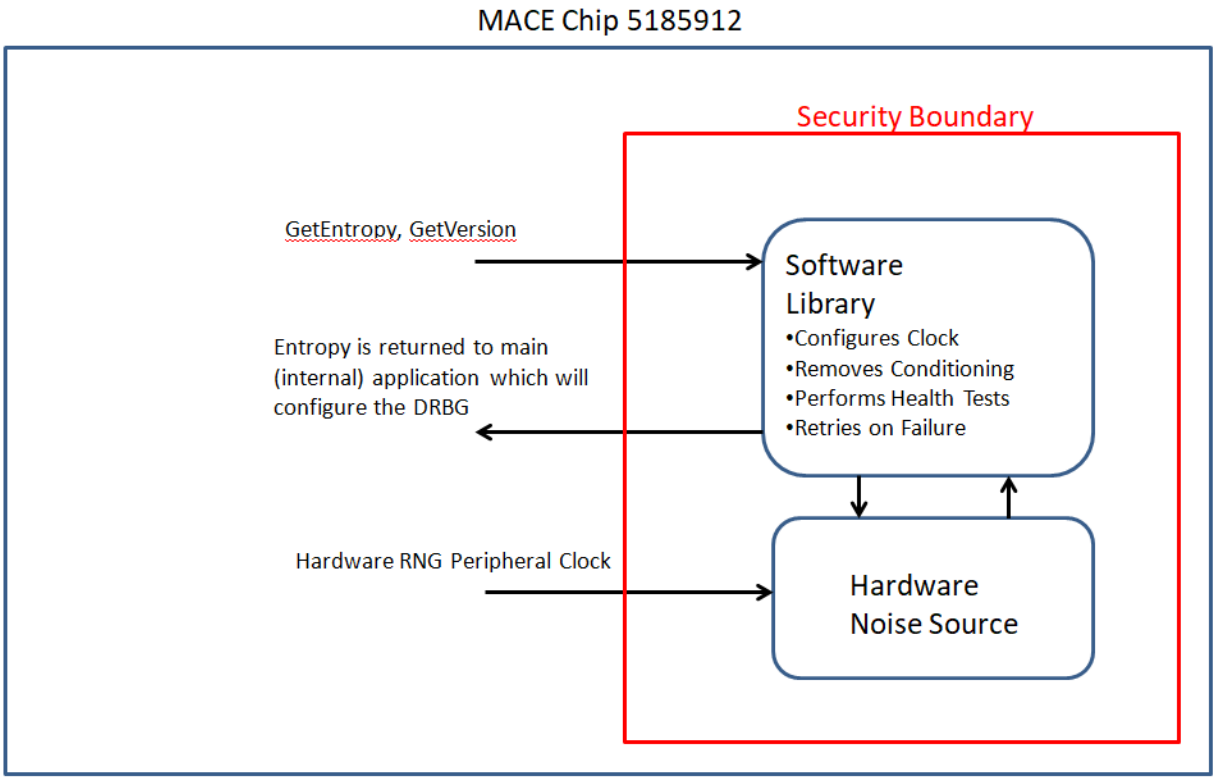
The Motorola Advanced Crypto Engine Entropy Source is a physical entropy source. It is designed to be compliant to the January 2018 version of the Special Publication 800-90B and the March 17th, 2023 version of the FIPS Implementation Guidance.

This entropy source is restricted to the vendor.

Security Boundary

The security boundary of the entropy source includes the hardware noise source as well as a software library that handles raw data collection and health testing.

The security boundary is shown below.



Operating Conditions

The entropy source operates correctly within the operation conditions shown in Table below.

Environmental Parameters	Operational Values	Description
Temperature	-38.1°C – 101.4°C	The expected entropy rate will be met or exceeded over this temperature range.
Voltage	1.65V – 2.03V	The expected entropy rate will be met or exceeded over this voltage range.

Configuration Settings

The Motorola Advanced Crypto Engine Entropy Source requires one configuration setting related to the frequency of the peripheral clock being provided to the hardware RNG. This is needed to properly configure the hardware RNG's internal clock such that it operates in the 100-200 kHz range. The configuration value is not persistent and is provided as part of the GetEntropy interface call.

Physical Security Mechanisms

The Motorola Advanced Crypto Engine Entropy Source is designed to meet FIPS 140-3 Level 3 Physical Security requirements.

The module is housed within the MACE 5185912 IC which is covered with a hard-opaque epoxy coating that provides evidence of attempts to tamper with the MACE.

Conceptual Interfaces

The user can access the following conceptual interfaces: GetEntropy, GetVersion.

Min-Entropy Rate

The Motorola Advanced Crypto Engine Entropy Source provides at least 0.138262 entropy per bit when operating within the defined operational limits.

This entropy source supports returning 1,024 – 65,536 continuous samples so that the user only has to call it once during device initialization to acquire the appropriate number of bits to initialize the DRBG for the required security strength.

Health Tests

The entropy source utilizes the Repetition Count Test and Adaptive Proportion Test as described in SP 800-90B. These tests are used for start-up and continuous testing. On demand testing is fulfilled by the start-up health tests triggered by a reset. The start-up health tests are run on the first 1024 raw samples. A failure of the start-up or continuous health tests causes a retry to occur. If three consecutive failures happen then the entropy source enters an error

condition and no data is output. Samples used during start-up are only available if all health tests pass.

In case of failure, the device can be power cycled to reinitiate the health tests.

Maintenance

The module does not support any entropy maintenance roles or services.

Required Testing

Built-in Health Tests described in the Health Tests section constantly check the validity of the noise source. No further testing is required.

Vendor Permissions and Relationship

The entropy source is restricted to the vendor.