SP 800-90B Non-Proprietary Public Use Document

ECC608 NRBG Entropy Source

V1.1.1

Microchip Technology Inc

1150 E. Cheyenne Mountain Rd.
Colorado Springs, CO 80906

September 11, 2023

Table of Contents

Revision History

Version	Date	Change
1.0.0	05/09/2023	Initial Release
1.1.0	06/22/2023	Inclusion of Operating Environments ATECC608B and ATECC608C
1.1.1	9/11/2023	Clarification that Entropy HI is the minimum NRBG entropy rate

Description

This document is a summary of the ECC608 product family NRBG Entropy Source function. For purposes of this documentation the NRBG entropy source is referred to as “ECC608 NRBG Entropy Source”. The “ECC608 NRBG Entropy Source” module v1.0.0, which has been implemented in the operating environment of the ATECC608A hardware device, has previously received ENT (P) status with no caveats for compliance to NIST specification SP800-90B and has been converted to ESV certification status.

This NRBG module complies with NIST specification SP800-90B January 2018. It has been developed for use within the Microchip ECC608 semiconductor device product family (identified as the operating environment for usage of this NRBG module) which also contains a complementary DRBG element with a Derivation Function frontend that complies with the NIST specification SP800-90A June 2015. “ECC608 NRBG Entropy Source” is included in all members of the Microchip ECC608 product family. ECC608 product family devices vary because of bug corrections or minor feature enhancements, predominantly through uCode changes in ROM memory or hardware configuration updates through fixed value settings. The “ECC608 NRBG Entropy Source” module is included in the operating environment identified as device ATECC608A. As of April 2023, the “ECC608 NRBG Entropy Source” V1.0.0 module is included in the operating environments identified as ATECC608A, ATECC608B and ATECC608C revisioned devices. All of these devices are manufactured in the same semiconductor process resulting in comparable performance statistics relative to entropy and compliance to SP800-90B.

The resultant minimum entropy rate of the NRBG noise source has been evaluated in accordance with SP800-90B to be 0.5071 per bit.

Based upon the DRBG function implemented in the ECC608 product family, the quantity of bits taken from the “ECC608 NRBG Entropy Source” module to seed the derivation function frontend of the complementary DRBG function is sufficient to guarantee that the entropy stream from the NRBG can dip as low as 33% and still guarantee a full entropy seed of 128-bits of security strength into the DRBG function. Health tests monitoring the NRBG bit stream will flag a drop in entropy at a level much higher than this, and the declared minimum entropy rate.

Security Boundary

The ECC608 product family RNG function is a simple construction of a single physical NRBG entropy source (“ECC608 NRBG Entropy Source”) directly connected to a mixed hardware and firmware DRBG function with firmware management. The security boundary of the “ECC608 NRBG Entropy Source” module includes analog circuitry to comprise the physical “Analog Noise Source” block followed by a “Digitization” function with digital logic to sample the resultant entropy bit stream along with digital logic for “Health Test” monitoring of the entropy bit stream and general configuration management. No conditioning component is included in the entropy source.

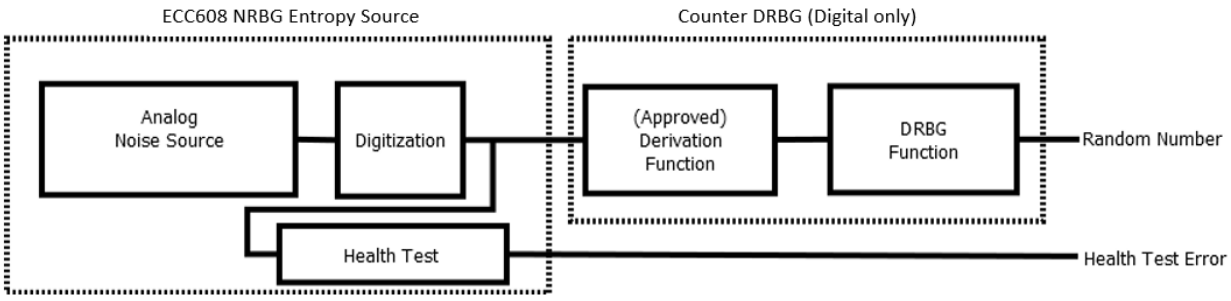

Figure 1-1: ECC608 RNG Function Block Diagram

The DRBG function pulls bits from the "ECC608 NRBG Entropy Source" entropy bit stream to instantiate the DRBG as well as to enhance the randomness during generate functions. This is managed by a derivation function (DF) frontend.

Operating Conditions

The "ECC608 NRBG Entropy Source" module is proven through theory and physical sampling to operate correctly within the designated operating environment defined by the hardware of the ECC608 product family currently including devices ATECC608A, ATECC608B and ATECC608C during all associated device activity. It is not intended for general usage in other operating environments. This device family functions across the environmental conditions; -40°C < T_A < 105°C and the supply voltage range 2.0V < Vcc < 5.5V.

Configuration Settings

Configuration settings for the "ECC608 NRBG Entropy Source" V1.0.0 module are set during the implementation of the operating environment in hardware or at Microchip manufacturing facilities during final product test. After leaving Microchip manufacturing facilities there are no configuration settings related to SP800-90B compliance of the "ECC608 NRBG Entropy Source" module that can be modified by Microchip or the end user of a device containing the "ECC608 NRBG Entropy Source" module.

All operating environments implemented around the "ECC608 NRBG Entropy Source" module must be manufactured in the same semiconductor process resulting in comparable performance statistics relative to entropy and compliance to SP800-90B.

1. There are configuration settings defined by hardware cells with fixed values (constants), or constants in ROM code that can be easily modified, for a specific implementation in the operating environment. These values may be changed for the operating environment implementation during hardware design but must be within the analysis range of the minimum entropy results. These **configuration settings are permanently defined in the hardware** surrounding the "ECC608 NRBG Entropy Source" module prior to initial device fabrication.

   The expected settings for these configurations related to the "ECC608 NRBG Entropy Source" V1.0.0 module are as follows:

a. The “ECC608 NRBG Entropy Source” module entropy bit stream sample size is defined by a hardware control register and is to be permanently set to a **sample size of 1 bit.**

b. The SP800-90B section 4.4.1 RCT and section 4.4.2 APT health tests have separate cutoff values for each implemented test. The cutoff values are to be permanently set by hardware constants to flag an error if the “ECC608 NRBG Entropy Source” entropy bit stream drops **lower than 75% entropy per bit** when the false positive rate is defined to be between 2^-20 and 2^-50. It is acceptable to configure the cutoff values to a higher (tighter) entropy minimum.

c. The health testing hardware enable control bit must be permanently set so **health tests will always run continuously** during normal operating modes, after device reset.

There are configuration settings defined by EEPROM code settings written during Microchip manufacturing device test operations. These values may be changed by the operating environment implementation during final manufacturing test but must be within the analysis range of the minimum entropy results. These configuration settings are defined to set hardware registers surrounding the “ECC608 NRBG Entropy Source” module to permanent constant values during final manufacturing configuration test.

The expected settings for these configurations related to the “ECC608 NRBG Entropy Source” V1.0.0 module are as follows:

d. The “ECC608 NRBG Entropy Source” module sample clock rate is defined by a hardware clock control register and is to be set at the Microchip manufacturing facility to be a ratio of the system clock that results in a nominal **sample clock being <= 200kHz range**.

There are no other designer selectable hardware settings prior to silicon manufacture or manufacture NVM configuration settings in the ECC608 product family that impact the “ECC608 NRBG Entropy Source” module.

The operating environment containing the “ECC608 NRBG Noise Source Module” V1.0.0 module can be identified through execution of the ECC608 product family member INFO command to identify the device revision (DevRev). The below table identifies ECC608 product family members and their corresponding DevRev response.

ECC608 Product Family Member	DevRev
ATECC608A	0x6002
ATECC608B	0x6003
ATECC608C	0x6005

Table 1-1 ECC608 Product Family Member Device Revision

Physical Security Mechanisms

Modules undergoing FIPS 140-3 validation that incorporate the “ECC608 NRBG Entropy Source” into their boundary must fulfill the physical security requirements appropriate to the targeted module type and security level.

Conceptual Interface

This section is N/A since the “ECC608 NRBG Entropy Source” module does not expose interfaces to the consuming application; the consuming application only has access to the output from the frontend complementary Counter DRBG from Figure 1-1.

Min-Entropy Rate

The minimum entropy rate of the “ECC608 NRBG Entropy Source” module output bit stream has been evaluated in accordance with SP800-90B to be 0.5071 per bit.

ECC608 Operating environments embedding the “ECC608 NRBG Entropy Source” V1.0.0 module are expected to contain a complementary DRBG function which is to include a derivation function frontend to receive sufficient bits from the “ECC608 NRBG Entropy Source” module to guarantee a full entropy seed of 128-bits of security strength into the DRBG module.

Health Tests

The “ECC608 NRBG Entropy Source” module is supported by the health tests defined in NIST SP800-90B; Repetition Count Test (RCT) and Adaptive Proportions Test (APT). These tests run one full cycle on initial power-up or wake from sleep before permitting usage of the output bit stream in cryptographic functions. Afterwards the tests run continuously while the device is awake. Users can trigger the restart of the initial health test cycle on-demand.

Should an error occur from the health testing at any time the “ECC608 NRBG Entropy Source” module alerts the operating environment via a hardware “Health Test Error” signal shown above in Figure 1-1, coming out of the module. The consuming operating environment in the ECC608 product family is expected to monitor this signal and perform the appropriate action relative to usage of the entropy bit stream.

See the associated “ECC608 OE NRBG Entropy Assessment Report” for further possible fault detection details.

Maintenance

There are no specific maintenance requirements for the user of the “ECC608 NRBG Entropy Source” V1.0.0 module. All ATECC608 family devices will go to a sleep state after a period of non-activity resulting in a future wake cycle that will re-instantiate the DRBG function with fresh entropy from the “ECC608 NRBG Entropy Source” module. If for some reason the device is not permitted to go to sleep, the DRBG function includes a reseed counter that will roll over after 2**32 generate functions forcing the DRBG to re-instantiate with fresh entropy from the “ECC608 NRBG Entropy Source” module.

Alternatively, the user can trigger an on-demand self-test of the RNG module at any time which will reset the reseed counter to 0, trigger a wait period for the completion of one full NRBG health test cycle and re-instantiate the DRBG with fresh entropy from the “ECC608 NRBG Entropy Source” module at the end of its testing, assuming a passing condition.

Required Testing

This section is N/A since the “ECC608 NRBG Entropy Source” module does not expose interfaces to the consuming application; the raw noise data is not available to the consuming application. The consuming application must rely on the status of Health Tests to understand if the entropy source is operating properly.

Vendor Permission and Relationship

Usage of the “ECC608 NRBG Entropy Source” V1.0.0 module encapsulated by a Microchip ECC608 product family operating environment, is not restricted to Microchip Technology Corp.

For more information on this topic, please contact Jim Hallman at jim.hallman@microchip.com.