SP 800-90B Non-Proprietary Public Use Document for Persistent Systems Wave Relay® Physical Entropy Source

Document Version: 0.3
Release Date: July 31, 2023
Hardware Version: NXP i.MX 6
Part Numbers: MCIMX6Q6AVT10A, MSCMMX6QZCK08A and MCIMX6Q7CZK08A

Prepared by:

PERSISTENT SYSTEMS

601 West 26th St. Suite 905
New York, NY 10001
www.persistentsystems. com

Template Revision History

Version	Date	Change
V0.1	06-28-2023	First draft
V0.2	07-26-2023	Second draft
V0.3	07-27-2023	Updated Description Table

Table of Contents

Description

This document describes the public use of the Persistent Systems Wave Relay® Physical Entropy Source (also called "Wave Relay® ES" in this document). Persistent Systems is using a physical free running ring oscillator to generate entropy input for instantiation and reseed of SP 800-90A compliant DRBGs in the Wave Relay® cryptographic kernel module and Wave Relay® cryptographic library module. The entropy source is the True Random Number Generator (TRNG) sub-component of an NXP i.MX6 SoC chip as seen in figure 1. The part numbers covered by this validation are MCIMX6Q6AVT10A, MSCMMX6QZCK08A and MCIMX6Q7CZK08A, which are different in terms of packaging, pin-count, operating voltage, manufacturing process and other IP outside of the entropy source.

Category	Description		
Part Number	MCIMX6Q6AVT10A	MSCMMX6QZCK08A	MCIMX6Q7CZK08A
Type	i.MX 6 SoC	SCM with i.MX 6 SoC + PMIC + FLASH	i.MX 6 SoC
Package	21 mm x 21 mm	14x17mm	12 mm x 12 mm
Pitch	0.8 mm	0.65mm	0.4mm
RAM Interface	External via bottom pins	Package on Package (PoP) via top pins	Package on Package (PoP) via top pins
Speed Grade	1000 MHz	800 MHz	800 MHz
Temperature Grade	-40 to +125C	-40 to +105C	-40 to +105C
Entropy Source Voltage	1.25V	1.175V	1.175V
Entropy Source System Clock	132 MHz	132 MHz	132 MHz
Entropy Category	Physical	Physical	Physical
Entropy Track	Non-IID	Non-IID	Non-IID

The design includes elements that correlate to the conceptual components contained within an SP 800-90B entropy source:

1) Analog Noise Source: Free-running Ring Oscillator
2) Digitization: Frequency Counter
3) Health Tests: Statistical Checker and Frequency Count Limit
4) Control Logic: Configuration, Sequencing, and Entropy Shifter

Security Boundary

The security boundary is the physical boundary of the chip itself. The following diagram is the physical block diagram:

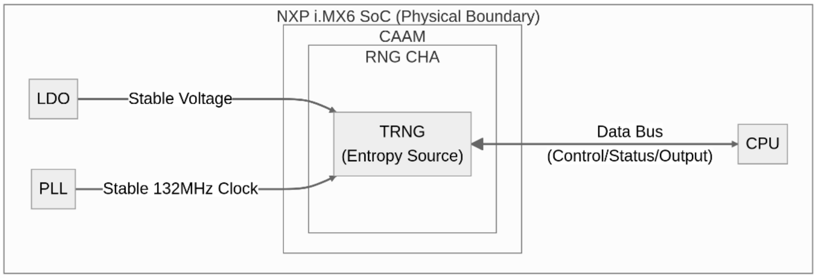

Figure 1. Wave Relay® Entropy Source – Physical Block Diagram

Operating Conditions

Parameter	Value	Description
Temperature	-40 to 80C	Operational temperature range
Entropy Source Voltage	1.175V to 1.25V	All HW variants have built-in voltage regulation, so noise source runs at a constant voltage. The voltage differs between the HW variants.
Entropy Source System Clock	132 MHz	The stable clock used for digital logic and as a time reference for Entropy Delay.

Configuration Settings

There are no configuration settings for the entropy source that are available to the operator.

Physical Security Mechanisms

The module is a single-chip embodiment. No additional operator actions are required to ensure that physical security is maintained. The physical security mechanisms include:

- Production Grade Components and production-grade opaque enclosure

Conceptual Interfaces

This section is N/A since the Wave Relay® System Physical Entropy Source does not expose interfaces to the consuming application; the consuming application only has access to the output from the DRBG.

Min-Entropy Rate

For this entropy source, $H_{\text{submitter}} = 0.824999 \, bits/bit$. The noise source sample size is 1 bit. The entropy source provides an output of 384 bits. This output provides 316 bits of entropy or 0.82 bit/bit of entropy.

Health Tests

The entropy source performs all required health tests of SP 800-90B, which includes continuous, start-up and on-demand health tests. All health tests are subject to $\alpha = 2^{-30}$.

The following continuous health tests are applied to each new 1024-bit sample block obtained from the noise source:

- Long Run Max Test – Developer Defined (Similar to Repetition Count Test)
- Monobit Test – Developer Defined (meets requirements of Adaptive Proportion Test)
- Run Length 1,2,3,4,5,6+ Test – Developer Defined
- Poker Test – Developer Defined
- Frequency Count Test – Developer Defined

The start-up test includes performing the continuous health tests on the first 1024-bit block.

The on-demand tests are the start-up tests and triggered by starting a generation sequence. Whenever a failure is detected during the health testing, entropy data is not returned to the caller; instead, a failure code is returned to enable the caller to determine the reason for the failure. The entropy source then halts and will refuse new requests for entropy. Upon return of the failure, the caller shall attempt to reset or reboot the entropy source. The entropy source will continue to operate after being reset and passing all start-up and continuous health tests.

Maintenance

There are no specific maintenance procedures for the entropy source outside of the ones required for the module to which the entropy source is bound.

Required Testing

This section is N/A since the Wave Relay® System Physical Entropy Source does not expose interfaces to the consuming application; the raw noise data is not available to the consuming application. Consuming applications must rely on the status of Health tests to understand if the entropy is operating properly.