SP 800-90B Non-Proprietary Public Use Document

nShield 5s Physical True Random Number Generator

Hardware Version:
Texas Instruments MSP430FR5969
Firmware Version:
1.0

Entrust
One Station Square
Cambridge, CB1 2GA
United Kingdom

Document Version 1.0
January 26, 2023

Revision History

Version	Change
1.0	First version for the Entrust TRNG v1.0 entropy source.

Table of Contents

Description 3

Operating Conditions 3

Configuration Settings 3

Physical Security Mechanisms 3

Min-Entropy Rate 3

Health Tests 3

Description

The nShield 5s Physical True Random Number Generator version 1.0 is a physical (P) entropy source built in the FIPS 140 Level 3 validated Entrust nShield Hardware Security Modules (HSMs). It is used as the basis for generating strong random bits for key generation and other uses within the HSM which require random bits.

Operating Conditions

The following table summarizes operating conditions.

Parameter	Value	Description
Temperature	-37°C to 82°C	The HSMs have EFP mechanisms which will trigger a tamper response if out of range temperature is detected.
Voltage	n/a	These values are enforced by the HSMs internal power circuitry and thus is not user controlled. The HSMs have EFP mechanisms which will trigger a tamper response if out of range voltage is detected.

Configuration Settings

There are no specific configuration settings for the entropy source.

Physical Security Mechanisms

The HSMs in which the entropy source is built in are validated to FIPS 140 Level 3 and provide an opaque enclosure consisting of an epoxy potting and an Environmental Failure Protection (EFP) mechanism.

Min-Entropy Rate

The nShield Physical True Random Number Generator entropy source provides 0.89 bits of min-entropy per output bit.

Health Tests

The NIST SP 800-90B Repetition Count Test (RCT) and Adaptive Proportion Test (APT) health tests are run at start up and continuously during operation. If either one of the tests fail, the entropy source raises a critical error. The operator must reboot to attempt to correct the operation of the RNG.