

SP800-90B Non-Proprietary Public Use Document Entropy Source of the JCOP 4.5 on P71D600 V1.0.0

Document Version 1.0

June 2024

Copyright 2024 NXP Semiconductors - may be reproduced only in its original entirety (without revision)

Table of Contents

1 Description 3
2 Security Boundary 4
3 Operating Conditions 5
4 Configuration Settings 5
5 Physical Security Mechanisms 5
6 Conceptual Interfaces 5
7 Min-Entropy Rate 5
8 Health Tests 5
9 Maintenance 5
10 Required Testing 5

NXP Semiconductors Public Material – may be reproduced only in its original entirety (without revision)

1 Description

This document describes the Entropy Source of the JCOP 4.5 on P71D600 product family. The entropy source (depicted in Figure 1) is implemented within the JCOP 4.5 on P71D600 Cryptographic Module and is composed of a few major sections which map to the conceptual components contained within an SP 800-90B entropy source; contains an entropy source which is composed of a noise source, health tests, and a conditioning component as shown in Figure 1 below.

The JCOP 4.5 on P71D600 cryptographic module is available under several commercial type names addressing the different market segments relevant for NXP, such as:

- JCOP 4.5 on P71D600
- JCOP ID 2 on P71D600
- SE052F
- NCJ37B0HN

This assessment was conducted using data and parameters measured in the evaluated version described In Table 1.

Table 1: Evaluated Entropy Source Specification

Identifier	Details
Entropy Source Name	Entropy Source of the JCOP 4.5 on P71D600
Part Numbers	P71D600 (N7122)
Hardware Revisions	N7122 A1 using ROM ID B3375FE9B5508BC4
Firmware Version	Platform ID J3R6000373181200 and ROM ID B3375FE9B5508BC4
Entropy Category	Physical (P)
Test Platform(s)	JCOP 4.5 on P71D600
Entropy Estimation Track (per SP 800-90B §3.1.2)	Non-IID

When used to seed an SP 800-90A DRBG, the seeding requirements listed in the table below must be met.

DRBG Security Strength	Samples Required to Instantiate (Nonce Provided)	Samples Required to Instantiate (Random Nonce)
128-bit	18 samples (144 bits)	27 samples (216 bits)
192-bit	27 samples (216 bits)	40 samples (320 bits)
256-bit	36 samples (288 bits)	53 samples (424 bits)

Copyright NXP Semiconductors 2024

NXP Semiconductors Public Material – may be reproduced only in its original entirety (without revision)

2 Security Boundary

The Entropy Source of the JCOP 4.5 on P71D600 is depicted in the block diagram below.

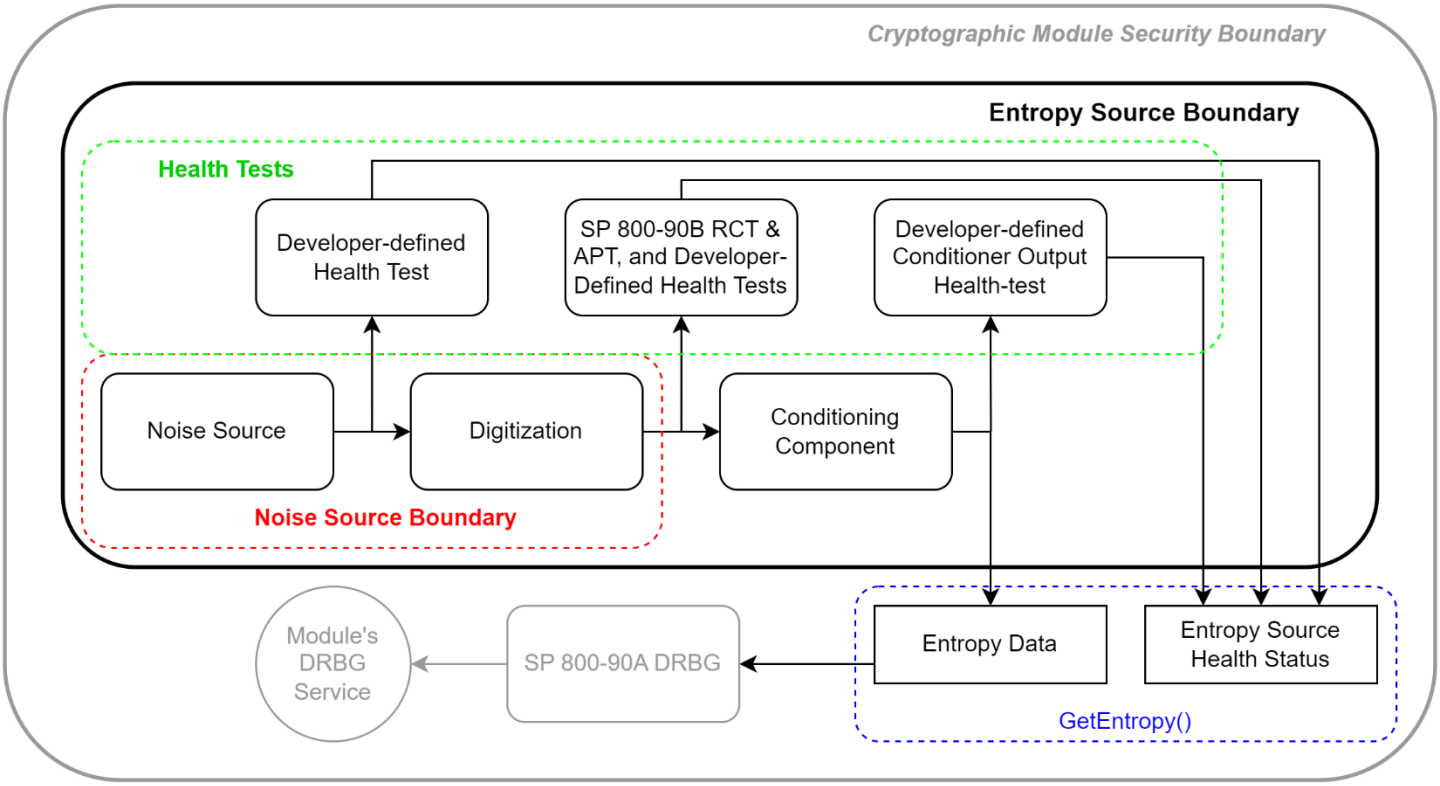


Figure 1: the entropy source fraction within the JCOP 4.5 on P71D600 –

The noise source is based on the repeated functional composition of a chaotic map. For the range of parameters that can arise in this implementation, this results in a 1-dimensional chaotic system.

Any bias and serial correlation present in the raw data is reduced by a conditioning algorithm which forms each bit of output using six time-shifted outputs from the noise sources for every bit produced. This conditioning algorithm takes in a total of 48 bits, and outputs 1 byte (8 bits).

Health testing occurs on both the raw data and on the conditioned data. If the results of the health tests are too far out of their expected range, then the health tests fail, and an error indicator is output.

Copyright NXP Semiconductors 2024

NXP Semiconductors Public Material – may be reproduced only in its original entirety (without revision)

3 Operating Conditions

The entropy-relevant operating conditions for all entropy source variants listed in Table 1 are given in Table 2.

Table 2: Entropy-Relevant Operating Conditions

Parameter	Value
Temperature	-60°C to 125°C

The internal voltage within this part is regulated, so variations in the input voltage are not expected to produce any significant change in behavior so long as the input voltage is within the allowed bounds. If the input voltage is out of the bounds for which this behavior cannot be assured, then the entropy source is disabled.

4 Configuration Settings

There are no configuration settings for the entropy source.

5 Physical Security Mechanisms

The Entropy Source of the JCOP 4.5 on P71D600 operates within a cryptographic module and inherits the physical protections of the module's SoC package. The physical protection mechanisms of the module's SoC cover the whole entropy source.

6 Conceptual Interfaces

The user of the entropy source is the module in which the entropy source is implemented. The module's software has access to the entropy output via a special function register. The abstracted GetEntropy() interface is defined to be the process in which the module accesses this SFR.

There is no direct access interface available to any user other than the module itself.

7 Min-Entropy Rate

The min-entropy rate for the Entropy Source of the JCOP 4.5 on P71D600 is 7.30359 bits/byte.

8 Health Tests

The entropy source continuously performs the RCT and APT defined within SP 800-90B on the output of its noise source. In addition, the entropy source performs developer-defined health tests on both raw data as well as conditioned data. The combined set of tests guarantee that the data used for instantiating and reseeding a DRBG is always healthy.

9 Maintenance

The Entropy Source of the JCOP 4.5 on P71D600 does not require maintenance.

10 Required Testing

The entropy source's health tests constantly check the validity of the produced output of the entropy source. Therefore, no further testing is required by the entropy source's user.

Copyright NXP Semiconductors 2024

NXP Semiconductors Public Material – may be reproduced only in its original entirety (without revision)