# SP 800-90B Non-Proprietary Public Use Document
# YDK QRNG Entropy Source
# Document Version: 1.0

YDK Co., Ltd.
1705, Oshitate, Inagi-shi, Tokyo, 206-0811
Japan

February 9, 2024

**Revision History**

| Version | Date | Change |
|---|---|---|
| V1.0 | February 9, 2024 | Initial release |

# Table of Contents


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

# 1. Description

YDK QRNG Entropy Source is a physical entropy source(P) based on quantum noise. It meets all requirements for IID compliance. The entropy source has been tested on yRNG-Q5G.

The yRNG-Q5G is a 19-inch 1U rack mounted high-speed random number generator that implements YDK QRNG Entropy Source. Maximum generation performance is 5Gbps. This product has an optical fiber interface based on IEEE802.3-2012 10Gigabit Ethernet standard. Random numbers can be transferred to servers, etc. at high speed.



**Figure 1 yRNG-Q5G overview**

**Table 1 Evaluated Entropy Source Specification**

| Identifier | Version |
|---|---|
| Entropy Source Name | YDK QRNG Entropy Source |
| Revision | 1.00 |
| Test Platform | yRNG-Q5G |
| Hardware version | 1.00 |
| Firmware version | 1.00 |
| FPGA version | 1.00 |

## 2. Security Boundary

YDK QRNG Entropy Source is depicted in block diagram below.

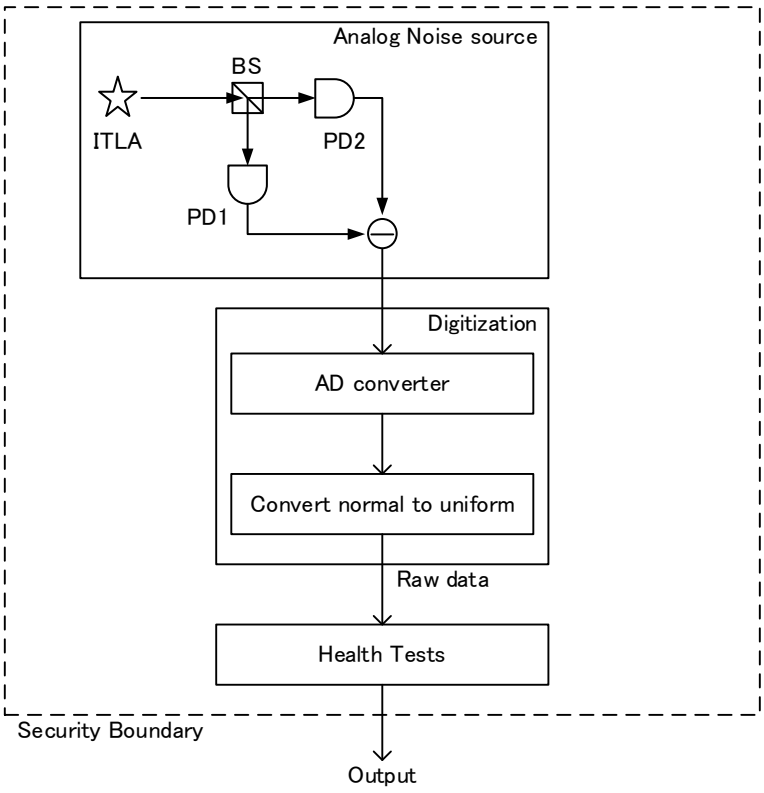



**Figure 2 Entropy Source Model**

## 3. Operating Conditions

Operating conditions are summarized in Table 2.

**Table 2 Operating Conditions**

| Parameter | Value |
|---|---|
| Temperature | 5 to 35°C |
| Voltage | 12V |

## 4. Configuration Settings

No setup required. When the power is turned on, it is automatically adjusted and starts generating random numbers.

## 5. Physical Security Mechanisms

As YDK QRNG Entropy Source, there is no physical security mechanism. However, equipment with this entropy source is protected by a steel casing.

## 6. Conceptual Interfaces

The output is provided to the caller from the entropy source via FIFO within the FPGA by the provided RTL wrapper.

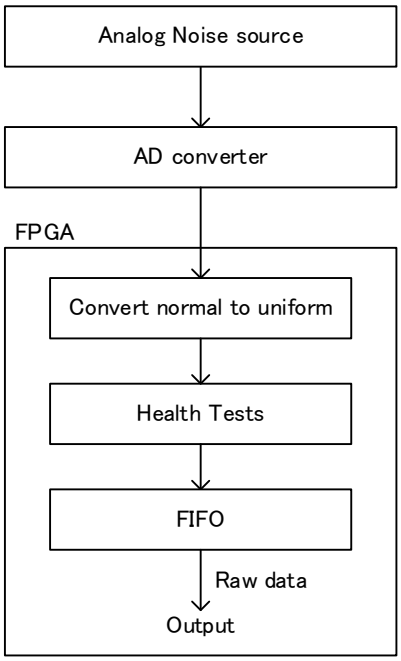



**Figure 3 Entropy Source Diagram**

## 7. Min-Entropy Rate

For a raw data symbol size of 3 bits, H_submitter = 2.95 bits per symbol.

## 8. Health Tests

YDK QRNG Entropy Source performs two health tests:

· Repetition Count Test
  Min-entropy $H$=3
  alpha value of $\alpha$=$2^{-31}$
  Cutoff value $C$=12

· Adaptive Proportion Test
  $W$=512
  Min-entropy $H$=3
  alpha value of $\alpha$=$2^{-31}$
  Cutoff value $C$=115

These tests are run at start up and then are run continuously during the operation of the entropy source. Health tests are implemented in FPGA logic and run on the raw data after it has been transformed into a uniform distribution. These tests comply with the requirements in section 4.4 of SP 800-90B.

If a health test fails, an error counter is set and can be checked with console commands.

## 9. Maintenance

There is no maintenance requirement.

## 10. Required Testing

Raw noise data can be obtained by operating a PC connected to the console port.