Classification: External

quadient

Quadient Postal Security Device SP 800-90B Public Use Document

Valid from:	02/15/2024
Version No.:	V 2.0

List of changes

Version	Date	Change
V1.0	12/20/23	Initial revision
V2.0	02/15/23	Added table of operating environments

Table of Contents

1. Description

The Quadient Postal Security Device Entropy Source is a physical (P) entropy source. It is certified under the January 2018 version of Special Publication 800-90B and the November 22, 2023 version of the FIPS Implementation Guidance.

Table 1 describes the evaluated version of the entropy source.

Model	Version
Quadient Postal Security Device Entropy Source	A0161460A

Table 1: Evaluated Version

Table 2 describes the operating environments on which the entropy source was tested.

Operating Environment
Quadient Postal Security Device (PSD)- Cesar
Quadient Postal Security Device (PSD) - Alcor

Table 2: Operating Environments

2. Security Boundary

The security boundary of the entropy source includes the digital noise source, the conditioning component, and the health tests which are performed on raw data. Figure 1 shows the security boundary of the entropy source, indicated in red.

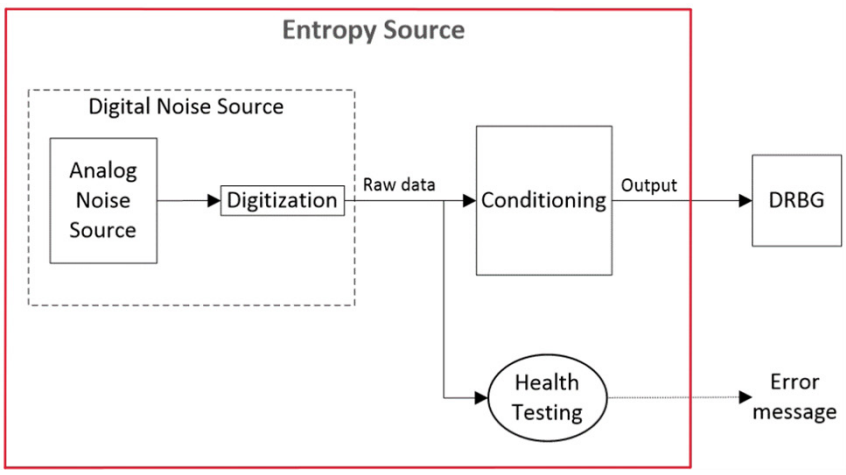

Figure 1: Entropy Source Block Diagram with Security Boundary

3. Operating Conditions

This section has been omitted, as the entropy source is restricted to the vendor.

4. Configuration Settings

There are no configuration or compilation settings that impact the entropy source.

5. Physical Security Mechanisms

This section has been omitted, as the entropy source is restricted to the vendor. Refer to the security policy for physical security mechanisms.

6. Conceptual Interfaces

A user can access the following conceptual interfaces: GetEntropy, HealthTest.

7. Min-Entropy Rate

The Quadient Entropy Source provides full entropy outputs.

8. Health Tests

The entropy source utilizes the Repetition Count Test (RCT) and Adaptive Proportion Test (APT) as described in SP 800-90B. The RCT and APT run both at start-up and continuously while the entropy source operates. To perform on-demand health testing, the user can restart the device.

If any health test detects an error, the entire device enters an error state where it can no longer perform cryptographic functions. The device must be power-cycled to recover from the error.

Anticipated failure modes include the entropy source becoming stuck, or the entropy rate degrading below the acceptable value. If the entropy source becomes stuck on a single value, it will be detected by the RCT. If the entropy rate degrades, it will change the ratio of symbols produced by the entropy source, and this failure will be detected by the APT.

There are no known failure modes which will not be detected by the RCT and APT.

9. Maintenance

The module does not support any entropy maintenance roles or services.

10. Required Testing

End users do not have access to raw data and must rely on the included health tests to detect any drops in entropy.