THALES

Building a future we can all trust

SP 800-90B Non-Proprietary Public Use Document CipherTrust Manager Core Security Module Entropy Source

FIRMWARE VERSION 1.0

Revision History

Version	Change
10 March 2023, Revision A	Initial release
16 March 2023, Revision B	Addressed internal comments
17 March 2023, Revision C	Error correction
21 March 2023, Revision D	Addressed lab comments

Table of Contents

1. Description

The SP800-90B compliant Entropy Source is the CipherTrust Manager Core Security Module Entropy Source version 1.0. It is a physical entropy source.

Entropy is provided using one of the following physical devices, either of which are able to act as the entropy source for the module:

- Intel® Xeon® E3-1275 v6 CPU; or
- Intel® Xeon® Gold 6252 CPU.

The entropy source is entirely embedded in the CPU hardware and can be considered independent of the software running.

Although both CPUs are derived from the Intel Skylake microarchitecture, the precise derivative microarchitectures are Kaby Lake and Cascade Lake, respectively. Any differences between the two devices are clearly indicated in the relevant sections in the remainder of this document.

This is a Non-IID source.

2. Security Boundary

The entropy source is contained entirely within the hardware internal to the target CPU.

Figure 2-1 presents the major components of the entropy source. This diagram is equally applicable to both the Intel® Xeon® E3-1275 v6 CPU and the Intel® Xeon® Gold 6252 CPU.

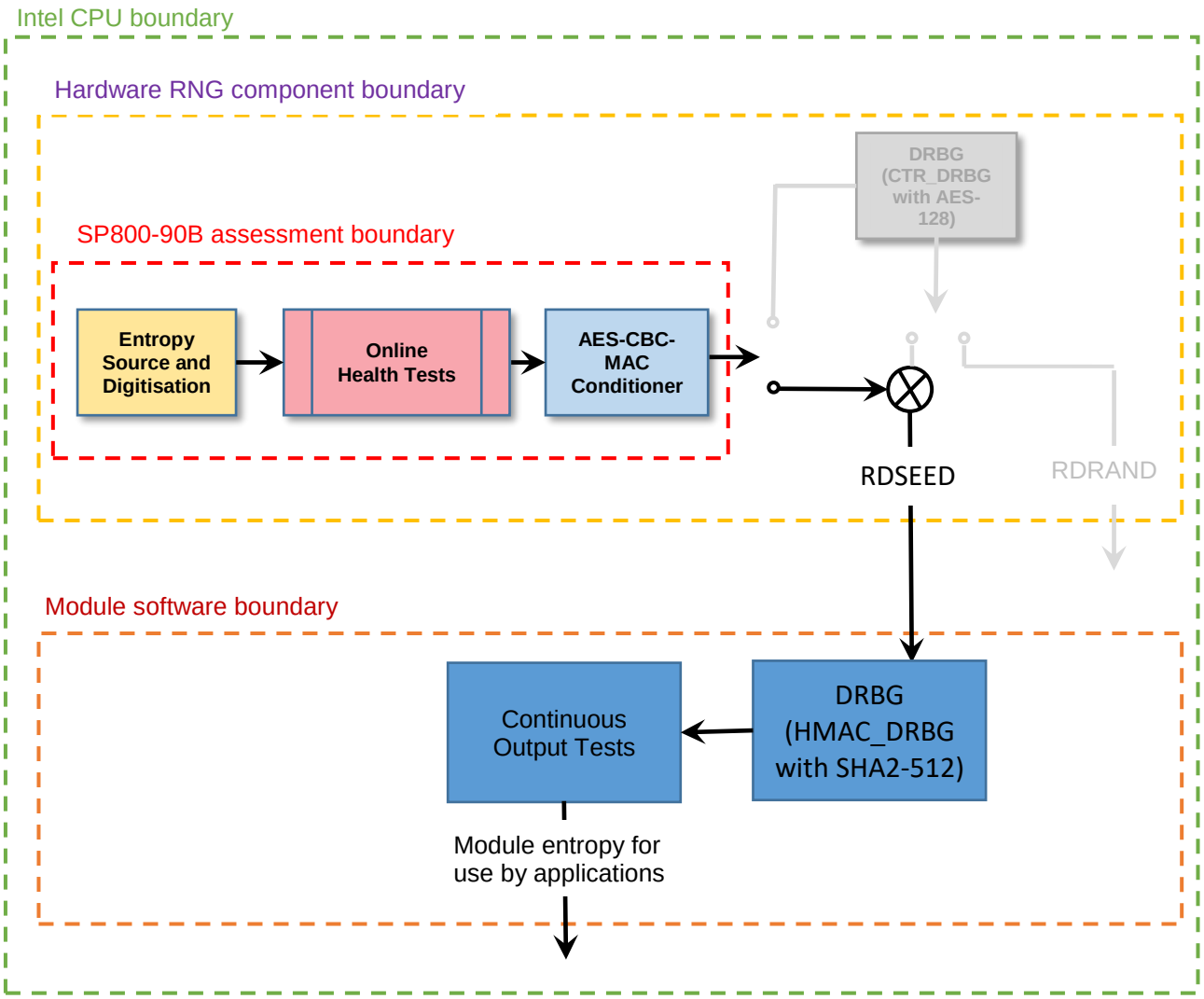

Figure 2-1: Entropy Source Components

3. Operating Conditions

The operating conditions for the entropy source are those applicable to the CPU, as noted in Table 3-1.

Table 3-1: Operating Conditions

CPU Property	Intel® Xeon® E3-1275	Intel® Xeon® Gold 6252
Minimum Operating Temperature	0° C	0° C
Maximum Operating Temperature	75° C	86° C
V_{core} Minimum	0.55 V	1.60 V
V_{core} Maximum	1.52 V	1.83 V

4. Configuration Settings

To place the cryptographic module into its approved mode of operation the Administrator must configure the entropy source to be used. This can be done by setting the source to be use the Intel® secure key RDSEED.

When selecting to use Intel® secure key RDSEED as the noise source, change the system entropy source to RDSEED using the command `kscfg system entropy-source -s RDSEED` followed by `kscfg system reset -y` to implement the change. This fixes RDSEED as the only noise source the module can use.

5. Physical Security Mechanisms

The CipherTrust Manager Core Security Module is a Security Level 1 software module within a multi-chip standalone embodiment. The module is implemented completely in software. The physical security is provided by the Intel® Xeon® E3-1275 CPU or the Intel® Xeon® Gold 6252 CPU, and the computing platform.

6. Conceptual Interfaces

Output from the physical noise source provides input to the logic implemented by the Intel® Secure Key RDSEED function. RDSEED provides the entropy source interface to the module.

7. Min-Entropy Rate

The entropy source provides 128 bits of min-entropy per 128-bit output, or full entropy (H_{out}). H_{out}, post conditioning, is 1.0.

8. Health Tests

The module continuously performs developer-defined Health Tests as described in SP 800-90B Section 4.5, Developer-Defined Alternatives to the Continuous Health Tests. Online Health Testing ensures the health of 256-bit blocks of entropy. If the health tests detect an error, a CPU register is set to identify the failure. This register indicates to the software that the device is not producing entropy on request. Calls to RDSEED will not be allowed access to entropy.

9. Maintenance

No maintenance activities are prescribed for this entropy source.

10. Required Testing

The Cipher Trust Manager Core Security Module entropy source was tested in accordance with SP 800-90B requirements. The interfaces used to collect raw unconditioned noise are internal interfaces only available in a dedicated privileged mode. These interfaces are not available in production chips; therefore, the user must rely on health tests to ensure that the entropy source is configured correctly and is working as expected.

No further testing is required.