Alibaba Cloud Computing Ltd.

Alibaba Cloud CPU Time Jitter RNG Entropy Source version 3.6.0

SP 800-90B Non-Proprietary Public Use Document

Document Version: 1.1

Document Date: 2026-07-15

Alibaba Cloud Computing Ltd.
Room 1-2-A06, Yungu Campus,1008 Dengcai Street, Sandun Town, Xihu District
Hangzhou, Zhejiang, China, 310030

Prepared by:
atsec information security Corporation
4516 Seton Center Parkway, suite 250
Austin, TX 78759, USA

©2026 Alibaba Cloud Computing Ltd.; atsec information security corporation

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Table of Contents

1 Description 3
2 Security Boundary 3
3 Operating Conditions 4
4 Configuration Settings 5
5 Physical Security Mechanisms 5
6 Conceptual Interfaces 5
7 Min-Entropy Rate 5
8 Health Tests 5
9 Maintenance 6
10 User Verification 6
11 Vendor Permissions and Relationship 6

List of Tables

Table 1: Entropy source and operational environment information. 3
Table 2: Operating Conditions for each Operational Environment 4

List of Figures

Figure 1: Entropy Source Design 4

©2026 Alibaba Cloud Computing Ltd.; atsec information security corporation

This document can be reproduced and distributed only whole and intact, including this copyright notice.

1 Description

The Alibaba Cloud CPU Time Jitter RNG Entropy Source version 3.6.0 is a non-physical entropy source implemented in multi-chip standalone embodiment. The noise generation of this entropy source is based on the tiny variations in the execution time of the same piece of code. The execution time of this piece of code is made unpredictable by the complexity of the different hardware components that comprise modern CPUs and the different internal states that the operating system can have at a certain point in time. The entropy source complies with IG D.J and D.K.

The information about the entropy source described in this document is contained in Table 1. The noise source was tested under the assumption that its output is non-IID.

Table 1: Entropy source and operational environment information.

Characteristic	Description
Vendor	Alibaba Cloud Computing Ltd.
Entropy source name	Alibaba Cloud CPU Time Jitter RNG Entropy Source
Standard, IGs	SP800-90B (2018) IG D.J, IG D.K, IG D.O (2025-09-02)
Entropy category	Non-physical (NP)
Entropy source version	3.6.0
Operational environment	Alibaba Cloud Linux 3.2104 LTS 64-bit running on Alibaba Cloud ECS ecs.c8ine.2xlarge with Intel Xeon Platinum 8575C Alinux3 running on Alibaba Cloud ECI ecs.c8ine.2xlarge with Intel Xeon Platinum 8575C Red Hat Enterprise Linux 9.6 64-bit running on Alibaba Cloud ECS ecs.c9i.2xlarge with Intel Xeon 6 6982P-C Ubuntu 24.04 64-bit running on Alibaba Cloud ECS ecs.c8ine.2xlarge with Intel Xeon Platinum 8575C
Embodiment and type (module)	Multi-chip standalone, software

2 Security Boundary

The boundary for this non-physical, software-based entropy source is the executable binary compiled from the C code that implements it (i.e., Userspace Standalone CPU Time Jitter RNG shared library).

Figure 1 depicts the overall design of the entropy source and its core operations.

©2026 Alibaba Cloud Computing Ltd.; atsec information security corporation

This document can be reproduced and distributed only whole and intact, including this copyright notice.

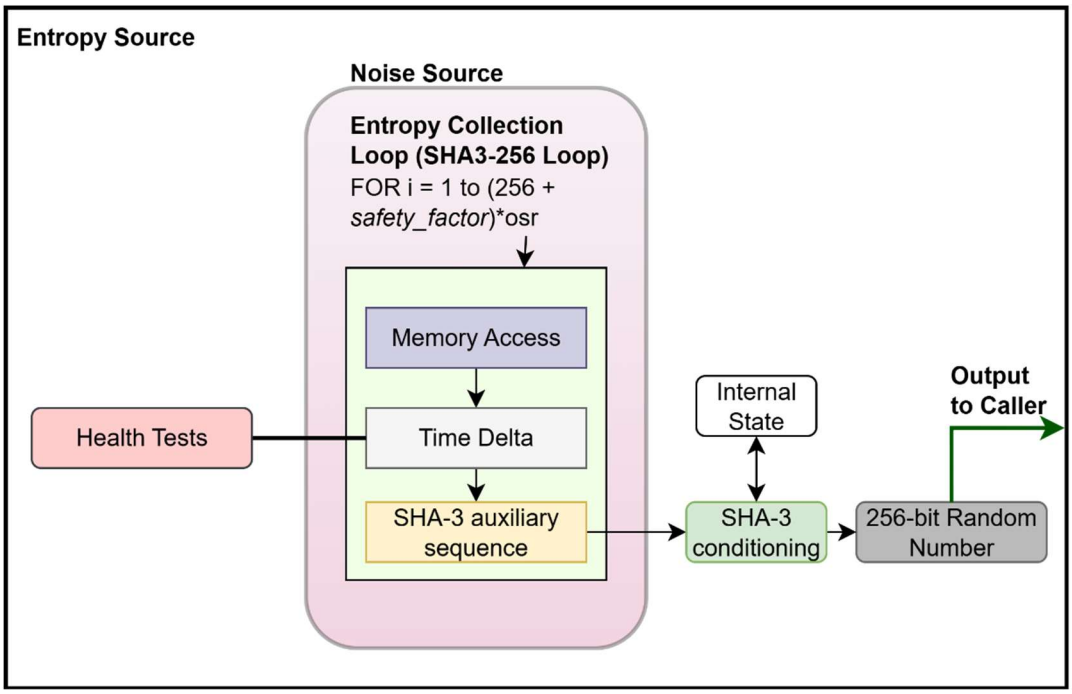


Figure 1: Entropy Source Design

The noise source is implemented by collecting and accumulating variances of the execution time of a defined set of instructions. The time jitter of the execution time is measured over time variances of variable memory accesses and variances in the execution time of a defined set of instructions, which includes an implementation of SHA3-256.

If the Repetition Count Test (RCT) or the Adaptive Proportion Test (APT) health tests fail, the noise data is discarded, the entropy source halts without outputting any data, and a failure code is returned to the caller.

3 Operating Conditions

The noise source is non-physical, and thus the operating conditions are inherited from the operational environment in which the entropy source is installed, as shown in Table 2.

Table 2: Operating Conditions for each Operational Environment

Manufacturer /Model	Temperature	Voltage	Clock Speed	Cache Sizes
Intel Xeon Platinum 8575C	0 °C - 71.4 °C	1.52 - 1.72 VDC	3.2 GHz	L1i 32 KB * 8 L1d 48 KB * 8 L2 2048 KB * 8 L3 327680 KB

©2026 Alibaba Cloud Computing Ltd.; atsec information security corporation

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Manufacturer /Model	Temperature	Voltage	Clock Speed	Cache Sizes
Intel Xeon 6 6982P-C	0 °C - 71.4 °C	1.52 - 1.72 VDC	2.8 GHz	L1i 64 KB * 128 L1d 48 KB * 128 L2 2048 KB * 128 L3 504 MB

4 Configuration Settings

The Alibaba Cloud CPU Time Jitter RNG Entropy Source is part of the Alibaba Cloud Crypto. The user does not have access to configure Alibaba Cloud CPU Time Jitter RNG Entropy parameters.

5 Physical Security Mechanisms

The noise source is non-physical.

The physical security mechanisms apply to the Alibaba Cloud Crypto Engine in which the entropy source is installed, and thus the entropy source inherits those mechanisms. See the Alibaba Cloud Crypto Non-Proprietary Security Policy for more information.

6 Conceptual Interfaces

The entropy source provides the following interfaces:

- Service call “Random number generation”: Obtains conditioned entropy from the module. This interface corresponds to the GetEntropy() conceptual interface from SP800-90B.

7 Min-Entropy Rate

The entropy source provides 256 bits of entropy per 256-bit conditioned output block (i.e., full entropy).

8 Health Tests

The entropy source implements the following continuous health tests:

- Repetition Count Test conforming to SP 800-90B section 4.4.1.
  - Intermittent cutoff value $C_i = 91$
  - Permanent cutoff value $C_p = 181$
- Adaptive Proportion test conforming to SP 800-90B section 4.4.2.
  - $W = 512$
  - Intermittent cutoff value $C_i = 459$
  - Permanent cutoff value $C_p = 479$
- Stuck (Non-Permanent) Test: The Stuck Test computes the first, second and third discrete derivatives of the time value that will be processed by SHA3-256. If any

©2026 Alibaba Cloud Computing Ltd.; atsec information security corporation

This document can be reproduced and distributed only whole and intact, including this copyright notice.

of these derivatives are zero, then the received time delta is considered stuck. In this case the input state to SHA3-256 is not updated, and the entropy value is not counted. The stuck test then triggers the RCT for further processing. The second derivative is in fact the RCT itself.

- Lag Predictor Test: The goal of this test is to detect a failure mode in which the outputs may become mostly deterministic. In essence, this test constructs a scoreboard and tracks the number of times that a subpredictor was correct. The subpredictor that scored the most correct predictions is used to predict the next value of a series. The lag predictor test is configured in this entropy source with the following parameters:
  - $\alpha = 2^{-22}$
  - Window size: 131072
  - Lag history size: 8
  - Global cutoff = 104761
  - Local cutoff = 111

The continuous-health tests are applied to each new sample obtained from the noise source. Whenever a failure is detected during the health testing specifically for the RCT and APT, entropy data is not returned to the caller; instead, a failure code is returned to enable the caller to acknowledge the failure. In the case of permanent failures, the entropy source then halts and will refuse new requests for entropy. Upon return of the permanent failure code, the caller shall attempt to reset or reboot the entropy source or return an error to its own operator. The stuck test is considered non-permanent, as positive stuck tests will be registered but will not immediately halt the entropy source.

Startup tests conduct the same set and parameters of the continuous health tests on 1024 samples of noise data. The data is discarded after the startup tests have completed successfully.

On-demand health tests of the noise source may be performed by rebooting the operational environment, which results in the immediate execution of the start-up tests. Typically, this entropy source designed for user space cannot be reloaded without restarting the executable. Similarly, the data used for the on-demand health tests are discarded after successful completion.

9 Maintenance

There are no maintenance requirements.

10 User Verification

The Alibaba Cloud CPU Time Jitter RNG Entropy Source is part of the Alibaba Cloud Crypto. The user could verify the hardware and firmware version via the “Show module name and version” service. See the Alibaba Cloud Crypto Non-Proprietary Security Policy for more information.

RAW noise data is not available for the module’s user, and the user must rely on health tests to detect any drops in entropy.

11 Vendor Permissions and Relationship

This entropy source validation is marked as “Reuse restricted to vendor”.

©2026 Alibaba Cloud Computing Ltd.; atsec information security corporation

This document can be reproduced and distributed only whole and intact, including this copyright notice.