



SafeLogic

Cryptography Simplified

SP 800-90B Non-Proprietary Public Use Document

CryptoComply Entropy Provider
Version: 1.1.1

Document Version: 1.4
Release Date: October 17, 2025

Prepared for:
SafeLogic, Inc.

Prepared by:

 Lightship Security
Aplus⁺
www.lightshipsec.com

Table of Contents

Description	3
Security Boundary	3
Operating Environments and Conditions	4
Configuration Settings	9
Conceptual Interfaces	10
Min-Entropy Rate	10
Health Tests	10
Maintenance	11
User Verification	11
Vendor Permissions and Relationship	11

Description

SafeLogic Inc.'s CryptoComply Entropy Provider version 1.1.1 implements CPU Jitter version 3.6.0 entropy source (ES) without any functional modifications.

The ES is a non-physical entropy source. It makes no IID claim and thus meets all the requirements for non-IID compliance. It is compliant to NIST Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation (Last Modified Date: January 2018), IG D.J (Last Modified Date: November 5, 2021) and IG D.K (Last Modified Date: March 17, 2023).

Table 1 summarizes the platforms and their respective processors for which testing was performed.

Security Boundary

The security boundary of the ES implementation is shown in Figure 1. The boundary of the implementation is the source code files provided as part of the software delivery.

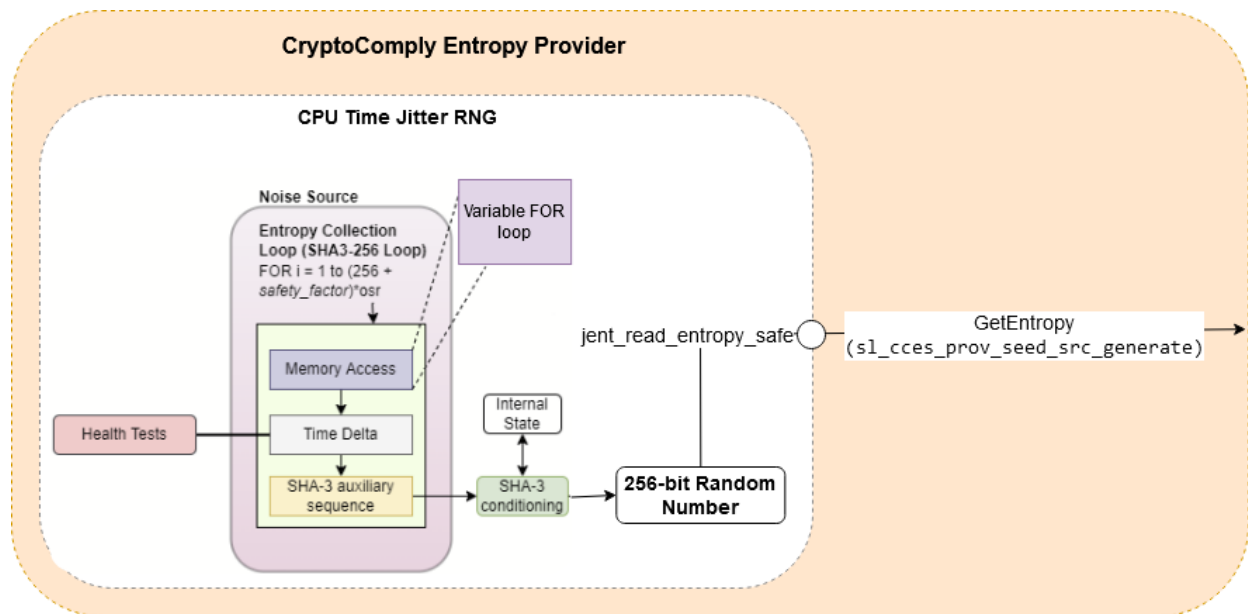


Figure 1: Security Boundar

Operating Environments and Conditions

Table 1 summarizes the operating conditions for each of the tested platforms.

Table 1: Operating Environments and Conditions

CPU	Operating System	CPU Conditions
Intel Xeon E5-4667v4	<ul style="list-style-type: none"> AlmaLinux 9 Debian 11 FreeBSD 13 Oracle Solaris 11.4 Red Hat Enterprise Linux 9 Rocky Linux 9 SUSE Linux Enterprise Server 15 Ubuntu 22.04 Windows 10 Windows 11 Windows Server 2019 Windows Server 2022 	<ul style="list-style-type: none"> Temperature Range: 0°C - 87°C Voltage Range: 1.2 V (±3%) CPU Clock Speed: 2.2 GHz L1 Cache: 32 KB L2 Cache: 256 KB caches L3 Cache: 45 MB shared cache
Google Tensor G2	Android 13	<ul style="list-style-type: none"> Temperature Range: 0°C - 35°C Voltage Range: 1.8 V - 5.5 V CPU Clock Speed: 1.80 - 2.85 GHz L1 Cache: up to 64 KB L2 Cache: up to 1 MB L3 Cache: 8MB shared cache
Apple A15 Bionic	iOS 16	<ul style="list-style-type: none"> Temperature Range: -25°C - 125°C Voltage Range: 0.595 V - 1.115 V CPU Clock Speed: 2.02 - 3.23 GHz L1 Cache: 256 KB L2 Cache: 12 MB L3 Cache: 32 MB

CPU	Operating System	CPU Conditions
Apple M1	iPadOS 17	<ul style="list-style-type: none"> • Temperature Range: -25°C - 125°C • Voltage Range: 0.595 V - 1.115 V • CPU Clock Speed: 2.06 - 3.22 GHz • L1 Cache: 2 MB • L2 Cache: 16 MB • L3 Cache: 8 MB
Apple M2	macOS 13 (Ventura)	<ul style="list-style-type: none"> • Temperature Range: -25°C - 125°C • Voltage Range: 0.595 V - 1.115 V • CPU Clock Speed: 2.42 - 3.48 GHz • L1 Cache: 2 MB • L2 Cache: 20MB • L3 Cache: 8 MB
Intel® Xeon® D-1527 (Broadwell)	Ubuntu 22.04	<ul style="list-style-type: none"> • Temperature Range: 5 °C - 77 °C • Voltage Range: 1.0 V – 2.5 V (±3%) • CPU Clock Speed: 2.2 GHz • L1 Instruction Cache: 2 x 32 KB • L1 Data Cache: 2 x 32 KB • L2 Cache: 2 x 256 KB • L3 Cache: 6 MB
Intel® Xeon® D-1541 (Broadwell)	Ubuntu 22.04	<ul style="list-style-type: none"> • Temperature Range: 5 °C - 77 °C • Voltage Range: 1.0 V – 2.5 V (±3%) • CPU Clock Speed: 2.1 GHz • L1 Instruction Cache: 4 x 32 KB • L1 Data Cache: 4 x 32 KB • L2 Cache: 4 x 256 KB • L3 Cache: 12 MB

CPU	Operating System	CPU Conditions
Intel® Xeon® D-1736NT (Ice Lake)	Ubuntu 22.04	<ul style="list-style-type: none"> • Temperature Range: 5 °C - 77 °C • Voltage Range: 1.0 V – 2.5 V (±3%) • CPU Clock Speed: 2.7 GHz • L1 cache: 8 x 32 KB • L2 cache: 8 x 1.25 MB • L3 cache: 15MB
Intel® Xeon® Gold 5218 (Cascade Lake)	Ubuntu 22.04	<ul style="list-style-type: none"> • Temperature Range: 5 °C - 87 °C • Voltage Range: 1.0 V – 2.5 V (±3%) • CPU Clock Speed: 2.3 GHz • L1 Instruction Cache: 2 x 32 KB • L1 Data Cache: 2 x 32 KB • L2 Cache: 2 x 1024 KB • L3 Cache: 22 MB
Intel® Xeon® Gold 6230 (Cascade Lake)	Ubuntu 22.04	<ul style="list-style-type: none"> • Temperature Range: 5 °C - 87 °C • Voltage Range: 1.0 V – 2.5 V (±3%) • CPU Clock Speed: 2.1 GHz • L1 Instruction Cache: 4 x 32 KB • L1 Data Cache: 4 x 32 KB • L2 Cache: 4 x 1024 KB • L3 Cache: 28 MB
Intel® Xeon® Platinum 8461V (Sapphire Rapids)	Ubuntu 22.04	<ul style="list-style-type: none"> • Temperature Range: 5 °C - 95 °C • Voltage Range: 0.8 V to 1.8 V (±3%) • CPU Clock Speed: 2.2 GHz • L1 Instruction Cache: 48 x 32 KB • L1 Data Cache: 48 x 48 KB • L2 Cache: 48 x 2048 KB • L3 Cache: 98 MB

CPU	Operating System	CPU Conditions
Intel® Xeon® Silver 4214 (Cascade Lake)	Ubuntu 22.04	<ul style="list-style-type: none"> • Temperature Range: 5 °C - 77 °C • Voltage Range: 1.0 V – 2.5 V (±3%) • CPU Clock Speed: 2.2 GHz • L1 Instruction Cache: 12 x 32 KB • L1 Data Cache: 12 x 32 KB • L2 Cache: 12 x 1024 KB • L3 Cache: 17 MB
Intel® Atom® C3338 (Denverton)	Rocky Linux 8.10	<ul style="list-style-type: none"> • Temperature Range: -40 °C – 70 °C • Voltage Range: 1.0 V – 3.3 V • CPU Clock Speed: 2.2 GHz • L1 Instruction Cache: 32 KB per core • L1 Data Cache: 24 KB per core • L2 Cache: 1 MB (two-core shared) • L3 Cache: None
Intel® Atom® C3538 (Denverton)	Rocky Linux 8.10	<ul style="list-style-type: none"> • Temperature Range: 0 °C – 87 °C • Voltage Range: 1.0 V – 3.3 V • CPU Clock Speed: 2.1 GHz • L1 Instruction Cache: 32 KB per core • L1 Data Cache: 24 KB per core • L2 Cache: 2 MB per core • L3 Cache: None
Intel® Atom® C2538 (Rangeley)	Rocky Linux 8.10	<ul style="list-style-type: none"> • Temperature Range: -40 °C – 70 °C • Voltage Range: 1.0 V – 3.3 V • CPU Clock Speed: 2.4 GHz • L1 Instruction Cache: 32 KB per core • L1 Data Cache: 24 KB per core • L2 Cache: 2 MB per core • L3 Cache: None

CPU	Operating System	CPU Conditions
Intel® Atom® C2758 (Rangeley)	Rocky Linux 8.10	<ul style="list-style-type: none"> • Temperature Range: -40 °C – 70 °C • Voltage Range: 1.0 V – 3.3 V • CPU Clock Speed: 2.4 GHz • L1 Instruction Cache: 32 KB per core • L1 Data Cache: 24 KB per core • L2 Cache: 1 MB (two-core shared) • L3 Cache: None
Intel® Pentium® D1519 (Broadwell)	Rocky Linux 8.10	<ul style="list-style-type: none"> • Temperature Range: -40 °C – 85 °C • Voltage Range: 1.0 V – 3.3 V • CPU Clock Speed: 1.5 GHz • L1 Instruction Cache: 32 KB per core • L1 Data Cache: 32 KB per core • L2 Cache: 256 KB per core • L3 Cache: None
Intel® Xeon® D-1518 (Broadwell)	Rocky Linux 8.10	<ul style="list-style-type: none"> • Temperature Range: 0 °C – 80 °C • Voltage Range: 1.0 V – 3.3 V • CPU Clock Speed: 2.2 GHz • L1 Instruction Cache: 32 KB per core • L1 Data Cache: 32 KB per core • L2 Cache: 256 KB per core • L3 Cache: None
Intel® Xeon® D-1527 (Broadwell)	Rocky Linux 8.10	<ul style="list-style-type: none"> • Temperature Range: 0 °C – 80 °C • Voltage Range: 1.0 V – 3.3 V • CPU Clock Speed: 2.2 GHz • L1 Instruction Cache: 32 KB per core • L1 Data Cache: 32 KB per core • L2 Cache: 256 KB per core • L3 Cache: None

Configuration Settings

Table 2 and Table 3 summarize the configuration settings used by SafeLogic Inc.'s CryptoComply Entropy Provider implementation of CPU Jitter. These settings must be preserved to comply with the ESV certificate.

Table 2: CPU Jitter Configuration Parameters

Parameter	Value	Description
JENT_CONF_DISABLE_LOOP_SHUFFLE	Defined	jitterentropy.h
JENT_HEALTH_LAG_PREDICTOR	Defined	jitterentropy.h
JENT_RANDOM_MEMACCESS	Defined	jitterentropy.h
ENTROPY_SAFETY_FACTOR	64	jitterentropy.h
JENT_MIN_OSR	3	jitterentropy.h
JENT_MEMORY_BITS	17	jitterentropy.h
JENT_MEMORY_BLOCKS	Not defined and irrelevant (due to definition of JENT_RANDOM_MEMACCESS).	jitterentropy.h
JENT_MEMORY_BLOCKSIZE	Not defined and irrelevant (due to definition of JENT_RANDOM_MEMACCESS).	jitterentropy.h
JENT_MEMORY_ACCESSLOOPS	128	jitterentropy.h
JENT_CONF_ENABLE_INTERNAL_TIMER	Used for iOS and macOS operating environments.	Makefile
JENT_APT_WINDOW_SIZE	512	jitterentropy.h
JENT_LAG_WINDOW_SIZE	2^{17}	jitterentropy.h
JENT_LAG_HISTORY_SIZE	8	jitterentropy.h
JENT_POWERUP_TESTLOOPCOUNT	1024	jitterentropy-base.c
CLEARCACHE	100	jitterentropy-base.c
MIN_HASH_LOOP	0	jitterentropy-noise.c
MIN_ACC_LOOP_BIT	0	jitterentropy-noise.c

Table 3: CPU Jitter Configuration Flags (for `jent_entropy_init_ex` and `jent_entropy_collector_alloc`)

Parameter	Status from Guidance	CryptoComply Entropy Provider Status	Argument Name	Meaning
JENT_DISABLE_MEMORY_ACCESS	Prohibited	Not Used.	flags	Disable the memory access timing.
JENT_FORCE_INTERNAL_TIMER	Allowed	Used for iOS and macOS operating environments.	flags	Force use of pthreads-based internal timer, rather than the

Parameter	Status from Guidance	CryptoComply Entropy Provider Status	Argument Name	Meaning
				underlying hardware timer.
JENT_DISABLE_INTERNAL_TIMER	Allowed	Not Used.	flags	Prevent the use of the pthreads-based internal timer.
JENT_FORCE_FIPS	Recommended	Always used.	flags	Force fips_enable to be set (enabling health test reporting and use of the safety factor).
JENT_MAX_MEMSIZE_*	Allowed	Not used.	flags	Allows for run-time selection of the memory region size.
osr	Suggested	JENT_MIN_OSR (3)	osr	Sets the internal osr rate to max(osr, JENT_MIN_OSR)

Conceptual Interfaces

SafeLogic Inc.'s CryptoComply Entropy Provider implements the OpenSSL provider API and wraps the CPU Jitter RNG (jitterentropy) library, so that the entropy source interfaces with and required functionalities are accessed through the CryptoComply Entropy Provider. The CryptoComply Entropy Provider conceptual interfaces are as follows:

HealthTest: sl_cces_prov_provider_self_test
 GetNoise: sl_cces_prov_hashtime
 GetEntropy: sl_cces_prov_seed_src_generate

Min-Entropy Rate

SafeLogic Inc.'s CryptoComply Entropy Provider generates an output that is considered to have full entropy. A request for 256 bits of entropy results in 256 bits of entropy per output sample, or full entropy.

Health Tests

Per the SP 800-90B requirements, health tests are run when the ES starts and are then run continuously while it is operating. All tests check for persistent failures based on their respective "cutoff" values, which represent expected error thresholds.

The ES implements four types of health tests:

- Stuck Test
- Repetition Count Test (RCT)
- Adaptive Proportion Test (APT)
- Lag Predictor Test

All health test failures are considered permanent failures. If one is triggered, the current instance of the ES will always remain in error state. The documentation of the API call `jent_read_entropy(3)` explains that the caller can only clear this error state by deallocating the ES instance followed by an allocation of a new ES instance to reset the noise source.

Maintenance

There are no maintenance requirements.

User Verification

The entropy report contains the results of the testing SafeLogic, Inc. did on their raw and restart data. Raw data was collected by running SafeLogic's data collection script, which includes the `invoke_testing.sh` script included in the CPU Jitter package. This script gathers 1,000,000 samples of 8 bits of raw time stamp data. It also gathers 1000 x 1000 samples of 8 bits of raw data after restarting the ES each time, thus eventually gathering 1,000,000 samples of raw data for the restart tests.

To verify that the CryptoComply Entropy provider is correctly set up with OpenSSL, the operator should first confirm it is listed as a provider by using the OpenSSL list command:

```
openssl list -providers
```

Then the operator should confirm it is listed as a seed source using the OpenSSL list command:

```
openssl list -random-generators
```

Raw Data Analysis

Each raw data sample consists of one timestamp, which is 64 bits long. The ES design states that the source can deliver full entropy if and only if the min-entropy is at least $1/osr$ ($osr = 3$) bits of entropy per time stamp. This ES implementation uses an oversampling rate of 3.

Restart Data Analysis

For the restart tests, the raw entropy data is collected for 1,000 Entropy Source instances allocated sequentially. That means, for one collection of raw entropy, one Entropy Source instance is allocated. After the conclusion of the data gathering, it is deallocated, and a new Entropy Source instance is allocated for the next restart test round.

Vendor Permissions and Relationship

The reuse of this ESV requires written and signed permission from SafeLogic, Inc.

The CryptoComply Entropy Provider provides FIPS 140 compliant entropy and is available for licensing. For more information, please reach out to sales@safelogic.com.