FIPS PUB 140-3

SP 800-90B Non-Proprietary Public Use Document
SAP CommonCryptoLib Entropy Collector 1.0.0

Document version: 1.3
Date: 2024-08-07

Table of Contents

Description 1
Security Boundary 2
Operating Conditions 4
Configuration Settings 4
Physical Security Mechanisms 4
Conceptual Interfaces 4
Min-Entropy Rate 4
Health Tests 4
Maintenance 1
Required Testing 1
Vendor Permissions and Relationship 1

© 2024 SAP SE or an SAP affiliate company. All rights reserved.
This document may be reproduced and distributed only in its original entirely without revision.

Description

SAP SE provides a software module named “SAP CommonCryptoLib Crypto Kernel” in version 8.6.1 which contains cryptographic algorithms. Part of this Crypto Kernel is the non-physical (NP) entropy source “SAP CommonCryptoLib Entropy Collector” (version is 1.0.0). This entropy source uses CPU jitter for collecting random (non-IID) values. The CPU jitter implementation in the entropy source generates entropy from variations in the execution time of some code instructions written in C accessing memory.

The Crypto Kernel, including the entropy source, is available and tested on these platforms:

- SLES 15 SP4 on AWS Nitro System running on Amazon EC2 c7g.16xlarge with AWS Graviton3
- SLES 15 SP4 on AWS Nitro System running on Amazon EC2 c7g.16xlarge with AWS Graviton3 with SHA512 Instructions
- Apple macOS 14 running on MacBook Pro (2019) with Intel Core i7-9750H
- Apple macOS 12 running on Mac mini (2020) with Apple M1
- Apple macOS 12 running on Mac mini (2020) with Apple M1 with SHA512 Instructions
- SunOS 5.10 running on Sun-4u – Fujitsu M4000 with Fujitsu SPARC64-VI
- HP-UX 11.31 (IA64) running on Hewlett-Packard rx2800 i4 with Intel Itanium Processor 9540
- SLES 15 SP2 on IBM z/VM 7.2.0 running on IBM z13 with IBM S390
- IBM AIX 7.2 on IBM PowerVM 3.1.4.21 running on IBM Power System S824 with IBM POWER9
- IBM AIX 7.2 on IBM PowerVM 3.1.4.21 running on IBM Power System S824 with IBM POWER9 with P8
- IBM AIX 6.1 on IBM PowerVM 3.1.4.21 running on IBM Power System S824 with IBM POWER8 (PV_7_Compat)
- SLES 15 SP4 (kernel 5.14.21) on QEMU (KVM) 6.2 on SLES 15 SP4 running on Ampere D12A-M1-AA with Arm Neoverse N1
- SLES 11 SP1 running on Hewlett-Packard rx2660 with Intel Itanium Processor 9120N
- SLES 12 SP5 on IBM PowerVM 3.1.4.21 running on IBM Power System E980 with IBM POWER8
- SLES 12 SP5 on IBM PowerVM 3.1.4.21 running on IBM Power System E980 with IBM POWER8 with P8
- SunOS 5.10 running on i86pc - Fujitsu Primergy RX600 S6 with Intel Xeon E7-4807
- Alpine Linux 3.18.2 on VMware Workstation 17.5.0 on Windows 11 Enterprise running on LENOVO_MT_20QU_BU_Think_FM_ThinkPad P1 Gen 2 with Intel Core i9-9880H
- SLES 15 SP5 on VMware ESXi 7.0.3 running on Dell EMC PowerEdge R840 with Intel Xeon Platinum 8260M
- Microsoft Windows Server 2022 Standard (64-bit) on VMware ESXi 7.0.3 running on DELL EMC PowerEdge R840 with Intel Xeon Platinum 8260M

© 2024 SAP SE or an SAP affiliate company. All rights reserved.
This document may be reproduced and distributed only in its original entirely without revision.



Security Boundary

The security boundary of this non-physical, software-based entropy source is the software library (i.e. the Crypto Kernel) which is linked to an external application and resides in the process memory. The noise source, health tests, and the SHA2-512 conditioning component are implemented as part of this software library.

Figure 1 shows the relevant components of the entropy source. The noise source is implemented by collecting and accumulating variances of the execution time of defined set of instructions. The jitter of the execution time is measured over time variances of memory accesses.

The output of the noise source is processed in a vetted conditioning component (SHA2-512, see Cert. #A5497).

© 2024 SAP SE or an SAP affiliate company. All rights reserved.
This document may be reproduced and distributed only in its original entirely without revision.

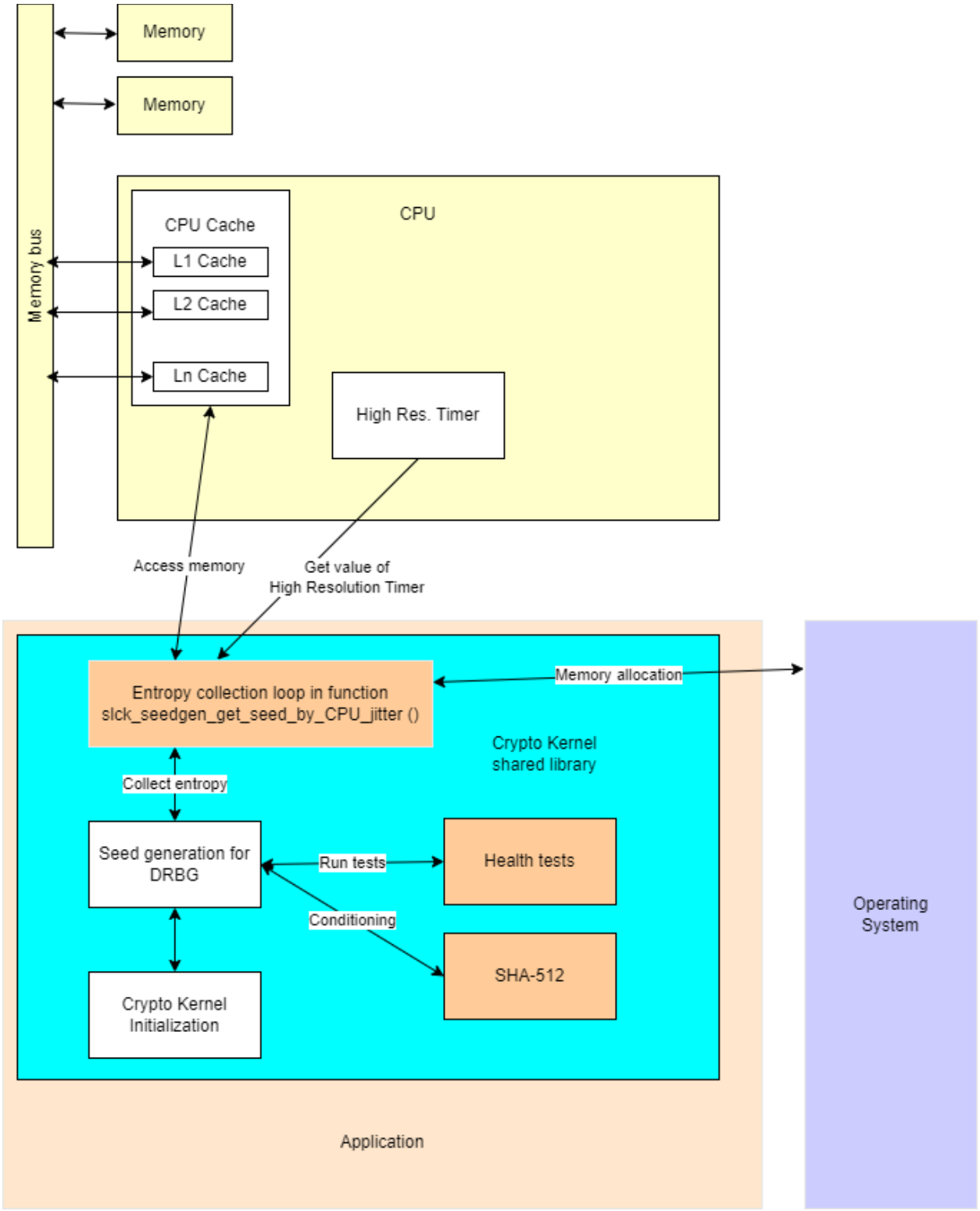


Figure 1: Noise source based on CPU jitter

© 2024 SAP SE or an SAP affiliate company. All rights reserved.
This document may be reproduced and distributed only in its original entirely without revision.

Operating Conditions

The entropy source was tested on the operational environments (OE) listed above. Each operational environment was tested under normal operating conditions only (i.e. room temperature).

Configuration Settings

No configuration is provided for the entropy source.

Physical Security Mechanisms

The entropy source is software based. The physical security mechanism is the mechanisms of the hardware on which the entropy source is installed.

Conceptual Interfaces

The entropy source is part of SAP CommonCryptoLib Crypto Kernel v8.6.1 and only used for the seeding of its internal DRBG. There is an internal function (slck_seedgen_get_seed_by_CPU_jitter) that is called during initialization of the Crypto Kernel to get entropy from the entropy source.
For testing purposes, the function crypt_get_seed_by_CPU_jitter can be used from external tools to get entropy from the entropy source.

Min-Entropy Rate

The entropy collection function returns 32-bit integers (Non-IID) with a Min-entropy of H_submitter = 0.1 bits per value. 6000 of these values are hashed with SHA-512 as conditioning function and the resulting digest is used as the seed for the internal DRBG of the Crypto Kernel. In summary, the entropy source provides random numbers with an entropy rate of 1 bit / 1 bit.

Health Tests

During the initialization of the Crypto Kernel 6000 32-bit random values are collected from the entropy source. After that, the following health tests are performed. In case one test fails, the Crypto Kernel ends the initialization step with an error and no cryptographic functions can be used.

Health tests with α = 2^−20:

- Adaptive proportion test as defined in SP 800-90B (W = 512, C = 502)
- Repetition count test as defined in SP 800-90B (C = 201)
- Further vendor-defined health tests based on the adaptive proportion test and repetition count test to detect specific patterns in the raw data generated by the noise source

© 2024 SAP SE or an SAP affiliate company. All rights reserved.
This document may be reproduced and distributed only in its original entirely without revision.

The entropy source only defines an intermittent failure mode. When such an intermittent failure is detected, the CryptoKernel shared library enters an error state and remain in this state until the module is reinitialized which corresponds to a full reset of the entropy source.
The entropy source does not distinguish between health tests performed during start-up and continuous health tests, as requesting additional entropy after module initialization corresponds to a re-initialization of the entropy source.
On demand health tests can be performed by re-initializing the CryptoKernel which also re-initialized the entropy source.
In case the health tests are successful, the tested raw data is compressed by a vetted conditioning function to generate the entropy source output, i.e., the raw data used for health testing is not discarded.

Maintenance

No maintenance is required. The entropy source is powered on and off by the initialization call of the Crypto Kernel.

Required Testing

By initialization of the Crypto Kernel, the entropy source is automatically tested with health tests. The API can be used to return the result of these tests.

For tests according to SP 800-90B it is required

- to generate 1000000 samples and
- to generate 1000 * 1000 samples with a restart of the entropy source after each block of 1000 samples

For this test a tool genseed is provided which generates the samples (with function crypt_get_seed_by_CPU_jitter) and truncates the 32-bit sample to 8 bits as required by the ea_non_iid and ea_restart tool.

Vendor Permissions and Relationship

Reuse is restricted to the vendor; no other vendors are currently allowed to use the certificate.

© 2024 SAP SE or an SAP affiliate company. All rights reserved.
This document may be reproduced and distributed only in its original entirely without revision.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. See http://www.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.

