Intel® Software Guard Extensions (Intel® SGX) Platform Software for Linux* OS Release Notes

27 March 2019

Revision: 2.5 Open Source (version: 2.5.100)

Contents:

1 Introduction

This document provides system requirements, installation instructions, limitations, and legal information for the Intel® Software Guard Extensions (Intel® SGX) Platform Software (PSW).

Product Contents

The Intel® Software Guard Extensions PSW package includes:

- Intel® SGX Application Enclaves
- Intel® SGX Runtime System Library
- Intel® SGX Application Enclave Service Manager (AESM)

2 What's New

Intel® Software Guard Extensions PSW includes the following changes in 2.5.100:

- Support ECDSA quote based remote attestation
- Fixed bugs

Changes in Previous Releases

Intel® Software Guard Extensions PSW includes the following changes in 2.4.100.48163

- Supported Intel® SGX Enclave Common Loader library

- Updated Intel® Architecture Enclaves to use Intel® IPP Cryptography 2019 Update 1 library
- Fixed bugs

Intel® Software Guard Extensions PSW includes the following changes in 2.3.100.46354:

- Added support for Ubuntu* 18.04 LTS 64-bit Desktop and Server version
- Updated the Intel® SGX PSW installer for Ubuntu*. The following changes are introduced:
    - Using .deb installer
    - Using name `libsgx-enclave-common_{version string}-1_amd64.deb`.
    - Installing the Intel® SGX Enclave Common loader library.
- Fixed SGX Quoting enclave bug, which caused the invalid signature error when a user upgraded the SGX PSW 1.6 version to a higher version and did remote attestation
- Updated the SGX Provisioning Cert Enclave to fix error code bug
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.2.100.45311:

- Added support for Switchless Calls, a new mode of operation to perform calls from/to SGX enclaves
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.1.103.44322 release:

- Update the cryptography lib to the Intel® Integrated Performance Primitives Cryptography 2018 Update 2.1. Mitigated security vulnerability CVE-2018-3617(https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-3617). For more details, refer to Intel Security Advisory INTEL-SA-00106(https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00106&languageid=en-fr) and INTEL-SA-00135(https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00135&languageid=en-fr).
- Update the Intel® SGX platform service Dal applet

- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.1.102.43402 release:

- Mitigated security vulnerability CVE-2018-3689 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3689). For more details, refer to Security Advisory INTEL-OSS-10004 (https://01.org/security/advisories/intel-oss-10004)
- Mitigated security vulnerability CVE-2018-3626 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3626). For more details, refer to Security Advisory INTEL-SA-00117 (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00117&languageid=en-fr).

Intel® Software Guard Extensions PSW includes the following changes in 2.1.101.42529 release:

- Updated security to the Intel® SGX PSW.

Intel® Software Guard Extensions PSW includes the following changes in version 2.1.100.42002:

- Added support for CentOS* 7.4
- Added support for SUSE* Linux Enterprise Server 12
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in version 2.0.100.40905:

- Added support for 3072 bit Intel® SGX provisioning server public key
- Added support for the Intel® SGX Enclave Dynamic Memory Management (EDMM)
- Added support for Red Hat* Enterprise Linux* Server 7.4.

Intel® Software Guard Extensions PSW includes the following changes in version 1.9.100.39124:

- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in version 1.8.100.37689:

- Added support for the Trusted Platform Service
- Added support for RedHat* and CentOS*.

3 System Requirements

Hardware Requirements

- 6th Generation Intel® Core™ Processor or newer.

Software Requirements

- Supported Linux* OS distributions:
    - Ubuntu* 16.04 LTS 64-bit Desktop and Server version
    - Ubuntu* 18.04 LTS 64-bit Desktop and Server version
    - Red Hat* Enterprise Linux* Server 7.4 (for x86_64)
    - CentOS* 7.5 (for x86_64)
    - SUSE* Enterprise Server 12 (for x86_64)
    - Fedora* 27 Server version

Note:

1. Intel® SGX PSW supports the Intel® Xeon® Processor E3 Server V5 and onwards platforms if the platform processor and BIOS supports the Intel® SGX. Please check with OEM/ODM regarding BIOS support for enabling the Intel® SGX.
2. If you need to use the Intel® SGX platform service, install the Intel® Management Engine (Intel® ME) software components. This is optional, you can skip this if you do not need to use the Intel® SGX platform service.
3. Intel® SGX platform service is not supported on the Intel® Xeon® Processor E3 Server platforms.

4 Known Issues and Limitations

- Occasionally Intel® SGX aesmd service fail to retrieve enclave launch white-list from internet after rebooting Linux, this may cause failure to load those enclaves which need latest enclave launch white-list support. User can work around this through restarting Intel® SGX aesmd service.

5 Disclaimer and Legal Information

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

Intel technologies features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at Intel.com, or from the OEM or retailer.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, the Intel logo, Xeon, and Xeon Phi are trademarks of Intel Corporation in the U.S. and/or other countries.

This software and the related documents are Intel copyrighted materials, and your use of them is governed by the express license under which they were provided to you (**License**). Unless the License provides otherwise, you may not use, modify, copy, publish, distribute, disclose or transmit this software or the related documents without Intel's prior written permission.

This software and the related documents are provided as is, with no express or implied warranties, other than those that are expressly stated in the License.

Optimization Notice
Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the

availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice.

Notice revision #20110804

* Other names and brands may be claimed as the property of others.