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

10 May 2018

Revision: 2.1.3 Open Source (version: 2.1.103.44322)

Contents:

1 Introduction

This document provides system requirements, installation instructions, limitations and legal information for 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 this release:

- Update the cryptography lib to 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 Intel® SGX platform service Dal applet.
- Bug fixes.

Changes in Previous Releases

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:

- Security updates to Intel® SGX PSW

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

- Support for CentOS* 7.4
- Support for SUSE* Linux Enterprise Server 12
- Bug fixes

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

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

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

- Bug fixes

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

- Trusted Platform Service support
- Support for RedHat and CentOS

3 System Requirements

Hardware Requirements

- 6th Generation Intel® Core™ Processor or newer

Software Requirements

- Supported Linux* OS distributions:
    - Ubuntu* 16.04.3 LTS 64-bit Desktop version
    - Ubuntu* 16.04.3 LTS 64-bit Server version
    - Red Hat* Enterprise Linux* Server 7.4 (for x86_64)
    - CentOS* 7.4 (for x86_64)
    - SUSE* Enterprise Server 12 (for x86_64)

Note:

1. Intel® SGX PSW supports Intel® Xeon® Processor E3 Server V5 and onwards platforms if the platform processor and BIOS supports Intel® SGX. Please check with OEM/ODM regarding BIOS support for enabling Intel® SGX.
2. Intel® SGX platform service is not supported in Intel® Xeon® Processor E3 Server platforms.

4 Disclaimer and Legal Information

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.

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.