Intel® Software Guard Extensions SDK for Linux* OS Release Notes

22 September 2016

Revision: 1.6 Open Source (Intel® SGX SDK version: 1.6.100.34922)

Contents:

1   Introduction

Intel® Software Guard Extensions (Intel® SGX) SDK is a software isolation technology that helps you protect your applications.

This document provides system requirements, installation instructions, limitations and legal information.

Product Contents

Intel® Software Guard Extensions SDK package includes:

- An Intel® Software Guard Extensions SDK installer for Linux* OS. It includes binaries to develop enclave applications. The main components include:

    - Trusted libraries, including the standard C library, C++ runtime support, and C++ STL

    - Development tools, including edger8r and a signing tool

    - Sample projects

2   What's New

Intel® Software Guard Extensions SDK includes the following changes in this release:

- New `setjmp/longjmp` APIs in the trusted C library

- Bug fixes

Changes in Previous Releases

- Support for profiling SGX applications using Intel® VTune™. To profile SGX applications, use VTune™ 2016 Update 2, which contains the `SGX Hotspots` analysis type

- Intel® SGX plug-in for the Eclipse* IDE that is able to create SGX enclave projects

- Support implicit Thread Local Storage (TLS)

- Support nested HW exception in a trusted environment

3 System Requirements

Software Requirements

- Supported Linux* OS distributions:

  o Ubuntu* 14.04.4 LTS 64-bit Desktop version

Note:

1. Please use the listed Linux* OS distribution. Other distributions are not supported.

2. For the hardware requirements of Intel® Software Guard Extensions Platform Software for Linux* OS, see the *Revision History* section of *Intel® Software Guard Extensions Platform Software for Linux* OS Release Notes.*

4 Known Issues and Limitations

- Intel® SGX for Linux* OS does not support power management.
- Intel® SGX for Linux* OS does not support setting different charsets in the GNU* Project Debugger (GDB*).

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.

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