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

15 December 2016

Revision: 1.7 Open Source (Intel® SGX PSW version: 1.7.100.36470)

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

Changes to Intel® Software Guard Extensions PSW include:

- Updated Intel® SGX Application Enclaves to use the Intel® Enhanced Privacy ID (Intel® EPID) SDK library version 2.0.0.
- Support for flexible provisioning.

- Support for retrieving enclave launch whitelist file from remote server.

3 System Requirements

Hardware Requirements

- 6th Generation Intel® Core™ Processor (Intel® microarchitecture code name Skylake). If the system is using an Intel reference BIOS, you need a 6th Generation Intel® Core™ Processor BIOS RC 0.7 or newer.

- 7th Generation Intel® Core™ Processor (Intel® microarchitecture code name Kaby Lake)

Software Requirements

- Supported Linux* OS distributions:

    - Ubuntu* 14.04.4 LTS 64-bit version (for desktop version only)

Note:

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

4 Installation Notes

Before installing Intel® SGX PSW, Intel® SGX must be enabled in BIOS. If the system is using an Intel reference BIOS, you may configure the BIOS options by following these steps:

Go to **Intel Advanced Menu -> CPU Configuration -> SW Guard Extensions (SGX)**. Set **SW Guard Extensions (SGX)** to **Enabled**.

- You may need to configure **Intel Advanced Menu -> CPU Configuration -> PRMRR**. You can set it to 32MB, 64MB or 128MB. The default option is 128MB.

Note:

This step may only be applicable to Intel reference BIOS and may be not applicable to OEM BIOS.

To install the Intel® SGX driver and PSW, use the following steps:

1. To install the Intel® SGX driver in the default directory, enter the following command:

```
sudo ./sgx_linux_x64_driver.bin
```

2. To install the Intel® SGX PSW in the default directory, enter the following command. The platform software is installed at `/opt/intel/sgxpsw`

   ```
   sudo ./sgx_linux_x64_psw_1.7.100.36470.bin
   ```

3. To uninstall the product, enter the following command:

   ```
   sudo /opt/intel/sgxpsw/uninstall.sh
   ```

5 Known Issues and Limitations

- Intel® SGX platform service is unavailable
- Intel® SGX for Linux* OS does not support power management.

6 Disclaimer and Legal Information

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.