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

Installation Guide and Release Notes

12 October 2015
Revision: 1.1

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

Intel® Software Guard Extensions PSW package includes the following software components:

Ingredient binary	Version string
Intel® SGX Windows* 7/8.1/10 driver (64 bit only)	1.0.26805.1389
Intel® SGX Enclaves	1.0.26826.1391
Intel® SGX Runtime System Library	1.1.28124.78
Intel® SGX Application Enclave Service (AESM)	1.1.28124.78

2 What's New

Intel® Software Guard Extensions PSW changes include:

- Support Microsoft Windows Threshold2
- Support Hyper-V mode in Microsoft Windows Threshold2
- SGX PSW DLLs (sgx_urts.dll and sgx_uae_service.dll) are installed into the system directory

3 System Requirements

Hardware Requirements

- 6th Generation Intel® Core™ Processor (codenamed “Skylake”)

Firmware Requirements

- CSME firmware 11.0.0.1125 or newer.
- If the system is using an Intel reference BIOS, you need 6th Generation Intel® Core™ Processor (codenamed “Skylake”) BIOS RC 0.7 or newer.

Software Requirements

- Supported operating systems for the Intel® SGX PSW installer:
    - Microsoft Windows* 7/8.1/10 64-bit version.
      Note: Intel® SGX PSW does not support Microsoft Windows* 7/8.1/10 32-bit operating system.
- If you need to use Intel® SGX platform service, you need to install:
    - Full set of Intel® Management Engine (ME) software components 11.0.0.1125 or newer
      Note: To install full set of Intel® Management Engine (ME) software components, you need to install with “SetupMe.exe” instead of “MEISetup.exe” (HECI driver only).

4 Installation Notes

Before installing Intel® SGX PSW, Intel® SGX must be enabled in BIOS.

For example, if the system is using an Intel reference BIOS, you may configure the BIOS options according to the following steps:

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

- If you set Software Controlled for the **SW Guard Extensions (SGX)** option, you need to enable Intel® SGX using **Intel® SGX Enabling Functions** after installing Intel® SGX PSW. See *Intel® SGX SDK User’s Guide for Windows* OS* for more details.
- If you set Enabled for the **SW Guard Extensions (SGX)** option, 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.

Please be aware that this step maybe only applicable to Intel reference BIOS and may be not applicable to OEM BIOS

You need administrator privilege to run the installer.

Once installed, you can see **Intel® Software Guard Extensions Platform Software** in the **Control Panel\Programs\Programs and Features** list.

To force Intel® SGX PSW installation with administrative account, use the following command:

```
msiexec /i SGX_PSW.msi FORCE_INSTALL=1
```

Silent/unattended installations can be done by adding the /qn or /quiet switch:

```
msiexec /i SGX_PSW.msi /qn
```

The Intel® SGX PSW installer does not uninstall the Intel SGX device driver after the uninstallation of the platform software. Subsequent installations of the Intel® SGX PSW update the driver to newer versions only (no downgrade is allowed).

To use Intel® SGX platform service, you need to install full set of Intel® Management Engine (ME) software components which includes Intel® Dynamic Application Loader(DAL) Host Interface Service. If you install Intel® ME driver only, Intel® SGX platform service would not be available.

Default Installation Folders

The default top-level installation folder for this product is:

- C:\Program Files\Intel\IntelSGXPSW

5 Known Issues and Limitations

- Intel® Software Guard Extensions only supports integrated Windows authentication proxy scheme. The Basic and the Digest authenticated proxy schemes are not supported.
- OEM must *not* post Intel® SGX PSW for end-users to download. Any Intel SGX PSW upgrade for end-users is through SGX applications provided by ISV only.
- If the BIOS setting “**Intel Advanced Menu -> CPU Configuration -> SW Guard Extensions (SGX)”** is set to “Software Controlled”, you will not be able to install Intel® SGX PSW by double-clicking the Intel® SGX PSW installer MSI file. To work around this issue, you can:
    - execute the Intel® SGX PSW installer as administrator
    - open the command prompt as administrator and run the installer from there
    - set the above BIOS setting to “Enabled”; in this case the Windows UAC (User Account Control) dialog will pop up when administrator privileges are required

6 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 which may cause deviations from published specifications.

MPEG-1, MPEG-2, MPEG-4, H.261, H.263, H.264, MP3, DV, VC-1, MJPEG, AC3, AAC, G.711, G.722, G.722.1, G.722.2, AMRWB, Extended AMRWB (AMRWB+), G.167, G.168, G.169, G.723.1, G.726, G.728, G.729, G.729.1, GSM AMR, GSM FR are international standards promoted by ISO, IEC, ITU, ETSI, 3GPP and other organizations. Implementations of these standards, or the standard enabled platforms may require licenses from various entities, including Intel Corporation.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

Intel, the Intel logo, BlueMoon, BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino Inside, Cilk, Core Inside, E-GOLD, Flexpipe, i960, Intel, the Intel logo, Intel AppUp, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, Intel Insider, the Intel Inside logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel Sponsors of Tomorrow., the Intel Sponsors of Tomorrow. logo, Intel StrataFlash, Intel vPro, Intel XScale, Intel True Scale Fabric, InTru, the InTru logo, the InTru Inside logo, InTru soundmark, Itanium, Itanium Inside, MCS, MMX, MPSS, Moblin, Pentium, Pentium Inside, Puma, skoool, the skoool logo, SMARTi, Sound Mark, Stay With It, The Creators Project, The Journey Inside, Thunderbolt, Ultrabook, vPro Inside, VTune, Xeon, Xeon Phi, Xeon Inside, X-GOLD, XMM, X-PMU and XPOSYS are trademarks of Intel Corporation in the U.S. and/or other countries.