Intel® Software Guard Extensions (Intel® SGX) SDK for Windows® OS
Release Notes

10 May 2018
Revision: 2.0.1 (Intel® SGX SDK version: 2.0.101.44237)

Contents:

Introduction
What's New
System Requirements
Known Issues and Limitations
Disclaimer and Legal Information

1 Introduction

Intel provides Intel® Software Guard Extensions (Intel® SGX) SDK, a software isolation technology, to help 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 Microsoft® Windows® OS. It includes binaries to develop enclave applications. The main components include:
  - Trusted libraries, including standard C library, C++ runtime support, C++ STL, etc.
  - Development tools, including edger8r, signing tool, Microsoft Visual Studio® IDE plug-in, etc.
  - Sample projects.
2 What's New

Intel® Software Guard Extensions SDK includes the following changes in version 2.0.1:


- Provided enhancements to the Intel® SGX Cryptographic library

- Bug fixes

Changes in Previous Releases

Intel® Software Guard Extensions SDK includes the following changes in version 2.0:

- Added the Intel® SGX Enclave Dynamic Memory Management (EDMM) Library that provides support for modifying permissions of committed pages in an enclave. The Intel® SGX EDMM behavior is only available on Intel® SGX 2.0 hardware platforms with the 2.0 Platform Software and Intel® SGX 2.0-capable Windows® OS

Intel® Software Guard Extensions SDK includes the following changes in version 1.9.106.43403:


Intel® Software Guard Extensions SDK includes the following changes in version 1.9.105.42474:

- Security updates to Intel® SGX SDK

- Support for Safe String APIs of the C library in enclaves

- Bug fixes

Intel® Software Guard Extensions SDK includes the following changes in version 1.8.105.40539:
• Changes in public header files:
  
  o **Renamed** SGX_FLAGS_LICENSE_KEYS as SGX_FLAGS_EINITTOKEN_KEY in sgx_attributes.h
  
  o **Renamed** SGX_KEYSELECT_LICENSE as SGX_KEYSELECT_EINITTOKEN in sgx_key.h
  
  o **Renamed** uint32_t extended_eid_group_id as uint32_t xeid in sgx_quote.h
  
  o **Added new error code declarations** in sgx_error.h
  
  o **Added a new interface** sgx_get_ps_sec_prop_ex to get Intel® SGX platform service property in sgx_tae_service.h
  
  o **Added a new interface** sgx_calc_quote_size to calculate Intel® SGX quote size in sgx_uae_service.h
  
  o **Deprecated the** sgx_get_quote_size API in sgx_uae_service.h

• Bug fixes

Intel® Software Guard Extensions SDK includes the following changes in version 1.7.100.35600:

• Upgrade the Cryptography for Intel® Integrated Performance Primitives (Intel® IPP) library to version 9.0 Update 4

• Support nested HW exception in a trusted environment

• Extended C11 and C++11 support

To improve support for C++11 in Windows, the SDK 1.7 includes a new trusted C++ library based on libc++ (see http://llvm.org/svn/llvm-project/libcxx/trunk). If you create a new enclave project with Visual Studio 2015 and check the “C++11” box under Additional Libraries, the new trusted library (sgx_tcxx) will be added to your project. If you update an enclave project to Visual Studio 2015, you are recommended to follow the instructions in the Developer Reference (section C++ Standard Library) to upgrade the C++ library. Otherwise, you will continue to use the trusted library based on STLPort (sgx_tstdcxx). Note that the Standard C++ Library based on STLPort (sgx_tstdcxx) will be deprecated in the next release.
- Support for Protected File System - a basic subset of the regular 'C' file API for Intel SGX enclaves that provides files with both confidentiality and integrity protection.

- Bug fixes

Intel® Software Guard Extensions SDK includes the following changes in version 1.6.101.33070:

- Changed the key exchange library to support remote attestation with a custom key derivation function (KDF).

- Added a new interface in the `sgx_uae_service` library to query the Intel® Enhanced Privacy ID (Intel® EPID) group ID.

- Removed the trusted library `sgx_tcrypto_opt.lib`.

- Linked the Intel® Integrated Performance Primitives (Intel® IPP) Cryptographic library into `sgx_tcrypto.lib` and provided direct access to its API. Included the Intel® IPP Cryptographic library in Intel SGX SDK under the Community Licensing for Intel Performance Primitives.

- Support for new trusted event synchronization library.

- Support for Macros and conditional compilation in EDL.

- Support for a portion of C11 and C++11 features.

- Support for a subset of OpenSSL® APIs in the Intel® SGX SSL library. Exposed APIs are fully compliant with unmodified OpenSSL APIs.

- Support for profiling Intel SGX applications using Intel® VTune™ Amplifier XE. To profile Intel SGX applications, use VTune™ Amplifier XE 2016 Update 2, which contains an analysis type “SGX Hotspots”.

- Provided new APIs (`sgx_mac_aadata`, `sgx_mac_aadata_ex` and `sgx_unmac_aadata`) in the `seal` library.

Intel® Software Guard Extensions SDK includes the following changes in version 1.1. 30214:

- Support Microsoft® Windows® 10 post-RTM Update (codenamed Threshold 2) along with Windows 8.1, Windows 7, and Windows 10

- Provide `sgx_enable_device` API in the `sgx_capable` library

- Deprecate `sgx_enum_enclaves` API
• Fix the localization issue with Microsoft Visual Studio® Plug-in

• Add the Key Exchange library built with the /MT option (sgx_ukey_exchangemt.lib)

Intel® Software Guard Extensions SDK includes the following changes in version 1.0:

• Support Microsoft Windows® 7 64-bit version

• Support Microsoft Windows® 10 64-bit version

3 System Requirements

Software Requirements

• Supported operating systems for Intel® SGX SDK installer:
  o Microsoft Windows® 7 64-bit version
  o Microsoft Windows® 10 November Update (version 1511) 64-bit version
  o Microsoft Windows® 10 Anniversary Update (version 1607) 64-bit version
  o Microsoft Windows® 10 Anniversary Update (version 1703) 64-bit version
  o Microsoft Windows® 10 Fall Creators Update (version 1709) 64-bit version
  o Microsoft Windows® 10 Spring Creators Update (version 1803) 64-bit version

• Supported compiler for Intel® SGX SDK installer:
  o Intel® Parallel Studio XE for Windows® Version 2016 Update 3

• Supported IDE for Intel® SGX SDK installer:
  o Microsoft Visual Studio® Professional 2015 with Update 3
  Microsoft Visual C++ compiler from Microsoft Visual Studio® Professional 2015 is required.

Notes:

1. The Visual Studio 2015 Add-in Tool has been designed to work with the Microsoft Visual Studio Professional 2015 environment. While Visual Studio® Professional 2015 is the recommended environment, the tools may also be installed with the Community and Enterprise versions of Visual Studio 2015.

2. For hardware requirements of Intel® Software Guard Extensions Platform Software for Windows® OS, see the Revision History section of Intel® Software Guard Extensions Platform Software for Windows® OS Release Notes.
4 Known Issues and Limitations

- `sgx_create_enclave` API does not respond if you call `sgx_create_enclave` API in global object of C++ class in DLL.

- Intel® SGX Debugger might stop working after reinstalling Intel SGX SDK because of an issue with Visual Studio* 2015. The workaround is to delete the contents of "%USERPROFILE%\AppData\Local\Microsoft\VisualStudio\14.0\ComponentModelCache" and restart Visual Studio.

- Intel® SGX debugger does not work for the X64 mode in the initial release of Windows 10 Anniversary Update (version 1607). Please update the OS Build to 14393.479 or later. More details on OS build numbers and corresponding KB articles are available at https://technet.microsoft.com/en-us/windows/release-info.aspx.

- The legacy (before 1.6 version) Intel SGX SDK installation entry cannot be removed from “Programs and Features” in Windows Control Panel if you install legacy Intel SGX SDK and upgrade with new installer (after 1.7 version). To work around the issue, please manually uninstall Intel SGX SDK before installing new version.

- At the time of the SDK release, VTune is not functioning with the latest Windows 10 OS versions. For details and updated status on this issue please refer to: https://software.intel.com/en-us/forums/intel-vtune-amplifier-xe/topic/773345
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, VTune, 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.