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

3 July 2019

Revision: 2.4 (Intel® SGX SDK version: 2.4.100.51291)

## Contents:

## 1 Introduction

Intel provides the Intel® Software Guard Extensions Software Development Kit (Intel® SGX SDK), a software isolation technology, to help you protect your applications.

This document provides system requirements, installation instructions, limitations, and legal information for the Intel SGX SDK.

### Product Contents

Intel® Software Guard Extensions SDK package includes:

- 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, and others.
    - Development tools including edger8r, signing tool, Microsoft Visual Studio* IDE plug-in, and other.
    - Sample projects.

# 2 What's New

Intel® Software Guard Extensions SDK (Intel® SGX SDK) includes the following changes in version 2.4:

- Added support for the TCMalloc library
- Added support for Intel® AVX-512 instructions and Intel® SHA Extensions New Instructions (SHA-NI) in trusted libraries.
- Added support for ECDSA based remote attestation.
- Removed support for profiling Intel® SGX applications using the Intel® VTune™ Amplifier XE
- Fixed bugs

## Changes in Previous Releases

Intel® Software Guard Extensions SDK (Intel® SGX SDK) includes the following changes in version 2.3.1:

- Added support for the Intel® SGX Protected Code Loader (Intel® SGX PCL). It is intended to protect Intellectual Property (IP) within the code for Intel® SGX enclave applications

Intel® Software Guard Extensions SDK (Intel® SGX SDK) includes the following changes in version 2.3:

- Added support for Switchless, a new mode of operation to perform calls from or to Intel® SGX enclaves
- Enhanced Edger8r with structure deep-copy feature
- Fixed bugs

Intel® Software Guard Extensions SDK (Intel® SGX SDK) includes the following changes in version 2.2.3:

- Intel® SGX SDK version 2.2.3 has been updated to include OpenSSL 1.1.1a in the installation framework of Intel® SGX SDK, which includes functional and security updates. Users should update to the latest version of the Intel® SGX SDK.

Intel® Software Guard Extensions SDK includes the following changes in version 2.2:

- Provided a new set of Intel SGX common loader APIs.

- Updated the cryptography library to the Intel® Integrated Performance Primitives Cryptography 2019 Update 1.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.1:

- Added support for the Microsoft Visual Studio* Professional 2017:
  - Transitioned to use the Microsoft® Visual C++ Compiler instead of the Intel® C++ Compiler. This is also reflected in the sample projects.
  - Added support to the Universal Windows Platform (UWP). Intel SGX-enabled UWP Applications are supported on Windows 10 October 2018 Update or later.
  - Removed support for the Microsoft Visual Studio* Professional 2013.
  - Deprecated STLPort (sgx_tstdcxx).
- Added support for the Key Separation and Sharing (KSS) feature.
- Added support for the Control Follow Guard inside enclave.
- Fixed bugs.

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

- Updated the cryptography library to the Intel® Integrated Performance Primitives Cryptography 2018 Update 2.1. Mitigated security vulnerability CVE-2018-3617 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3617 ). For more details, refer to the Security Advisory INTEL-SA-00106 (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA00106&languageid=en-fr) and INTEL-SA-00135 (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA00135&languageid=en-fr).
- Provided enhancements to the Intel® SGX Cryptographic library.
- Fixed bugs.

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

- Added the Intel® SGX Enclave Dynamic Memory Management (EDMM) Library, which 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 the Intel® SGX 2.0-capable Windows* OS.

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

- Mitigated security vulnerability CVE-2018-3626 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3626). For more details, refer to the Security Advisory INTEL-SA-00117 (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00117&languageid=en-fr).

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

- Updated security for the Intel® SGX SDK.
- Added support for Safe String APIs of the C library in enclaves.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.8.105.40539:

- Changed public header files:
  - Renamed `SGX_FLAGS_LICENSE_KEYS` as `SGX_FLAGS_EINITTOKEN_KEY` to `sgx_attributes.h`
  - Renamed `SGX_KEYSELECT_LICENSE` as `SGX_KEYSELECT_EINITTOKEN` to `sgx_key.h`
  - Renamed `uint32_t extended_epid_group_id` as `uint32_t xeid` to `sgx_quote.h`
  - Added new error code declarations in `sgx_error.h`
  - Added a new interface `sgx_get_ps_sec_prop_ex` to get the Intel® SGX platform service property in `sgx_tae_service.h`
  - Added a new interface `sgx_calc_quote_size` to calculate the Intel® SGX quote size in `sgx_uae_service.h`
  - Deprecated the `sgx_get_quote_size` API in `sgx_uae_service.h`
- Fixed bugs.

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

- Upgraded the Intel® Integrated Performance Primitives (Intel® IPP) cryptography library to version 9.0 Update 4.

- Added support for a nested HW exception in a trusted environment.

- Extended C11 and C++11 support.

To improve support for C++11 on 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 Microsoft Visual Studio 2015 and check the "C++11" box under Additional Libraries, the new trusted library (sgx_tcxx) is added to your project. If you update an enclave project to Microsoft Visual Studio 2015, 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 the STLPort (sgx_tstdcxx). Note that the Standard C++ Library based on the STLPort (sgx_tstdcxx) will be deprecated in future releases.

- Added support for the Protected File System - a basic subset of the regular 'C' file API for the Intel® SGX enclaves that provides files with both confidentiality and integrity protection.

- Fixed bugs.

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) Cryptography library to the `sgx_tcrypto.lib` and provided direct access to its API. Included the Intel® IPP Cryptography library in the Intel® SGX SDK under the Community Licensing for the Intel® Performance Primitives.

- Added support for a new trusted event synchronization library.

- Added support for Macros and conditional compilation in EDL.

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

- Added support for a subset of OpenSSL* APIs in the Intel® SGX SSL library. Exposed APIs are fully compliant with unmodified OpenSSL APIs.
- Added support for profiling Intel® SGX applications using the Intel® VTune™ Amplifier XE. To profile Intel® SGX applications, use the 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:

- Added support for the Microsoft* Windows* 10 post-RTM Update (codenamed Threshold 2) along with Windows 8.1, Windows 7, and Windows 10.
- Provided `sgx_enable_device` API to the `sgx_capable` library.
- Deprecated `sgx_enum_enclaves` API.
- Fixed the localization issue with the Microsoft Visual Studio* Plug-in.
- Added 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:

- Added support for the Microsoft Windows* 7 64-bit version.
- Added support for the Microsoft Windows* 10 64-bit version.

# 3 System Requirements

## Software Requirements

- Supported operating systems for the Intel® SGX SDK installer:
  - Microsoft Windows* 7 64-bit version
  - Microsoft Windows* 10 November Update (version 1511) or later, including versions 1607, 1703, 1709, 1803 and 1809
- Supported compiler and IDE for the Intel® SGX SDK installer:

- Microsoft Visual Studio* Professional 2017
  Microsoft Visual C++ compiler from Microsoft Visual Studio* Professional 2017 is required.

**Notes:**

1. Visual Studio 2017 Add-in Tool is designed to work with the Microsoft Visual Studio Professional 2017 environment. While Visual Studio* Professional 2017 is the recommended environment, the tools may also be installed with the Community and Enterprise versions of Visual Studio 2017.

2. For hardware requirements of the 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 does not work for the X64 mode in the initial release of Microsoft Windows* 10 Anniversary Update (version 1607). Please, update the OS Build to 14393.479 or higher. For more details on OS build numbers and corresponding KB articles, refer to 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 the Windows Control Panel if you install the legacy Intel® SGX SDK and upgrade it with a new installer (after 1.7 version). To work around the issue, please manually uninstall the Intel® SGX SDK before installing a new version.

- Intel® SGX debugger for Windows* does not support "Conditional Breakpoint" or watching Thread Local Storage variables in the enclave.

- The addresses of all stack variables are randomized. The randomization comes at the expense of increased stack usage. Enclaves built with the Windows 2.2 SDK should increase their stack size setting by 4 KB.

# 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.