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

18 September 2024

Revision: 2.25 Open Source (version: 2.25.100.3)

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 Linux* 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, and others.
    - Sample projects.

2 What's New

Intel® Software Guard Extensions SDK includes the following changes in version 2.25:

- Upgraded to OpenSSL 3.0.14.

- Upgraded to Intel® Integrated Performance Primitives (IPP) Cryptography library version 2021.12.1.
- Supported FIPS 140-3 Certifiable IPP Crypto based Trusted Library.
- Fixed bugs.

Changes in Previous Releases

Intel® Software Guard Extensions SDK includes the following changes in version 2.24:

- Upgraded to OpenSSL 3.0.13.
- Upgraded to Intel® Integrated Performance Primitives (IPP) Cryptography library version 2021.11.
- Upgraded to Protobuf 3.23.2.
- Upgraded MbedTLS to 3.5.2.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.23:

- Supported new OS: Ubuntu* 23.10 64-bit Server version.
- Upgraded to OpenSSL 3.0.12.
- Upgraded MbedTLS to 3.5.0.
- Added SM2 encrypt/decrypt algorithm to the GM/SM (PRC National Commercial Cryptographic Algorithms) sample code.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.22:

- Upgraded to OpenSSL 3.0.10.
- Added interoperable RA-TLS support which follows CCC design.
- Enhanced Protect File System performance and added additional dependency libsgx_pthread.a.
- Added the Constant Time instruction Decoder (CTD) into the default AEX-Notify mitigation handler in order to prevent the introduction of any additional subtle side-channel leakages within the default handler.

- Added Mistletoe 3 mitigations to the IPP Cryptography Library to the AES-ECB, AES-GCM, and AES-CMAC algorithms. These have been incorporated transparently into the sgx_tcrypto library.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.21:

- Upgraded to OpenSSL 1.1.1u.
- Fixed bugs.

Note: This is the final release that will support Ubuntu 18.04 LTS. The next release of this software will not include pre-built packages for Ubuntu 18.04 LTS, aligning with Ubuntu's LTS release Standard Support policy.

Intel® Software Guard Extensions SDK includes the following changes in version 2.20:

- Supported the AEX (Asynchronous Enclave Exit) Notify feature.
- Supported Mbed-TLS Cryptography library (excluding SSL/TLS portion) in Enclave.
- Applied patches to OpenSSL 1.1.1t, fixed CVE-2023-1255, CVE-2023-0465 and CVE-2023-0466.
- Upgraded to Intel® Integrated Performance Primitives (IPP) Cryptography library version 2021.7.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.19:

- Supported the Key Separation and Sharing (KSS) feature in Simulation mode.
- Upgraded to OpenSSL 1.1.1t.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.18:

- Along with the latest processor microcode address CVE-2022-21233.
    - Modified the Switchless library to have mitigations for the associated issue.
- Added support for the Linux kernel APIs for the Enclave Dynamic Memory Management (EDMM) features that are available with the Linux kernel v6.0 or later.

Refer to the SGX SDK developer reference for details on new trusted APIs and enclave configuration for the EDMM features.

- Enabled C++17 within SGX SDK.
- Supported AMX (Advanced Matrix Extensions) in Enclave.
- Replace hardcoded Enclave signing keys in all sample projects with dynamically generated keys.
- Added a new API to allow user to configure enclave internal cache size in the Protected File System library.
- Upgraded to OpenSSL 1.1.1q.
- Supported new OS: Ubuntu* 22.04 LTS 64-bit Server version, CentOS* 8.3 64bits, Red Hat* Enterprise Linux* Server 8.6 (for x86_64), SUSE* Linux* Enterprise Server 15.4 64bits, Debian* 10 and Anolis* OS 8.6.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.17.1:

- Along with the latest processor microcode address CVE-2022-21233.
    - Modified the Edger8r to generate code with mitigations for the associated issue.
    - Modified the API memcpy and memcpy_s to have mitigations for the associated issue.

Intel® Software Guard Extensions SDK includes the following changes in version 2.17:

- Along with the latest processor microcode address CVE-2022-21123, CVE-2022-21125 and CVE-2022-21166.
- Upgraded to Protobuf 3.20.
- Upgraded to OpenSSL 1.1.1o.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.16:

- Upgraded to OpenSSL 1.1.1m.

- Provided RA-TLS (Remote Attestation based Transport Layer Security) APIs and Samples.
- Supported PKRU (Protection Key rights Register) in Enclave.
- Added APIs of SHA384 and VerifyReport2 to support TDX.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.15.1:

- Upgraded to OpenSSL 1.1.1l.

Intel® Software Guard Extensions SDK includes the following changes in version 2.15:

- Added software prevention of fault injection attacks.
- Upgraded to Intel® Integrated Performance Primitives (IPP) Cryptography library version 2021 update 3.
- Upgraded to GNU Binutils 2.36.1. Stopped providing ld.gold (developers should use ld instead).
- Supported Google Protobuf C++.
- Enabled C++14 within SGX SDK.
- Added SM2/3/4 (PRC National Commercial Cryptographic Algorithms) Samples.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.14:

- Supported loading enclave at 0 address.
- Supported the SIGSEGV and SIGFPE exception handling inside Enclave in Simulation mode.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.13.3:

- Upgraded to Intel® Integrated Performance Primitives (IPP) Cryptography library version 2020 update 3.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.13:

- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.12:

- Supported new OS: Ubuntu 20.04 and CentOS 8.2.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.11:

- Supported new OS: RHEL 8.2 and SUSE 15.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.10:

- Provided a reproducible SDK.
- Supported new OS: RHEL 8.1, CentOS 8.1 and Fedora 31.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.9.1:

- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.9:

- Fixed bugs.
- Changes to address CVE-2020-0551.

Intel® Software Guard Extensions SDK includes the following changes in version 2.8:

- Supported open source version of Intel® Integrated Performance Primitives (Intel® IPP) cryptography library.
- Support for the Intel® Deep Neural Network Library (DNNL) library, OpenMP library* and POSIX Threads (Pthread) library*.

  (*) Limited support only. Refer to the Developer Reference for additional details.
- Refactored the switchless library. Developers have to opt-in, i.e. import the sgx_tswitchless.edl into their enclave EDL file and link with the trusted library

(sgx_tswitchless.a) and untrusted library (sgx_uswitchless.a), in order to do enclave transitions using threads.

- Removed sgx_uae_platform.h, sgx_tae_service.h, sgx_tae_service.edl, libsgx_platform.so and libsgx_platform_sim.so
- Updated Local Attestation sample project to demonstrate key exchange flow between multiple processes.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.7.1:

- Enhancements to address CVE-2019-14565 and CVE-2019-14566.
- Added new memory allocation APIs. For more details, please refer to INTEL-SA-00219.

Intel® Software Guard Extensions SDK includes the following changes in version 2.7:

- Added a command option "-resign" for Signing Tool.
- Split the header file of Un-trusted Architecture Services.
    - Split sgx_uae_service.h to sgx_uae_epid.h, sgx_uae_launch.h, sgx_uae_platform.h and sgx_uae_quote_ex.h.
- Supported Red Hat* Enterprise Linux* Server 8.0 (for x86_64).
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.6:

- Added support for Reproducible Enclave Build using Docker file.
- Added support for Intel® AVX-512 instructions and Intel® SHA Extensions New Instructions (SHA-NI) in trusted libraries.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.5.2:

- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.5:

- Added new APIs in `sgx_uae_service.h` and `sgx_ukey_exchange.h`. The set of legacy APIs supports EPID only and the set of new APIs supports ECDSA quotes.
- Enhanced Edger8r with structure deep-copy feature.
- Fixed bugs.

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

- Added support for the Key Separation and Sharing (KSS) feature.
- Provided a set of new encryption and decryption functions such as sgx_hmac256_*.
- Provided a new untrusted API: `sgx_get_target_info.`
- Provided a new untrusted API: `sgx_create_enclave_from_buffer_ex.`
- 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 2.3:

- Added support for the Ubuntu* 18.04 LTS 64-bit Desktop and Server version.
- Provided a new set of the Intel SGX common loader APIs in sgx_enclave_common.h.
- Provided a sample code for the Switchless Call.
- Provided a new API in tcrypto: `sgx_ecc256_calculate_pub_from_priv`.
- Changed the `sgx_create_enclave` API: the function ignores the parameter of a launch token and does not update it after the function succeeds.
- Fixed bugs.

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

- Added support for Switchless, a new mode of operation to perform calls from or to Intel SGX enclaves.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.1.3:

- Updated the cryptography library to 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 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.
- 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.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 2.1.2:

- Mitigated security vulnerability CVE-2018-3626 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3626). For more details, refer to 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 2.1.1:

- Updated security to the Intel® SGX SDK.
- Added the new `sgx_register_wl_cert_chain` API that allows the Intel® SGX application to register an enclave.
- Added support for the CentOS* 7.4.
- Added support for the SUSE* Linux Enterprise Server 12.
- Fixed bugs.

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

- Added support for the Intel® SGX Enclave Dynamic Memory Management (Intel® SGX EDMM) to dynamically manage enclave memory: dynamic heap expansion, dynamic stack expansion, dynamic thread creation, and page attribute modification.
- Added support for the Red Hat* Enterprise Linux* Server 7.4.

- Added support for Safe String APIs of the C library in an enclave.
- Added an option to build the Intel® SGX SDK using the Intel® SGX SSL crypto library instead of the Intel® Integrated Performance Primitives Cryptography open source version.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.9.100.39124:

- Added C++11 support

  To improve support for C++11 on the Linux* OS, the Linux* SDK 1.9 includes a new trusted C++ library based on libc++ (see http://llvm.org/svn/llvm-project/libcxx/trunk). Note that the Standard C++ Library based on 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 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 1.8.100.37689:

- Added support for the TCMalloc library.
- Added support for new Linux* distributions.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.7.100.36470:

- Updated the cryptography for the Intel® Integrated Performance Primitives (Intel® IPP) library to version 9.0 Update 4.
- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes in version 1.6.100.34478:

- Added new `setjmp/longjmp` APIs in the trusted C library.

- Fixed bugs.

Intel® Software Guard Extensions SDK includes the following changes before version 1.5.100.32783:

- Added support for profiling Intel® SGX applications using the Intel® VTune™ Amplifier. To profile Intel® SGX applications, use the VTune™ Amplifier 2016 Update 2, the "Intel SGX Hotspots" analysis type.
- Added the Intel® SGX Eclipse* plug-in to create Intel® SGX enclave projects.
- Added support for the implicit Thread Local Storage (TLS).
- Added support for a nested HW exception in a trusted environment.

3 System Requirements

- Supported Linux* OS distributions:
    - Ubuntu* 20.04 LTS 64-bit Desktop and Server version
    - Ubuntu* 22.04 LTS 64-bit Server version
    - Ubuntu* 24.04 LTS 64-bit Server
    - CentOS* 8.3 64bits
    - CentOS* Stream 9
    - Red Hat* Enterprise Linux* Server 9.2 (for x86_64)
    - SUSE* Linux* Enterprise Server 15.4 64bits
    - Debian* 10
    - Anolis* OS 8.6

NOTE: It is highly recommended to use the listed Linux* OS distributions. Other distributions have not been tested.

Intel® SGX developers need GCC 7.3 or later and latest GNU Binutils in order to address CVE-2020-0551 in their enclaves. Intel is posting latest as, ld, objdump and gold executables from GNU Binutils here.

4 Known Issues and Limitations

- The GM/SM Samples are solely for reference purposes. If intending to use them in production, ensure a thorough cryptographic code review is conducted.
- When utilizing the trusted cryptography library with SGXSSL/OpenSSL 3.0, it's necessary to adjust the value in the enclave signing configuration XML file, specifically within the <HeapMaxSize> tag. This adjustment is particularly important for enclaves that involve multiple threads.
- In Intel® SGX SDK 2.18, big TCS number will potentially cause Enclave to crash. This is due to the compiler using SSE instructions/XMM registers for optimization and the failure in SDK to preserve the contents of XMM registers during exception handling. It is recommended that users add the "-mno-sse" option when compiling the EDMM enabled Enclave to avoid this error.
- Intel® SGX SDK 2.17.1 has memcpy performance degradation because of the security fix for CVE-2022-21233. We have enhanced memcpy performance in 2.18.
- If AMX is enabled and causes ssa_frame_size to exceed 1 page, the debugger will not work as expected because correct ssa_gpr info cannot be obtained or set until thread_data is initialized in tRTS.
- Considering the potential impact on performance and the limited security implication, we decided to not mitigate CVE-2022-21233 for the Switchless library in Linux 2.17.1.
- ippsPRNGenRDRAND/ippsPRNGenRDRAND_BN/ippsTPRNGenRDSEED/ippsTPRNGenRDSEED_BN are not supported on Gemini Lake platform in intel® Integrated Performance Primitives (IPP) Cryptography library.
- Intel® Integrated Performance Primitives (IPP) Cryptography library version 2020 Update 3 contains a bug in the implementation of the AES-GCM algorithm that takes advantage of the new cryptographic instructions introduced to Ice Lake processors. To work around this issue, the trusted library sgx_tcrypto in Intel® SGX SDK 2.13.3 release does not include any IPP Cryptography specific optimizations for the Ice Lake architecture family.
- Intel® SGX SDK 2.9 and later versions requires GCC 7.3 or above.
- The SDK installer will not be provided for below OSes because the native GCC version doesn't meet the requirement:
    - Ubuntu 16.04 LTS Server 64bits
    - Red Hat Enterprise Linux Server release 7.4 64bits
    - Red Hat Enterprise Linux Server release 7.6 64bits
    - CentOS 7.5 64bits
    - Fedora 27 Server 64bits
    - SUSE Linux Enterprise Server 12 64bits

- Intel® SGX for Linux* OS does not support setting a different charset in GNU* Project Debugger (GDB*).
- Building the Intel® SGX SDK sample project “RemoteAttestation” is possible only within the Intel® SGX SDK installation folder.
- Intel® SGX does not support the “long long” type in C++ templates.
- `sgx-gdb` depends on GDB* 7.9.1 or later versions. Please upgrade GDB* if its version is lower than 7.9.1.
- If Intel® SGX EDMM feature is used, you should use the version 2.2 or higher of both Intel® SGX PSW and Intel SGX SDK 2.2.
- `sgx-gdb` does not support 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 Linux 2.4 SDK should increase their stack size setting by 4 KB.
- Intel® SGX PCL interaction with KSS: In Intel® SGX SDK 2.4, if the Intel® SGX PCL sealing enclave is configured to support KSS (Enclave configuration XML includes entry EnableKSS with value 1) then when sealing the Intel® SGX PCL decryption key, the Intel® SGX PCL sealing enclave cannot use sgx_seal_data. Instead, the Intel® SGX PCL sealing enclave must use sgx_seal_data_ex and assign key_policy such that SGX_KEYPOLICY_MRSIGNER bit is set to 1 and KSS bits (SGX_KEYPOLICY_CONFIGID, SGX_KEYPOLICY_ISVFAMILYID and SGX_KEYPOLICY_ISVEXTPRODID) are set to 0.

5 Disclaimer and Legal Information

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.

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.