Intel® Software Guard Extensions (Intel® SGX) Platform Software for Linux OS*

Release Notes

25 April 2024

Revision: 2.24.1 Open Source (version: 2.24.100.3)

Contents:

Introduction

This document provides system requirements, installation instructions, limitations, and legal information for the Intel® Software Guard Extensions (Intel® SGX) Platform Software (PSW).

Product Contents

The Intel® Software Guard Extensions PSW package includes:

- Intel® SGX Architecture Enclaves
- Intel® SGX Runtime System Library
- Intel® SGX Architecture Enclave Service Manager (AESM)

What's New

Intel® Software Guard Extensions PSW includes following changes in 2.24.100.3:

- Upgraded Intel® DCAP Ring3 Abstraction Layer (R3AAL) library to support ConfigFS-TSM as communication channel between host and guest for TDX remote attestation
- Upgraded Intel® DCAP Quote Verification Enclave to integrate OpenSSL/SgxSSL 3.0.13
- Upgraded new TDX attestation result "TD_RELAUNCH_ADVISED" in Intel® DCAP Quote Verification Library (QVL) and Appraisal Engine
- Fixed bugs

Changes in Previous Releases

Intel® Software Guard Extensions PSW includes following changes in 2.23.100.2:

- Introduced the Intel® DCAP Appraisal Engine within quote verification library, empowering users to evaluate verification results against diverse policies
- Upgraded Intel® SGX Quote Verification Enclave to integrate OpenSSL/SgxSSL 3.0.12
- Added Rust wrapper for quote provider library APIs
- Fixed bugs

Intel® Software Guard Extensions PSW includes following changes in 2.22.100.3:

- Resigned all Intel® SGX Architecture Enclaves
- Upgraded Intel® SGX Quote Verification Enclave to integrate OpenSSL/SgxSSL 3.0.10
- Added Attestation Library support for Intel(R) TDX Migration TD
- Added Rust wrapper for low-level Quote Generation APIs
- Enabled 'SE_TRACE' log in release binary
- Updated Rust QVL wrapper to use native Rust structure for quote verification collateral
- Added a limitation in the DCAP QVL to only allow the user to set the QvE load policy once
- Fixed bugs

Intel® Software Guard Extensions PSW includes following changes in 2.21.100.1:

- Introduced Intel® TDX 1.4 & 1.5 support
- Upgraded Ring3 Abstraction Layer (R3AAL) library to support Intel® TDX MVP 6.2 kernel
- Enhanced quote verification performance in multi-thread scenarios
- Upgraded Intel® SGX Quote Verification Enclave to integrate latest OpenSSL/SgxSSL 1.1.1u
- Fixed bugs

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 PSW includes following changes in 2.20.100.4:

- Applied CVE-2023-1255, CVE-2023-0465, and CVE-2023-0466 patches to SgxSSL/OpenSSL 1.1.1t
- Upgraded Intel® SGX Quote Verification Enclave to integrate updated SgxSSL
- Enhanced the attestation local cache functionality by giving users the option to provide their own cache file
- Enabled QPL/QCNL log in DCAP samples
- Fixed bugs

Note: Reference LE (A reference implementation of Launch Enclave for 'Flexible Launch Control') will be deprecated from this release.

Intel® Software Guard Extensions PSW includes following changes in 2.19.100.3:

- Upgraded Intel® SGX Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1t
- Added new API in quote verification library to extract FMSPC (Family-Model-Stepping-Platform-CustomSKU) value from ECDSA quote
- Added Rust support for SGX ECDSA quote generation
- Added Linux kernel 5.19 support in TDX R3AAL (Ring 3 Attestation Abstraction Layer)
- Removed Protobuf in TDX QGS (Quote Generation Service) and R3AAL (Ring 3 Attestation Abstraction Layer)
- Fixed bugs

Intel® Software Guard Extensions PSW includes following changes in 2.18.101.1:

- Fixed enclave load failure in environments where no symbolic links, /dev/sgx/{enclave, provision} are created to point to the default SGX device nodes exported by kernel, /dev/{sgx_enclave, sgx_provision}, respectively

Intel® Software Guard Extensions PSW includes following changes in 2.18.100.3:

- Upgraded Intel® SGX Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1q
- Upgraded Intel® SGX QE3 to make it backward compatible
- Improved ECDSA quote generation and verification performance by caching PCK certificates and collaterals in memory and disk drive
- Added Java support for quote verification library
- Added new APIs to unify Intel® SGX and TDX quote verification in Quote Verification Library
- Added Advisory ID in ECDSA quote verification supplemental data
- Added Intel® TDX support in RA-TLS (Remote Attestation based TLS) library
- Improved TDX quote generation throughput in vsock mode
- Added Rust support for TDX quote generation

- 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
- Fixed bugs

The download.01.org directory layout restructuring – Possible Impact

1. Debian repository/packages:

You may continue accessing the Debian repo/packages in the sgx_repo directory, as suggested in the Linux Installation Guide.

Directly accessing individual Debian packages from the directories listed below is no longer be possible:

a) From latest directory
b) From a specific release under sgx-linux directory
c)From a specific release under sgx-dcap directory

2. DCAP tools will be moved to the distro directory and the tools directory will be removed.

If you access the tools in your project and get a download failure, please update the URL accordingly.

Intel® Software Guard Extensions PSW includes following changes in 2.17.100.3:

- Re-signed all the Intel® SGX Architecture Enclaves (AEs) to address CVE-2022-21123, CVE-2022-21125 and CVE-2022-21166
- Added Intel® TDX Attestation support
- Added Rust support for ECDSA quote verification
- Upgraded Intel® ECDSA Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1o
- Fixed bugs

Note: There is no official support for some newer Linux distros yet, such as Ubuntu 21.10. But note that newer Linux distros may restrict access to the SGX enclave device node, "/dev/sgx_enclave", to members of the "sgx" group. In that case, please add the group to the user ID to run enclave apps using this command: " usermod -aG sgx <uid>"

Intel® Software Guard Extensions PSW includes following changes in 2.16.100.4:

- Enhanced QPL (Quote Provider Library) to support caching Intel® PCK (Provisioning Certificate Key) certificate chain in local memory, or retrieving Intel® PCK cert chain from local HTTP/S address
- Upgraded Intel® ECDSA Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1m
- Introduced Intel® ID enclave for QE identity generation
- Fixed bugs

Intel® Software Guard Extensions PSW includes following changes in 2.15.101.1:

- Upgraded Intel® ECDSA Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1l
- Fixed bugs

You can refer to README to get the source code of Intel® Software Guard Extensions prebuild Architecture Enclaves

Intel® Software Guard Extensions PSW includes the following changes in 2.15.100.3:

- Upgraded Intel® Integrated Performance Primitives (IPP) Cryptography library to version 2021 update 3
- Upgraded Intel® SGX Architecture Enclaves based on new IPP crypto library
- Added support in Intel® Quote Provider Library (QPL) to retrieve SGX ECDSA quote verification endorsements from Intel® Provisioning Certificate Service (PCS). User can configure PCCS or PCS in QPL's config file
- Updated SGX ECDSA quote verification library (QVL) and quote verification enclave (QvE) to support CRL in different encoding
- Updated SGX ECDSA quote verification library (QVL) and quote verification enclave (QvE) to hardcode Intel® root public key instead of root certificate
- Fixed bugs

Intel® Software Guard Extensions PSW includes the following changes in 2.14.100.2:

- Supported loading enclave at address 0
- Upgraded Intel® Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1k
- Updated the DCAP driver V1.33 with stability fixes, released as V1.33.2. This is to support legacy solutions not ready to transition to the latest DCAP driver V1.41 or kernel 5.11+
- Fixed bugs

SGX support has been built in mainline kernels since release 5.11. To avoid future incompatibility issues, it is strongly recommended for solutions using the DCAP driver to transition to use kernel 5.11 or above.

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

- Upgraded Intel® Integrated Performance Primitives (IPP) Cryptography library to version 2020 update 3
- Upgraded Intel® SGX Architecture Enclaves based on new IPP crypto library

This is the final release that will support Ubuntu 16.04 LTS. The next release of this software will not include pre-built packages for Ubuntu 16.04 LTS aligning with Ubuntu's LTS release Standard Support policy

Intel® Software Guard Extensions PSW includes the following changes in 2.13.100:

- Added more log information in PSW components to help identifying possible issues
- Upgraded OpenSSL and SgxSSL to latest version 1.1.1i in DCAP components
- Added data base migration support in PCCS
- Fixed bugs

Intel® Software Guard Extensions PSW includes the following changes in 2.12.100:

- Added Ubuntu 20.04 and CentOS 8.2 support
- Added Intel® Provisioning Certification Service V3 API support for ECDSA attestation

- Fixed bugs

Intel® Software Guard Extensions PSW includes the following changes in 2.11.100:

- Supported Red Hat Enterprise Linux 8.2 and CentOS 8.2
- Provided standalone Intel® SGX DCAP Quote verification library installer
- Added Intel® SGX DCAP Platform Certificate ID Retrieval Tool and Multi-package Registration Agent (MPA) installers into SGX installation repo.
- Fixed bugs

Intel® Software Guard Extensions PSW includes the following changes in 2.10.100:

- Supported Fedora 31, CentOS 8.1 and Red Hat Enterprise Linux 8.1.
- Supported user to specify platform id in PCK Cert ID Retrieval Tool's command line option.
- Added ability to execute Platform Cert ID Retrieval Tool on multi-package platforms without loading enclaves. PCCS now supports this functionality. The platform still needs to support SGX.
- Updated Platform Cert ID Retrieval Tool and Multi-package registration tool to align with BIOS platform manifest changes.
- Added .deb and .rpm installers for Platform Cert ID Retrieval Tool and Multi-package Registration Agent.
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.9.101:

- Supported to query Intel® SGX attestation key ID list
- Provided Intel® SGX Data Center Attestation Primitive (DCAP) driver to support ECDSA attestation on platforms which support Intel® SGX Flexible Launch Control.
    - Please note this new DCAP driver does not support Intel® SGX EDMM feature.
    - This DCAP driver is in addition to the existing SGX driver (Out of Tree driver) which is still provided in the download point, side by side.
    - So now there are two drivers in the download repo and user should and only needs to install one of the two drivers.
    - Please refer to <<Intel SGX Installation Guide for Linux OS.pdf>>'s "Intel® SGX Driver Installation" section to know when to use and know how to install Intel® SGX DCAP driver.
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.9.100:

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

Intel® Software Guard Extensions PSW includes the following changes in 2.8.100:

- Added support for modularized installation.
- Added support for running SGX applications inside Docker containers.
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.7.101:

- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.7.100:

- Added support for new version Intel® Provisioning Certification Server interfaces.
- Added new libraries libsgx_epid.so, libsgx_launch.so, libsgx_platform.so and libsgx_quote_ex.so.
- Removed Intel® SGX Platform Service Operation and Provisioning bundles. As a result, tae_service library API and sgx_report_attesation_status() API would return error code which indicates the service is unavailable.
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.6.100:

- Added support for both EPID and ECDSA-based quote for quoting related interfaces in sgx_uae_service library.
- Updated key exchange library to support both EPID and ECDSA-based remote attestation.
- Added support for a new interface to check platform information blob from remote attestation response message.
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.5.100:

- Added support for ECDSA quote based remote attestation.
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.4.100.48163

- Supported Intel® SGX Enclave Common Loader library
- Updated Intel® Architecture Enclaves to use Intel® IPP Cryptography 2019 Update 1 library
- Fixed bugs

Intel® Software Guard Extensions PSW includes the following changes in 2.3.100.46354:

- Added support for Ubuntu* 18.04 LTS 64-bit Desktop and Server version
- Updated the Intel® SGX PSW installer for Ubuntu*. The following changes are introduced:
    - Using .deb installer
    - Using name `libsgx-enclave-common_{version string}-1_amd64.deb`.
    - Installing the Intel® SGX Enclave Common loader library.
- Fixed SGX Quoting enclave bug, which caused the invalid signature error when a user upgraded the SGX PSW 1.6 version to a higher version and did remote attestation
- Updated the SGX Provisioning Cert Enclave to fix error code bug
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.2.100.45311:

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

Intel® Software Guard Extensions PSW includes the following changes in 2.1.103.44322 release:

- Updated the cryptography lib 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=2018-3617). For more details, refer to Intel Security Advisory INTEL-SA-00106(https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00106&languageid=en-fr) and INTEL-SA-00135(https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00135&languageid=en-fr).
- Updated the Intel® SGX platform service Dal applet.
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in 2.1.102.43402 release:

- Mitigated security vulnerability CVE-2018-3689 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3689). For more details, refer to Security Advisory INTEL-OSS-10004 (https://01.org/security/advisories/intel-oss-10004)
- 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 PSW includes the following changes in 2.1.101.42529 release:

- Updated security to the Intel® SGX PSW.

Intel® Software Guard Extensions PSW includes the following changes in version 2.1.100.42002:

- Added support for CentOS* 7.4
- Added support for SUSE* Linux Enterprise Server 12
- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in version 2.0.100.40905:

- Added support for 3072 bit Intel® SGX provisioning server public key
- Added support for the Intel® SGX Enclave Dynamic Memory Management (EDMM)
- Added support for Red Hat* Enterprise Linux* Server 7.4.

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

- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in version 1.8.100.37689:

- Added support for the Trusted Platform Service
- Added support for RedHat* and CentOS*.

System Requirements

Hardware Requirements

- 6th Generation Intel® Core™ Processor or newer.

Software Requirements

- Supported Linux* OS distributions:
    - Ubuntu* 20.04 LTS 64-bit Desktop and Server version
    - Ubuntu* 22.04 LTS 64-bit Server version
    - Ubuntu* 23.10 64-bit Server version
    - 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:

1. Intel® SGX PSW supports the Intel® Xeon® Processor E3 Server V5 and onwards platforms if the platform processor and BIOS supports the Intel® SGX. Please check with OEM/ODM regarding BIOS support for enabling the Intel® SGX.
2. If you need to use the Intel® SGX platform service, install the Intel® Management Engine (Intel® ME) software components. This is optional, you can skip this if you do not need to use the Intel® SGX platform service.
3. Intel® SGX platform service is not supported on the Intel® Xeon® Processor E3 Server and onwards platforms.

Known Issues and Limitations

- Intel® SGX PSW 2.24.1 release has a known vulnerability (CVE-2024-21511) in the mysql2 module installed by PCCS. To address this issue, execute "sudo -u pccs npm audit fix" in the PCCS directory following the installation.
- Intel® SGX PSW 2.9.1 does not include the latest functional and security updates in 3rd part components (OpenSSL). The next release of the Intel® SGX SDK for Windows is targeted to be released in May 2020 and will include additional functional and security updates. Customers should update to the latest version as it becomes available.
- Intel® SGX PSW 2.8 does not include the latest functional and security updates. Intel® SGX PSW 2.8.1 is targeted to be released in March 2020 and will include additional functional and security updates. Customers should update to the latest version as it becomes available.
    - OpenSSL 1.1.1d with an unmitigated CVE (CVE-2019-1551) is used in untrusted part. The CVE is not exploitable in SGX software stack.
- Occasionally Intel® SGX aesmd service fail to retrieve the enclave launch allow list from internet, this may cause failure to load those enclaves that need the latest enclave launch allow list support. The user can work around this through restarting Intel® SGX aesmd service.

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, Xeon, and Xeon Phi are trademarks of Intel Corporation in the U.S. and/or other countries.

This software and the related documents are Intel copyrighted materials, and your use of them is governed by the express license under which they were provided to you (**License**). Unless the License provides otherwise, you may not use, modify, copy, publish, distribute, disclose or transmit this software or the related documents without Intel's prior written permission.

This software and the related documents are provided as is, with no express or implied warranties, other than those that are expressly stated in the License.

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.