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

2 July 2019
Revision: 2.4.1

Contents:

1   Introduction

This document provides system requirements, limitations, and legal information for the Intel® Software Guard Extensions (Intel® SGX) platform software (PSW) for Windows* OS.

Product Contents

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

Ingredient Binary	Version String
Intel® SGX Runtime System Library	2.4.100.51291
Intel® SGX Launcher Enclave (LE)	2.4.100.50851
Intel® SGX Platform Services Initialization Enclave (PSE-pr)	2.4.100.50851
Intel® SGX Quoting Enclave (QE)	2.4.100.50851
Intel® SGX Provisioning Enclave (PvE)	2.4.100.50851
Intel® SGX Provisioning Cert Enclave (PcE)	2.4.100.50851
Intel® SGX Platform Services Operation Enclave (PSE-op)	2.4.100.50851
Intel® SGX Application Enclave Service (AESM)	2.4.100.51291
Intel® SGX device driver for Windows* 7 (64 bit only)	2.4.100.51020
Intel® SGX device driver for Windows* 10 October 2018 Update (version 1809) 64-bit version	2.4.100.51228

Windows* 10 Fall Creators Update (Version 1709)

Windows* 10 April 2018 Update (version 1803)

Windows* 10 October 2018 Update (version 1809)

Intel® SGX PSW package conforms to the new driver model that Microsoft* requires on Windows* systems (Universal Windows Driver/UWD – DCH).

To learn more about the driver model, follow the links below:

https://channel9.msdn.com/Events/WinHEC/WinHEC-Online/Understanding-Extension-INFs-and-Component-INFs

https://docs.microsoft.com/en-us/windows-hardware/drivers/install/using-an-extension-inf-file

The Intel SGX DCH implementation is as follows:

- Base INF provides a fundamental driver:

    o It attaches to the Intel® SGX ACPI device when the Intel® SGX is enabled on a system: ACPI\INT0E0C.

    o Base INF version is 2.4.100.51228 and it is hosted by the Windows* Update. For details, see the Microsoft* Update Catalog: http://www.catalog.update.microsoft.com/Search.aspx?q=INT0E0C

- Extension INFs are used by OEMs to customize and provide additional features.

    o Extension INF attaches to the same hardware device as the base INF. For the Intel® SGX, the hardware device is ACPI\INT0E0C.

    o In addition, the INF creates a new Software Component device: swc\ven_int&dev_0e0c.

    o Due to current limitations, the extension INF functionality is merged into the base INF.

- Component INFs are typically used by the OEMs. The component INFs attach to the software device (swc\ven_int&dev_0e0c) created by the extension INF.

    o Component INF version is 2.4.100.51291.

    o In the current implementation, the component INF for the Intel® SGX PSW uses a series of INF directives (CopyFile, AddReg, and others) but does NOT use the traditional desktop EXE installer (via AddSoftware, CoInstaller, or other mechanisms).

    o If the Intel® SGX Application Enclave Services Manager (Intel® SGX AESM), libraries, or something else require update, you do not need to modify the base INF. The component INF package can be updated independently without modifying the base driver package.

2   What's New

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.4.1:

- o   Support ECDSA based Quote and corresponding key exchange library interface
- o   Support new interface to check platform information blob from remote attestation response message
- o   Updated SGX Window7 driver to remove 2M EPC size reservation for Intel® Provisioning Certificate Enclave (PCE), Intel® Quoting Enclave (QE) and Intel® Provisioning Enclave (PvE)
- o   Bug fixes

Changes in previous releases

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.3.2:

- o   Bug fixes

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

- o   Bug fixes

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.2.4:

- o   Updated sgx_psw.inf to fix bug.

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

- o   Intel® SGX PSW version 2.2.3 has been updated to include OpenSSL 1.0.2q in Intel® SGX Application Enclave Service (AESM) and OpenSSL 1.1.1a in the installation framework of the EXE version of Intel® SGX PSW, which includes functional and security updates. Users should update to the latest version of the Intel® SGX PSW.

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.2.102.49005:

- o   Updated Intel® SGX Platform Service DAL Applet

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.2.101.48504:

- o Support Intel® CSME version 1040 and above

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) includes the following changes in version 2.2.100.47975:

- o Added support for the Intel® SGX Launch Configuration Service and the Intel® SGX Enclave Common Loader library in Microsoft Windows* 10 Anniversary Update, version 1607 or higher.

- o Enhancement to address security vulnerability INTEL-SA-00203 (https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00203.html)

- o Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in version 2.1.100.46245:

- o Updated the Intel SGX Launcher Enclave and the Intel SGX Windows* 7 device driver to support enclave loading using the Key Separation and Sharing feature if this feature is available. For details on the feature, see the Intel® Software Developer Manual.

- o Fixed the Intel SGX Quoting enclave bug that caused the invalid signature error when a user upgraded the Intel SGX PSW 1.6 version and did a remote attestation.

- o Updated the Intel SGX Platform Services Operation Enclave to use the Intel SGX local attestation library version 2.

- o Updated the Intel SGX Provisioning Cert Enclave and the Intel SGX Provisioning Enclave to fix error code bugs.

- o Fixed other bugs.

Intel® Software Guard Extensions PSW includes the following changes in version 2.0.101.44269:

- o 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=2018-3617). For more details, refer to the 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).

- o Updated the Intel® SGX platform service Dal applet.
- o Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in version 2.0.100.43647:

- o Added support for the Intel® SGX 2.0 instruction set.
- o Fixed bugs.

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

- o 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)
- o Updated the Intel® SGX PSW installer to prevent installation of the Intel SGX PSW 1.6 and 1.7 version installers.

Intel® Software Guard Extensions PSW includes the following changes in version 1.9.105.42329:

- Added the Intel® SGX PSW .inf installer to support the Microsoft Windows* 10 Fall Creators Update (version 1709) 64-bit version and above. The Intel® SGX PSW .inf installer stores files to the Microsoft Windows* DriverStore instead of the Program Files location.

- Intel® SGX PSW installer application (.exe) stopped supporting the Microsoft Windows* 10 Fall Creators Update (version 1709) 64-bit version and higher.

- Removed the DotNetSystemProxy.dll from the Intel® SGX PSW .inf installer.

- Updated security for the Intel® SGX Application Enclave Service (AESM) and the Intel® SGX Application Enclaves.

- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in version 1.9.100.41172:

- Added support for the Intel® SGX Platform Services in the 8th Generation Intel® Core™ Processor (Intel® microarchitecture code name Coffee Lake) platform.

- Added support for the 3072 bits Intel® SGX provisioning server public key.

- Fixed bugs.

Intel® Software Guard Extensions PSW includes the following changes in version 1.8.106.40803:

- Fixed the "Unknown Device" issue on the Windows* 10 Fall Creator Update (version 1709). The Intel® SGX now automatically installs the device driver, which can also be installed as a Windows* update.

- Intel® SGX provisioning backend server started using port 80.

3 System Requirements

Hardware Requirements
- 6th Generation Intel® Core™ Processor or newer

Software Requirements
- Supported 64bit operating systems for the Intel® SGX PSW installer:

  o Microsoft Windows* 7 64-bit version
  o Microsoft Windows* 10 November Update (version 1511) or later, including versions 1607, 1703, 1709, 1803 and 1809.
  o Microsoft Windows Server 2016
  o Microsoft Windows Server 2019
  Note:
  o Intel® SGX PSW does not support the Microsoft Windows* 32-bit operating system.
  o Microsoft Windows Server editions supported on Intel® Xeon® Processor E3 Server V5 and V6 platforms.

- If you need to use the Intel® SGX platform service, install the full set of Intel® Management Engine (Intel® ME) software components.

  Note: To install the full set of Intel® ME software components, perform installation with `SetupMe.exe` instead of `MEISetup.exe` (HECI driver only).

4 Known Issues and Limitations

- Intel® SGX only supports the integrated Windows* authentication proxy scheme. The Basic and the Digest authenticated proxy schemes are not supported.
- You cannot load any enclave in Windows 7/8.1 if the Microsoft* Universal C Runtime (CRT) is not installed on the system. To resolve this issue, you can install the Windows Update for the Universal CRT (KB2999226) on Windows.
- You cannot install the Intel® SGX PSW when you install Windows* OS in a legacy mode and the Intel® SGX is set as "Software Controlled" in BIOS. Configure the Intel® SGX as "Enabled" in BIOS before you install the Intel® SGX PSW.
- Legacy (before 1.6 version) Intel® SGX PSW installation entry cannot be removed from "Programs and Features" in the Windows* Control Panel if you install the legacy Intel® SGX PSW and upgrade it with a new installer (after 1.7 version). To resolve the issue, manually uninstall the Intel® SGX PSW before installing a new version.
- Intel® SGX PSW .exe installer returns an error if a higher version of the Intel SGX PSW installer is already installed.
- Applications that use the Intel® SGX PSW in Microsoft Windows* 10 Version 1709/1803/1809 and do not have proxy settings for their users, require a system proxy setting. Alternatively, the Intel® SGX AESM proxy configuration tool can be used.
- After installing the Intel® SGX PSW .inf installer, the Intel® SGX AESM service status is set to "stopped". It does not impact enclave loading by the Intel® SGX application. When the enclave is loaded, the Intel® SGX AESM service status is set to "running".
- Installation of the Intel® SGX PSW .inf installer has no impact on the Intel SGX PSW .exe installer of version 1.7 but it can affect the Intel SGX PSW .exe installer of version 1.8 or higher.
- User can't verify Intel® ECDSA QE's report outputted from sgx_get_quote_ex() function when user installs Intel® Quote Provider Library and Intel® Platform Certificate Service (PCS) Cache Server installer.

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, 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.

© Intel Corporation