Intel® Software Guard Extensions Data Center Attestation Primitives Installation Guide

For Windows* OS

Revision <1.0>

<3/10/2020>

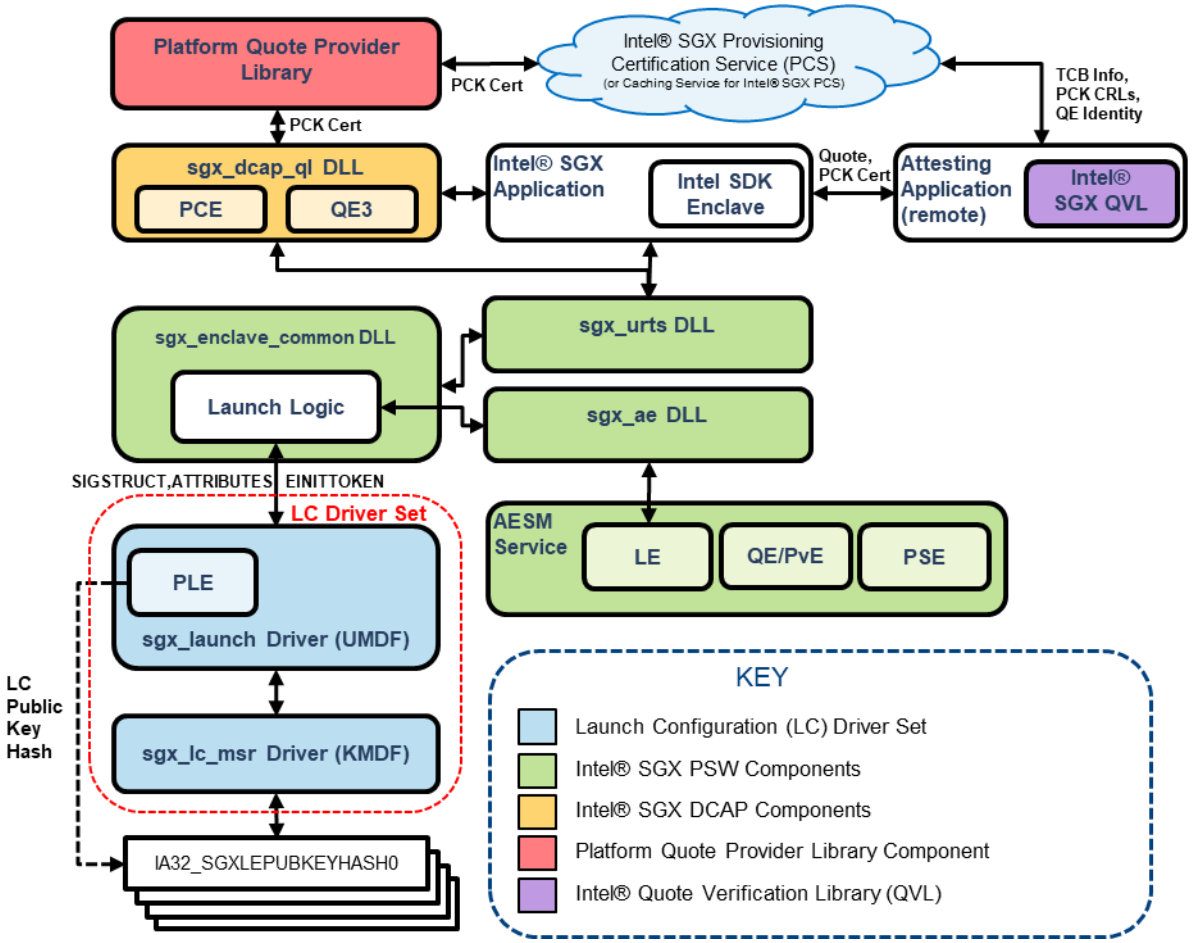
Table of Contents

Introduction

This document provides information on the Intel® Software Guard Extensions (Intel® SGX) Platform Software (PSW) components including the Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) and describes how to install them. The figure below illustrates the target platform software components of the Intel SGX PSW and the Intel SGX DCAP. The higher level components are the following:

- Intel® SGX Launch Configuration Driver Set, which configures the platform launch and provides launch tokens.
- Intel® SGX Platform Software (Intel® SGX PSW), which loads and manages enclaves. It also contains the Intel® SGX Architectural Enclave Service Manager (Intel® SGX AESM), which provides Legacy Launch Support, EPID Provisioning and Attestation, and Platform Services (PSE – for platforms that support PSE).
- Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP), which provides Data Center Attestation.

Platform Quote Provider Library, which is shown on the scheme but not covered in the document, provides PCK Certificates to the Intel® SGX DCAP Components and the Intel® SGX Quote Verification Library (Intel® SGX QVL) for Intel SGX DCAP, which can be used by a local or remote attesting application to verify quotes.



In addition to the presented components, an SDK and NuGet Packages are provided for developers.

Components – Detailed Description

The provided components are listed below:

- Doc: provides the following documentation:
  - Release Notes
- Launch Configuration Driver Set: Packages are provided for both Windows* Server 2016 LTSC and Windows* Server 2019 LTSC. The packages contain the following:
  - Windows* Server 2016 LTSC: The driver is installed not as a part of a hardware device but as a Root Enumerated Software Device. It can be installed only on Windows* Server 2016 LTSC.
    - **sgx_lc_msr.sys:** Kernel Mode Driver, which configures Launch Control Configuration Public Key Hash Registers (LC MSRs).
    - **sgx_launch.dll:** User Mode Driver, which loads the Launch Enclave and issues EINITTOKENs.
    - **sgx_base_dev.inf:** .inf file for the Launch Configuration Driver set installation. You must install this .inf file manually using devcon.exe, which creates a root enumerated Software Device and installs the driver set for that device.

        - **sgx_base_dev.cat:** catalog file for the Launch Configuration Driver set.
    - Windows* Server 2019 LTSC: The driver set is a functional driver for the ACPI/INT0E0C device on the platform.
        - **sgx_lc_msr.sys:** Kernel Mode Driver, which configures Launch Control Configuration Pub Key Hash Registers (LC MSRs).
        - **sgx_launch.dll:** User Mode Driver, which loads the Launch Enclave and issues EINITTOKENs.
        - **sgx_base.inf:** .inf file for Launch Configuration Driver set installation. The driver set is installed as a functional driver for the ACPI\INT0E0C device. It also creates software Components to support Intel® SGX enclaves:
            - **psw_installer** with Component ID: VEN_INT&DEV_0E0C
            - **dcap_installer** with Component ID: VEN_INT&DEV_0E0C_DCAP. This component is only created on Windows* Server 2019 and later. It cannot be created on Windows* 10.
        - **sgx_base.cat:** catalog file for the Launch Configuration Driver set.

- Intel® SGX Platform Software (Intel® SGX PSW) Components: different packages are provided for the Windows* Server 2016 LTSC and the Windows* Server 2019 LTSC. These packages are also used on corresponding releases of Windows* 10 RS1 – RS5. The packages contain the following:
    - Windows* Server 2016 LTSC: the Intel SGX PSW is installed using a self-extracting executable installer. You can download the installation file from the Intel® Developer Zone.
        - **Intel(R)_SGX_Windows_x64_PSW_<version>.<build>.exe**
    - Windows* Server 2019 LTSC and Windows 10 RS3 and higher versions: the installation is an .inf software component install. The following files contain descriptions of the installer files:
        - **sgx_psw.inf/sgx_psw.cat:** .inf file that installs the Intel SGX PSW and a signed catalog file for the package.
        - **sgx_enclave_common.dll**: dynamic-link library that provides the Common Enclave Loader API for loading enclaves (a 32 bit version is located in the win32 directory).
        - **sgx_urts.dll**: dynamic-link library that provides the untrusted run-time (uRTS) library with presents APIs for loading or running Intel® SGX SDK based enclaves (a 32 bit version is located in the win32 directory).
        - **sgx_uae_service.dll**: dynamic-link library that provides APIs to interface to the AESM (a 32 bit version is located in the win32 directory).
        - **aesm_service**.exe: the AESM Service.
        - **Documentation** includes **Intel SGX SW Collateral.pdf, Intel Software License Agreement <date>.pdf,** and **third party.rtf,** which provide license information.
- Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) Components: installation files for the Intel SGX DCAP components. This package is only installed on the Windows* Server 2016 LTSC and later. The installation package depends on the version of the Windows Server:
    - Windows* Server 2016 LTSC: The Intel SGX DCAP Components are installed as a Software Device using an .inf file. You can download the files from the Intel® Developer Zone.
        - **sgx_dcap_dev.inf:** .inf file that installs the Intel SGX DCAP software as a device root\SgxDevice_DCAP.
        - **sgx_dcap_dev.cat:** signed catalog file for the package.

        - **sgx_dcap_ql.dll**: dynamic-link library that provides Intel SGX DCAP APIs. It loads and uses the following signed enclave files:
            - **pce.signed.dll** : PCE enclave
            - **qe3.signed.dll** : Quoting Enclave.
    - Windows* Server 2019 LTSC: the Intel SGX DCAP is installed as a software component created by sgx_base.inf when the ACPI\INT0E0C device is installed. You can download the files from the Intel® Developer Zone**.**
        - **sgx_dcap.inf:** .inf file that installs the Intel SGX DCAP component with ID VEN_INT&DEV_0E0C_DCAP.
        - **sgx_dcap.cat:** signed catalog file for the package.
        - **sgx_dcap_ql.dll:** dynamic-link library that provides Intel SGX DCAP APIs. It loads and uses the following signed enclave files:
            - **pce.signed.dll:** PCE enclave
            - **qe3.signed.dll:** Quoting Enclave.

Additional components for developers are provided for download on the Intel® Developer Zone. These components are listed below:

- NuGet* Installers: NuGet Installer Packages for Developers:
    - **EnclaveCommon API.<version>.nupkg**: package that allows you to build applications that load enclaves using the Enclave Common API.
    - **DCAP_Components.<version>.nupkg**: package that allows you to build applications that use the Intel SGX DCAP Libraries. This package requires **EnclaveCommon API.<version>.nupkg.**
- DCAPSampleProject: Intel SGX DCAP Sample Code, which contains the following:
    - QuoteGenerationSample: sample application that demonstrates how to use Quote Generation APIs.
    - QuoteProviderSample: sample application that demonstrates how to use the Quote Provider Library for development.
- Intel® SGX Software Development Kit (Intel® SGX SDK) for Windows* OS.
    - **Intel(R)_SGX_Windows_SDK_<version>.<build>.exe:** Installer for the Intel SGX SDK. For the prerequisites, see Intel® SGX SDK documentation.

Platform Configuration

Each platform BIOS presents a different UI to configure the Intel® SGX feature. Thus, the information on configuring the platform depends on the platform. The following configurations should be applied to any platform:

- Enable the Intel® SGX in BIOS with PRMRR reserved for the maximum size. It should not be set to SW Controlled because the code to enable Intel SGX from SW Controlled may not be executed.
- Launch Control Configuration (LCC) must be supported and enabled on the platform:
    - Launch Control Configuration is supported on Intel® Xeon E platforms with specific BIOS support.
    - If the Launch Control Configuration is not enabled, the following happens:

- The Launch Configuration driver set reports that the LCC is not supported and it will not attempt to configure the LCC Public Key Hash registers.
- Legacy Launch through the AESM provides access to the Intel® Launch Enclave: using the Intel® Platform Software (and corresponding uRTS) allows for the loading of Intel® SGX Enclaves. Enclaves must either be signed with a key that is included in the whitelist or be run as debug enclaves. Intel SGX DCAP Attestation will not work as it is not whitelisted.

Windows* Server OS Support

The Intel® Software Guard Extensions (SGX) Platform Software (PSW) Components including the Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) are configured to run on the Windows* Server 2016 (Long-Term Servicing Channel) version 1607 or Windows* Server 2019 (Long-Term Servicing Channel).

This section describes how to configure each Windows* Server OS to load and run Intel SGX Enclaves. The table below shows the difference between the Windows Server 2016 and the Windows Server 2019 with respect to the Intel® SGX PSW. The main difference is in how the OS supports the enumeration of the Intel SGX EPC ACPI Device (ACPI/INT0E0C).

The Intel SGX EPC ACPI Device is provided in the ACPI Differentiated System Descriptor Table (DSDT), which contains details of the Intel SGX existence on the platform and the size and location of EPC memory. Loading of Intel SGX enclaves was originally supported with a Kernel Mode Driver, the Intel SGX Driver starting from Windows 7. This driver was a functional driver for the Intel SGX EPC ACPI Device. In the Windows* 10 TH2 release, Enclave API functions were added to the Windows Kernel to support loading of Intel SGX Enclaves. Thus, the OS suppressed the enumeration of the Intel SGX EPC ACPI Device. The suppression prevents loading of the Intel SGX Driver and, thus, it does not manage EPC memory on the platform.

In more recent updates to Windows 10 and also on the Windows Server 2019, the suppression of the Intel SGX EPC ACPI device was removed. The Windows* driver for the device (the Launch Config Driver Set) can now manage Launch Configuration on the platform, though loading of enclaves to Intel SGX EPC memory is still provided through Windows* Enclave APIs. It also allows the Intel® SGX Platform Software to be loaded as a Software Component to the Intel SGX EPC ACPI Device. On Windows* Server 2019, the Intel SGX DCAP Components are also loaded as a Software Component to the Intel SGX EPC ACPI Device.

Windows* Server Version	Intel® SGX Support Info/Changes	Impact to the Intel® SGX PSW Installation	Comments
2016 LTSC	Intel SGX EPC ACPI Device (ACPI\INT0E0C) enumeration is suppressed.	Intel® SGX PSW is not installed automatically, you must use the .exe installer Launch Config Driver must be installed as a Software Enumerated Root Device.	You must manually install each software component.

		Intel SGX DCAP can be installed as Software Enumerated Root Device.	
2019 LTSC	Intel SGX EPC ACPI Device (ACPI\INT0E0C) enumeration is **not** suppressed.	Windows Server 2019 – Intel SGX EPC ACPI Device installation: • Installs the Launch Config Driver • Creates the Intel SGX PSW Software Component • Creates the Intel SGX DCAP component.	Components are installed through separate .inf files, which can be automatically pulled from the Windows* Update

Table 1 Summary of Windows Server Support for SGX

Installation Instructions

Installation of the Intel® SGX Software including the Launch Config Driver Set, the Intel® SGX Platform Software, and the Intel® SGX DCAP Component depends on the operating system. Though the Platform Software is supported on Windows* releases from Windows* 7 through the latest Windows* 10 update, the Launch Config Driver Set and Intel SGX DCAP components are only supported on Windows* Server 2016 LTSC and Windows* Server 2019 LTSC.

Windows* Server 2016 LTSC

On Windows* Server 2016 LTSC, you must individually obtain and install software packages.

Downloading the Software

Download the software packages from Intel® SGX SDK and install them.

Installation

On Windows* Server 2016 LTSC, you must install the software packages individually:

1. To install the Launch Configuration Driver Set, use the *devcon* utility, which is provided with the Windows* 10 Driver Kit and located in the following directory: *C:\Program Files (x86)\Windows Kits\10\tools\x64\devcon.exe".* You may need to add this directory to your paths.
   Run the following command in the Administrator Command Window:

```
devcon.exe install sgx_base_dev.inf root\SgxLCDevice
```

2. To install the Intel SGX Platform Software Components, run the self-extracting executable and follow the dialog instructions:

```
Intel(R)_SGX_Windows_x64_PSW_<version>.<build>.exe
```

3. To install the Intel SGX DCAP Components, run the following command in the Administrator Command Window:

```
devcon.exe install sgx_dcap_dev.inf root\SgxLCDevice_DCAP
```

Windows* Server 2019 Installation

Downloading the Software

The software packages for Windows* Server 2019 are available for automatic download from the Windows Update. You can also download them manually from the Intel® Developer Zone.

Installation

On Windows* Server 2019, the ACPI\INT0E0C device is present when the Intel® SGX is enabled. The software installation progresses as follows:

1. The ACPI Device Class Installer is invoked to search for a driver to the ACPI\INT0E0C device. You can configure the system in one of the following ways:
    - Install the LC Driver Set to the Driver Store – the class installer will automatically find the driver and install it.
    - Let the platform automatically search for the LC Driver Set on the Windows Update. The driver will be downloaded and installed.
    - Manually download the LC Driver set and point the installer to the downloaded package. The installer will install the package.
2. The LC Driver Set installation through sgx_base.inf creates the following components on Windows Server 2019:
    - psw_installer with Component ID: VEN_INT&DEV_0E0C
    - dcap_installer with Component ID: VEN_INT&DEV_0E0C_DCAP.
3. The SofwareComponent class installer installs a software package for each of the components. You can provide the packages in the optional methods detailed in step 1.

Intel® Software Guard Extensions Launch Configuration Opt-in Registry Setting

The Launch Config Driver Set provides a Launch Token to the PCE enclave to run. The PCE provides information specific to the platform on which it is running. This indicates a privacy concern for the platform

owner. When an enclave on the platform attests to another platform, the remote platform can detect whether the platform has been attested before. Because of this privacy concern, the platform *administrator* must opt-in to the Intel SGX DCAP attestation feature. The administrator must configure the Launch Config Driver so that the PCE enclave can run and share the platform rooted information with it.

To do the opt-in, an administrator accessible registry key must be set on the platform. An administrator must create the following DWORD value in the parameter key of the Launch Config Driver:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sgx_lc_msr\Parameters]

"SGX_Launch_Config_Optin"=dword:00000001

You might need to reboot the system to apply this configuration.

Intel® SGX DCAP Provisioning Certificate Caching Service

1. Download the source code from https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration/pccs
2. Install node.js
   Open https://nodejs.org/en/download/ and download the Windows installer, then install it. Check on "Automatically install the necessary tools" during installation.
3. Go to pccs root directory
   a. Update configuration file (./config/default.json)
      i. "hosts" : Leave it unchanged if the PCCS is running on local system. Change it to "0.0.0.0" if the PCCS is running on a remote system.
      ii. "ApiKey" : To obtain an API key, goto https://api.portal.trustedservices.intel.com/provisioning-certification and click on 'Subscribe'. You need to create an account first if you don't have one.
      iii. "proxy" : Set it to "`http://your-proxy-server:port`" only if the system is behind a proxy server, otherwise leave it blank.
      iv. "UserToken" : Sha512 hashed token for the PCCS client user to register a platform. For example, PCK Cert ID retrieval tool will use this token to send platform information to pccs.
      v. "AdminToken" : Sha512 hashed token for administrator to perform priveleged operations.
      You can generate the UserToken and AdminToken with the help of openssl, open a command window and run :
      `<nul: set /p password="usertoken" | openssl dgst -sha512`
      vi. "CachingFillMode" : The method used to fill the cache DB. Can be one of the following: REQ/LAZY/OFFLINE. For more details please check README.md in pccs root directory.

   b. Generate key and public certificate for HTTPS server and put the generated files into `ssl_key/` sub directory. If you have openssl installed, run below commands:

```
openssl genrsa 1024 > private.pem
openssl req -new -key private.pem -out csr.pem
openssl x509 -req -days 365 -in csr.pem -signkey private.pem
       -out file.crt
```

   NOTE : This is only for development environment. For production environment, please use formal private key and certificates.

If you use self-signed certificate, please change the registry for the default Quote Provider Library accordingly:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\SGX\QCNL]
"USE_SECURE_CERT"=dword:00000000
```

4. Open windows command prompt as administrator and go to pccs root directory.
   1) Config proxy for npm first if the system connects to internet through proxy server

      ```
      npm config set http-proxy http://your-proxy-server:port
      npm config set https-proxy http://your-proxy-server:port
      npm config set proxy http://your-proxy-server:port
      ```

   2) Run install.bat
   3) Check pccs service is running without error

      ```
      pm2 status
      ```

   4) Check pccs service is working as expected

      Open this link in your browser : https://localhost:8081/sgx/certification/v2/rootcacrl

      There should be a security warning, choose “ignore” to continue (the warning message is different for different browsers) and the root CA CRL should be retrieved successfully.

Application Configuration

This section provides details on how to configure an application to run Intel® SGX enclaves.

Building Intel® SGX Enclave Applications

To build and run applications that use Intel® SGX Enclaves, build the application with Intel® SGX SDK tools first.

Prerequisite Tools

The prerequisite tools for building Intel® SGX Enclaves are the following:

- Microsoft Visual Studio* Professional 2017 Update 3
- Microsoft Visual C++* Compiler from Microsoft Visual Studio Professional 2014 or 2017

For more information, see the latest Release Notes for the Intel® SGX SDK available at https://software.intel.com/en-us/sgx-sdk/documentation.

Intel® SGX SDK Installation

You can download the Intel® SGX SDK from https://software.intel.com/en-us/sgx-sdk/download. Before the download, create an account at the Intel® Developer Zone. Registered users can receive notifications of the Intel® SGX SDK and Intel® SGX PSW updates.

Additional NuGet* Packages

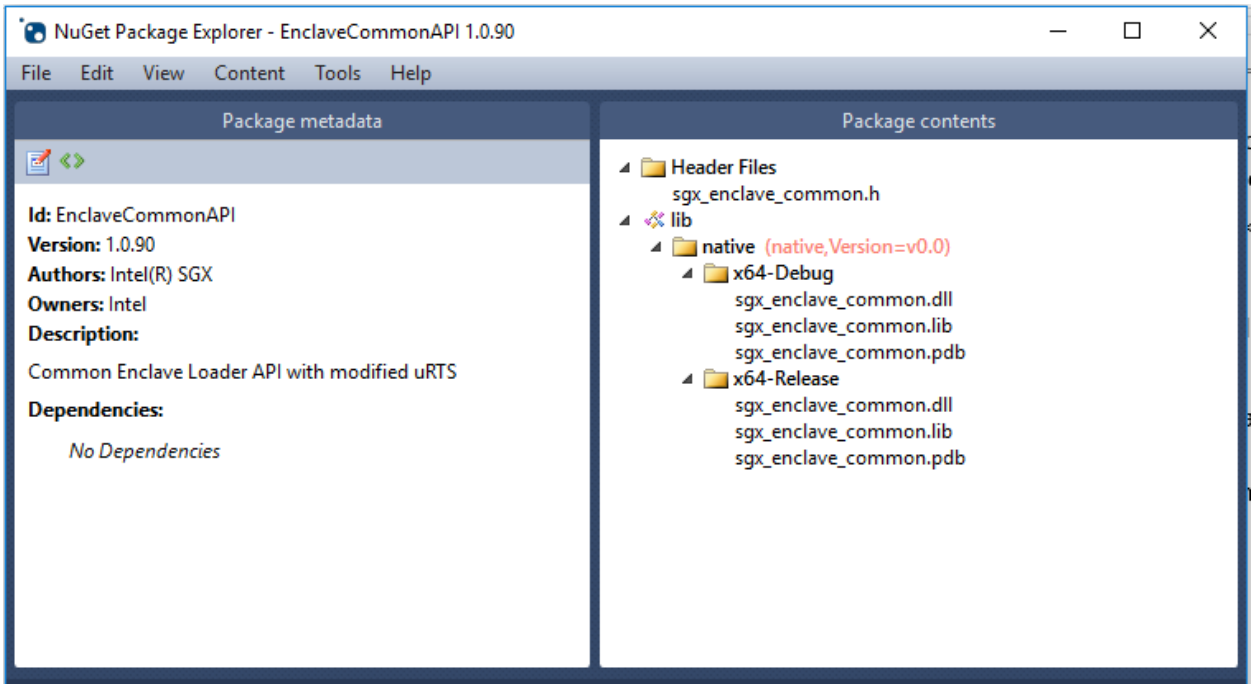
Two additional components are provided for developers:

- Intel SGX Enclave Common Loader API (sgx_enclave_common.dll) to load Intel SGX Enclaves
- Intel SGX DCAP (sgx_dcap_ql.dll) to provide attestation.

Developer files for these components are provided in NuGet* Packages. You can download the NuGet packages from the Intel® Developer Zone and install them using the instructions below.

Enclave Common API NuGet* Package

The Enclave Common API NuGet* Package (EnclaveCommon API.<version>.nupkg) contains files that allow you to build applications that load enclaves using the Enclave Common API. You may only need this package for building a module with an enclave loader. For example, the Open Enclave SDK uses the Linux* version of the Enclave Common Loader API to load enclaves. The screenshot below provides details of the package contents:



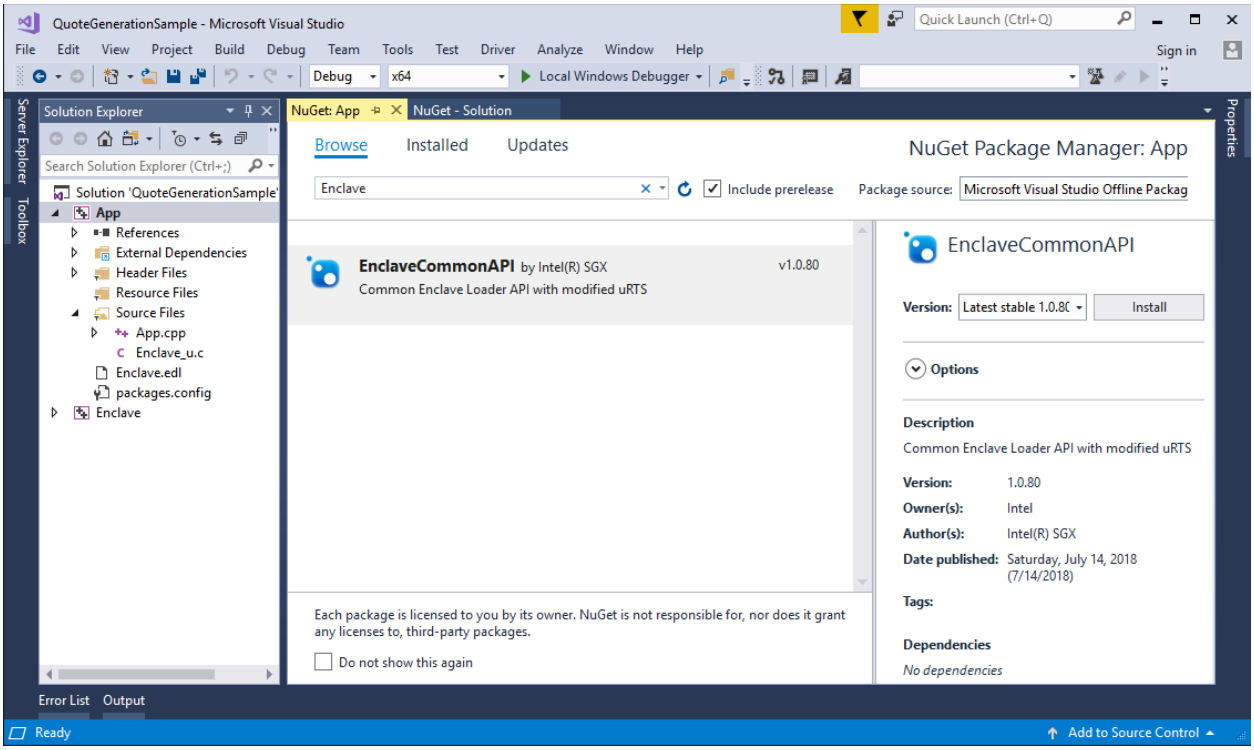
To install the package to a local source and then to a project:

1. Ensure that NuGet.exe is installed. For more information, see https://docs.microsoft.com/en-us/nuget/tools/nuget-exe-cli-reference.
2. You can install NuGet* packages from an online NuGet repository like NuGet.org or a local package source on the local system. For the Microsoft Visual Studio* Professional 2017, the default local package source is *C:\Program Files (x86)\Microsoft SDKs\NuGetPackages*.
   To use the second installation option, add the package to the local package source first. To copy the local package source, run the following command:

```
nuget add EnclaveCommonAPI.<version>.nupkg -source <sourcePath>
```

Where `<sourcePath>` is the path to the local package source. **Note:** the filename may change due to the version changing.

3. Install the package into the Visual Studio* Project:
    a. Right click on the project in Visual Studio and select **NuGet Package Manager**.
    b. In the opened **NuGet Package Manager: App** window, search for **EnclaveCommonAPI** and select it.
    c. Click the **Install** button.



Intel® SGX DCAP Components NuGet* Package

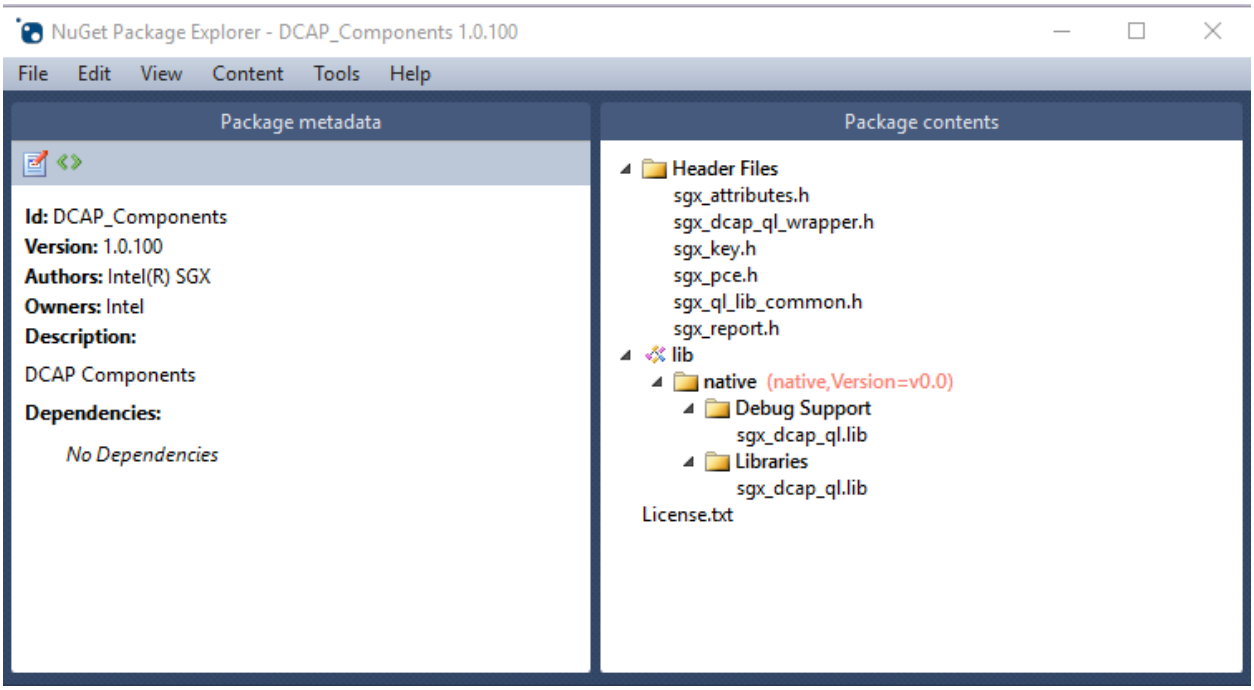
The Intel® SGX Data Center Attestation Primitives (DCAP) Components NuGet* Package (DCAP_Components.<version>.nupkg) contains files that allows you to build applications that use the Intel SGX DCAP. This package requires the Enclave Common API NuGet Package.

To install the package to a local source and then to a project:

1. Ensure that NuGet.exe is installed. For more information, see https://docs.microsoft.com/en-us/nuget/tools/nuget-exe-cli-reference.
2. To add the Intel SGX DCAP Components NuGet package to the local package source, run the following command:

```
nuget add DCAP_Components.<version>.nupkg -source <sourcePath>
```

3. Install the package to the Visual Studio* Project:
    a. Right click on the project in Visual Studio and select **NuGet Package Manager**.
    b. In the opened **NuGet Package Manager: App** window, search for **DCAP_Components** and select it.
    c. Click the **Install** button.



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.