



Intel® Software Guard Extensions Data Center Attestation Primitives Installation Guide

For Linux* OS

Revision <1.0>

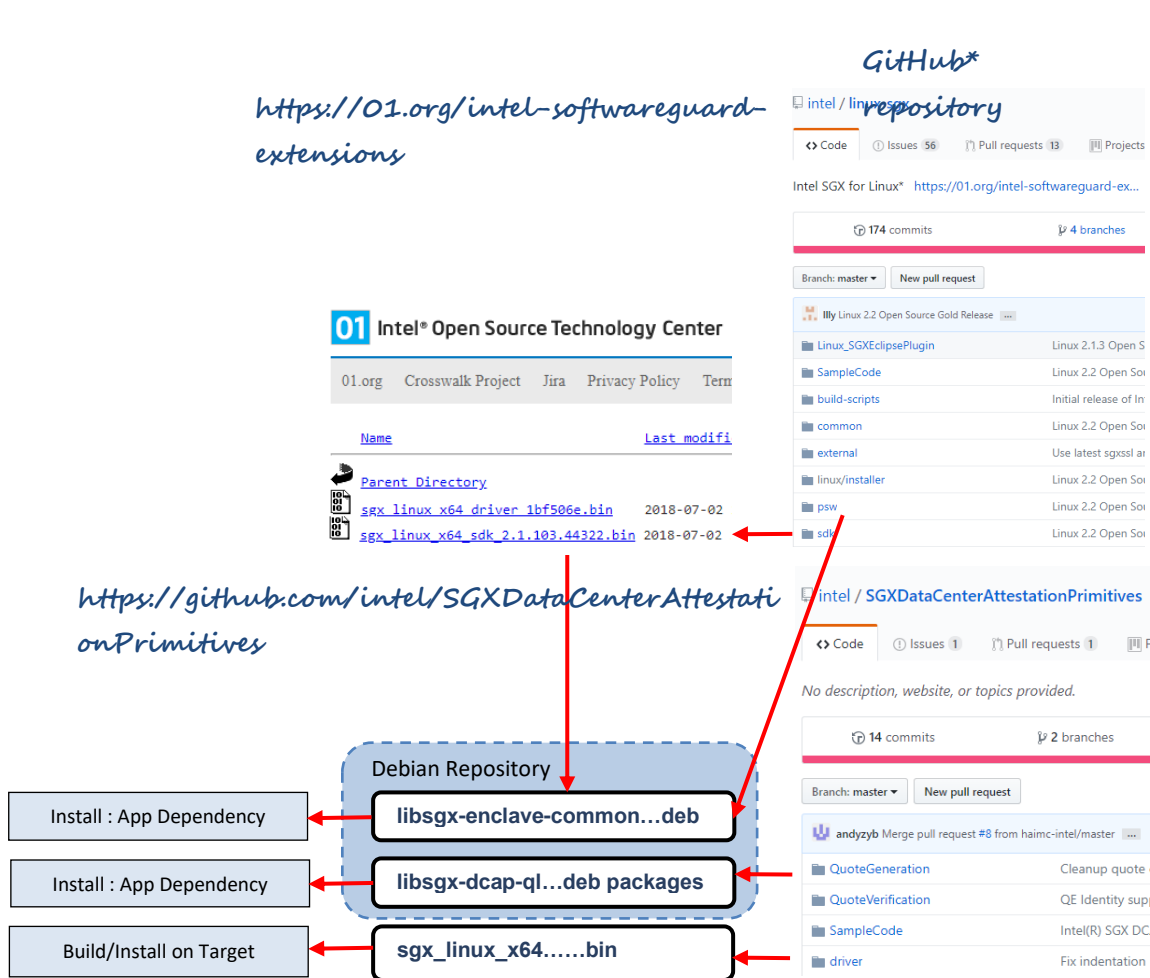
<3/10/2020>

Table of Contents

Table of Contents	2
Introduction	3
Intel® Software Guard Extensions - Software Packages	4
Intel® SGX Software Development Kit for Linux* OS	4
Intel® SGX Platform Software.....	4
Intel® SGX Data Center Attestation Primitives.....	5
Intel® SGX Driver	8
Installation Instructions	10
Intel® SGX Application User.....	10
Intel® SGX Application Developer	13
Building the Intel® SGX Software Stack.....	15
Disclaimer and Legal Information	16

Introduction

This document describes installation of the Intel® Software Guard Extensions (Intel® SGX) Software Development Kit (SDK) and Platform Software (PSW) for Linux* OS and the Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) for Linux* OS. The figure below illustrates the delivery flow of the software components from the source code on GitHub* to the builds of install packages, which you can download directly from <https://01.org/intel-software-guard-extensions> or from a Debian* repository located at https://download.01.org/intel-sgx/sgx_repo/ubuntu/.



Intel® Software Guard Extensions - Software Packages

Intel® SGX Software Development Kit for Linux* OS

The Intel® Software Guard Extensions Software Development Kit (Intel® SGX SDK) for Linux* OS provides libraries, tools, reference code, and documentation that help you code, build, and sign Intel SGX enclaves and the applications that host Intel SGX enclaves.

The Intel® SGX SDK installation is provided as a binary file:

- Location: <https://download.01.org/intel-sgx/> linux-<version>/<OS><OS version>
- Filename: `sgx_linux_x64_sdk_<version>.<build>.bin`

Dependencies

- `build-essential`
- `python`
- `libsgx-urts` and other SGX packages (required by sample code)

See *Install the Intel® SGX SDK: Prerequisites* here: <https://github.com/intel/linux-sgx/blob/master/README.md>.

Source

Source code for the Intel® SGX SDK for Linux* OS is located on GitHub*:

- Source code: <https://github.com/intel/linux-sgx>.
- Build instructions: <https://github.com/intel/linux-sgx/blob/master/README.md>. This document contains detailed instructions on platform configuration and build procedures for the Intel SGX SDK and the Intel SGX PSW for Linux* OS.
- Build dependencies: <https://github.com/intel/linux-sgx/blob/master/README.md>. This document defines installation prerequisites and build dependencies.

Intel® SGX Platform Software

The Intel SGX Platform Software (Intel SGX PSW) for Linux* OS mainly contains uRTS, Enclave Common API and the Architectural Enclave Service Manager (AESM) in different packages.

The Intel® SGX PSW is provided as several Debian* packages:

- Location:
 - The Debian* repository: https://download.01.org/intel-sgx/sgx_repo/ubuntu/.

- Packages (including special developer packages):
 - https://download.01.org/intel-sgx/sgx_repo/ubuntu/pool/main/libs/libsgx-*
 - https://download.01.org/intel-sgx/sgx_repo/ubuntu/pool/main/libs/sgx-aesm-service/
- Filename: libsgx-*_\${version}-\${revision}-\${os}_\${arch}.deb
sgx_aesm_service_\${version}-\${revision}-\${os}_\${arch}.deb

Dependencies

The Intel® SGX Platform Software depends on the following modules:

- libc6
- libcurl3
- libgcc1
- libprotobuf9v5
- libssl1.0.0
- libstdc++6

See *Install the Intel® SGX PSW: Prerequisites* here: <https://github.com/intel/linux-sgx/blob/master/README.md>.

Source

Source code for the Intel SGX Platform Software is located in the same GitHub* repository where the Intel SGX SDK for Linux* OS is stored:

- Source code : <https://github.com/intel/linux-sgx>.
- Build instructions: <https://github.com/intel/linux-sgx/blob/master/README.md>. This document contains detailed instructions on platform configuration and build procedures for the Intel SGX PSW and the Intel SGX SDK.
- Build dependencies: see <https://github.com/intel/linux-sgx/blob/master/README.md>. This document defines installation prerequisites and build dependencies.

Intel® SGX Data Center Attestation Primitives

The Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) contains the following components:

1. Intel® SGX DCAP Quote Generation Library, which is used to generate quotes from the attester.
2. Intel® SGX DCAP Default Quote Provider Library, which is used to retrieve PCK certificates from Provisioning Certificate Caching Service(PCCS).
3. Intel® SGX DCAP Provisioning Certificate Caching Service, which is a caching server for Intel PCS

4. Intel® SGX DCAP Quote Verification Library, which the attestee uses to verify quotes.
5. Intel® SGX Driver. This is an out-of-tree driver, which runs on systems that support the Launch Control Configuration.

Intel® SGX DCAP Quote Generation Library

The components of the Intel® SGX DCAP Quote Generation Library are provided in a Debian* package:

- Location:
 - The Debian* repository: https://download.01.org/intel-sgx/sgx_repo/ubuntu/.
 - Packages (including separate developer and debugger packages):
 - https://download.01.org/intel-sgx/sgx_repo/ubuntu/pool/main/libs/libsgx-dcap-ql/
 - https://download.01.org/intel-sgx/sgx_repo/ubuntu/pool/main/libs/libsgx-dcap-ql-dev/
 - https://download.01.org/intel-sgx/sgx_repo/ubuntu/pool/main/libs/libsgx-dcap-ql-dbg/
 - Intel® SGX DCAP release directory that also contains packages: <https://01.org/intel-softwareguard-extensions/>.
- Filename: `libsgx-dcap-ql_${version}-${revision}-${os}_${arch}.deb`

Dependencies

The Intel® SGX Data Center Attestation Primitives depend on the following modules:

- `libsgx-urts`, `libsgx-ae-qe3`, `libsgx-ae-pce` and `libsgx-ae-qve`

Source

The source code is in the following repository:

- Source Code :
<https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration>
- Build instructions and dependencies:
<https://github.com/intel/SGXDataCenterAttestationPrimitives/blob/master/QuoteGeneration/RADME.md>. This document also provides instructions on including the prebuilt or signed enclaves.

Intel® SGX DCAP Default Quote Provider Library

The components of the Intel® SGX DCAP Default Quote Provider Library are provided in a Debian* package:

- Location:
 - The Debian* repository: https://download.01.org/intel-sgx/sgx_repo/ubuntu/.
 - Packages:

- https://download.01.org/intel-sgx/sgx_repo/ubuntu/pool/main/libs/libsgx-dcap-default-gpl/
- Intel® SGX DCAP release directory that also contains packages: <https://01.org/intel-softwareguard-extensions/>.
- Filename: `libsgx-dcap-default-gpl_${version}-${revision}-${os}_${arch}.deb`

Source

The source code is in the following repository:

- Source Code :
<https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration/qpl/>
- Build instructions and dependencies:
<https://github.com/intel/SGXDataCenterAttestationPrimitives/blob/master/QuoteGeneration/qpl/README.md>

Intel® SGX DCAP Provisioning Certificate Caching Service

The components of the Intel® SGX DCAP Provisioning Certificate Caching Service are provided in a Debian* package:

- Location:
 - The Debian* repository: https://download.01.org/intel-sgx/sgx_repo/ubuntu/.
 - Packages:
 - https://download.01.org/intel-sgx/sgx_repo/ubuntu/pool/main/web/sgx-dcap-pccs/
 - Intel® SGX DCAP release directory that also contains packages: <https://01.org/intel-softwareguard-extensions/>.
- Filename: `sgx-dcap-pccs_${version}-${revision}-${os}_${arch}.deb`

Source

The source code is in the following repository:

- Source Code :
<https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration/pccs/>
- Install instructions and dependencies:
<https://github.com/intel/SGXDataCenterAttestationPrimitives/blob/master/QuoteGeneration/pccs/README.md>

Intel® SGX DCAP Quote Verification Library

The Intel® SGX DCAP Quote Verification Library is provided as a source code.

Dependencies

For information on dependencies, see

<https://github.com/intel/SGXDataCenterAttestationPrimitives/blob/master/QuoteVerification/README.md>.

Source

The source code is in the following repository:

- Source Code :
<https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteVerification>
- Build instructions and dependencies:
<https://github.com/intel/SGXDataCenterAttestationPrimitives/blob/master/QuoteVerification/README.md>.

Intel® SGX Driver

See Intel® SGX Driver.

Intel® SGX Driver

The Intel® SGX Driver for Linux* OS is provided for distributions that run on systems supporting the Launch Control Configuration.

- Location: <https://download.01.org/intel-sgx/dcap-1.0/> for dcap-1.0, the location is <https://download.01.org/intel-sgx/dcap-1.0/>
- Filename (for version 1.0): [sgx linux x64 driver license updated dcap_a06cb75.bin](#).

Dependencies

The Intel® SGX Driver for Linux* OS depends on the following:

- build-essential
- ocaml
- automake
- autoconf
- libtool
- wget
- python

- `libssl-dev`

Source

The source code is located on GitHub*:

- Source code: <https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/driver>
- Build instructions and dependencies: <https://github.com/intel/SGXDataCenterAttestationPrimitives/blob/master/driver/linux/README.md>.

Installation Instructions

The installation of the Intel® Software Guard Extensions (Intel® SGX) software packages for Linux* OS depends on the intended use. Choose the role that describes your needs best:

- **Intel SGX Application User:** you want to install an Intel SGX application, which runs an Intel SGX enclave on the system.
- **Intel SGX Application Developer:** you want to build or develop an Intel SGX application, which runs an Intel SGX enclave on the system.
- **Intel SGX Software Stack Developer or Builder:** you want to build or develop the Intel SGX Software Stack: The Intel SGX Software Development Kit (Intel SGX SDK), the Intel SGX Platform Software (Intel SGX PSW), or the Intel SGX Data Center Attestation Primitives (Intel SGX DCAP).

This section provides shortcuts on system configuration for the needs described above.

Intel® SGX Application User

To run an Intel® SGX Application built with the Intel SGX SDK, install appropriate versions of the Intel SGX Driver, the Intel SGX Platform Software (Intel SGX PSW), and, if used, the Intel SGX DCAP. To install the Intel SGX Platform Software, use the `libsgx-urts` Debian* package.

To configure the system to run an Intel SGX application:

1. It's strongly recommended to update the system first:

```
sudo apt update
sudo apt upgrade
```

2. Install the Intel® SGX Driver package:

- a. Since the Intel SGX Driver is built from the driver package, install the required components that support the Intel SGX PSW installation.

Note: This command line contains modules needed beyond the Intel SGX Driver installation.

```
sudo apt-get install build-essential ocaml automake autoconf
libtool wget python libssl-dev
```

- b. Download the latest Intel SGX Driver binary file from the Intel SGX DCAP download directory: <https://download.01.org/intel-sgx/latest/dcap-latest/linux/distro>

For example, to download the driver for Ubuntu server 18.04, use the following command:

```
sudo wget - https://download.01.org/intel-sgx/latest/dcap-latest/linux/distro/ubuntuServer18.04/sgx\_linux\_x64\_driver\_1.21.bin
```

- c. Set the protections to allow for the .bin file execution:

```
chmod 777 sgx_linux_x64_driver_1.21.bin
```

- d. Install the driver using the following command:

```
sudo ./sgx_linux_x64_driver_1.21.bin
```

The installer also loads the Intel® SGX Driver and sets it to be auto-load when the system reboots.

After the Intel® SGX Driver installation, you can see a generated script `uninstall.sh` under the `/opt/intel/sgxdriver` directory. You can use this script to uninstall the driver.

- e. (Optional)The enclave user needs to be added to the group of "sgx_prv" if customers want to use their own provision enclave:

```
sudo usermod -aG sgx_prv user
```

3. If you aim to install `sgx-dcap-pccs`, install `node.js` first with the following command because `sgx-dcap-pccs` depends on it:

```
curl -sL https://deb.nodesource.com/setup_13.x | sudo -E bash -  
sudo apt-get install -y nodejs
```

Make sure the correct node version was installed(13.x):

```
node --version
```

4. Install the DCAP packages (`libsgx-urts`, `libsgx-dcap-ql`, `libsgx-dcap-default-qp1`, `sgx-dcap-pccs`) with one of the following methods:

- a. Connect to the network and open a terminal

- b. Add the following repository to your sources:

- i. For Ubuntu* 16.04:

```
echo 'deb [arch=amd64] https://download.01.org/intel-  
sgx/sgx_repo/ubuntu xenial main' | sudo tee  
/etc/apt/sources.list.d/intel-sgx.list
```

- ii. For Ubuntu* 18.04:

```
echo 'deb [arch=amd64] https://download.01.org/intel-  
sgx/sgx_repo/ubuntu bionic main' | sudo tee  
/etc/apt/sources.list.d/intel-sgx.list
```

- c. Add a key to the list of trusted keys used by the apt to authenticate packages

```
wget -qO - https://download.01.org/intel-  
sgx/sgx_repo/ubuntu/intel-sgx-deb.key | sudo apt-key add -
```

- d. Update the apt and install the latest package

```
sudo apt-get update  
sudo apt-get install libsgx-urts libsgx-dcap-ql libsgx-dcap-  
default-qp1 sgx-dcap-pccs
```

- e. (Optional) upgrade the packages using one of the following commands

```
sudo apt-get upgrade
```

```
sudo apt-get dist-upgrade
```

To determine the best option for your system, consult the apt-get manual

- f. **(Optional)** to debug with `sgx-gdb`, install the debug symbol package
For Ubuntu* 16.04, the debug symbols are included in the executable.
For Ubuntu* 18.04, the debug symbols are included in the following package

```
sudo apt-get install libsgx-enclave-common-dbgsym libsgx-dcap-qpl-  
dbgsym libsgx-dcap-default-qpl-dbgsym
```

5. Setup the Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) Provisioning Certificate Caching Service:

By default, the debian package installer will guide you through the configuration of the PCCS service. If you want to change the configuration later after installation was completed, please check

<https://github.com/intel/SGXDataCenterAttestationPrimitives/blob/master/QuoteGeneration/pccs/README.md>

You can run the following command to make sure the PCCS service is working correctly (assume the service is running on localhost with insecure certificate) :

```
curl --noproxy "*" -v -k -G  
"https://localhost:8081/sgx/certification/v2/rootcacrl"
```

The root CA CRL should be retrieved successfully.

Important:

If you are using insecure certificate for the PCCS service, after installed the `libsgx-dcap-default-qpl` package, please set "USE_SECURE_CERT"=FALSE in `/etc/sgx_default_qcnl.conf`

6. By default, Architectural Enclave Service Manager (AESM) will be installed. If it is not needed, use "--no-install-recommends" option to avoid installing it. You can also disable it as follows if it is installed:

- a. Stop the AESM service:

```
sudo systemctl stop aesmd
```

- b. Disable the AESM Service. You can manually re-enable and restart it.

```
sudo systemctl disable aesmd
```

Note: The AESM Service provides the legacy Launch Control and EPID based attestation. Disable the AESM service if your system supports these services and/or you want to use them.

7. Upgrade from a legacy installation:

Before release 2.8, SGX PSW is installed as a single package named as `libsgx-enclave-common`. Starting with the 2.8 release, SGX PSW is split into smaller packages. `libsgx-enclave-common` is one of them. As a result, a simple upgrade will end up with a subset of the SGX PSW being installed on the system. You need to install additional packages to enable the required feature. At the same

time, you will encounter some error message when you try to upgrade to release 2.8 from an old installation. You can use 2 methods to address it.

- a. Uninstall the old installation first, then install new packages.
- b. Add `-o Dpkg::Options::="--force-overwrite"` option to overwrite existing files and use “dist-upgrade” instead of “upgrade” to install new packages when upgrading. In short, you should use this command:

```
apt-get dist-upgrade -o Dpkg::Options::="--force-overwrite"
```

Intel® SGX Application Developer

In addition to installing the Intel® Software Guard Extensions Platform Software (Intel® SGX PSW), you should also install the Intel® SGX Software Development Kit (Intel® SGX SDK) and the prerequisite software. To install the Intel SGX SDK:

1. Install the prerequisite software. For more information about prerequisites, see *Install the Intel® SGX SDK: Prerequisites*: <https://github.com/intel/linux-sgx/blob/master/README.md>. Run the following command:

```
sudo apt-get install build-essential python
```

2. Download the Intel SGX SDK and install it.

Note: The following commands are specific to the Linux* 2.3 release. For subsequent releases, specify a new release directory and a filename.

- a. In the following command line, specify the Intel SGX DCAP version (for example, 1.0), the operation system and its version (for example, ubuntu16.04), the Intel SGX SDK version (for example, 2.3.100), the build (for example, 46354), and run the command:

```
wget - https://download.01.org/intel-sgx/latest/dcap-latest/<OS>/distro/<OS_version>/sgx_linux_x64_sdk_<version>.<build>.bin
```

- b. Adjust the file permissions:

```
chmod +x sgx_linux_x64_sdk_2.3.100.46354.bin
```

- c. Start interactive setup by running the following command (run with sudo if necessary):

```
$ ./sgx_linux_x64_sdk_2.3.100.46354.bin
```

- d. When the question **Do you accept this license? [yes/no]** appears, type **yes** and press **Enter** to continue.
- e. When the question **Do you want to install in current directory? [yes/no]** appears, choose one of the following:
 - o If you want to install the components in the current directory, type **yes** and press **Enter**.

- If you want to provide another path for the installation, type **no** and press **Enter**.

Now the Intel SGX SDK package is installed into the directory [Your Input Location]/sgxsdk. In this location you can also find a generated script `uninstall.sh`, which you can use to uninstall the Intel SGX SDK.

- f. To set all environment variables, run:

```
source [User Input Path]/sgxsdk/environment
```

- 3. Install the appropriate developer packages ***libsgx-enclave-common-dev***, ***libsgx-dcap-ql-dev*** and ***libsgx-dcap-default-qpl-dev*** with one of the following methods

```
sudo apt-get install libsgx-enclave-common-dev libsgx-dcap-ql-dev  
libsgx-dcap-default-qpl-dev
```

Building the Intel® SGX Software Stack

Intel® SGX - Platform Software and Software Development Kit

The source code for the Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) and the Intel® Software Guard Extensions Software Development Kit (Intel® SGX SDK) is located in the following GitHub* repository: <https://github.com/intel/linux-sgx>. To build and deploy the packages, follow the instructions detailed in <https://github.com/intel/linux-sgx/blob/master/README.md>.

Prebuilt Binaries

To run Intel® SGX enclaves on systems that do not support the Flexible Launch Control and to properly provision and use the EPID attestation, you must build specific enclaves and sign them using Intel® applications. You can download these pre-built enclaves for the Intel® SGX Linux* 2.3 release from https://download.01.org/intel-sgx/linux-2.3/prebuilt_ae_2.3.tar.gz.

In addition, the Intel SDK provides prebuilt optimized libraries in the binary form. You can get these libraries from https://download.01.org/intel-sgx/linux-2.3/optimized_libs_2.3.tar.gz.

Check the SHA256 hash of downloaded libraries using https://download.01.org/intel-sgx/linux-2.3/SHA256SUM_prebuilt_2.3.txt.

Intel® SGX Data Center Attestation Primitives

The source code for the Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) is located in the following GitHub* repository:

<https://github.com/intel/SGXDataCenterAttestationPrimitives>. To build and deploy the packages, follow the instructions detailed in <https://github.com/intel/SGXDataCenterAttestationPrimitives/blob/master/README.md>.

Prebuilt Binaries

To use the Intel SGX DCAP, you must sign specific enclaves using Intel® applications. This includes enclaves used by the Intel® SGX DCAP Quote Generation Library, which are located here: https://download.01.org/intel-sgx/sgx-dcap/1.4/linux/prebuilt_dcap_1.4.tar.gz. For release notes and other details, see <https://01.org/intel-softwareguard-extensions/downloads/intel-sgx-dcap-linux-1.4-release>.

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.

Copyright 2014-2020 Intel Corporation.

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.