Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) for Linux* OS
Release Notes

18 September 2018

Revision: 1.0 Gold (version: 1.0.100.46460)

Contents:

Introduction
What's New
System Requirements
Disclaimer and Legal Information

1 Introduction

Attestation is the process of demonstrating that a software executable has been properly instantiated on a platform. Intel® SGX attestation allows a remote party to gain confidence that the intended software is securely running within an enclave on an Intel® SGX enabled platform. This document provides system requirements, limitations and legal information.

2 What's New

- 1.0 Gold release
- Provide the Quote Verification Library and sample project. Please note this library is only provided in source code in the Intel® SGX DCAP project repo
- Provide the Quote Generation Library and sample project
- Provide the sample project for Platform Provider Library

3 System Requirements

Hardware Requirements

- Intel® Xeon® E Processor based Server
- Intel® SGX option enabled in BIOS with Flexible Launch Control support

Software Requirements

- Supported Linux* OS distributions:
    - Ubuntu* 16.04 LTS 64-bit Server version
    - Ubuntu* 18.04 LTS 64-bit Server version

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

4 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