

Intel® SGX Data Center Attestation Primitives for Linux* OS

Release Notes

23 June 2020

Revision: 1.7.0 Open Source (version: 1.7.100.2)

Contents:

[Introduction](#)

[What's New](#)

[System Requirements](#)

[Known Issues and Limitations](#)

[Disclaimer and Legal Information](#)

1 Introduction

Attestation is a process of demonstrating that a software executable is properly instantiated on a platform. The Intel® Software Guard Extensions (Intel® SGX) attestation allows a remote party to ensure that a particular 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

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.7.0:

- Updated Quote Verification Enclave(QvE) and wrapper library to support platform certificate's new fields.
- Added a trusted library to verify QvE's identity.
- 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.

Changes in Previous Releases

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.6.0:

- Added APIs to configure file directory for DCAP quoting Enclave, quote provider library and quote verification library
- Fixed bugs.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.5.0:

- Added APIs to retrieve Intel® Quote Verification Enclave (QVE)'s identity in quote verification library
- Updated Quote Verification Sample project to use new APIs in quote verification library
- Changes to address CVE-2020-0551.
- Fixed bugs.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.4.0:

- Updated Provisioning Certificate Caching Server (PCCS) and added PCCS Administration tool to support retrieving platform certificates in offline mode
- Added non-QvE (Quote Verification Enclave) based quote verification support
- Updated Quote verification sample project to demonstrate library interface change
- Added new Platform Certificate Selection Library interface to return CPUSVN configuration information
- Fixed bugs.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.3.1:

- Fixed bugs.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.3:

- Added Intel® Quote Verification library and enclave.
- Added support for new version Intel® Provisioning Certificate Service interfaces.

- Fixed bugs.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.1:

- Fix bugs.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.0.1:

- Updated the cryptography library to the Intel® Integrated Performance Primitives Cryptography 2019 Update 1.

Intel® Software Guard Extensions DCAP includes the following changes in version 1.0 (Intel® SGX DCAP 1.0 Gold release):

- Provided the Quote Verification Library and a corresponding sample project. Note that this library is only provided in source code in the Intel® SGX DCAP project repository.
- Provided the Quote Generation Library and a corresponding sample project.
- Provided a sample project for the Platform Provider Library.

3 System Requirements

Hardware Requirements

- Intel® Xeon® E Processor based Server
- Intel® SGX option enabled in BIOS with the 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
 - Red Hat* Enterprise Linux* Server 8.0 (for x86_64)

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

4 Known Issues and Limitations

- Intel® SGX DCAP 1.6 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 DCAP 1.4 does not include the latest functional and security updates. Intel® SGX DCAP 1.4.1 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.
- During the current release we have learned that the DKMS infrastructure uses the driver version as an arbitrary string and not as a numeric value. As a result, installing an old version on top of a new version will work, moreover, when more than one version is installed and a kernel update occurs there is no guarantee that the new version will be used in the new kernel – apparently either of the existing versions may be used.

To address these issues, the 1.10 driver installer will uninstall a previously installed driver if exists.

Note: The uninstall may fail if the driver is in use by an enclave or the AESM, in this case the user will be notified and will be required to manually uninstall the driver.

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.