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

25 April 2024

Revision: 1.21 Open Source (version: 1.21.100.3)

Contents:

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 following changes in version 1.21.100.3:

- Upgraded Intel® DCAP Ring3 Abstraction Layer (R3AAL) library to support ConfigFS-TSM as communication channel between host and guest for TDX remote attestation
- Upgraded Intel® DCAP Quote Verification Enclave to integrate OpenSSL/SgxSSL 3.0.13
- Upgraded new TDX attestation result "TD_RELAUNCH_ADVISED" in Intel® DCAP Quote Verification Library (QVL) and Appraisal Engine
- Fixed bugs

Changes in Previous Releases

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes following changes in version 1.20.100.2:

- Introduced the Intel® DCAP Appraisal Engine within quote verification library, empowering users to evaluate verification results against diverse policies
- Upgraded Intel® SGX Quote Verification Enclave to integrate OpenSSL/SgxSSL 3.0.12
- Added Rust wrapper for quote provider library APIs
- Fixed bugs

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes following changes in version 1.19.100.3:

- Resigned all Intel® SGX Architecture Enclaves
- Upgraded Intel® SGX Quote Verification Enclave to integrate OpenSSL/SgxSSL 3.0.10
- Added Attestation Library support for Intel(R) TDX Migration TD
- Added Rust wrapper for low-level Quote Generation APIs
- Enabled 'SE_TRACE' log in release binary
- Updated Rust QVL wrapper to use native Rust structure for quote verification collateral
- Added a limitation in the DCAP QVL to only allow the user to set the QvE load policy once
- Fixed bugs

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes following changes in version 1.18.100.1:

- Introduced Intel® TDX 1.4 & 1.5 support
- Upgraded Ring3 Abstraction Layer (R3AAL) library to support Intel® TDX MVP 6.2 kernel
- Enhanced quote verification performance in multi-thread scenarios
- Upgraded Intel® SGX Quote Verification Enclave to integrate latest OpenSSL/SgxSSL 1.1.1u
- Fixed bugs

Note: This is the final release that will support Ubuntu 18.04 LTS. The next release of this software will not include pre-built packages for Ubuntu 18.04 LTS, aligning with Ubuntu's LTS release Standard Support policy.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes following changes in version 1.17.100.3:

- Applied CVE-2023-1255, CVE-2023-0465, and CVE-2023-0466 patches to SgxSSL/OpenSSL 1.1.1t
- Updated Intel® SGX Quote Verification Enclave to integrate updated SgxSSL
- Enhanced the attestation local cache functionality by giving users the option to provide their own cache file
- Enabled QPL/QCNL log in DCAP samples
- Fixed bugs

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes following changes in version 1.16.100.2:

- Upgraded Intel® SGX Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1t
- Added new API in quote verification library to extract FMSPC (Family-Model-Stepping-Platform-CustomSKU) value from ECDSA quote
- Added Rust support for SGX ECDSA quote generation
- Added Linux kernel 5.19 support in TDX R3AAL (Ring 3 Attestation Abstraction Layer)
- Removed Protobuf in TDX QGS (Quote Generation Service) and R3AAL (Ring 3 Attestation Abstraction Layer)
- Fixed bugs

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes following changes in version 1.15.100.3:

- Upgraded Intel® SGX Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1q
- Upgraded Intel® SGX QE3 to make it backward compatible
- Improved ECDSA quote generation and verification performance by caching PCK certificates and collaterals in memory and disk drive
- Added Java support for quote verification library
- Added new APIs to unify Intel® SGX and TDX quote verification in Quote Verification Library
- Added Advisory ID in ECDSA quote verification supplemental data
- Added Intel® TDX support in RA-TLS (Remote Attestation based TLS) library

- Improved TDX quote generation throughput in vsock mode
- Added Rust support for TDX quote generation
- Added support for the Linux kernel APIs for the Enclave Dynamic Memory Management (EDMM) features that are available with the Linux kernel v6.0 or later. Refer to the SGX SDK developer reference for details on new trusted APIs and enclave configuration for the EDMM features
- Fixed bugs

The download.01.org directory layout restructuring – Possible Impact

1. Debian repository/packages:

You may continue accessing the Debian repo/packages in the sgx_repo directory, as suggested in the Linux Installation Guide.

Directly accessing individual Debian packages from the directories listed below is no longer be possible:

a) From latest directory
b) From a specific release under sgx-linux directory
c) From a specific release under sgx-dcap directory

2. DCAP tools will be moved to the distro directory and the tools directory will be removed.

If you access the tools in your project and get a download failure, please update the URL accordingly.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes following changes in version 1.14.100.3:

- Re-signed all the Intel® SGX Architecture Enclaves (AEs) to address CVE-2022-21123, CVE-2022-21125 and CVE-2022-21166
- Added Intel® TDX Attestation support
- Added Rust support for ECDSA quote verification
- Upgraded Intel® ECDSA Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1o
- Fixed bugs

Note: There is no official support for some newer Linux distros yet, such as Ubuntu 21.10. But note that newer Linux distros may restrict access to the SGX enclave device node,

"/dev/sgx_enclave", to members of the "sgx" group. In that case, please add the group to the user ID to run enclave apps using this command: " usermod -aG sgx <uid>"

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes following changes in version 1.13.100.4:

- Enhanced QPL (Quote Provider Library) to support caching Intel® PCK (Provisioning Certificate Key) certificate chain in local memory, or retrieving Intel® PCK cert chain from local HTTP/S address
- Upgraded Intel® ECDSA Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1m
- Introduced Intel® ID enclave for QE identity generation
- Fixed bugs

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes following changes in version 1.12.101.1:

- Upgraded Intel® ECDSA Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1l
- Fixed bugs

You can refer to README to get the source code of Intel® Software Guard Extensions prebuild Architecture Enclaves

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.12.100.3:

- Upgraded Intel® Integrated Performance Primitives (IPP) Cryptography library to version 2021 update 3
- Upgraded Intel® SGX Architecture Enclaves based on new IPP crypto library
- Added support in Intel® Quote Provider Library (QPL) to retrieve SGX ECDSA quote verification endorsements from Intel® Provisioning Certificate Service (PCS). User can configure PCCS or PCS in QPL's config file
- Updated SGX ECDSA quote verification library (QVL) and quote verification enclave (QvE) to support CRL in different encoding
- Updated SGX ECDSA quote verification library (QVL) and quote verification enclave (QvE) to hardcode Intel® root public key instead of root certificate
- Fixed bugs

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.11.100.2:

- Upgraded Intel® Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1k

- Updated the DCAP driver V1.33 with stability fixes, released as V1.33.2. This is to support legacy solutions not ready to transition to the latest DCAP driver V1.41 or kernel 5.11+
- Fixed bugs

SGX support has been built in mainline kernels since release 5.11. To avoid future incompatibility issues, it is strongly recommended for solutions using the DCAP driver to transition to use kernel 5.11 or above.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.10.3:

- Upgraded Intel® Integrated Performance Primitives (IPP) Cryptography library to version 2020 update 3
- Upgraded Intel® SGX Architecture Enclaves based on new IPP crypto library

This is the final release that will support Ubuntu 16.04 LTS. The next release of this software will not include pre-built packages for Ubuntu 16.04 LTS aligning with Ubuntu's LTS release Standard Support policy

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.10.100:

- Upgraded OpenSSL and SgxSSL to latest version 1.1.1i in DCAP components
- Added data base migration support in PCCS
- Fixed bugs

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.9.100:

- Added Ubuntu 20.04 support
- Added Intel® Provisioning Certification Service V3 API support for ECDSA attestation
- Fixed bugs.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.8.100:

- Provided standalone Intel® SGX DCAP Quote verification library installer.
- Provided standalone Intel® SGX DCAP Platform Certificate ID retrieval tool installation package.
- Fixed bugs.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.7.100:

- 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.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.6.100:

- 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 1.5.100:

- 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 1.4.100:

- 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 1.3.101:

- Fixed bugs.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.3.100:

- 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 1.1.100:

- Fix bugs.

Intel® Software Guard Extensions Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.0.100:

- 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* 20.04 LTS 64-bit Desktop and Server version
    - Ubuntu* 22.04 LTS 64-bit Server version
    - Ubuntu* 23.10 64-bit Server version
    - CentOS* 8.3 64bits
    - CentOS* Stream 9
    - Red Hat* Enterprise Linux* Server 9.2 (for x86_64)
    - SUSE* Linux* Enterprise Server 15.4 64bits
    - Debian* 10
    - Anolis* OS 8.6

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 1.21.1 release has a known vulnerability (CVE-2024-21511) in the mysql2 module installed by PCCS. To address this issue, execute "sudo -u pccs npm audit fix" in the PCCS directory following the installation.
- Multi-package system only. If PCCS is configured to use LAZY mode, and the platform doesn't have the latest uCode patch, PCCS may return 462 error when the client requests for PCK certificate. Applying the latest uCode patch can fix this issue, or if you don't have the latest patch, you can change PCCS to REQ mode temporarily, and use the PCK ID retrieval tool to register the platform.
- RHEL only. When installing PCCS on Redhat, you may see errors when executing "sudo -u pccs ./install.sh". To workaround this issue, please go to /opt/intel/sgx-dcap-pccs/ directory, change the owner of all files and sub-folders to user "pccs" with "sudo chown -R pccs:pccs *", and run the install script again.
- Provisioning Certificate Caching Server (PCCS) 1.10.100 doesn't support upgrade installation on RHEL and CentOS. Please uninstall the old version and install v1.10.100 PCCS. Details please refer to DCAP installation guide.
- Provisioning Certificate Caching Server (PCCS) in Intel® DCAP 1.9 release only support Provisioning Certification Service (PCS) V3 API. If you want to use previous PCS API version such as V2, please use PCCS in previous DCAP release.

    - In order to make DCAP 1.9 software stack work with previous version PCCS, please configure correct PCCS URL in Quote Provider Library (QPL) configuration file, make sure the PCCS version number is also lower than 3. For sample, "PCCS_URL=https://localhost:8081/sgx/certification/**v2**/"
- 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

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.