Intel® Software Guard Extensions Data Center Attestation Primitives for Windows* OS

Release Notes

29 December 2025

Revision: 1.24.100.2

Contents:

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.

Product Contents

Intel® Software Guard Extensions Platform Software (Intel® SGX PSW) package includes the following software components:

Ingredient Binary	Version String
Intel® SGX DCAP NUGET installers	1.24.100.2
Intel® SGX DCAP Sample projects	N/A

What's New

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.24.100.2:

- Moved PCCS source to a separate repository: https://github.com/intel/confidential-computing.tee.dcap.pccs.
- Split PCCS Admin Tool into two: PCS Client Tool for Intel PCS interactions and PCCS Admin Tool for PCCS administrative operations.
- Extended QvE enclave size to support long Certificate Revocation List.
- Improved QVL to return complete collection of SA lists.
- Upgraded Intel® DCAP Quote Verification Enclave to integrate OpenSSL/SGXSSL 3.0.17.
- DCAP 1.24.100.2 package contains PCCS binaries built from the 1.23.100.1 source code that contains updated dependencies. Packages created from new PCCS repository will be available in the next release.
- Bug fixes.

Note: Intel anticipates ending Service Updates for Windows-based versions of the below products by the end of 2026. This includes:

- Intel SGX SDK for Windows OS
- Intel SGX Platform Software for Windows OS
- Intel SGX/TDX Data Center Attestation Primitives

These plans do not affect the Linux-based versions currently supported. At this time, we anticipate the final release that includes Windows support for these products will be in 2H 2026, and encourage appropriate action to ensure preparedness.

Changes in previous releases

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.23.100.1:

- Upgraded to OpenSSL 3.1.2.
- Fixed bugs

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.22.100.3:

- Upgraded Intel® Integrated Performance Primitives (IPP) Cryptography library to version 2021.12.1
- Upgraded Intel® SGX Architecture Enclaves based on new IPP crypto library
- Upgraded Intel® DCAP Quote Verification Enclave to integrate OpenSSL/SgxSSL 3.0.14

- Removed Intel® DCAP PCCS from repository
- Added Windows Server 2025 support
- Fixed bugs

Note:

Note that PCCS is not available from this release. Please follow DCAP installation guide to use 'PCCSAdminTool' to retrieve the attestation collaterals or use old version PCCS.

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.21.100.3:

- 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)
- Fixed bugs

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

- Upgraded Intel® SGX Quote Verification Enclave to integrate OpenSSL/SgxSSL 3.0.12
- Fixed bugs

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

- Enhanced quote verification performance in multi-thread scenarios
- Upgraded Intel® SGX Quote Verification Enclave to integrate latest OpenSSL/SgxSSL 1.1.1u
- Fixed bugs

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the 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

- Upgraded 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® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.16.100.2:

- Upgraded Intel® SGX Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1t
- Upgraded SQLite3 to version 3.40.1
- Added new API in quote verification library to extract FMSPC (Family-Model-Stepping-Platform-CustomSKU) value from ECDSA quote
- Fixed bugs

From this release, we will upload ZIP format release package to IDZ (Intel® Developer Zone).

You can use Powershell to extract the .zip file to %TEMP% (the default location for the previous releases), you can execute, for example:

Expand-Archive   '.\Intel SGX DCAP for Windows v1.16.100.2.zip' $env:temp

To expand the archive in the current directory:

Expand-Archive   '.\Intel SGX DCAP for Windows v1.16.100.2.zip'

Or right click on the zip file and click on "Extract All"

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.15.100.2:

- 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
- Fixed bugs

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the 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
- Upgraded Intel® ECDSA Quote Verification Enclave to integrate SgxSSL/OpenSSL version 1.1.1o
- Introduced Intel® ID enclave for QE identity generation

- Fixed bugs

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the 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
- Removed support for Windows Server 2016
- Fixed bugs

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

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

Intel® SGX 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® SGX 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
- Fixed bugs

Intel® SGX 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

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

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

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

- Fixed bugs.

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.7.100.2:

- 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.
- Fixed bugs.

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.6.100.2:

- Fixed bugs.

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.5.100.2:

- 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® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.4.100.1:

- 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® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.3.101:

- Fixed bugs.

Intel® SGX 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® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.2.101:

- Fixed bugs.

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.2.100:

- Updated Intel(R) SGX Launch Configuration Service driver to support Key Separation State (KSS) feature enabled enclave.
- Fixed bugs.

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.1.100:

- Fixed bugs.

Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) includes the following changes in version 1.0.101:

- Provided support for the Intel® SGX DCAP open source package and used it for building the current installer
- Fixed bugs.

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

- Provided support for the Windows* Server 2019 64-bit version
- Provided support for the Intel® SGX enclave common loader library
- Updated the Intel® Quoting enclave to use the Intel® Integrated Performance Primitives (Intel® IPP) Cryptography 2019 Update 1 library
- Fixed bugs.

System Requirements

Hardware Requirements

- Intel® Xeon® E processors on V5 and V6 platforms

- 3rd Generation Intel® Xeon® Scalable Processors

Software Requirements

- Supported operating systems:
    - Microsoft Windows* Server 2019 64-bit version.
    - Microsoft Windows* Server 2022 64-bit version.
    - Microsoft Windows* Server 2025 64-bit version.

Known Issues and Limitations

- Intel® SGX PSW 1.21.1 release has a known vulnerability (CVE-2024-21511) in the mysql2 module installed by PCCS. To address this issue, execute "npm audit fix" in the PCCS directory following the installation.

- PCCS doesn't support upgrade installation in Windows DCAP 1.15 release

- In Windows DCAP 1.13 release, PCCS may cannot be started after installation due to a known bug in node-windows 1.0.0-beta.7, please downgrade node-windows to 1.0.0-beta.6 as workaround.

  >npm uninstall -g node-windows

  >npm install -g node-windows@1.0.0-beta.6

- 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.

- 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.

  - SQLite 3.30.1 with unmitigated CVEs (CVE-2019-19244, CVE-2019-19645 and CVE-2019-19880) is used in untrusted part. The CVEs are not exploitable in SGX software stack.

  - 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.

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.

* Other names and brands may be claimed as the property of others.

Copyright 2019 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.

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