

# Intel® SGX Data Center Attestation Primitives for Linux\* OS

---

## *Release Notes*

9 March 2026

Revision: 1.25.100.1

# Table of Contents

Introduction.....	3
What's New.....	3
Changes in Previous Releases.....	3
System Requirements.....	10
Known Issues and Limitations.....	11
Disclaimer and Legal Information.....	12

## 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.

## What's New (in version 1.25.100.1)

- Added Intel® Trust Domain Extensions (Intel® TDX) enhancements including:
  - Trust Domain (TD) partitioning support (including quote definition, Trust Domain Quoting Enclave (TDQE), Quote Verification Library (QVL) updates), and
  - Runtime Measurement Register (RTMR) sysfs extension logic for Linux\* kernel v6.16+.
- Added Quote Appraisal Enclave (QAE) implementation.
  - The Open Policy Agent (OPA)-based evaluation algorithm (qal\_script.rego) used by the Quote Appraisal Library (QAL) and the QAE through WebAssembly (WASM) processing engine is now compiled directly into the QAL/QAE. The appraisal continues to be guided by the JWT-based policy inputs.
- OpenSSL updated to 3.0.19.
- The DCAP package now includes the PCCS binary built from the current PCCS repository sources (version 1.25).
- Added support for CentOS\* Stream 10 and Red Hat\* Enterprise Linux\* 10.
- Adjusted TCB Date Tag behavior to return the lower TCB date of platform TCB and QE TCB.
- Bug fixes.

Note: The next release of DCAP PCCS will no longer support Node.js v18 which is already End-of-Life (EOL) and v20 which will reach End-of-Life (EOL) status soon. Future releases will only support Node.js LTS versions that are in Active LTS or Maintenance LTS status according to the official [Node.js release schedule](#).

## Changes in Previous Releases

### Version 1.24.100.2

- Added support for Azure Linux 3.0, Debian 12 and Anolis 8.10.

- 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.
- Increased 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.

### Version 1.23.100.0

- Added support for Red Hat\* Enterprise Linux\* Server 9.4 (for x86\_64) and SUSE\* Linux\* Enterprise Server 15.6 64-bits.
- Added support for the FIPS 140-3 Certifiable QvE (Quote Verification Enclave) **as an experimental feature**.
- Fixed bugs

### Version 1.22.100.2

- 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 Ubuntu\* 24.04 LTS 64-bit Server support
- Fixed bugs

Note that PCCS is **not available** in this release. Please follow DCAP installation guide to use 'PCSCClientTool' to retrieve the attestation collaterals or use older version of PCCS.

### 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

## 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

## 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

## 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.

## 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

## 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

## 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 vssock 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 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 were moved to the [distro](#) directory and the [tools](#) directory was removed. If you access the tools in your project and get a download failure, please update the URL accordingly.

### 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>"`

### 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

### 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

### 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

### 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.

### 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

### Version 1.10

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

### Version 1.9

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

### Version 1.8

- Provided standalone Intel® SGX DCAP Quote verification library installer.

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

### Version 1.7

- 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.

### Version 1.6

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

### Version 1.5

- 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.

### Version 1.4

- 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.

### Version 1.3.1

- Fixed bugs.

### Version 1.3

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

### Version 1.2

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

### Version 1.1

- Fix bugs.

### Version 1.0.1

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

### 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.

## 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\* 22.04 LTS
  - Ubuntu\* 24.04 LTS
  - CentOS\* Stream 9

- CentOS\* Stream 10
- Red Hat\* Enterprise Linux\* Server 9.4
- Red Hat\* Enterprise Linux\* Server 10.0
- SUSE\* Linux\* Enterprise Server 15.6
- Debian\* 10
- Debian\* 12
- Azure\* Linux\* 3.0
- Anolis\* OS 8.10

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

## Known Issues and Limitations

- In SGX PSW 2.26/DCAP 1.23, we added support for the OpenSSL FIPS provider to the SGX SDK. However, as this is an experimental feature, this release won't include a FIPS Certifiable Quote Verification Enclave (QVE) built with the OpenSSL FIPS provider by default. If you plan to turn on the FIPS mode and require a full FIPS 140-3 Certifiable SGX DCAP solution, you may request a QVE built using the OpenSSL FIPS provider.

## 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](http://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](http://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.