Product brief

Intel Security System Software
Intel® Software Guard Extensions (Intel® SGX)

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

Orientation Guide

Attestation is the process of demonstrating that a software executable is properly instantiated on a platform. The Intel® Software Guard Extensions (Intel® SGX) remote attestation allows a remote party to check that the intended software is securely running within an enclave on a system with the Intel® SGX enabled.

Third party users of Intel® SGX may now author their own attestation infrastructure for Intel® SGX. The usage of third party attestation addresses the following limitations:

- Entities run large parts of their networks in environments where the Internet-based services cannot be reached at runtime.
- Entities are risk-averse in outsourcing trust decisions to third parties.
- Certain application models working in a very distributed fashion (for example, Peer-to-Peer networks) benefit from not relying on a single point of verification.
- Environments have requirements that conflict with the privacy properties that Intel® Enhanced Privacy Identifier (EPID) provides.

To address issues of this type, Intel offers an architecture that allows you to benefit from remote attestations without using Intel remote attestation services to validate the Intel® SGX attestation request at runtime.

For more information on Intel® solutions for third party remote attestations, see the Supporting Third Party Attestation for Intel® SGX Data Center Attestation Primitives (Intel® SGX DCAP) whitepaper.

This orientation guide describes various attestation collaterals provided by Intel that third parties can use to enable remote attestation of Intel® SGX platforms in a data center environment. The diagram on page 2 illustrates the architecture of a third party attestation for data centers.
The scheme includes a brief description of each block and the location of its documentation, source code and binaries. Note that only Intel® Xeon® E Processor based servers with the Intel® SGX flexible launch control feature enabled in BIOS are currently supported.

1. Intel® SGX Provisioning Certification Service

The Intel® SGX Provisioning Certification Service offers APIs for retrieving provisioning certification key (PCK) certificates, certificate revocation lists, Trusted Computing Base (TCB) information, the Intel quoting enclave (QE) identity, and the Intel quote verification enclave (QVE) identity. The QE and QVE identities are optional for third parties who choose to write and sign their own versions of these enclaves.

a. API Portal
All APIs that return PCK certificates require client authentication using an API key. All other API's are open and do not require client authentication. To acquire an API key, register yourself with the Intel® SGX provisioning certification service using the API portal. For more information, see https://api.portal.trustedservices.intel.com/provisioning-certification.

b. Intel® SGX Provisioning Certification Service API Documentation
Available on the API portal, see https://api.portal.trustedservices.intel.com/documentation#pcs-certificate.

c. PCK Certificate and CRL Profile Specification
Intel® SGX Provisioning Certification Service provides PCK certificates used for remote attestation and their certificate revocation lists (CRLs). You can find the certificate definitions at https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/SGX_PCK_Certificate_CRL_Spec-1.4.pdf .

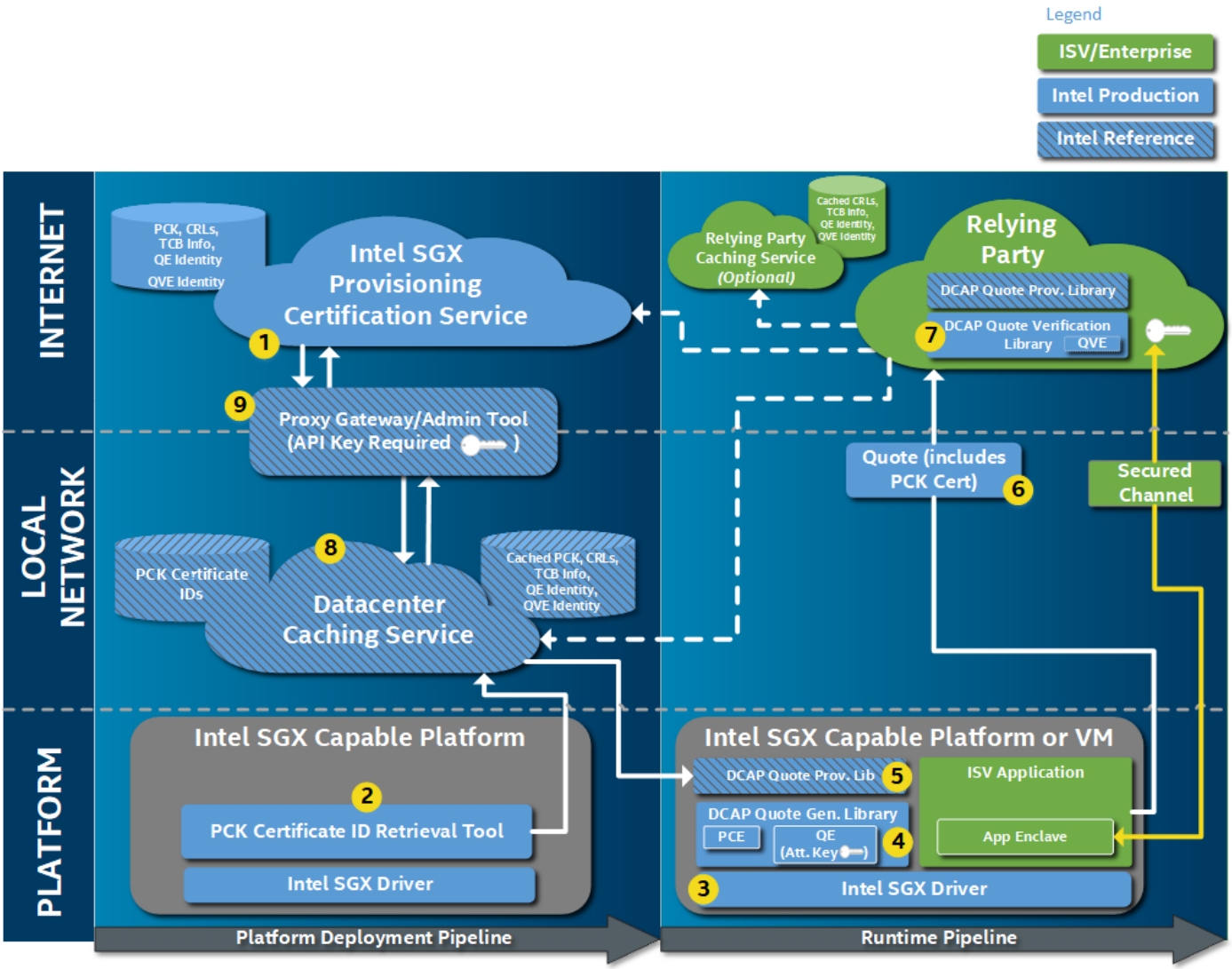

Figure 1: Architecture of a Third-Party Attestation for Data Centers

2. Intel® SGX PCK Certificate ID Retrieval Tool

Intel® SGX PCK certificate ID retrieval tool runs on an Intel® SGX capable platform owned by the data center and collects the information required to retrieve the platform PCK certificate from the Intel® SGX provisioning certification service. The resulting PCK certificate and other platform collaterals are loaded into the caching service and used during runtime attestation requests.

This tool works for both single package platforms as well as multi-package platforms but must be run on bare-metal or the host VM for multi-package platforms. This tool is provided as both opens source for Linux* and Windows* and as a Linux* and Windows* OS binary.

- Get the Linux binary package from: https://download.01.org/intel-sgx/latest/dcap-latest/linux/distro/
- Get the Windows binary package from: https://registrationcenter.intel.com/en/products/download/3610/
- Get the source code from the GitHub* project: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/tools/PCKRetrievalTool
- Documentation is stored in the following locations:
  - Intel® SGX ECDSA quote library API Reference: https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_ECDSA_QuoteLibReference_DCAP_API.pdf
  - Intel® SGX DCAP Multi-Package SW document: https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_DCAP_Multipackage_SW.pdf

For Linux* installation and usage instructions, see README.txt located in the package.

For more information on the Intel® SGX DCAP Linux* releases, see Intel® SGX for Linux* OS.

3. Intel SGX DCAP Driver

Intel® SGX driver package for the Intel® SGX DCAP is derived from the planned upstream version of the Intel® SGX driver. Once the Linux Intel® SGX driver is fully up streamed, this driver will not be needed.

Download the package using one of the following methods:

- Get the Linux* binary package from: https://download.01.org/intel-sgx/latest/dcap-latest/linux/distro/
- Get the source code from the GitHub* project: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/driver

Documentation is stored in the following locations:

- Binary installation guide: https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_SW_Installation_Guide_for_Linux.pdf
- README.md with source build instructions: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/driver

For more information on the Intel® SGX DCAP Linux* releases, see Intel® SGX for Linux* OS.

4. Intel® SGX Elliptic Curve Digital Signature Algorithm (ECDSA) Quote Generation Library for Intel® SGX DCAP

Intel® SGX ECDSA quote generation library is a library developed by Intel that generates ECDSA-based remote attestation quotes using a set of Intel-signed architecture enclaves called the provisioning certification enclave and the ECDSA quoting enclave. The Intel® SGX ECDSA quote generation library exposes a set of APIs that your application can use to generate the quote.

Download the package using one of the following methods:

- Get the binary package (libsgx-dcap-ql*.deb) from:

  https://download.01.org/intel-sgx/latest/dcap-latest/linux/distro/

- Get the source code from the GitHub project: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration

Documentation is stored in the following locations:

- Intel® SGX ECDSA quote generation library API Reference: https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_ECDSA_QuoteLibReference_DCAP_API.pdf
- Binary installation guide: https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_SW_Installation_Guide_for_Linux.pdf.
- Source build instructions: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration
- Sample application code: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/SampleCode/QuoteGenerationSample

For more information on the Intel® SGX DCAP Linux* releases, see Intel® SGX for Linux* OS.

5. Platform Quote Provider Library

The platform quote provider library provides a set of APIs that abstract platform implementation specific functions. This allows the Intel® SGX ECDSA quote generation library and the Intel® SGX ECDSA quote verification library to get data and services on a range of platforms and attestation environments. For example, attestation environments that cache PCK certificates need to provide the Intel® SGX ECDSA quote generation library with the proper Trusted Computing Base (TCB) matching the TCB of one of the PCK certificates in its cache. Relying parties that need to verify quotes will require additional information from Intel. Intel provides a reference platform quote provider library that works in conjunction with the reference caching service (see 'Caching Service for the Intel® SGX provisioning certification service' below) to provide this information to the quote libraries.

- Get the binary package (libsgx-dcap-default-qpl*.deb) from:

  https://download.01.org/intel-sgx/latest/dcap-latest/linux/distro

- Get the reference source code from: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration/qpl

Documentation is stored in the following locations:

- Binary installation and configuration guide: https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_SW_Installation_Guide_for_Linux.pdf
- Source build and configuration instructions: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration/qpl

For more information on the Intel® SGX DCAP Linux* releases, see Intel® SGX for Linux* OS.

6. ECDSA Quote Format

Intel has developed a quote format for Intel® SGX ECDSA-based quotes. This format is used by both the Intel® SGX ECDSA quote generation library and the Intel® SGX ECDSA quote verification library. The format of the quote is described in the Intel® SGX quote library API reference, appendix A.

For the Intel® SGX ECDSA quote generation library API reference, see https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_ECDSA_QuoteLibReference_DCAP_API.pdf

For more information on the Intel® SGX DCAP Linux* releases, see Intel® SGX for Linux* OS.

7. Intel® SGX ECDSA Quote Verification Library for Intel® SGX DCAP

Intel provides a quote verification library that implements a set of APIs to verify an ECDSA quote. You can integrate this library into a central relying party verification service on the local/remote network or integrate it directly on a

platform to provide peer-to-peer verification. This library utilizes the platform quote provider library APIs to retrieve the verification collateral (CRLs, TCB Info, and quoting enclave identity) needed for quote verification. It will perform signature and format checking for the quote, PCK certificates, and the verification collateral. It will then evaluate the quote to produce a verification result.

The quote verification library can run on both platforms with SGX and without SGX. When the platform supports SGX, the library can return an SGX REPORT authenticating the verification result was produced by the Intel® SGX Quote Verification Enclave (QVE).

- Get the binary package (libsgx-dcap-ql*.deb) from:

  https://download.01.org/intel-sgx/latest/dcap-latest/linux/distro

- Get the source code from the GitHub* project: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteVerification

Documentation is stored in the following locations:

- Intel® SGX ECDSA quote generation library API Reference: https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_ECDSA_QuoteLibReference_DCAP_API.pdf
- Binary installation guide: https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_SW_Installation_Guide_for_Linux.pdf.
- Source build instructions: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteVerification
- Sample application code: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/SampleCode/QuoteVerificationSample

For more information on the Intel® SGX DCAP Linux* releases, see Intel® SGX for Linux* OS.

8. Caching Service for Intel® SGX Provisioning Certification Service

Many cloud service providers (CSPs) and data center owners prevent their platforms from accessing the Internet directly. In addition, they avoid relying on an externally hosted service to perform runtime operations

The caching service for the Intel® SGX provisioning certification service allows a CSP or a datacenter to cache PCK certificates, PCK certificate revocation lists (CRL), TCB Information, QE identity and QVE Identity structures for all platforms in its data center. The PCK certificates, PCK CRLs, TCB information, and QE/QVE identity structures are all signed and published by Intel via the Intel® SGX provisioning certification service. All of these structures are required to perform the ECDSA based Intel® SGX remote attestation.

The CSP or data center can request the attestation data structures from Intel for each of its platforms during a deployment phase. A proxy server or administration tool with controlled access to the Internet is used to request the attestation data from the Intel® SGX provisioning certification service,

During runtime, the ECDSA-based Intel® SGX quote can be generated and verified using the data cached in the caching service without requiring access to the internet based service. Attestation collateral including TCB Information, Certificate Revocation Lists and QE/QVE Identities, needs to be refreshed periodically (per policies established by CSP/data center owners but not less frequent than the validity of each collateral).

Intel provides a reference caching service. The CSP or datacenter is expected to modify the reference to work within their infrastructure. The current release of the reference can be configured to fill its cache in a few ways.

i. Fill the cache using a push mechanism.

   The caching service will queue the PCK Certificate IDs uploaded by the PCK Certificate ID Retrieval Tool. Sometime later, an administration tool can download the PCK Certificate IDs and request the attestation collateral from the Intel® SGX provisioning certification service and provide them back to the caching service.

ii. Fill the cache using a pull mechanism.

   The caching service will only request attestation collateral from the Intel® SGX provisioning certification service when the PCK Certificate ID Retrieval Tool uploads a PCK Certificate ID.

iii. Fill the cache using a pull mechanism at run-time

   This is only suitable to environments that allow access to the Internet at run-time. In this case, the caching service will retrieve the attestation collateral from the Intel® SGX provisioning certification service during runtime quote generation or quote verification. In this mode, the availability of Intel® SGX provisioning certification service may impact the datacenter's or CSP's SLA during runtime.

- Get the binary package (libsgx-dcap-pccs*.deb) from:

  https://download.01.org/intel-sgx/latest/dcap-latest/linux/distro/

- Get the source code from the GitHub project: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration/pccs

Documentation is stored in the following locations:

- Binary installation and configuration guide: https://download.01.org/intel-sgx/latest/dcap-latest/linux/docs/Intel_SGX_SW_Installation_Guide_for_Linux.pdf
- Source build and configuration instructions: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration/pccs

For more information on the Intel® SGX DCAP Linux* releases, see Intel® SGX for Linux* OS.

9. Proxy Gateway/Admin Tool

This tool works in conjunction with the cache fill using a pull mechanism described in the 'Caching Service for Intel

SGX provisioning certification service' section. It is provided as a python script and can be found here: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/tools/PccsAdminTool.