Product brief

Intel Platform Security
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. Using 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 EPID provides.

To address issues of this type, Intel offers proposed 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 third party attestation collaterals provided by Intel that you 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 and implementation. 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 certificate service

The Intel® SGX provisioning certificate service offers APIs for retrieving provisioning certification key (PCK) certificates, revocation lists, Trusted Computing Base (TCB) information, and the quoting enclave (QE) identity for platforms with Intel® SGX enabled, all provided to an on-premise caching service for the Intel® SGX provisioning certificate service.

a. API portal
To get an API key, register yourself with the Intel® SGX provisioning certificate service because APIs that support returning PCK certificates require the API key. For more information, see https://api.portal.trustedservices.intel.com/

b. Intel® SGX provisioning certification services API documentation
See https://api.portal.trustedservices.intel.com/documentation#pcs-certificate

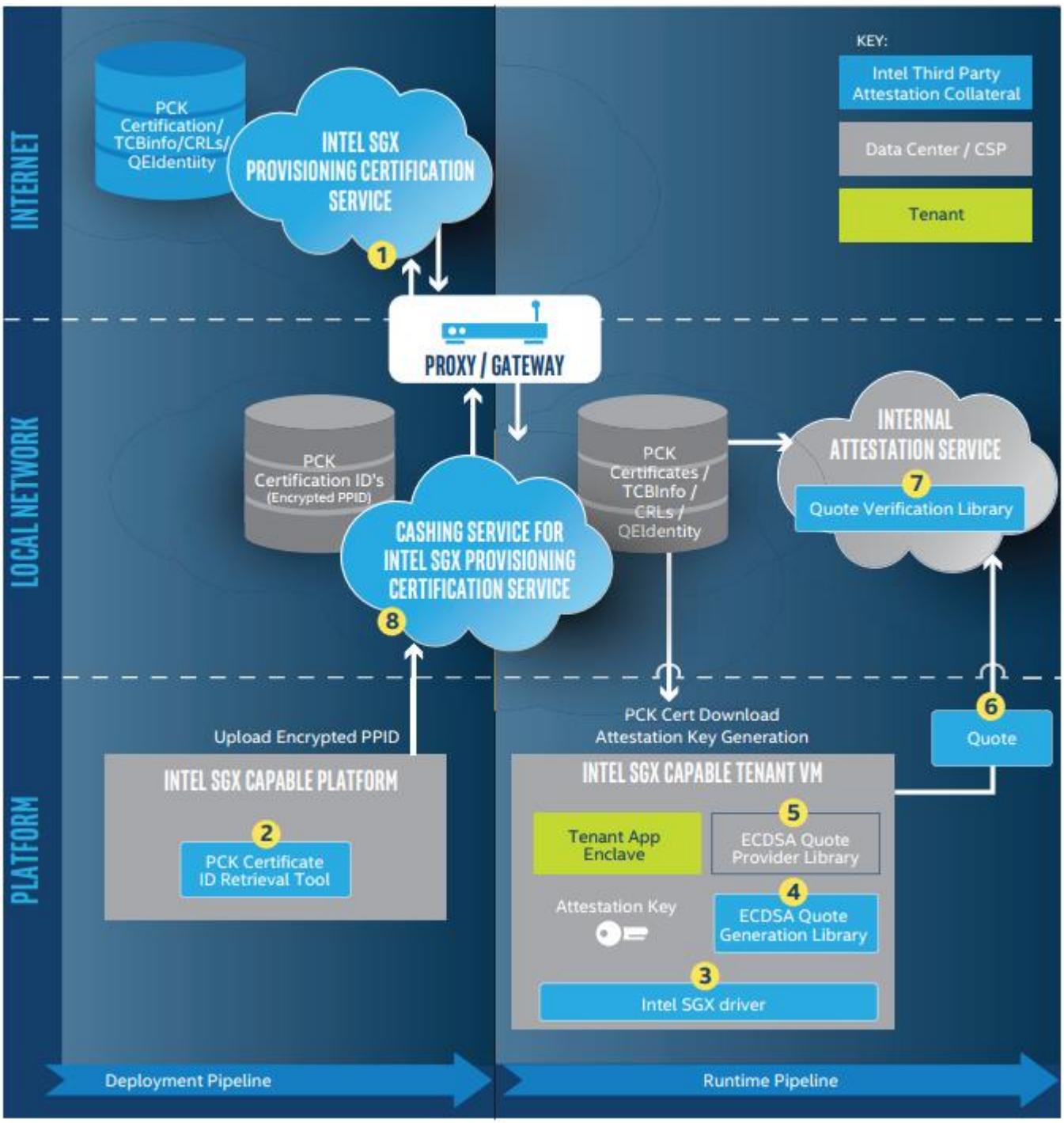
c. PCK Certificate and CRL Profile Specification
Intel SGX provisioning certificate service provides PCK certificates used for remote attestation and their certificate revocation list (CRL) certificates. You can find the certificate definitions at https://download.01.org/intel-sgx/dcap-1.1/linux/docs/Intel_SGX_PCK_Certificate_CRL_Spec-1.1.pdf

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 certificate service. The resulting PCK certificate is loaded into the on-premise caching service for Intel® SGX provisioning certificate service and used during runtime attestation requests. This tool is provided as a Linux* OS binary only.

Download the Intel® SGX provisioning service certificate ID retrieval tool from this https://download.01.org/intel-sgx/dcap-1.1/linux/dcap_installers/

Figure 1: Architecture of a third party attestation for data centers



For 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 upstream version of the Intel® SGX driver, including the in-driver launch enclave. Once the Intel® SGX driver is fully up streamed, this driver will not be needed.

Download the package using one of the following methods:

- Get the binary package from https://download.01.org/intel-sgx/dcap-1.1/linux/dcap_installers/
- 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/dcap-1.1/linux/docs/Intel_SGX_DCAP_Linux_SW_Installation_Guide.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 directly from:

- For Ubuntu* 16.04: https://download.01.org/intel-sgx/dcap-1.1/linux/dcap_installers/ubuntuServer16.04/
- For Ubuntu 18.04: https://download.01.org/intel-sgx/dcap-1.1/linux/dcap_installers/ubuntuServer18.04/
- 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/dcap-1.1/linux/docs/Intel_SGX_ECDSA_QuoteGenReference_DCAP_API_Linux_1.1.pdf
- Binary installation guide: https://download.01.org/intel-sgx/dcap-1.1/linux/docs/Intel_SGX_DCAP_Linux_SW_Installation_Guide.pdf.
- Source build instructions: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration
- Sample application code: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/SampleCode

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 allow the Intel® SGX ECDSA quote generation library to get platform specific services. 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. Intel provides a reference platform quote provider library that works in conjuction with the reference caching service for Intel® SGX provisioning certificate service (see 8 below).

For the reference source build instructions and library configuration, see https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration/qpl

For platform quote provider library API documentation, see https://download.01.org/intel-sgx/dcap-1.1/linux/docs/Intel_SGX_ECDSA_QuoteGenReference_DCAP_API_Linux_1.1.pdf

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 generation library API reference, appendix A.

For the Intel® SGX ECDSA quote generation library API reference, see https://download.01.org/intel-sgx/dcap-1.1/linux/docs/Intel_SGX_ECDSA_QuoteGenReference_DCAP_API_Linux_1.1.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 reference code that implements a set of APIs to ease the ECDSA quote verification. You can integrate this library into a central remote attestation server on the local network or within a peer-to-peer verification library. These APIs provide the quote and certificate parsing as well as signature and format checking for the quote, PCK certificates, CRLs, TCB Info, and quoting enclave identity.

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

Download the sample application from https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteVerification/Src/AttestationApp

Documentation is stored in the following locations:

- Build instructions: https://github.com/intel/SGXDataCenterAttestationPrimitives/blob/master/QuoteVerification/README.md.
- Intel® SGX ECDSA Quote Verification Library API Reference: https://github.com/intel/SGXDataCenterAttestationPrimitives/blob/master/QuoteVerification/Src/AttestationLibrary/include/SgxEcdsaAttestation/QuoteVerification.h.

8. Caching Service for Intel SGX provisioning certificate service

Many cloud service providers (CSPs) and data centers prevent their platforms from accessing the Internet directly. In addition, they do not rely on an externally hosted service to perform runtime operations (for example, the Intel® SGX remote attestation service).

The caching service for Intel® SGX provisioning certification service allows a CSP or a datacenter to cache PCK certificates, PCK certificate revocation lists (CRL), TCB Information, and QE identity structures for all platforms in its cloud or data center. The PCK certificates, PCK CRLs, the TCB information, and QE identity structures are all signed and published by Intel. To provide these structures, Intel hosts a service called the Intel® SGX provisioning certificate 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. To request the attestation data from the Intel® SGX provisioning certificate service, a proxy server with controlled access to the Internet is used. During runtime, the ECDSA based Intel® SGX quote can be verified using the data cached in the caching service for the Intel® SGX provisioning certificate service.

Intel does provide a reference caching service for Intel® SGX provisioning certificate service. The CSP or datacenter is expected to modify the reference to work within their infrastructure. The current release of the reference does have some functional limitations. The main limitation is that it requires run-time access to the internet to acquire the PCK certificates from the Intel® SGX provisioning certificate service. I.e. it does not support APIs to retrieve PCK certificates at deployment time.

For the reference source build instructions, server configuration and usage instructions, see: https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/QuoteGeneration/pcs.