Intel® Software Guard Extensions ECDSA - Attestation for Data Center 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.

Intel® SGX now allows third parties to author their own Intel® SGX attestation infrastructure to address the following issues:

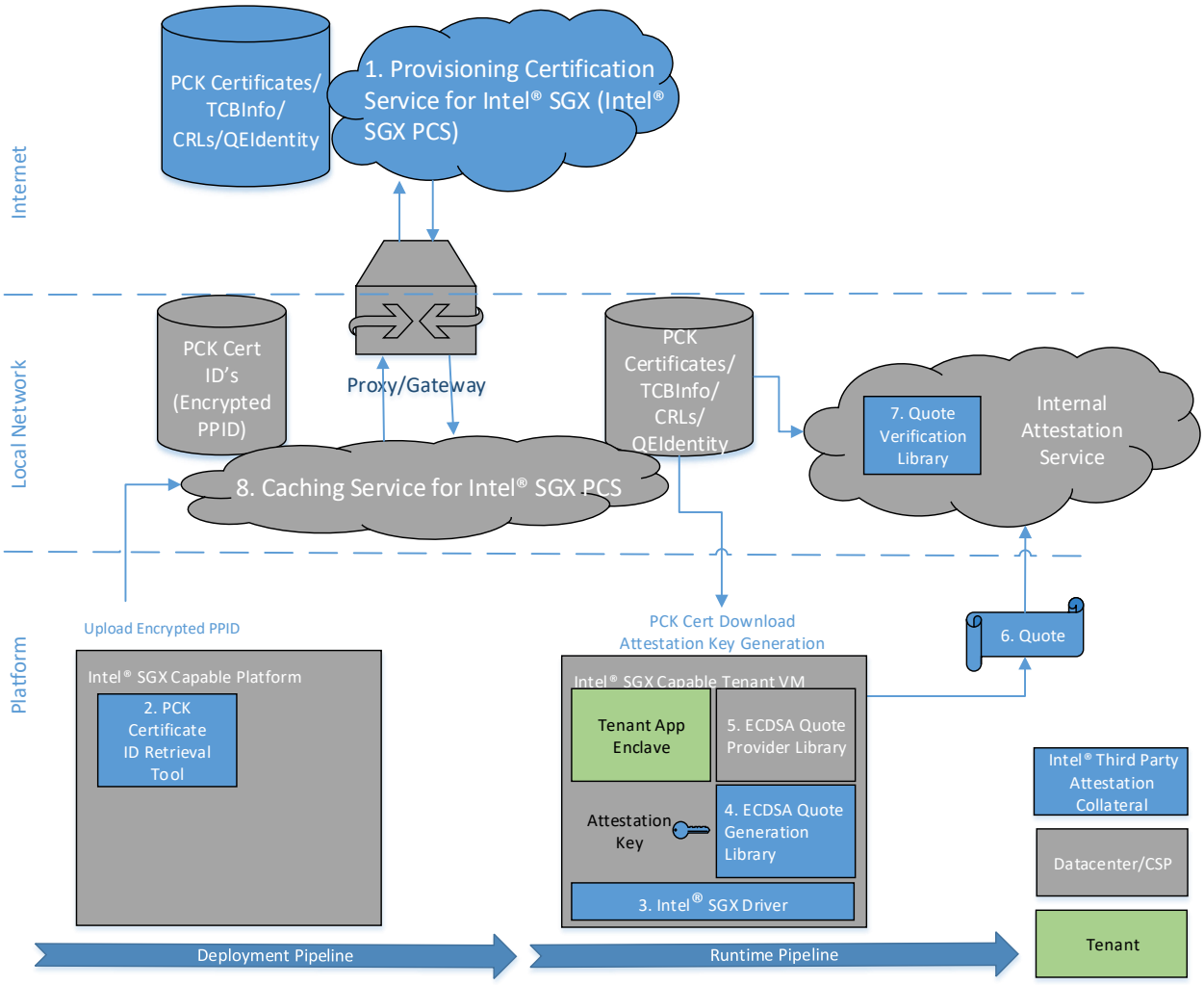
- Entities run large parts of their networks in environments where the Internet based services cannot be reached at runtime.
- Entities are risk averse in outsourcing trust decisions to third parties.
- Certain application models working in a very distributed fashion (for example, Peer-to-Peer networks) 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® SGX provides an architecture that allows you to benefit from remote attestations without using Intel® SGX services to validate the attestation at runtime.

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

This 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 below 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 Intel® SGX Flexible Launch Control feature enabled in BIOS are currently supported.



1. ***Intel® SGX Provisioning Certification Service (Intel® SGX PCS)***
   The Intel® SGX Provisioning Certification Service (Intel® SGX PCS) offers APIs for retrieving Provisioning Certification Key certificates, revocation lists, trusted computing base (TCB) information, and the QE Identity for platforms with Intel® SGX enabled, all provided to an on-premise Caching Service for Intel® SGX PCS.
   a. **API Portal**
      To get an API key, register yourself with the Intel® SGX PCS because APIs that support returning PCK Certificates require the API key. For more information, see https://api.portal.trustedservices.intel.com/.
   b. **Intel® SGX PCS API Documentation.**
      See https://api.portal.trustedservices.intel.com/documentation
   c. **PCK Certificate and CRL Profile Specification**

Intel® SGX PCS provides PCK Certificates used for remote attestation and their Certificate Revocation List Certificates. You can find the certificate definitions at https://download.01.org/intel-sgx/dcap-1.0.1/docs/SGX_PCK_Certificate_CRL_Spec-1.0.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 PCS. The resulting PCK Certificate is loaded into the on-premise Caching Service for Intel® SGX PCS and used during runtime attestation requests. This tool is provided as a Linux* OS binary only.

   Download the Intel® SGX PCK Certificate ID Retrieval Tool from: https://download.01.org/intel-sgx/dcap-1.0.1/dcap_installer/ubuntuServer1604/PCKIDRetrievalTool_v1.0.100.48192.tar.gz

   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 Driver for Data Center Attestation Primitives***

   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 SGX driver is fully upstreamed, 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-1.0.1/dcap_installer/ubuntuServer1804/sgx_linux_x64_driver_dcap_4f32b98.bin.
   - 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-1.0.1/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 ECDSA Quote Generation Library for Intel SGX DCAP***

   Intel® SGX ECDSA Quote Generation Library (Intel® SGX ECDSA QGL) 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 (PCE) and the ECDSA Quoting Enclave (ECDSA QE). The Intel® SGX ECDSA QGL 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-1.0.1/dcap_installer/ubuntuServer1604/
    - For Ubuntu* 18.04: https://download.01.org/intel-sgx/dcap-1.0.1/dcap_installer/ubuntuServer1804/.
- 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 QGL API Reference: https://download.01.org/intel-sgx/dcap-1.0.1/docs/Intel_SGX_ECDSA_QuoteGenReference_DCAP_API_Linux_1.0.1.pdf
- Binary installation guide: https://download.01.org/intel-sgx/dcap-1.0.1/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 QGL to get platform specific services. Attestation environments that cache PCK Certificates need to provide the Intel® SGX ECDSA QGL with the proper trusted computing base (TCB) matching the TCB of one of the PCK Certificates in its cache. The platform and attestation infrastructure owner is responsible for writing this library. Intel provides a sample Platform Quote Provider Library.
   Download the sample from:
   https://github.com/intel/SGXDataCenterAttestationPrimitives/tree/master/SampleCode/QuoteProviderSample.
   For the Intel® SGX ECDSA QGL API Reference, see https://download.01.org/intel-sgx/dcap-1.0.1/docs/Intel_SGX_ECDSA_QuoteGenReference_DCAP_API_Linux_1.0.1.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 (Intel® SGX ECDSA QGL) and the Intel® SGX Quote Verification Library (Intel® ECDSA SGX QVL). The format of the Quote is described in the Intel® SGX QGL API Reference, Appendix A.

   For the Intel® SGX ECDSA QGL API Reference, see https://download.01.org/intel-sgx/dcap-1.0.1/docs/Intel_SGX_ECDSA_QuoteGenReference_DCAP_API_Linux_1.0.1.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 QE 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 PCS***

   Many 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).

   The Caching Service for Intel® SGX Provisioning Certification Service (Intel® SGX PCS) allows a CSP or a datacenter to cache PCK Certificates, PCK Certificate Revocation Lists (CRL), TCBInfo, and QE Identity structures for all platforms in its cloud or data center. The PCK Certificates, PCK CRLs, the TCBInfo, and QE Identity structures are all signed and published by Intel. To provide these structures, Intel hosts a service called the Intel® SGX Provisioning Certification Service (Intel® SGX PCS). 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 PCS, 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 Intel® SGX PCS.

   Intel does not currently deliver the Caching Service for Intel® SGX PCS or a reference for it. The CSP or datacenter must provide its own implementation of the Caching Service for Intel® SGX PCS and update the attestation data structures appropriately.