INTEL® SGX'S OPEN SOURCE APPROACH TO 3RD PARTY ATTESTATION

Dan Zimmerman
Security Technologist
@zimmerd

S21c - ICMC 2019

Legal Disclaimer

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate 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. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

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

Agenda

Intel® Software Guard Extensions (Intel® SGX)

Intel SGX Remote Attestation

Intel SGX Datacenter Attestation Primitives

Summary

Intel® Software Guard Extensions (Intel® SGX)

CPU instructions that enable the creation of memory regions (with security features) called ‘enclaves’

- Encrypted memory with strong access controls
- Updatable Trusted Computing Base (TCB)
- Hardware based attestation capability

Developers leverage the Intel SGX SDK and PSW to create application enclaves

- Relocate sensitive code and data to the enclave
- Per process Trusted Execution Environment (TEE)

Use Cases

- Key Protection, Crypto Module Isolation, Confidential Computing, etc.

Intel SGX Remote Attestation

Intel SGX Remote Attestation

- A demonstration that software has been properly instantiated on a platform
- Allows a Relying Party increased confidence that intended software is:
  - Running within an enclave
  - On a fully patched and updated Intel SGX enabled platform in good standing
- Occurs before provisioning secrets to application enclave

Attestation Evidence Conveys

- Identity of Software Being Attested
- Associated Report Data
- Details of unmeasured state (e.g., execution mode)

Intel SGX Remote Attestation: Two Approaches

Intel SGX Attestation Service

- Client platform focused
- Privacy Preserving and based on Enhanced Privacy ID (EPID) signatures
- Verification as a Service
- Provisioning and Attestation at workload runtime

Intel SGX Datacenter Attestation Primitives (Intel® SGX DCAP)

- Datacenter and Cloud Service Provider focused
- Flexible provisioning and based on ECDSA signatures
- ‘Primitives’ allow for construction of on-prem Attestation Services
- Leverages Flexible Launch Control available in new Intel SGX enabled platforms
- Opensource

Intel SGX Datacenter Attestation Primitives (Intel SGX DCAP)

Enables 3rd parties to build their own Intel SGX Attestation Infrastructure

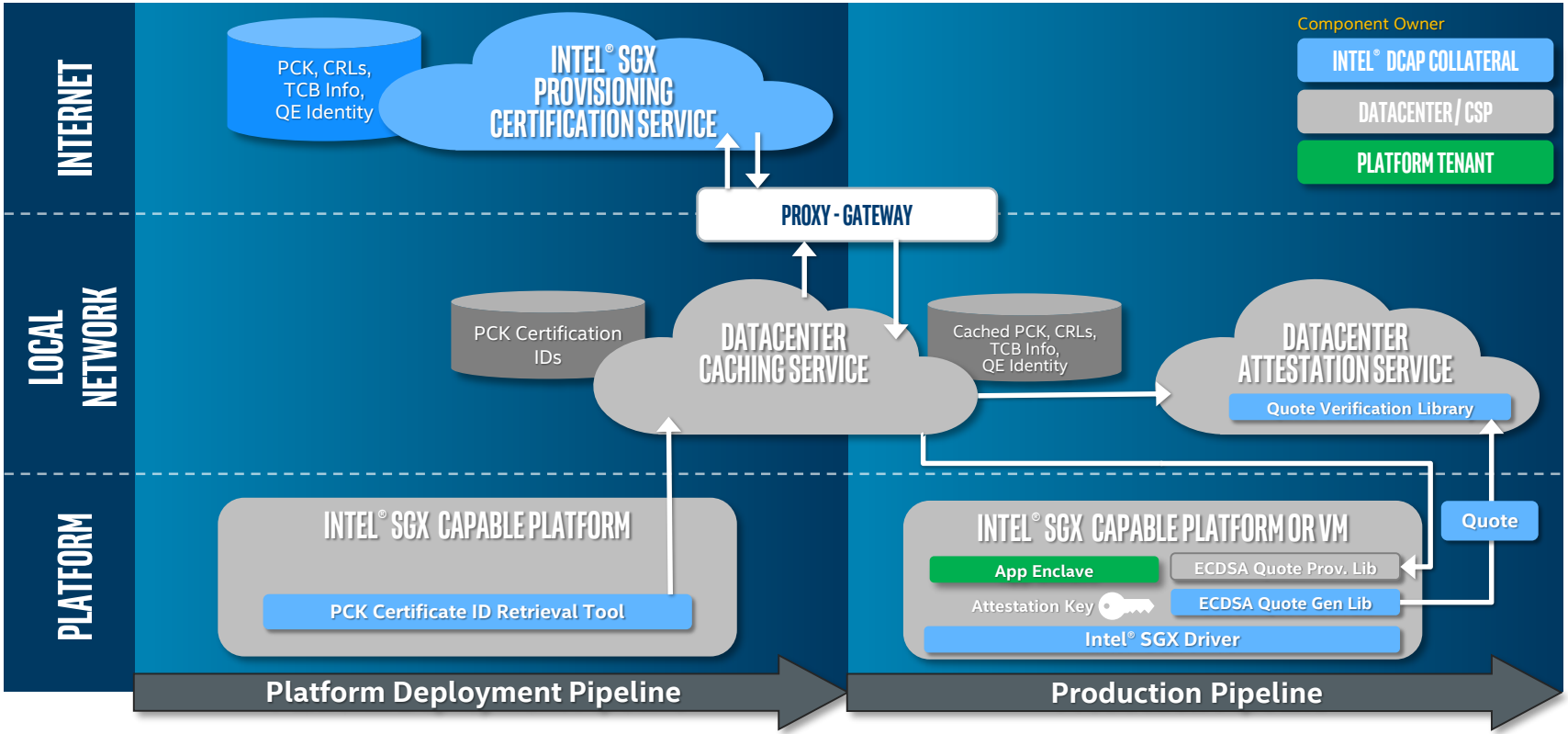
Ideal for :

- Environments where internet services are not accessible at workload runtime
- Entities who are risk-averse in outsourcing trust decisions to 3rd parties

Building blocks support three key attestation processes:

- Provisioning Certification Key and TCB Information Retrieval
- Quote Generation
- Quote and TCB Verification

High Level Architecture



Platform Certification Key (PCK) Retrieval

PCK Certificate

- Intel issues a PCK Certificate for each of its processors at various TCBs

PCK Certificate ID Retrieval Tool

- Extracts Platform Provisioning ID info for Intel PCS service request

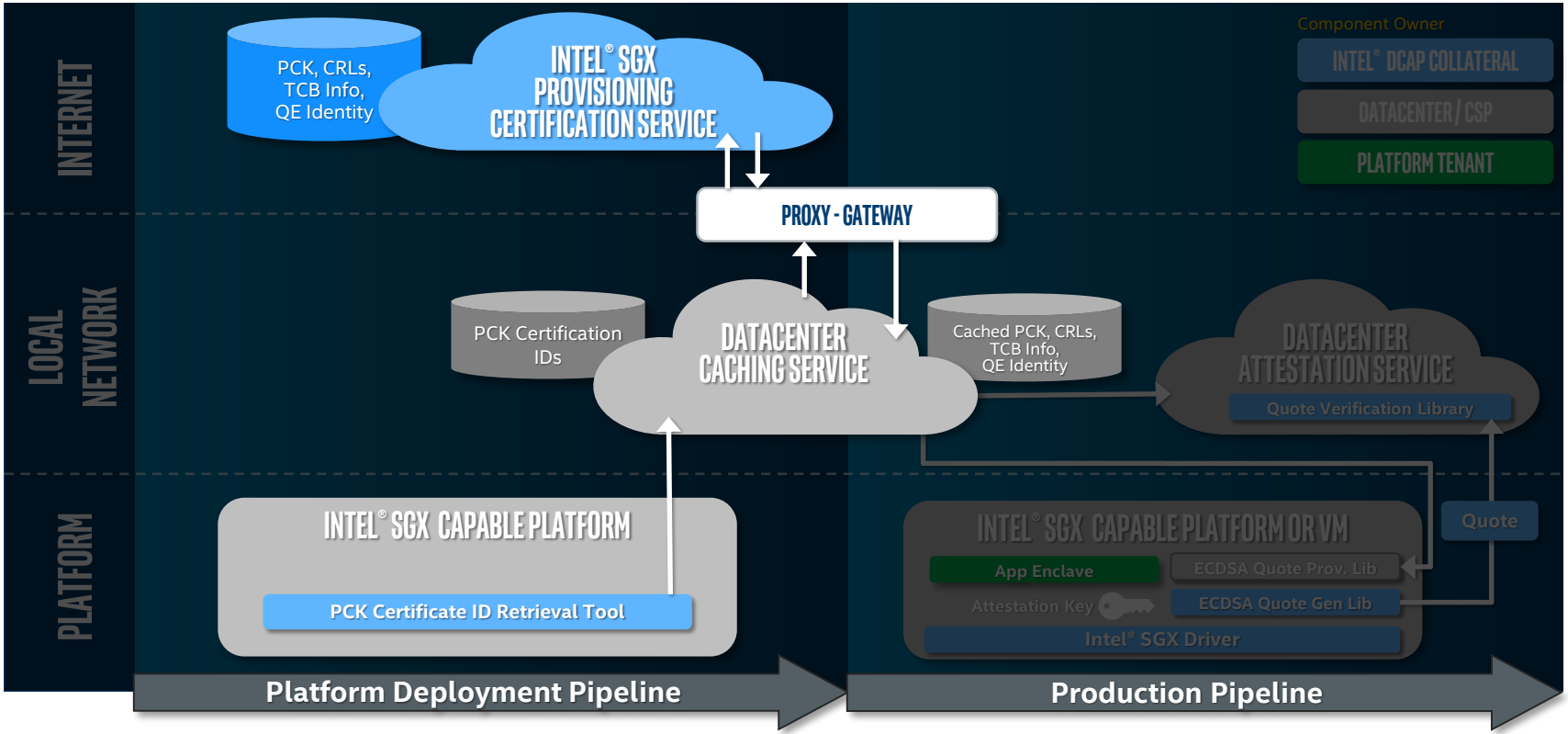
Intel Provisioning Certification Service (Intel PCS)

- Provisioning Certification Key (PCK) Certificate retrieval
- Intel SGX specific TCB information for a given processor type

PCK Caching Service

- Caches all PCK Certificates and associated TCB Info for each Intel SGX enabled platform in the datacenter
- Local to the datacenter for quick access

Platform Certification Key (PCK) Retrieval

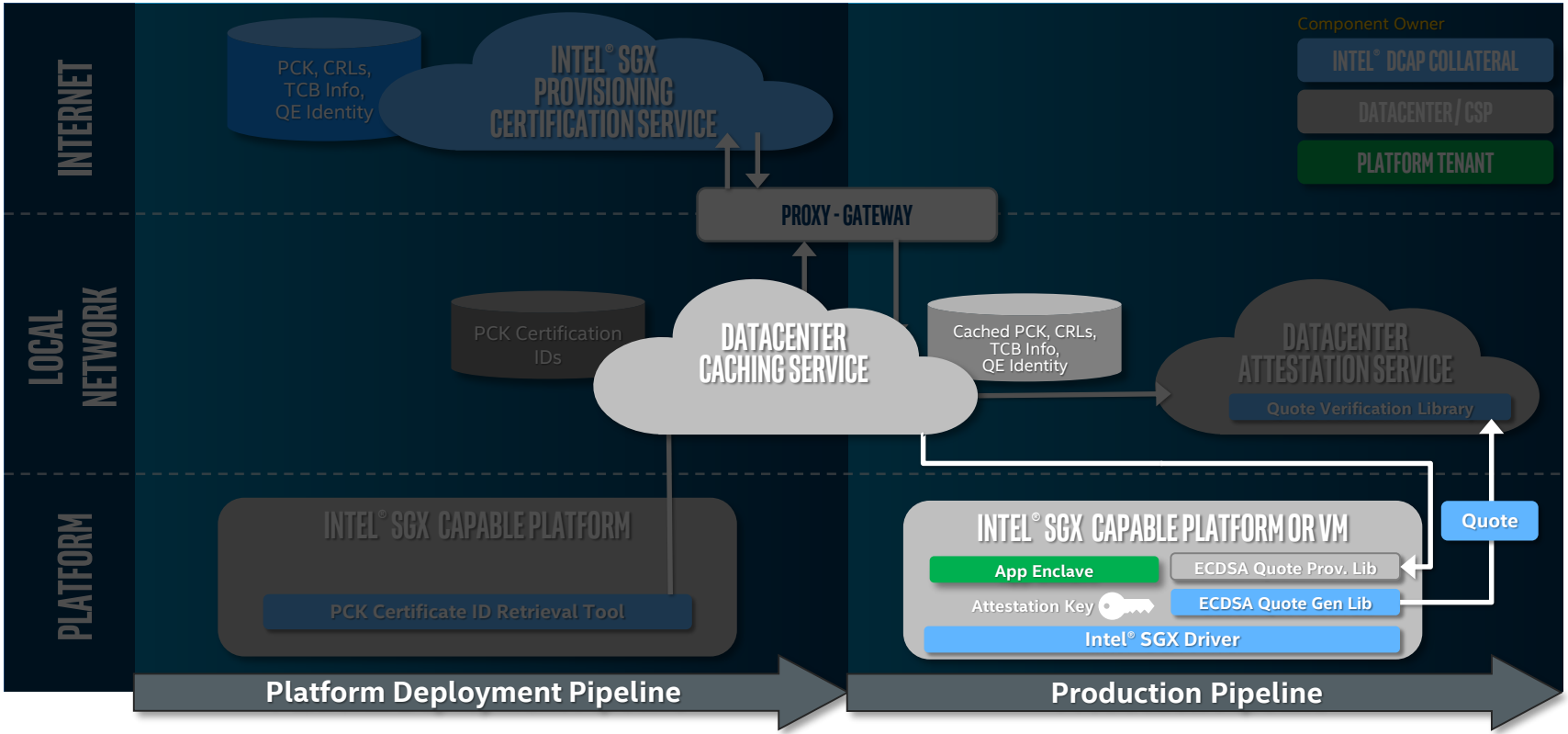


Quote Generation

Quote Generation Library

- API for generating attestation evidence for an Intel SGX based enclave
- Platform Certification Enclave
  - Local Certificate Authority for Quoting Enclaves (QE)
  - Provides some verification and then Certifies QE Attestation Keys
  - Signing key generated by SGX hardware specific to the TCB level associated with the PCK Certificate for the platform
- Quoting Enclave
  - Verifies and then signs the application enclave report resulting in a Quote

Quote Generation

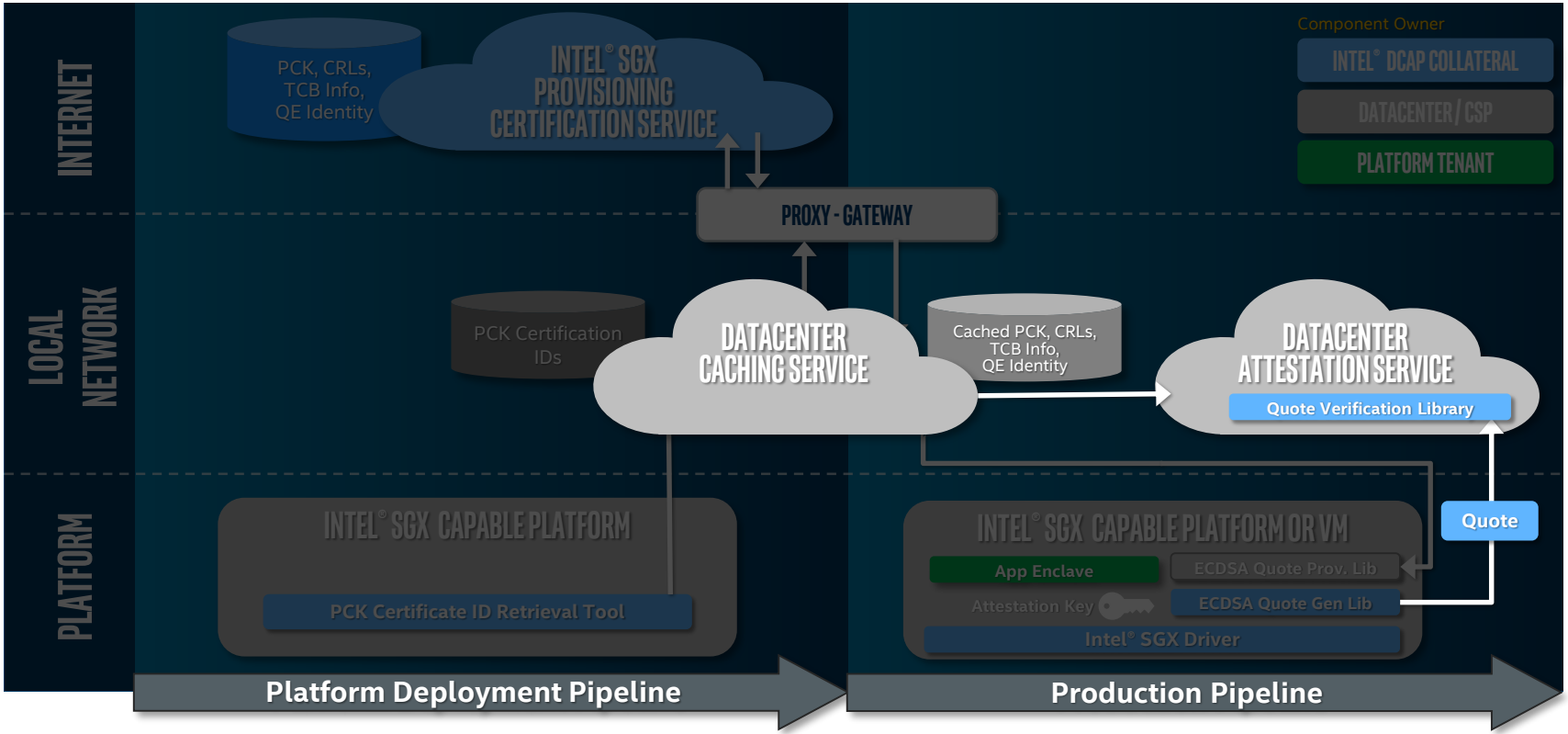


Quote & TCB Verification

Quote Verification Library (QVL) provides some validation as to:

- PCK Cert
- Platform TCB Info
- Quoting Enclave Identity
- ECDSA Verification of Quote
  - Determines if Relying Party should have more trust in the enclave being attested
- Note: App Enclave Identity verification is performed by the service providing some verification services (Attestation Service) and not the QVL itself

Quote & TCB Verification



Summary

Why is Intel SGX Remote Attestation Important?

- A successful attestation provides increased confidence to Relying Parties prior to deploying secrets to application enclaves
- And, allows for policy-based decisions based on Quote verification outcomes

Intel SGX DCAP allows 3rd parties to create their own Intel SGX Attestation Infrastructure for the Datacenter and Cloud

- Flexibility
- On-Prem Trust Decision
- SLA Ownership
- Opensource

More Information

Intel DCAP v1.1

- https://01.org/intel-softwareguard-extensions/downloads/intel-sgx-dcap-linux-1.1-release

Intel Provisioning Certification Service

- https://api.portal.trustedservices.intel.com/provisioning-certification

Source Code

- https://github.com/intel/SGXDataCenterAttestationPrimitives

Intel SGX Landing Zone

- https://software.intel.com/sgx

Slides Shared in Future Blog Post

- **https://intel.ly/2JflA2O**

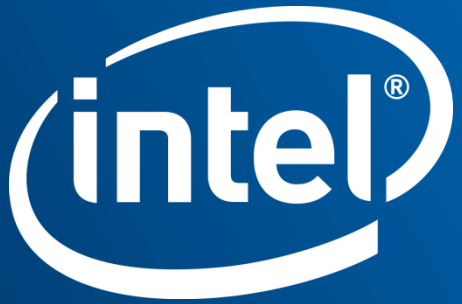
QUESTIONS, COMMENTS?

Dan Zimmerman

Security Technologist

@zimmerd

https://intel.ly/2JflA2O


intel®