OpenAnolis
龙 蜥 社 区

Intel SGX SDK/PSW/DCAP & TDX DCAP 简介

抽奖活动

OpenAnolis龙蜥

奖品

1、关注【OpenAnolis龙蜥】公众号

回复关键字"龙蜥直播"参与抽奖

2、奖品：小龙抱枕、龙蜥徽章、龙蜥笔本套装

中奖后，公众号后台回复"兑奖"填写兑奖信息

龍蜥
社區

/ 目录 /

Contents

01 / SGX 背景知识介绍

02 / Intel SGX SDK/PSW/DCAP技术栈

03 / Anolis OS 适配

01

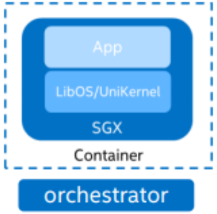
PART ONE

SGX 背景知识介绍

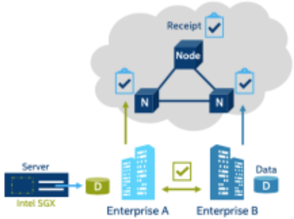
机密计算典型使用场景

Cloud Infrastructure

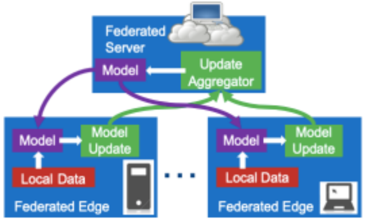
Secure Native Application Hosting



Trusted Multi-party Compute



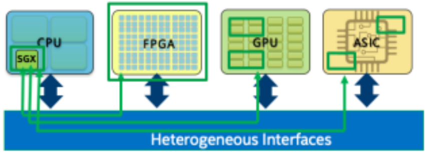
Federated Learning



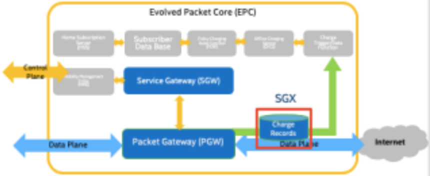
Secure Database

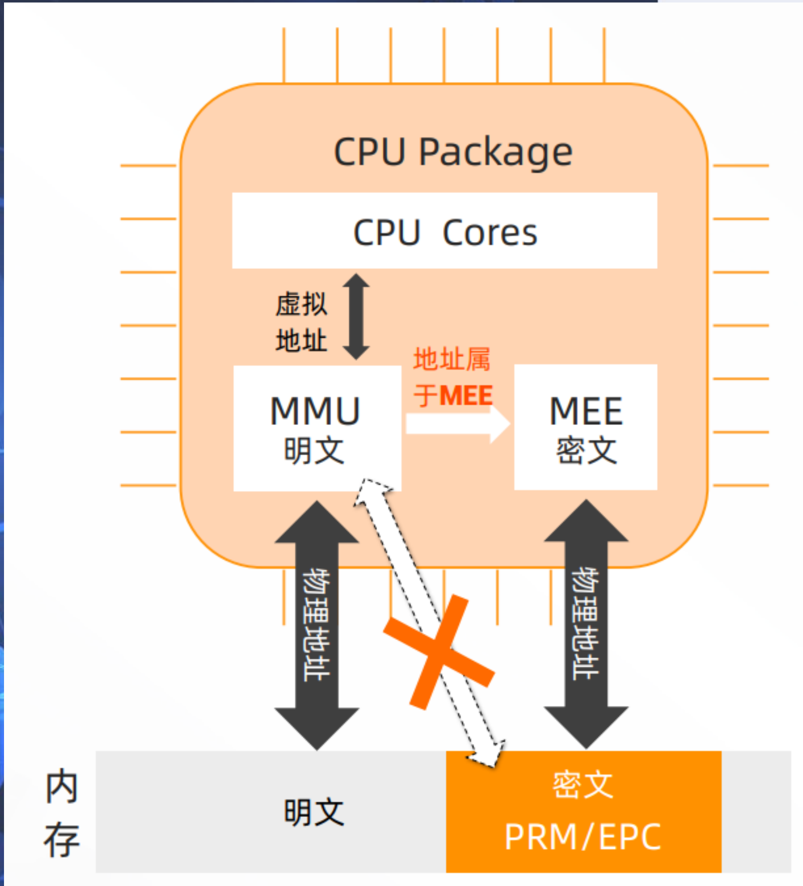
Crypto Key Management

Accelerated Secure Compute



Secure Networking





CPU/平台硬件特性

- SGX扩展指令集
- MEE（Memory Encryption Engine），每次重启会生成一个随机密钥，用于运行时加密
- PRM（Processor Reserved Memory）和内存访问机制
- SGX远程证明机制（英特尔或者第三方提供的在线服务）

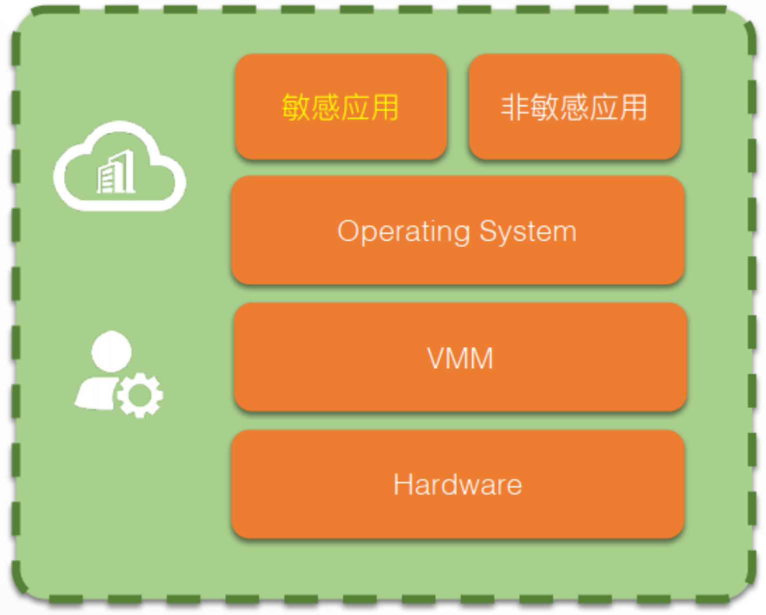
Enclave

Enclave是一段进程私有的可信内存，存放Enclave中的数据和代码被MEE加密，即使特权代码也无法访问。

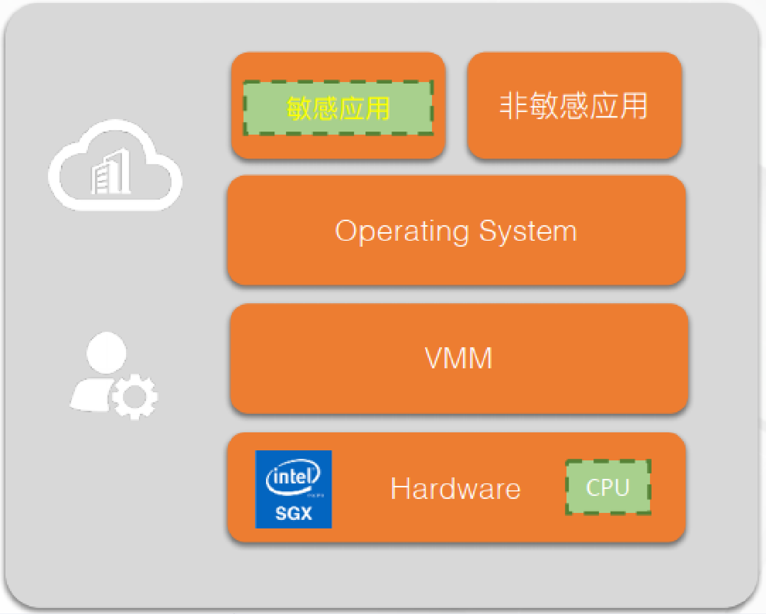
PRM

BIOS使能SGX, 保留一段物理内存为PRM（Processor Reserved Memory), 用E820表报告给操作系统。SGX使用这段内存创建和维护Enclave。

SGX对敏感数据的保护



普通运行环境无法保护敏感App的安全性

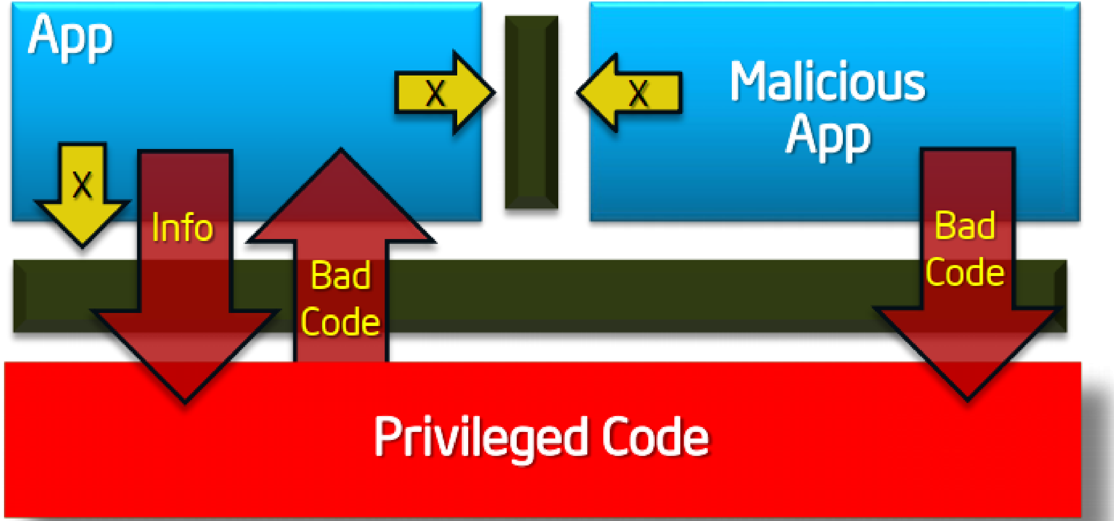


基于Intel SGX Enclave的可信执行环境能够有效保护敏感App的安全性

OpenAnolis
龙 蜥 社 区

The Basic Issue: Why Aren't Compute Devices Trustworthy?

Protected Mode (rings) protects OS from apps …



… and apps from each other …

… UNTIL a malicious app exploits a flaw to gain full privileges and then tampers with the OS or other apps

Apps not protected from privileged code attacks

Reduced attack surface with SGX

Application gains ability to defend its own secrets

- Smallest attack surface (App + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

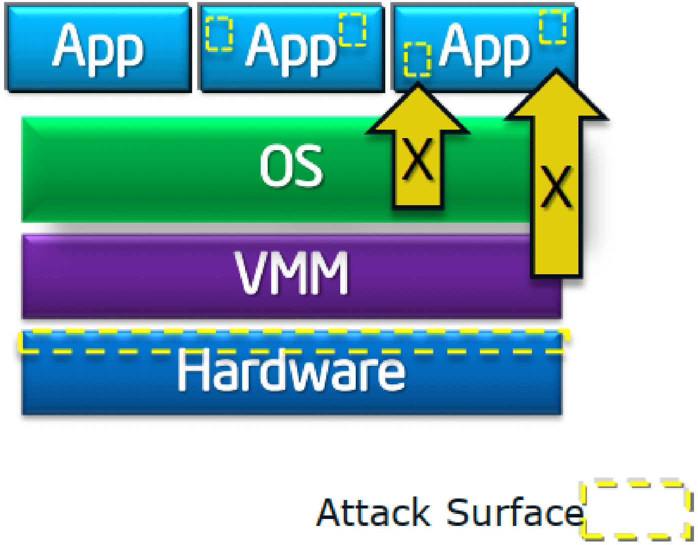
Familiar development/debug

- Single application environment
- Build on existing ecosystem expertise

Familiar deployment model

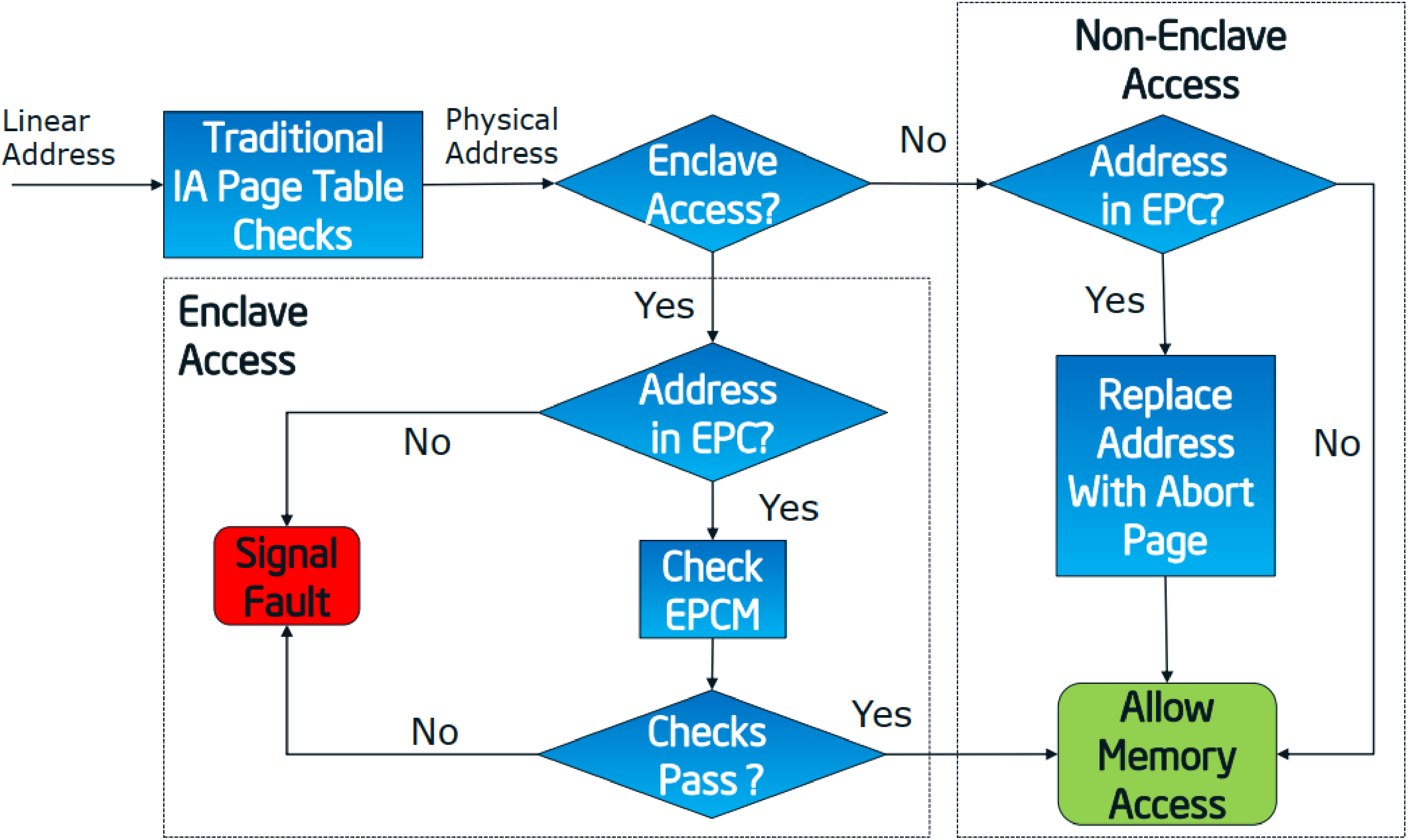
- Platform integration not a bottleneck to deployment of trusted apps

Attack surface with Enclaves

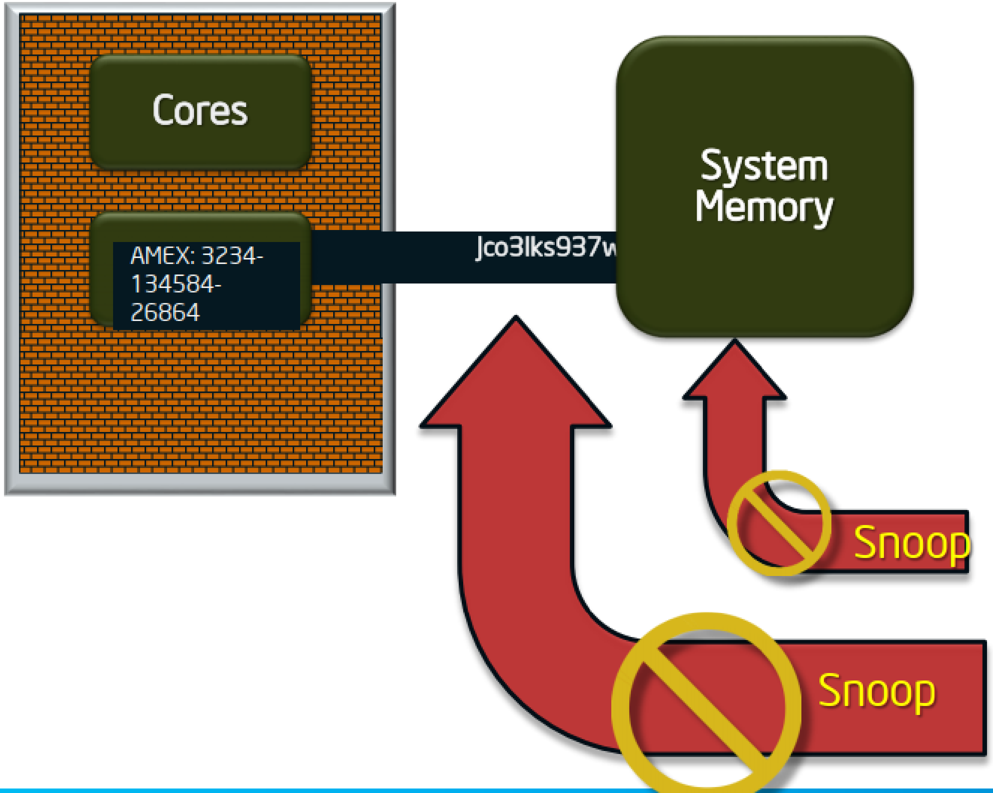


Scalable security within mainstream environment

SGX Access Control



Protection vs. Memory Snooping Attacks



Non-Enclave Access

- Security perimeter is the CPU package boundary
- Data and code unencrypted inside CPU package
- Data and code outside CPU package is encrypted and/or integrity checked
- External memory reads and bus snoops see only encrypted data

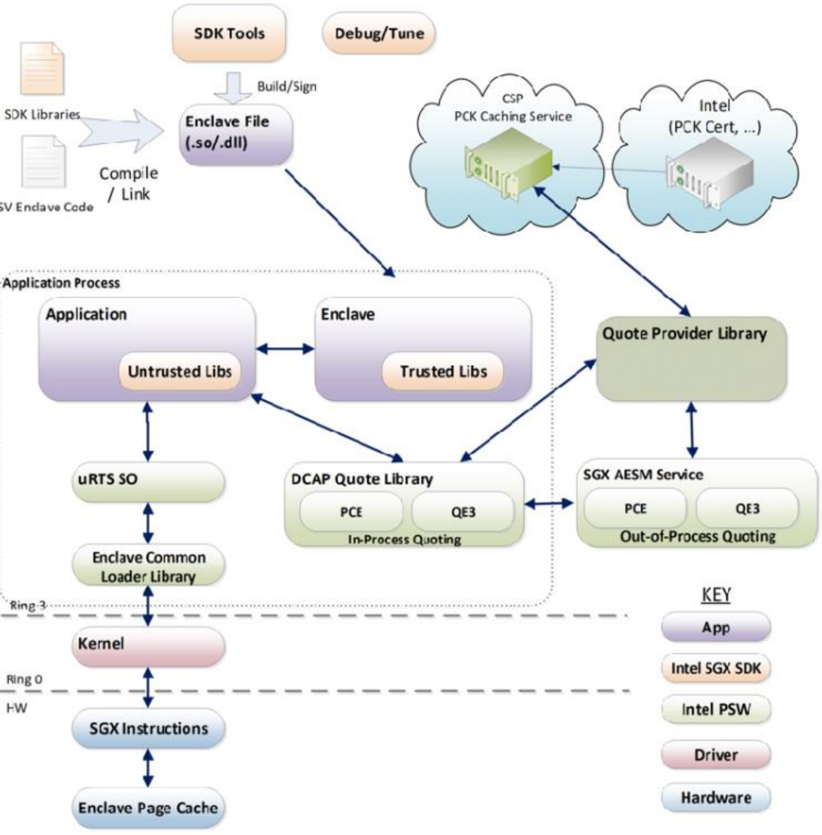
02

PART TWO

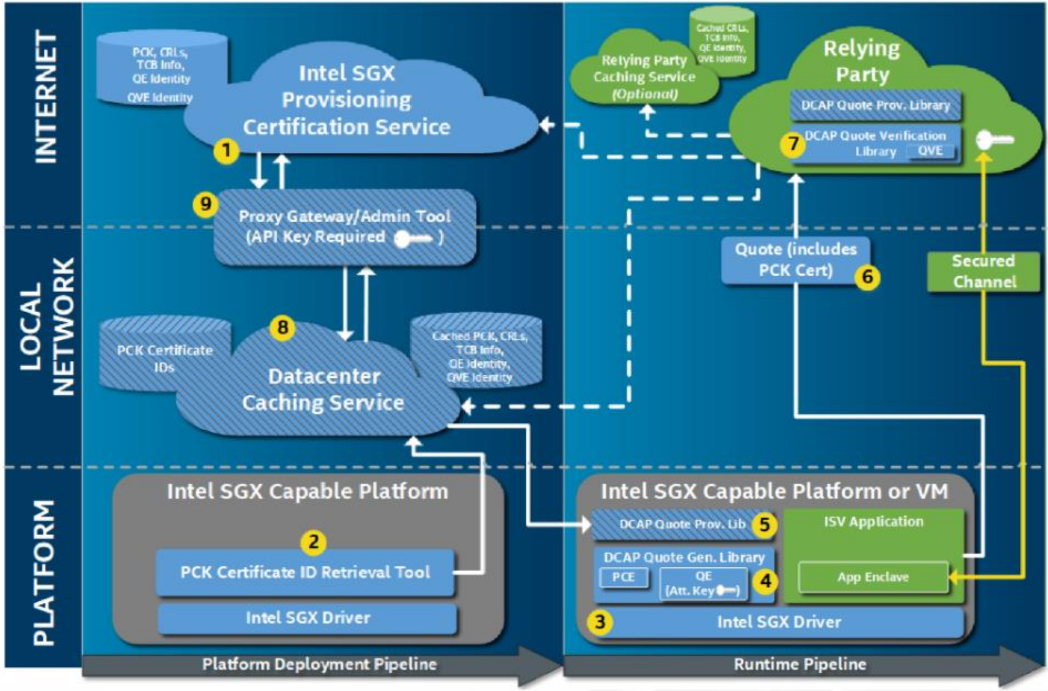
Intel SGX SDK/PSW/DCAP 技术栈

Intel SGX SDK & PSW & DCAP技术全栈

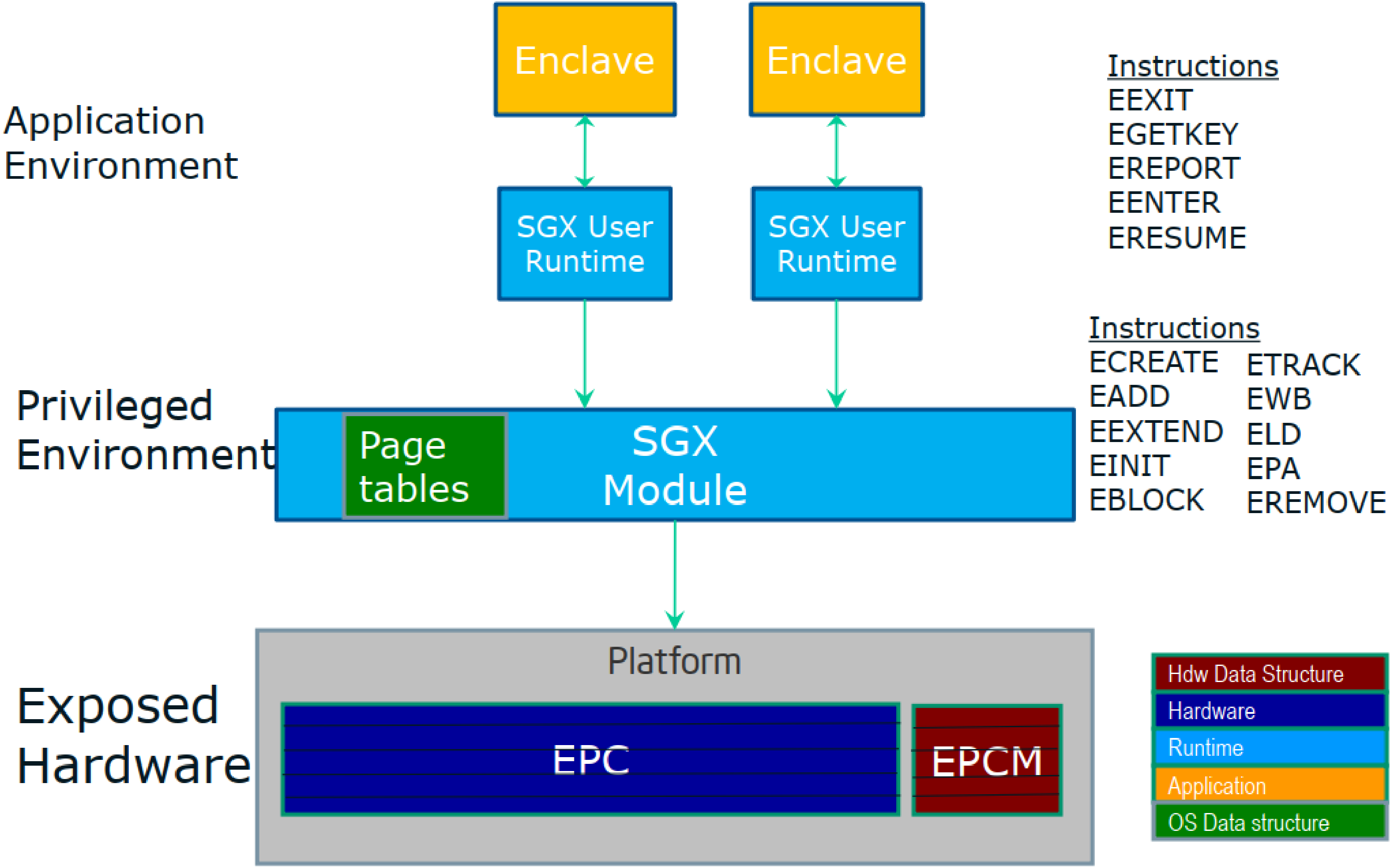
- SDK提供开发敏感应用的开发框架
- PSW为敏感应用提供运行时服务和库的支持
- DCAP为敏感应用提供远程证明的支持



Legend
- ISV/Enterprise
- Intel Production
- Intel Reference


INTERNET
LOCAL NETWORK
PLATFORM
PCK, CRLs, TCB Info, QE Identity QVE Identity
Intel SGX Provisioning Certification Service
1
9
Proxy Gateway/Admin Tool (API Key Required)
8
PCK Certificate IDs
Datacenter Caching Service
Cached PCK, CRLs, TCB Info, QE Identity, QVE Identity
Intel SGX Capable Platform
2
PCK Certificate ID Retrieval Tool
Intel SGX Driver
Relying Party Caching Service (Optional)
Cached CRLs, TCB Info, QE Identity, QVE Identity
Relying Party
DCAP Quote Prov. Library
7
DCAP Quote Verification Library
QVE
Quote (includes PCK Cert)
6
Secured Channel
Intel SGX Capable Platform or VM
DCAP Quote Prov. Lib
5
ISV Application
DCAP Quote Gen. Library
PCE
QE (Att. Key)
4
App Enclave
3
Intel SGX Driver
Platform Deployment Pipeline
Runtime Pipeline

SGX High-level HW/SW Picture



Application Environment

Enclave

Enclave

SGX User Runtime

SGX User Runtime

Instructions
EEXIT
EGETKEY
EREPORT
EENTER
ERESUME

Privileged Environment

Page tables

SGX Module

Instructions
ECREATE
EADD
EEXTEND
EINIT
EBLOCK
ETRACK
EWB
ELD
EPA
EREMOVE

Exposed Hardware

Platform

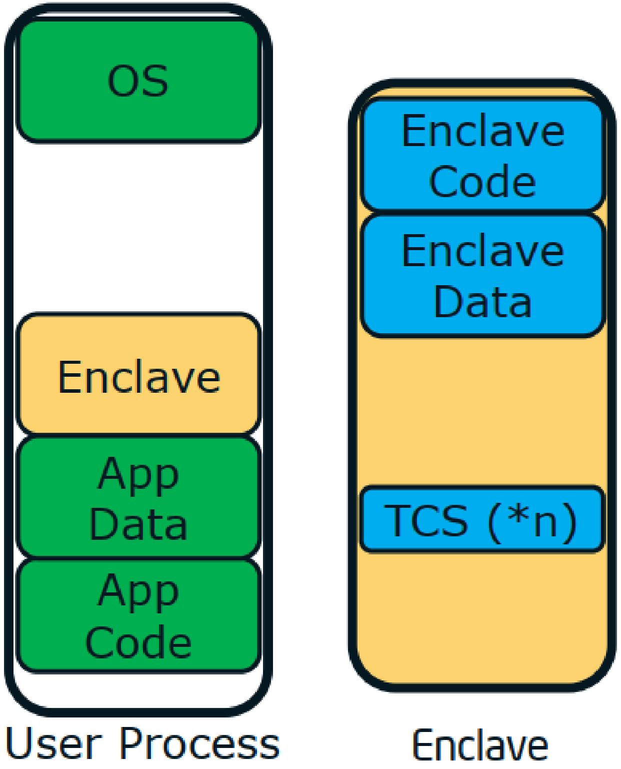
EPC

EPCM

Hdw Data Structure
Hardware
Runtime
Application
OS Data structure

SGX Programming Environment

Trusted execution environment embedded in a process



With its own code and data

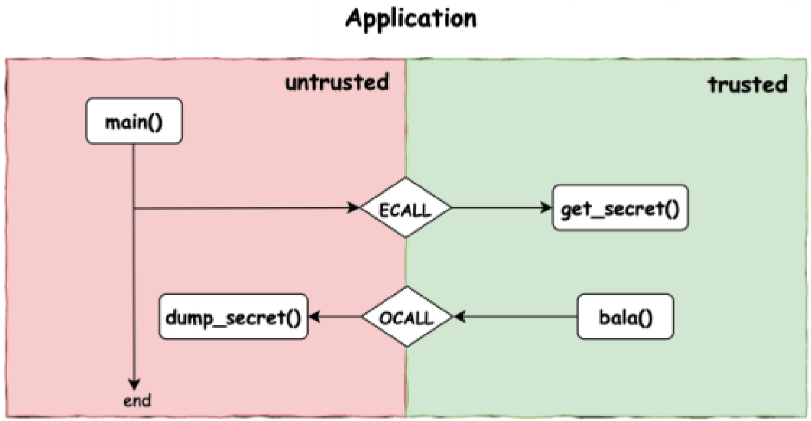
Provide Confidentiality

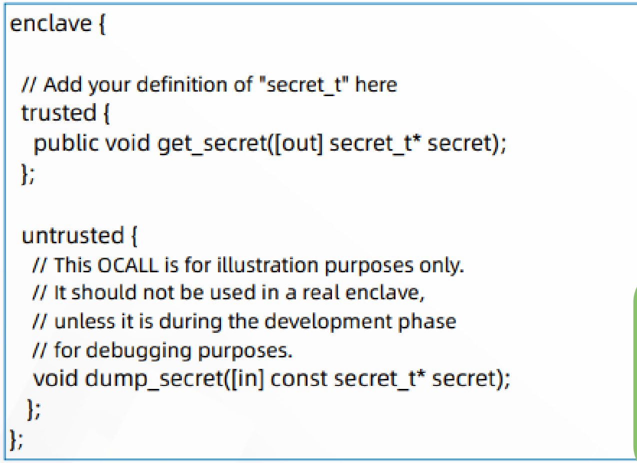
Provide integrity

With controlled entry points

Supporting multiple threads

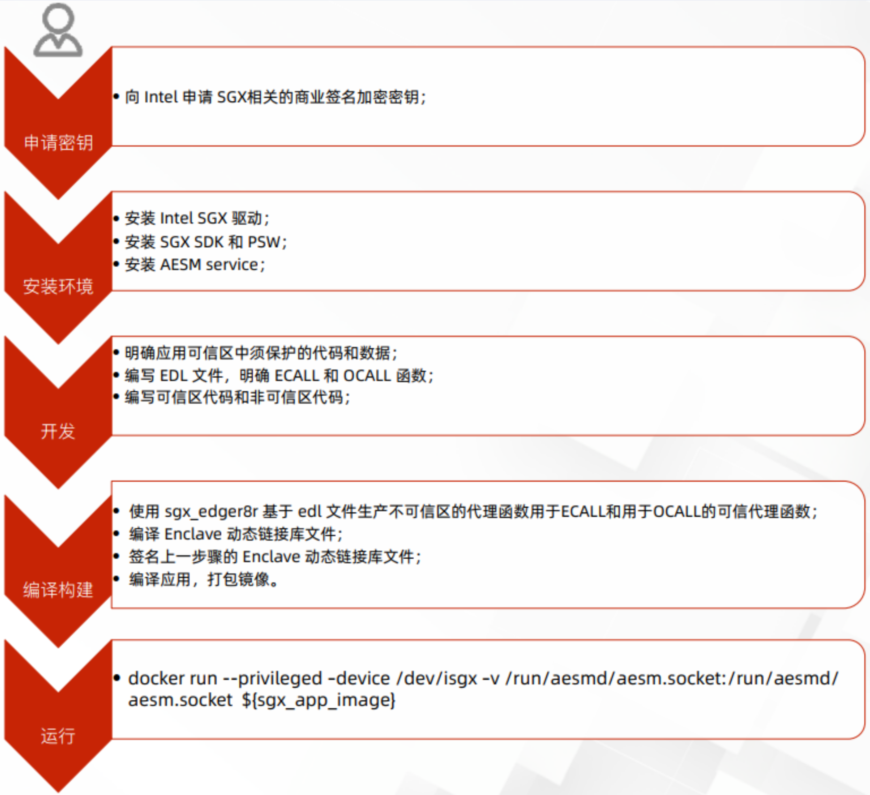
With full access to app memory




```
enclave {

 // Add your definition of "secret_t" here
 trusted {
   public void get_secret([out] secret_t* secret);
 };

 untrusted {
  // This OCALL is for illustration purposes only.
  // It should not be used in a real enclave,
  // unless it is during the development phase
  // for debugging purposes.
  void dump_secret([in] const secret_t* secret);
  };
};
```



- 向 Intel 申请 SGX相关的商业签名加密密钥；

- 安装 Intel SGX 驱动；
- 安装 SGX SDK 和 PSW；
- 安装 AESM service；

- 明确应用可信区中须保护的代码和数据；
- 编写 EDL 文件，明确 ECALL 和 OCALL 函数；
- 编写可信区代码和非可信区代码；

- 使用 sgx_edger8r 基于 edl 文件生产不可信区的代理函数用于ECALL和用于OCALL的可信代理函数；
- 编译 Enclave 动态链接库文件；
- 签名上一步骤的 Enclave 动态链接库文件；
- 编译应用，打包镜像。

- docker run --privileged -device /dev/isgx -v /run/aesmd/aesm.socket:/run/aesmd/aesm.socket ${sgx_app_image}

SGX 编程模型
SGX 2.0/DCAP/FLC 之后的几点变化：
1. 无需向Intel申请Enclave商业签名密钥
2. DCAP使用In-kernel SGX Driver
3. AESM service可选

OpenAnolis
龙 蜥 社 区

Overview of Intel® SGX DCAP

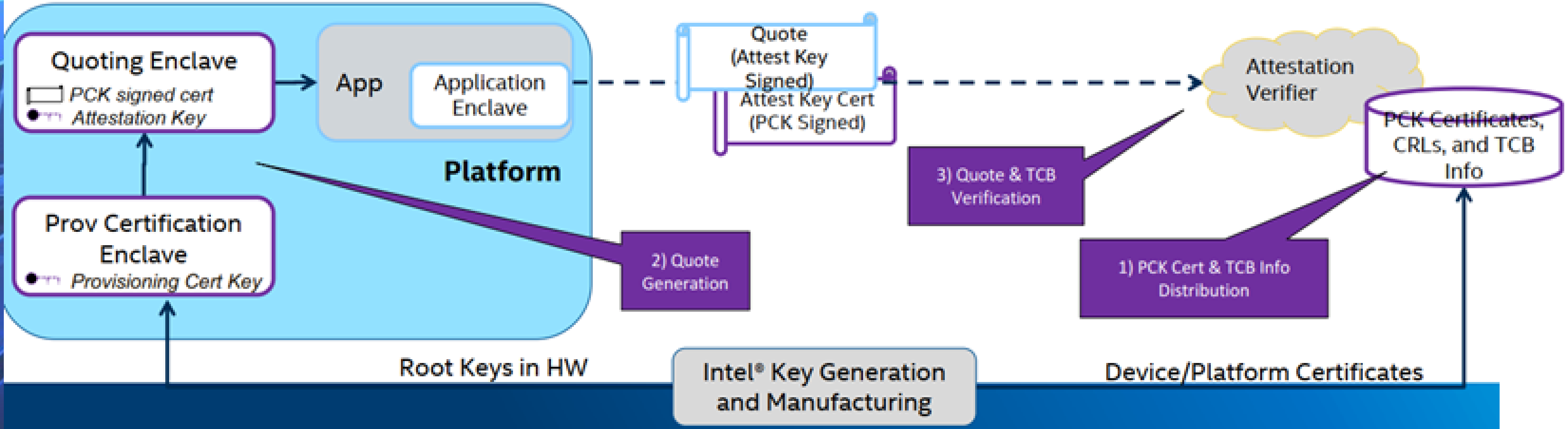
Manufacturing puts unique HW keys into each device and issues certificates for signing keys derived from those HW keys.

New Provisioning Certification Enclave (PCE) uses the signing keys to issue “certificates” for attestation keys generated by Quoting Enclaves.

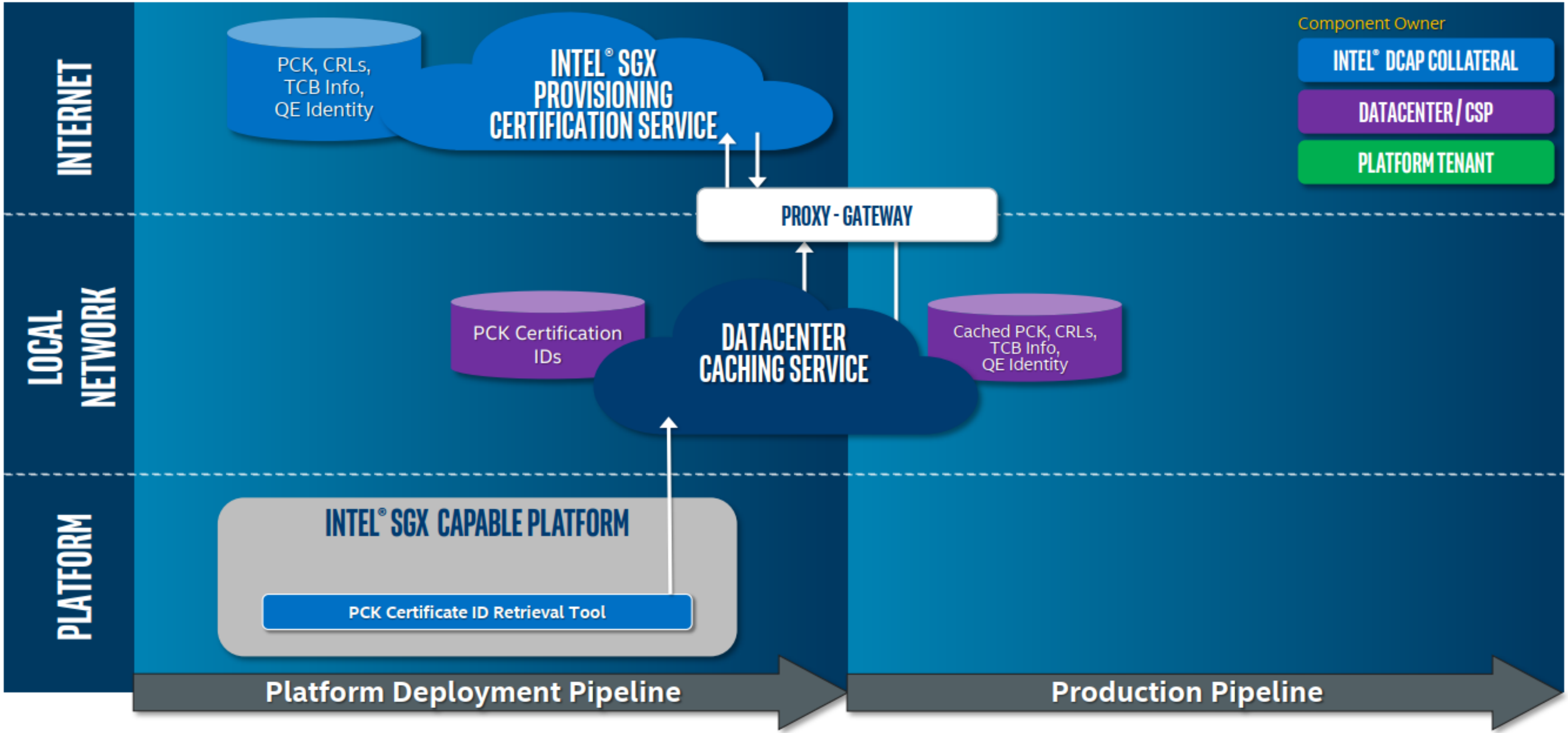
New Quoting Enclave generates attestation key locally and retrieves a “certificate” from PCE.

Quotes are signed by attestation key and include attestation key’s certificate.

Attestation Verifier inspects certificate chain rooted in device/platform certs and TCB Info.

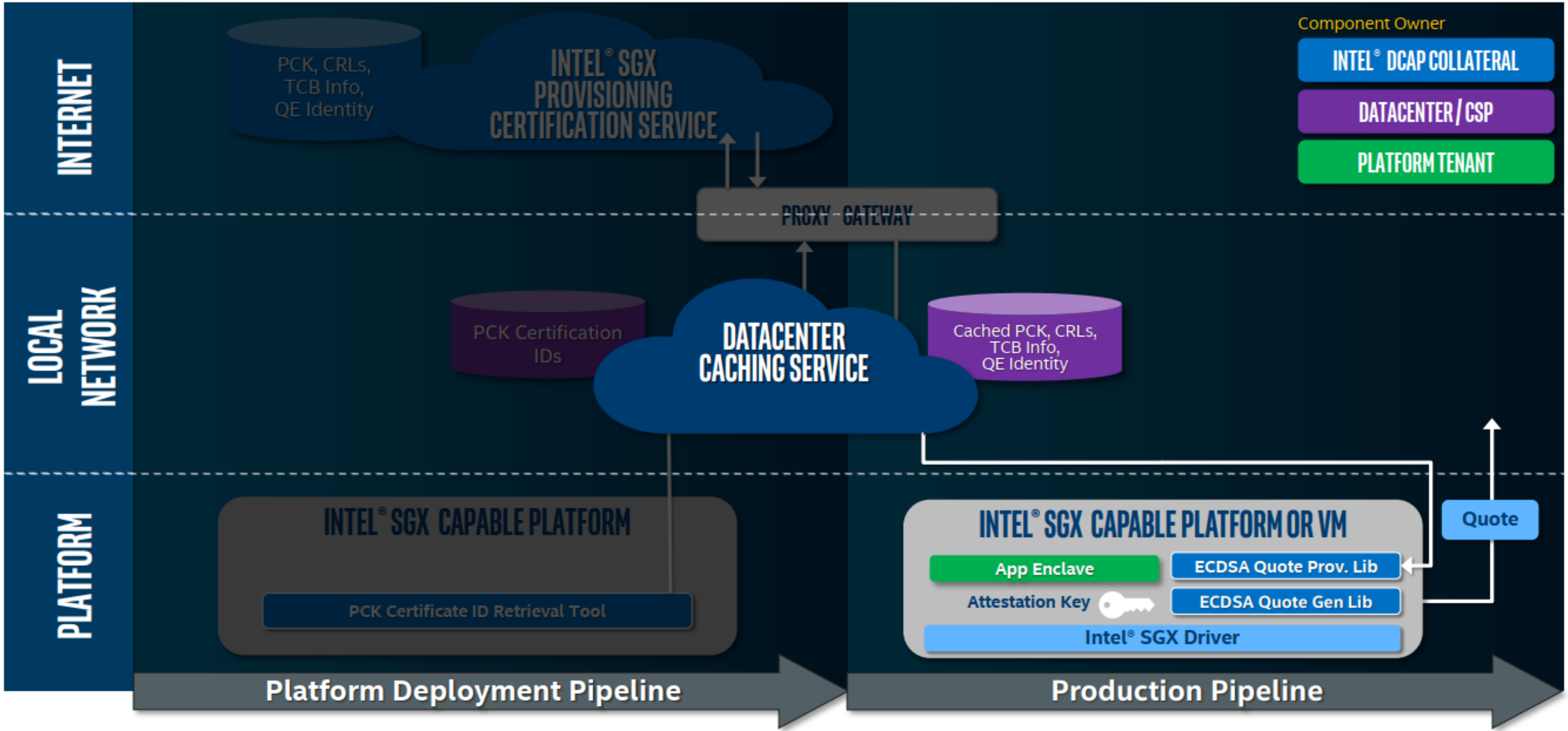

Quoting Enclave
PCK signed cert
Attestation Key
App
Application Enclave
Platform
Prov Certification Enclave
Provisioning Cert Key
Quote (Attest Key Signed)
Attest Key Cert (PCK Signed)
Attestation Verifier
PCK Certificates, CRLs, and TCB Info
3) Quote & TCB Verification
2) Quote Generation
1) PCK Cert & TCB Info Distribution
Root Keys in HW
Intel® Key Generation and Manufacturing
Device/Platform Certificates

Platform Certification Key (PCK) Certificate Retrieval

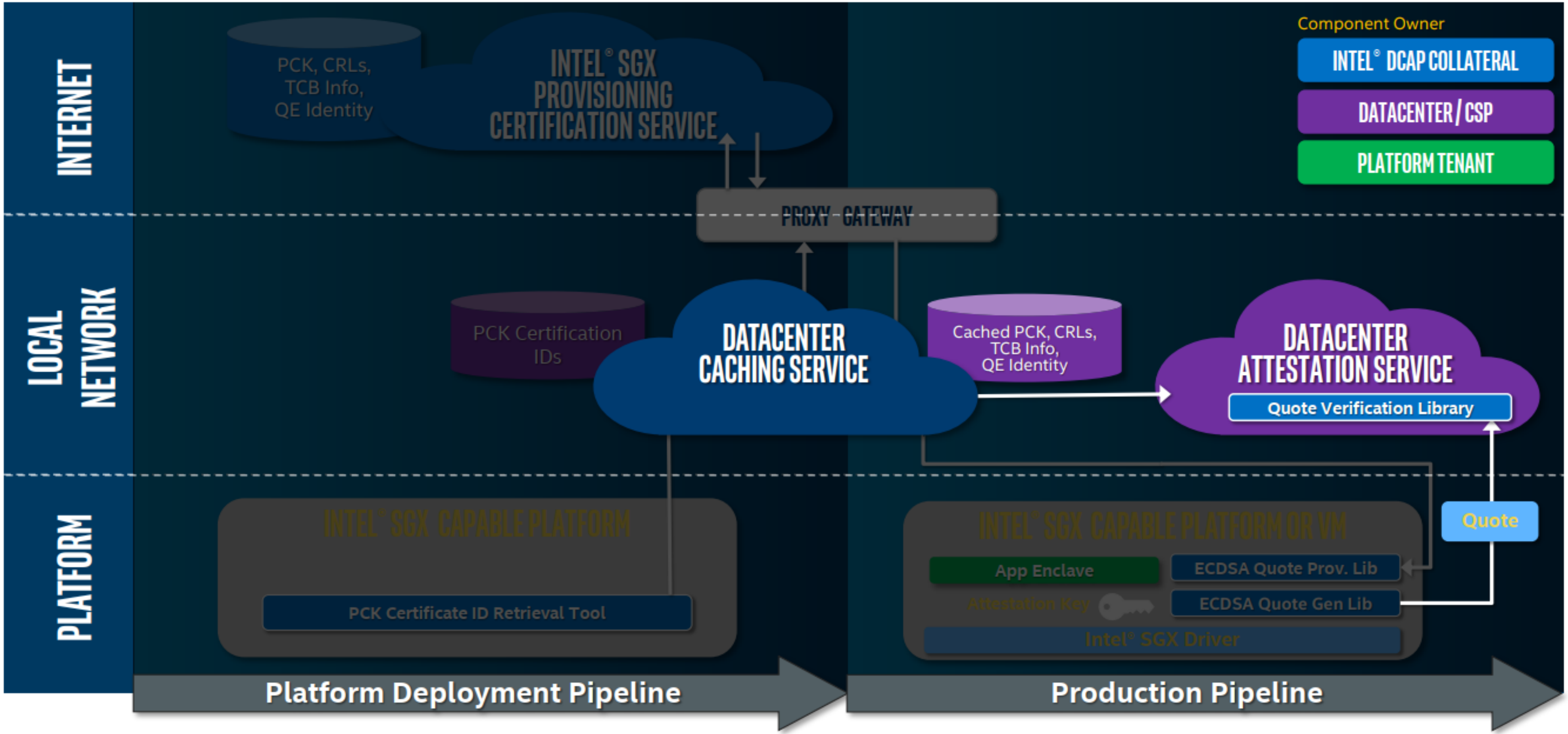

Component Owner
INTEL® DCAP COLLATERAL
DATACENTER / CSP
PLATFORM TENANT
INTERNET
LOCAL NETWORK
PLATFORM
PCK, CRLs, TCB Info, QE Identity
INTEL® SGX PROVISIONING CERTIFICATION SERVICE
PROXY - GATEWAY
PCK Certification IDs
DATACENTER CACHING SERVICE
Cached PCK, CRLs, TCB Info, QE Identity
INTEL® SGX CAPABLE PLATFORM
PCK Certificate ID Retrieval Tool
Platform Deployment Pipeline
Production Pipeline

OpenAnolis
龙 蜥 社 区

Quote Generation


Component Owner
INTEL® DCAP COLLATERAL
DATACENTER / CSP
PLATFORM TENANT
INTERNET
LOCAL NETWORK
PLATFORM
PCK, CRLs, TCB Info, QE Identity
INTEL® SGX PROVISIONING CERTIFICATION SERVICE
PROXY GATEWAY
PCK Certification IDs
DATACENTER CACHING SERVICE
Cached PCK, CRLs, TCB Info, QE Identity
INTEL® SGX CAPABLE PLATFORM
PCK Certificate ID Retrieval Tool
INTEL® SGX CAPABLE PLATFORM OR VM
App Enclave
ECDSA Quote Prov. Lib
Attestation Key
ECDSA Quote Gen Lib
Intel® SGX Driver
Quote
Platform Deployment Pipeline
Production Pipeline

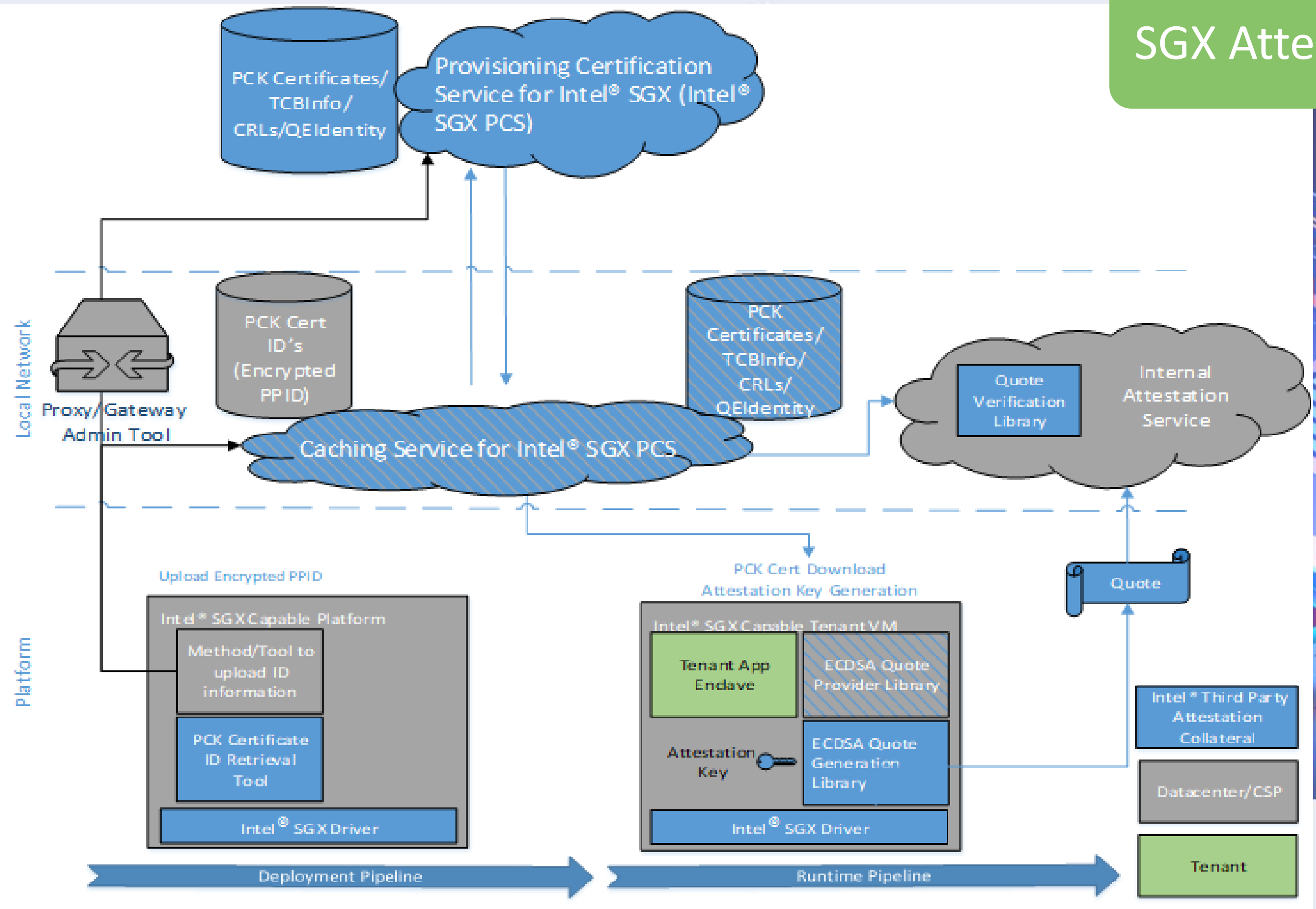
Quote & TCB Verification

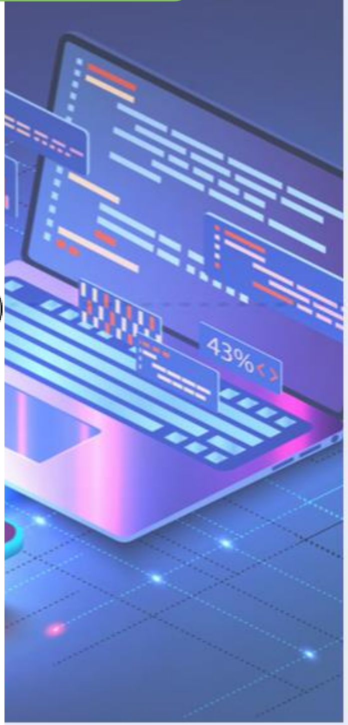

Component Owner
INTEL® DCAP COLLATERAL
DATACENTER / CSP
PLATFORM TENANT
INTERNET
LOCAL NETWORK
PLATFORM
PCK, CRLs, TCB Info, QE Identity
INTEL® SGX PROVISIONING CERTIFICATION SERVICE
PROXY GATEWAY
PCK Certification IDs
DATACENTER CACHING SERVICE
Cached PCK, CRLs, TCB Info, QE Identity
DATACENTER ATTESTATION SERVICE
Quote Verification Library
Quote
INTEL® SGX CAPABLE PLATFORM
PCK Certificate ID Retrieval Tool
INTEL® SGX CAPABLE PLATFORM OR VM
App Enclave
ECDSA Quote Prov. Lib
Attestation Key
ECDSA Quote Gen Lib
Intel® SGX Driver
Platform Deployment Pipeline
Production Pipeline

Remote Attestation

- Attestation is the concept of a HW entity or of a combination of HW and SW gaining the trust of a provider or producer of some sort
  - Converts HW generated Report to a Quote
  - Quote is a Report signed by an asymmetric key called the Attestation Key (AK)
- SGX Remote Attestation
  - ISV Enclave running with SGX protections can generate a Enclave Report
  - Enclave Report:
    - Measurements and configuration of the ISV Enclave
    - Security version of the CPU
    - Data to be reported for the ISV Enclave (ReportData)
    - MAC'd with a HW key and verified by HW.
  - Remote parties have access to the AK Root signing key Certificate to verify Quotes (PCK Certificates).
  - Verifiers then check the ISV Enclave Report's context.

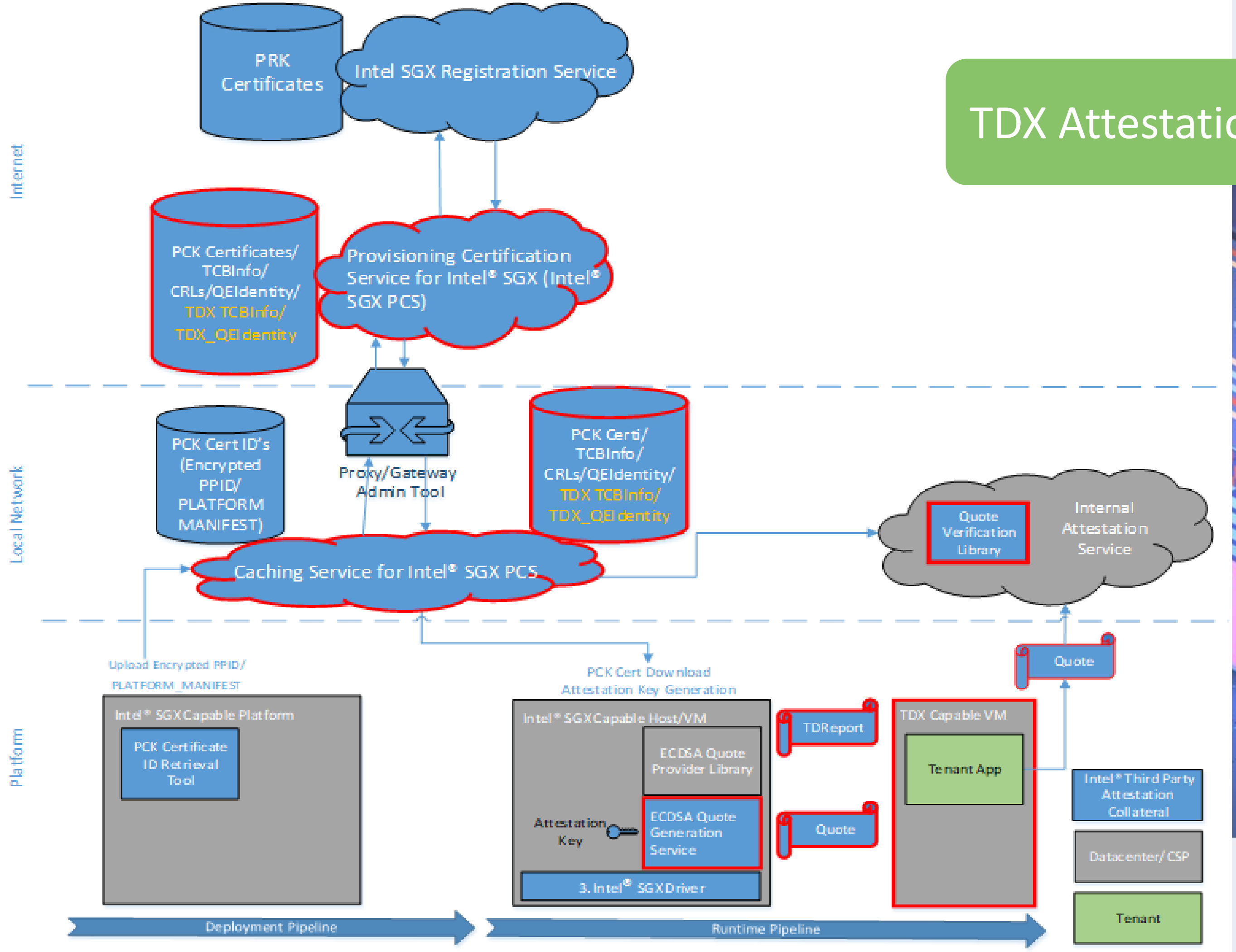
SGX Attestation


PCK Certificates/ TCBInfo/ CRLs/QEIdentity
Provisioning Certification Service for Intel® SGX (Intel® SGX PCS)
Local Network
Proxy/Gateway Admin Tool
PCK Cert ID's (Encrypted PPID)
PCK Certificates/ TCBInfo/ CRLs/ QEIdentity
Caching Service for Intel® SGX PCS
Quote Verification Library
Internal Attestation Service
Upload Encrypted PPID
PCK Cert Download
Attestation Key Generation
Quote
Platform
Intel® SGX Capable Platform
Method/Tool to upload ID information
PCK Certificate ID Retrieval Tool
Intel® SGX Driver
Intel® SGX Capable Tenant VM
Tenant App Enclave
ECDSA Quote Provider Library
Attestation Key
ECDSA Quote Generation Library
Intel® SGX Driver
Intel® Third Party Attestation Collateral
Datacenter/CSP
Tenant
Deployment Pipeline
Runtime Pipeline



- Intel Hosts two servers to support Remote Attestation
  - Registration Server
    - Certifies MP Platform Packages
    - Generates Platform Certification Key (PCK) Certs
  - Provisioning Certification Server(PCS)
    - Delivers PCK Certs
    - Provides SGX Quote Verification reference values (Collateral/Endorsements)
      - SGX TCBInfo – Used to verify a quote was generated using the latest up-to-date SGX TCB
      - SGX QEIdentity – Identification structure for the SGX Quoting Enclave
      - CRLs –Certification Revocation Lists
      - QvE Identity – Identification structure for Quote Verification Enclave.
      - TDX TCBInfo – Contains SGX TCBInfo + TDX modules TCBInfo (Added with V4 APIs)
      - TDX QEIdentity – Identification structure for the TDX Quoting Enclave (Added with V4 APIs)

TDX Attestation


PRK Certificates
Intel SGX Registration Service
Internet
PCK Certificates/ TCBInfo/ CRLs/QEIdentity/ TDX TCBInfo/ TDX_QEIdentity
Provisioning Certification Service for Intel® SGX (Intel® SGX PCS)
PCK Cert ID's (Encrypted PPID/ PLATFORM MANIFEST)
Proxy/Gateway Admin Tool
PCK Certi/ TCBInfo/ CRLs/QEIdentity/ TDX TCBInfo/ TDX_QEIdentity
Local Network
Caching Service for Intel® SGX PCS
Quote Verification Library
Internal Attestation Service
Upload Encrypted PPID/ PLATFORM_MANIFEST
PCK Cert Download
Attestation Key Generation
Quote
Platform
Intel® SGX Capable Platform
PCK Certificate ID Retrieval Tool
Intel® SGX Capable Host/VM
ECDSA Quote Provider Library
Attestation Key
ECDSA Quote Generation Service
3. Intel® SGX Driver
TDReport
Quote
TDX Capable VM
Tenant App
Intel® Third Party Attestation Collateral
Datacenter/CSP
Tenant
Deployment Pipeline
Runtime Pipeline

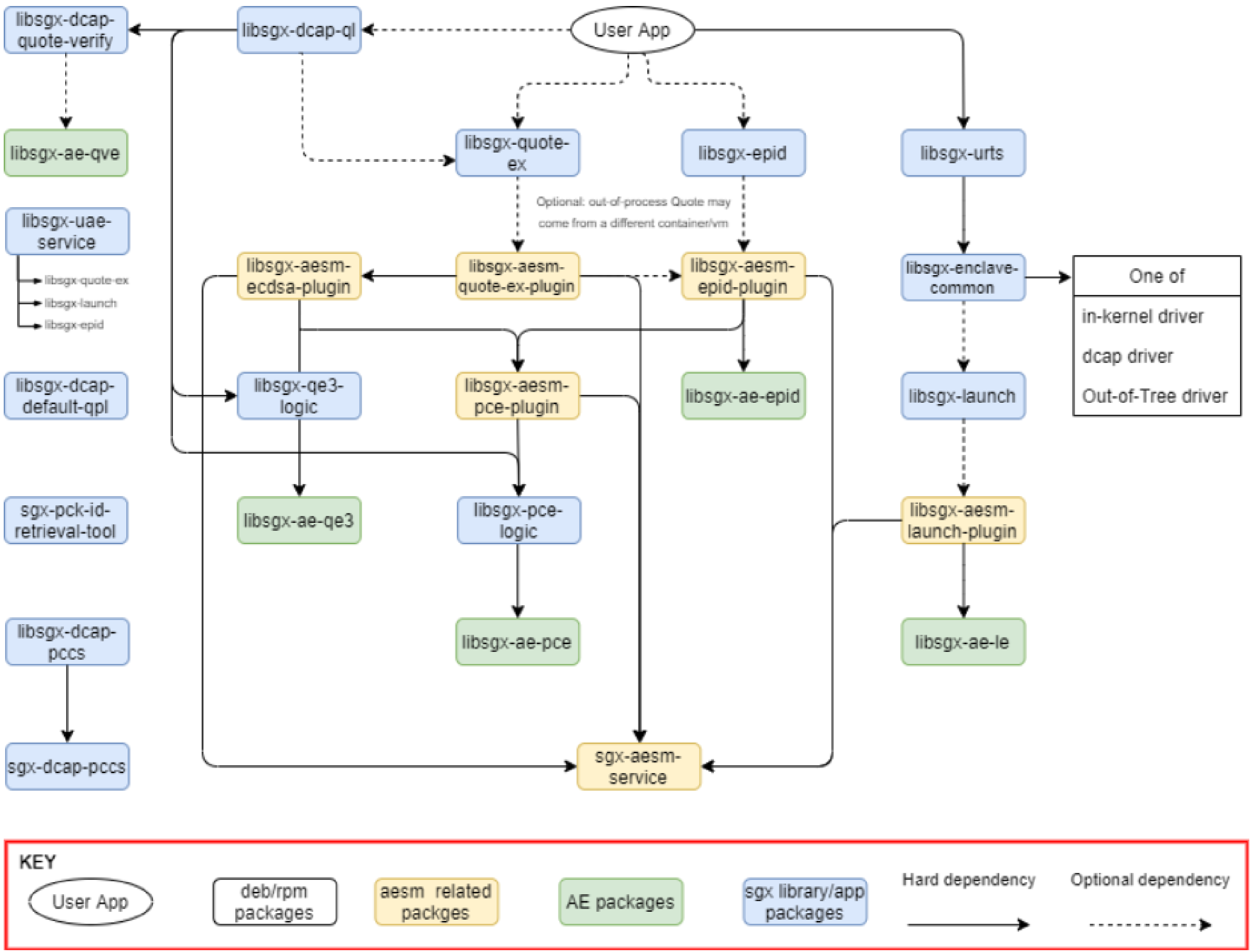
03

PART THREE

Anolis OS 适配

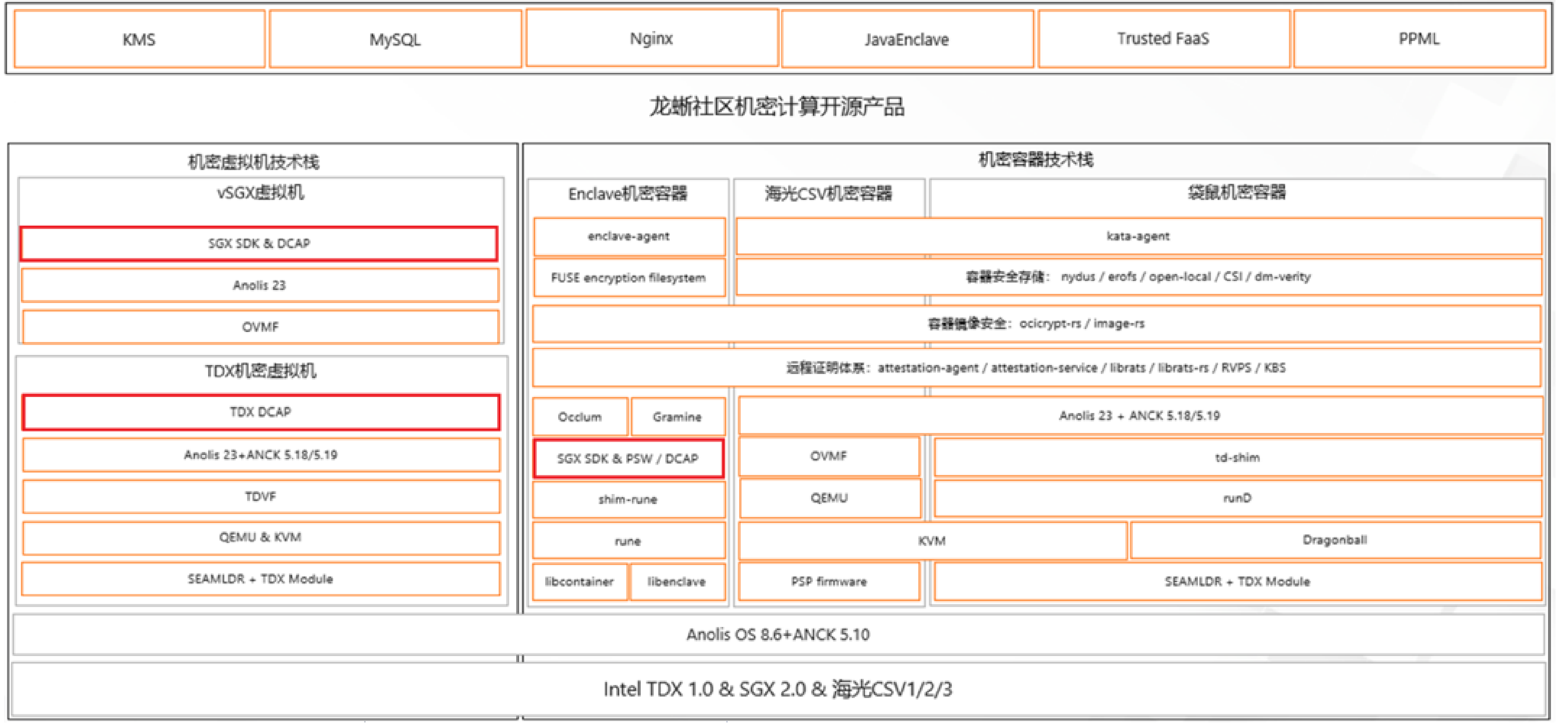
SGX 软件栈

- SGX SDK
  - https://github.com/intel/linux-sgx
- SGX PSW/DCAP
  - https://github.com/intel/SGXDataCenterAttestationPrimitives



Intel(R) SGX PSW and Intel(R) SGX DCAP for Linux Package Structure

SGX 在龙蜥技术栈的落地



KMS | MySQL | Nginx | JavaEnclave | Trusted FaaS | PPML

龙蜥社区机密计算开源产品

机密虚拟机技术栈

vSGX虚拟机
- SGX SDK & DCAP
- Anolis 23
- OVMF

TDX机密虚拟机
- TDX DCAP
- Anolis 23+ANCK 5.18/5.19
- TDVF
- QEMU & KVM
- SEAMLDR + TDX Module

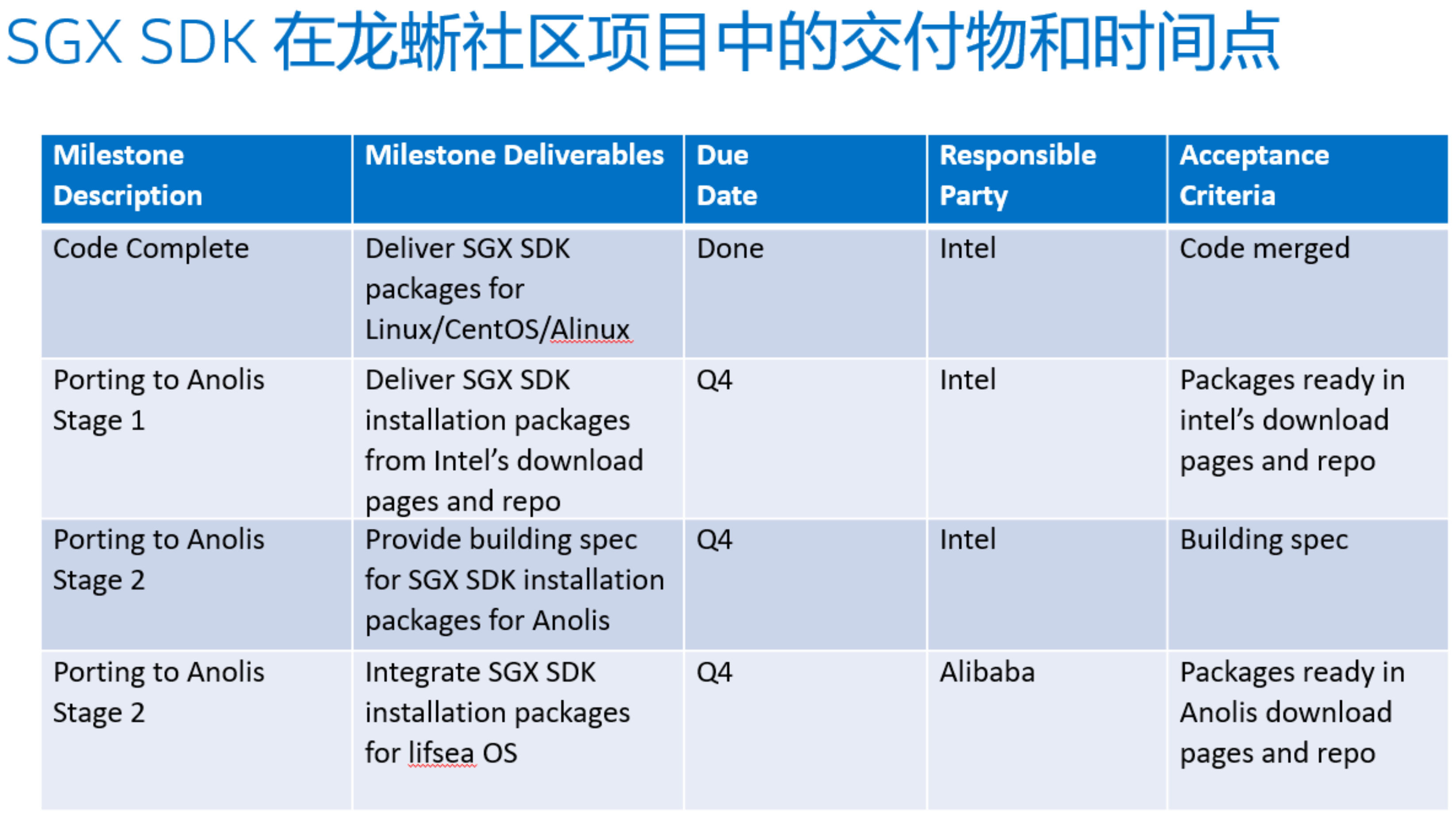
机密容器技术栈

Enclave机密容器 | 海光CSV机密容器 | 袋鼠机密容器

- enclave-agent
- FUSE encryption filesystem
- kata-agent
- 容器安全存储： nydus / erofs / open-local / CSI / dm-verity
- 容器镜像安全： ocicrypt-rs / image-rs
- 远程证明体系： attestation-agent / attestation-service / librats / librats-rs / RVPS / KBS
- Occlum | Gramine
- SGX SDK & PSW / DCAP
- shim-rune
- rune
- libcontainer | libenclave
- Anolis 23 + ANCK 5.18/5.19
- OVMF | td-shim
- QEMU | runD
- KVM | Dragonball
- PSP firmware | SEAMLDR + TDX Module

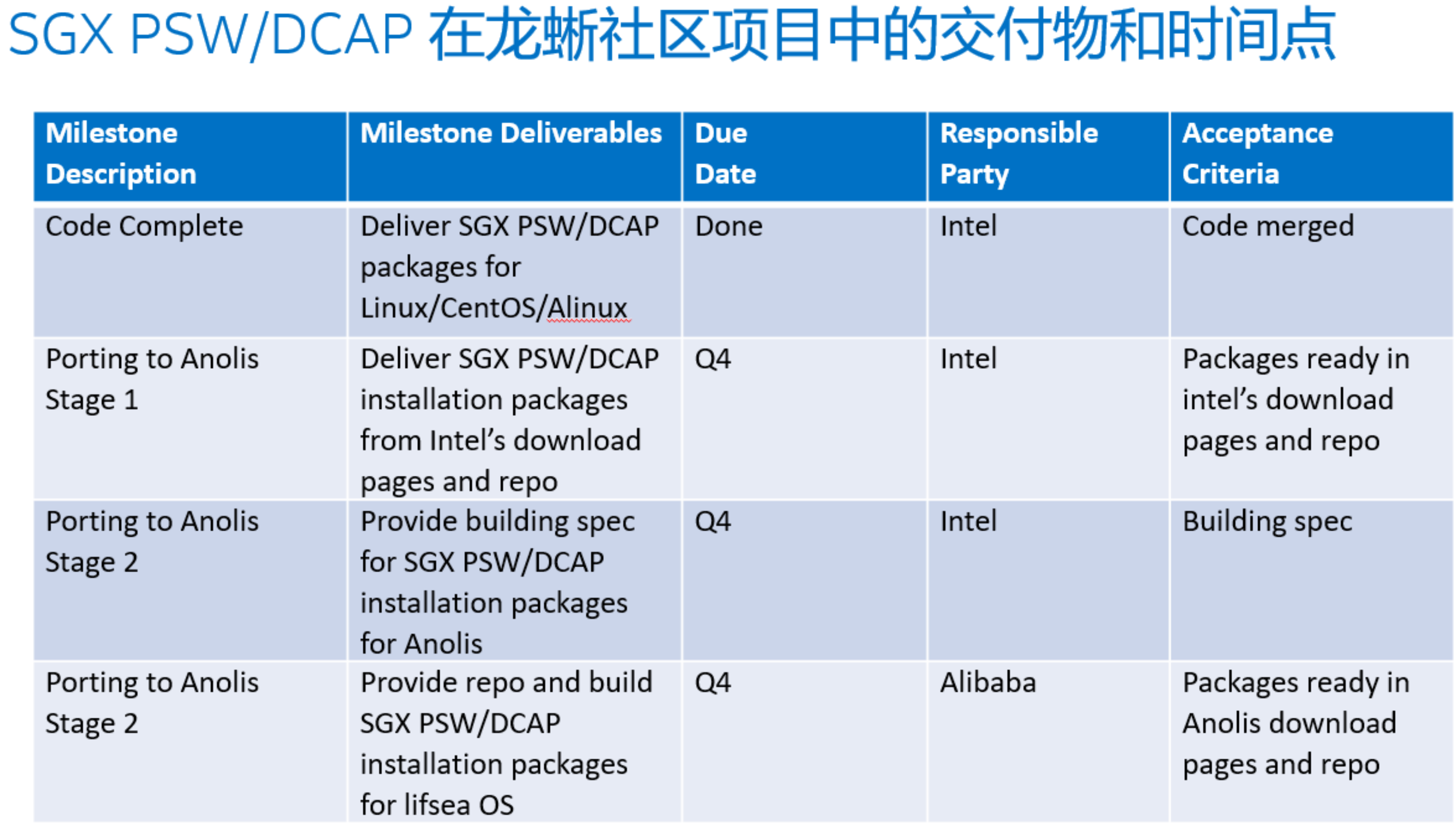
Anolis OS 8.6+ANCK 5.10

Intel TDX 1.0 & SGX 2.0 & 海光CSV1/2/3



SGX SDK 在龙蜥社区项目中的交付物和时间点

Milestone Description	Milestone Deliverables	Due Date	Responsible Party	Acceptance Criteria
Code Complete	Deliver SGX SDK packages for Linux/CentOS/Alinux	Done	Intel	Code merged
Porting to Anolis Stage 1	Deliver SGX SDK installation packages from Intel's download pages and repo	Q4	Intel	Packages ready in intel's download pages and repo
Porting to Anolis Stage 2	Provide building spec for SGX SDK installation packages for Anolis	Q4	Intel	Building spec
Porting to Anolis Stage 2	Integrate SGX SDK installation packages for lifsea OS	Q4	Alibaba	Packages ready in Anolis download pages and repo



SGX PSW/DCAP 在龙蜥社区项目中的交付物和时间点

Milestone Description	Milestone Deliverables	Due Date	Responsible Party	Acceptance Criteria
Code Complete	Deliver SGX PSW/DCAP packages for Linux/CentOS/Alinux	Done	Intel	Code merged
Porting to Anolis Stage 1	Deliver SGX PSW/DCAP installation packages from Intel’s download pages and repo	Q4	Intel	Packages ready in intel’s download pages and repo
Porting to Anolis Stage 2	Provide building spec for SGX PSW/DCAP installation packages for Anolis	Q4	Intel	Building spec
Porting to Anolis Stage 2	Provide repo and build SGX PSW/DCAP installation packages for lifsea OS	Q4	Alibaba	Packages ready in Anolis download pages and repo

THANKS

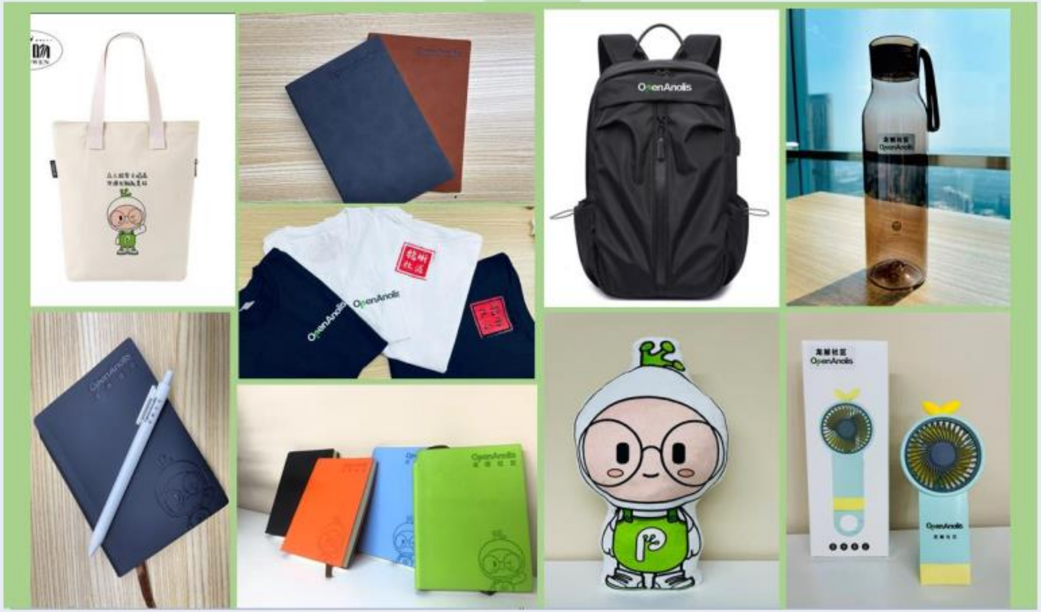
欢迎大家扫码关注

公众号：
OpenAnolis**龙蜥**

钉钉群聊：
龙蜥云原生机密计算 SIG

龍蜥
社區

Q & A 环节



积极与讲师互动，也有机会获得**社区小礼品**哦~

龍蜥
社區

OpenAnolis
龙蜥社区

关于回放&课件

往期回放合集

往期课件合集

龍蜥社區