SYSTEX 2019
SCALING TOWARDS CONFIDENTIAL COMPUTING

Simon Johnson, Snr Principal Engineer
SGX Program Architect

Legal Disclaimer

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.

Legal Disclaimer

This presentation contains the general insights and opinions of Intel Corporation ("Intel"). The information in this presentation is provided for information only and is not to be relied upon for any other purpose than educational. Use at your own risk! Intel accepts no duty to update this presentation based on more current information. Intel is not liable for any damages, direct or indirect, consequential or otherwise, that may arise, directly or indirectly, from the use or misuse of the information in this presentation.

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

Agenda

Confidential Compute Eco-system

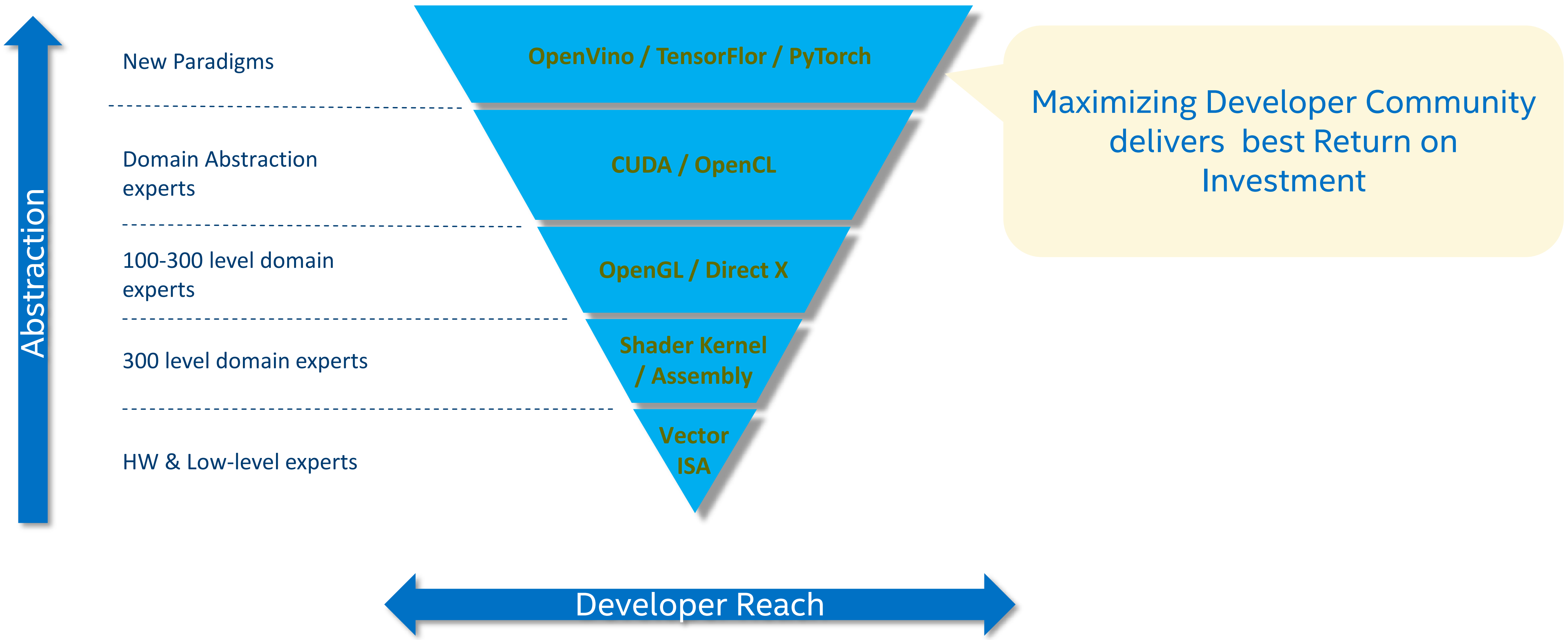
Confidential Compute HW needs

Attestation

Future Challenges

Well established
In development
In planning

How SW Ecosystems Develop

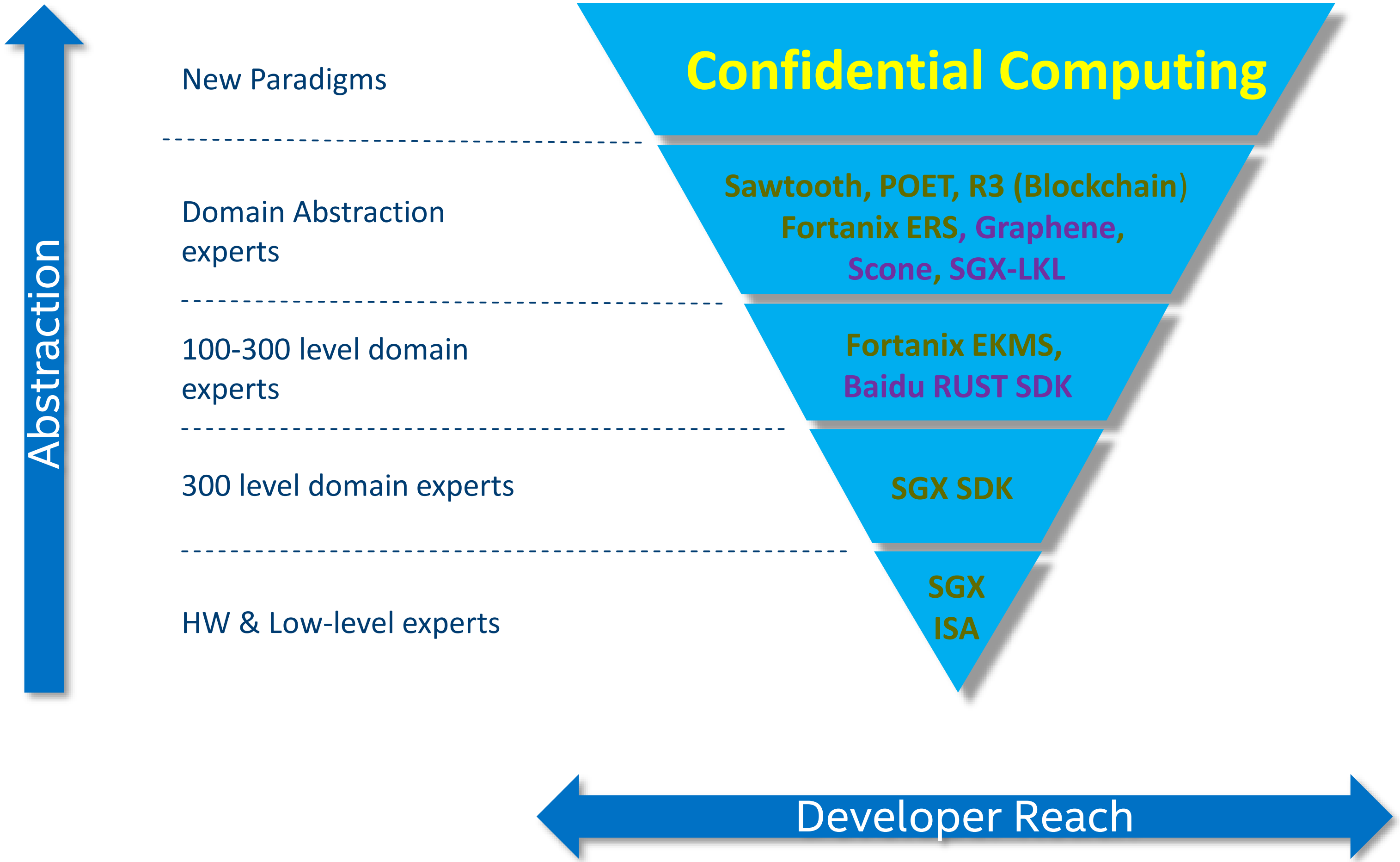


SGX Ecosystem: Publicly Announced SDKs

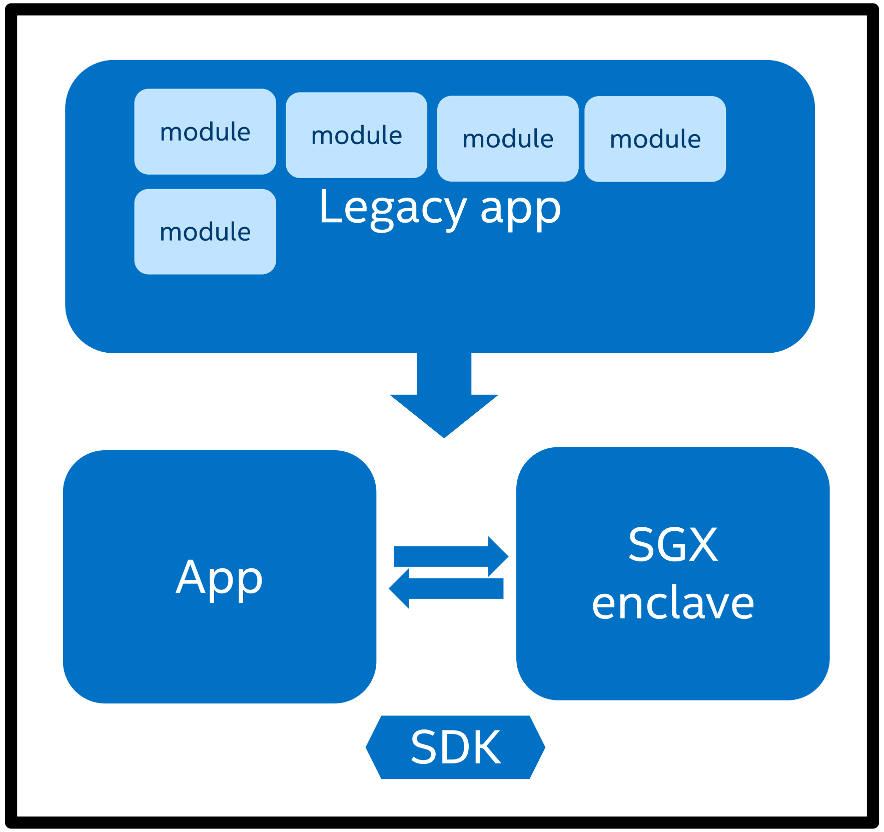
- Intel SGX SDK 1.0 Windows 2014
- Intel SGX SDK 1.0 for Linux 2016
- Graphene-SGX July 2017
- Cryptsoft KMIP SDK Linux Nov 2017
- RUST · SGX Baidu Rust May 2018
- Google Asylo May 2018
- Mesa TEE mid 2018
- Microsoft Open Enclave Sept 2018
- Fortanix Enclave Development Platform March 2019
- Graphene-SGX Stable 2H 2019

Well established
In development

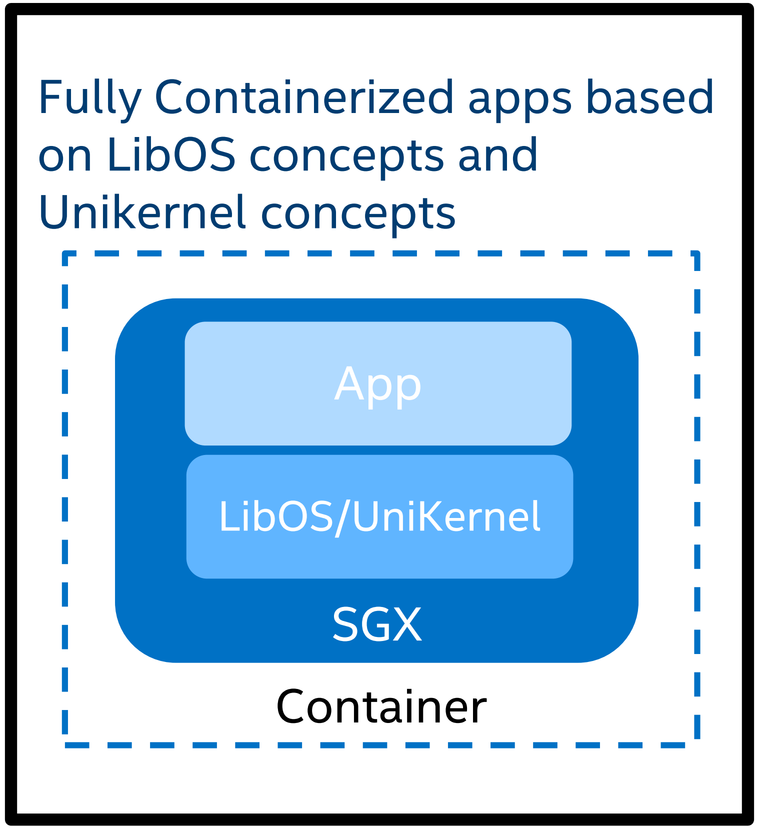
How the SGX Ecosystem is developing



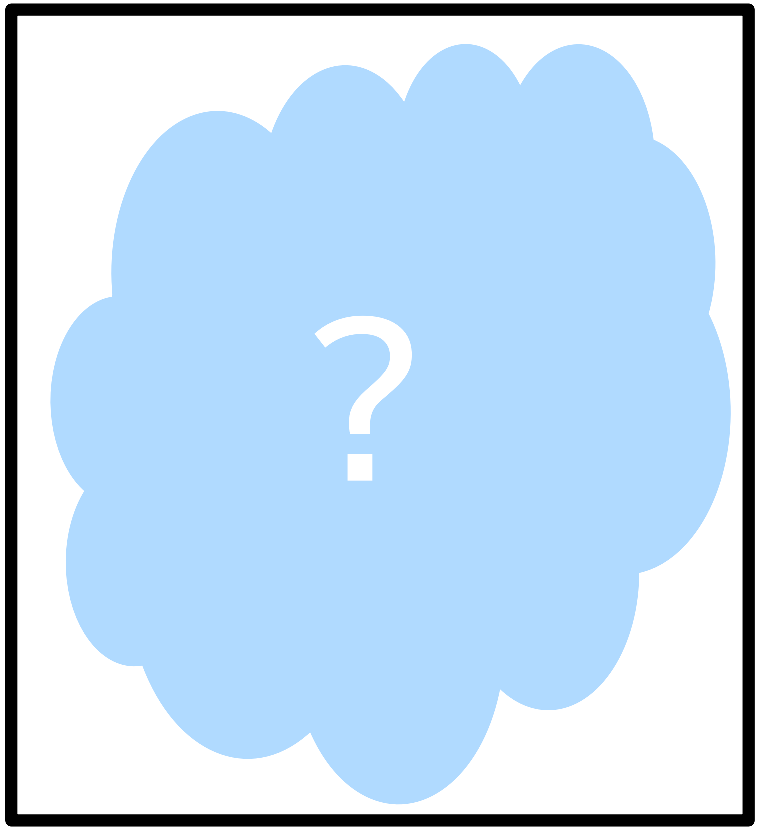
NOW....	NEXT....	FUTURE!



Today you can build you own apps using the SDK... best TCB requires some expertise



Isolated containerization of apps is fast gaining traction



Let's talk about this a little later...

A community focused on projects securing data in use and accelerating the adoption of confidential computing through open collaboration.

confidentialcomputing.io

CONFIDENTIAL COMPUTING CONSORTIUM

CCC: Mission and Goals

Confidential computing enables new public cloud scenarios (e.g., migrating extremely sensitive data to the cloud, and enabling multi-party sharing scenarios that have been difficult to build due to privacy, security, and regulatory requirements).

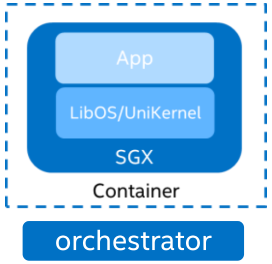
The Confidential Computing Consortium is the platform through which partners will invest across the value chain to allow customers to realize this vision. The Consortium will:

1. Define confidential computing and accelerate acceptance and adoption in the market.
2. Develop enterprise-grade building blocks (e.g., specifications and open source licensed projects) with the latest technologies to enable easy development and management of enterprise-grade confidential compute applications
3. Define foundational services and frameworks that are confidential-aware and minimize the need for trust.

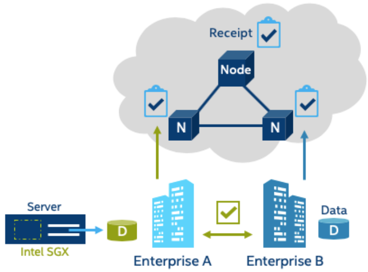
Potential Confidential Compute Use cases

Cloud Infrastructure

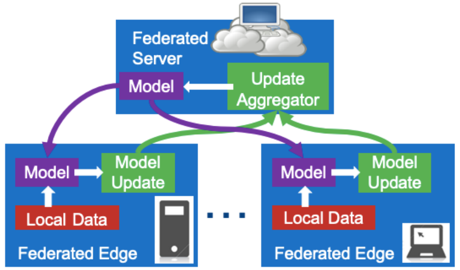
Secure Native Application Hosting



Trusted Multi-party Compute

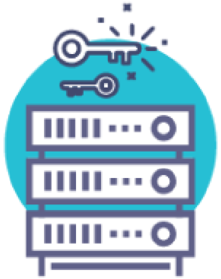


Federated Learning

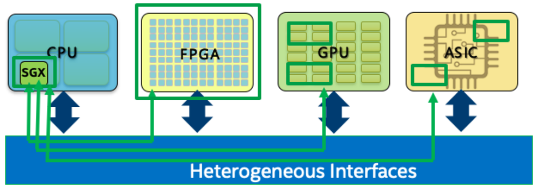


Secure Database

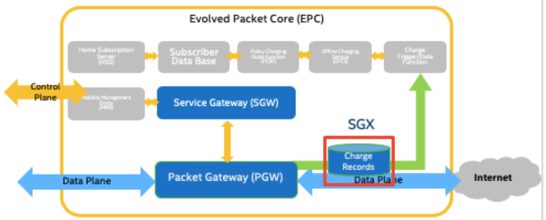
Crypto Key Management



Accelerated Secure Compute



Secure Networking



HW Needs to Deliver Scale

SGX saw its introduction on 6th Generation Intel® Core™ (skylake), feedback since then includes:

- enable 3rd party attestation services
- provide flexible approach to control which applications can run
- provide more memory with protection features
- provide additional key separation mechanisms
- multi-socket CPU support

HW Needs to Deliver Scale

SGX saw its introduction on 6th Generation Intel® Core™ (skylake), feedback since then includes:

- enable 3rd party attestation services
  - DCAP
- provide flexible approach to control which applications can run
  - Flex Launch Control
- provide more memory with protection features
  - Increasing memory sizes
- provide additional key separation mechanisms
  - New Key Separation and Sharing capability
- multi-socket CPU support

Overview of Intel® SGX DCAP

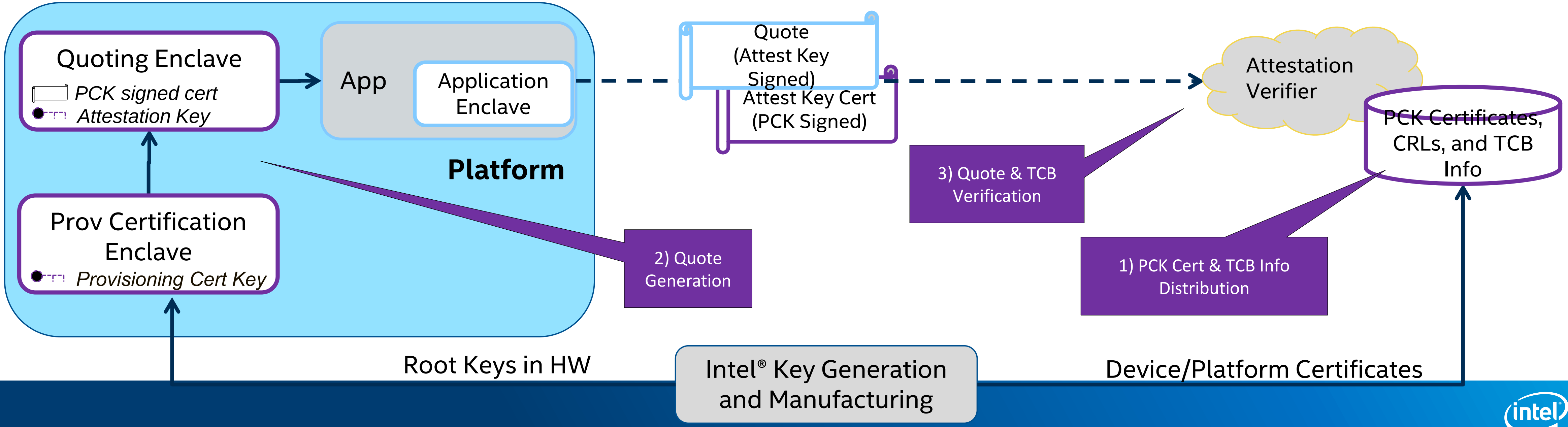
Manufacturing puts unique HW keys into each device and issues certificates for signing keys derived from those HW keys.

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

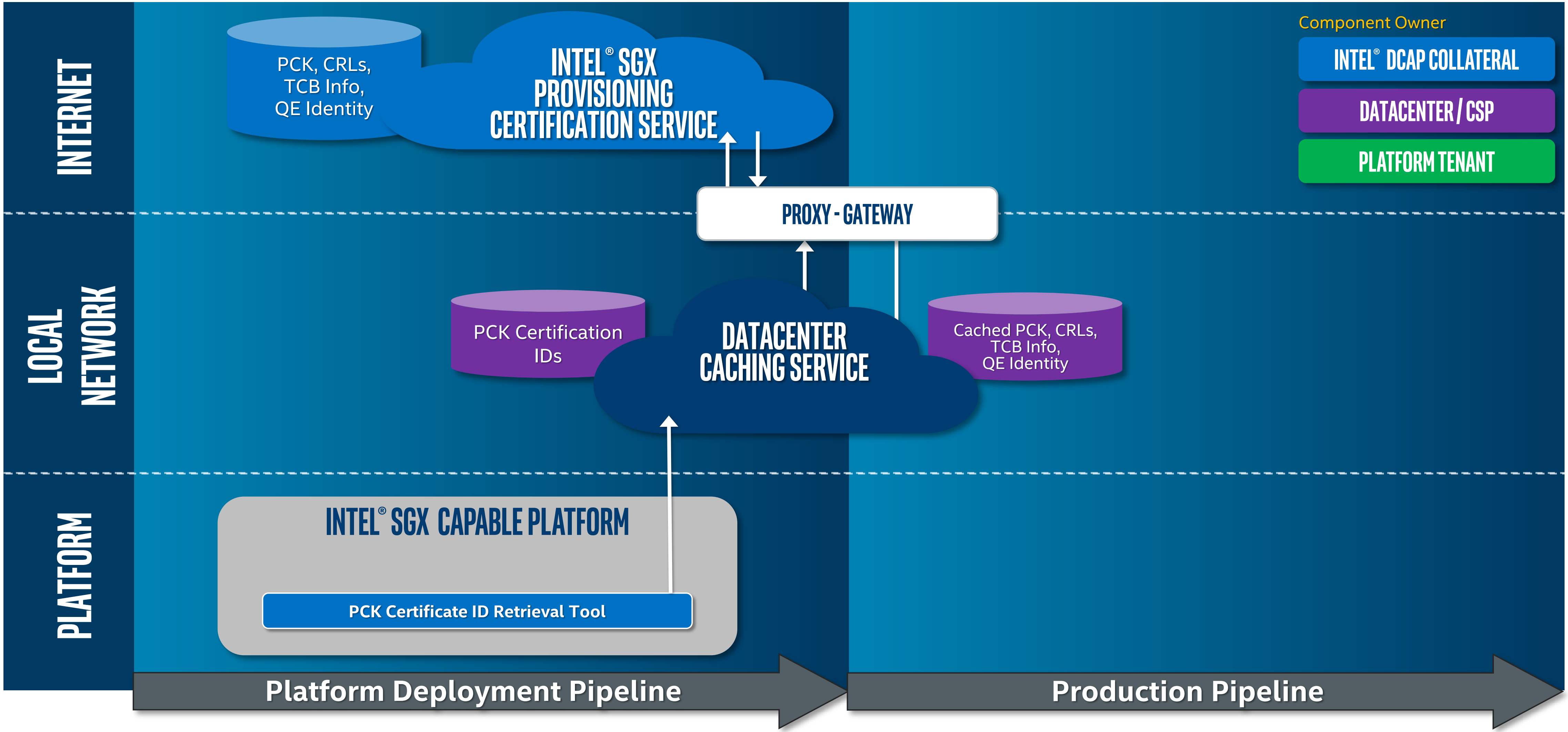
New Quoting Enclave generates attestation key locally and retrieves a "certificate" from PCE.

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

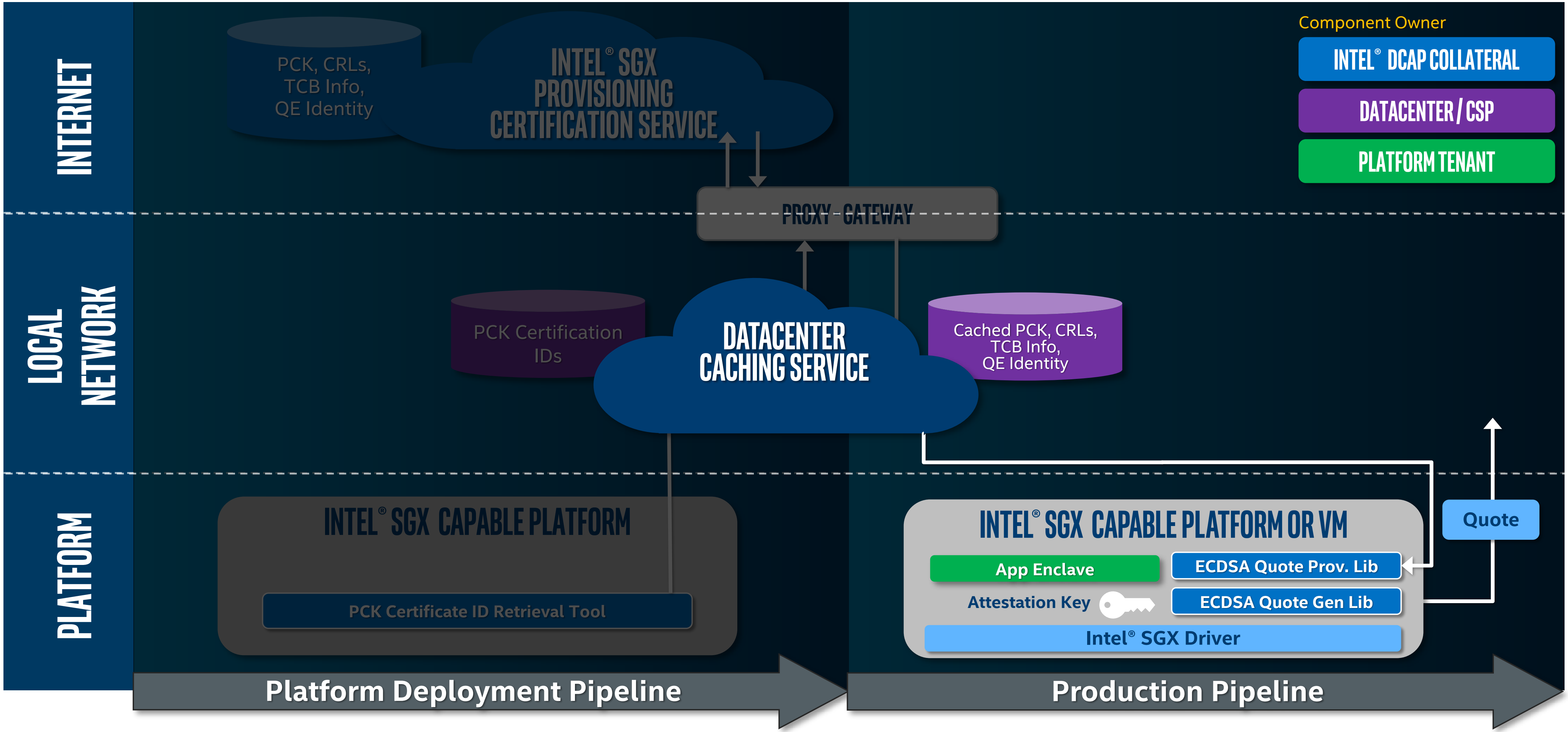
Attestation Verifier inspects certificate chain rooted in device/platform certs and TCB Info.



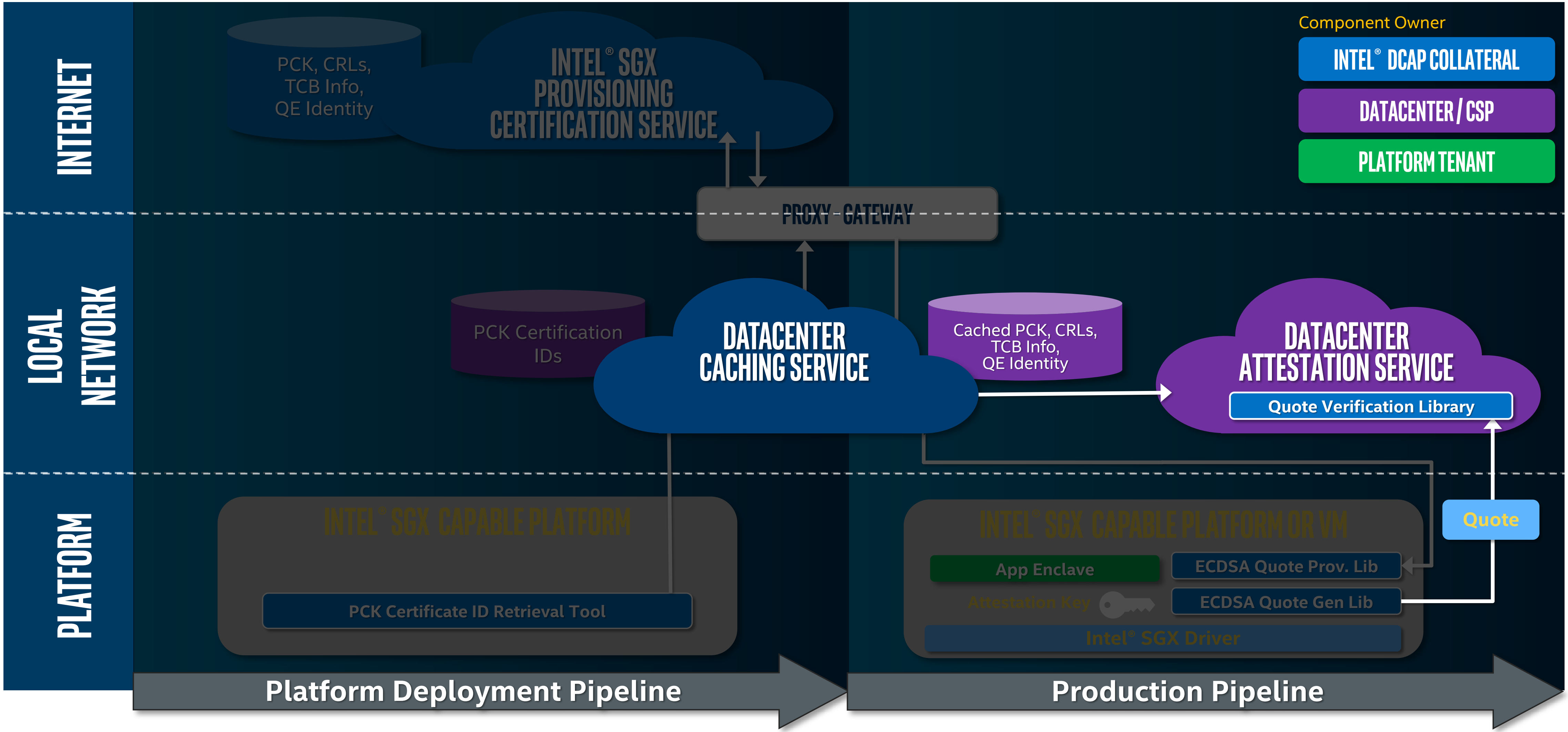
Platform Certification Key (PCK) Certificate Retrieval



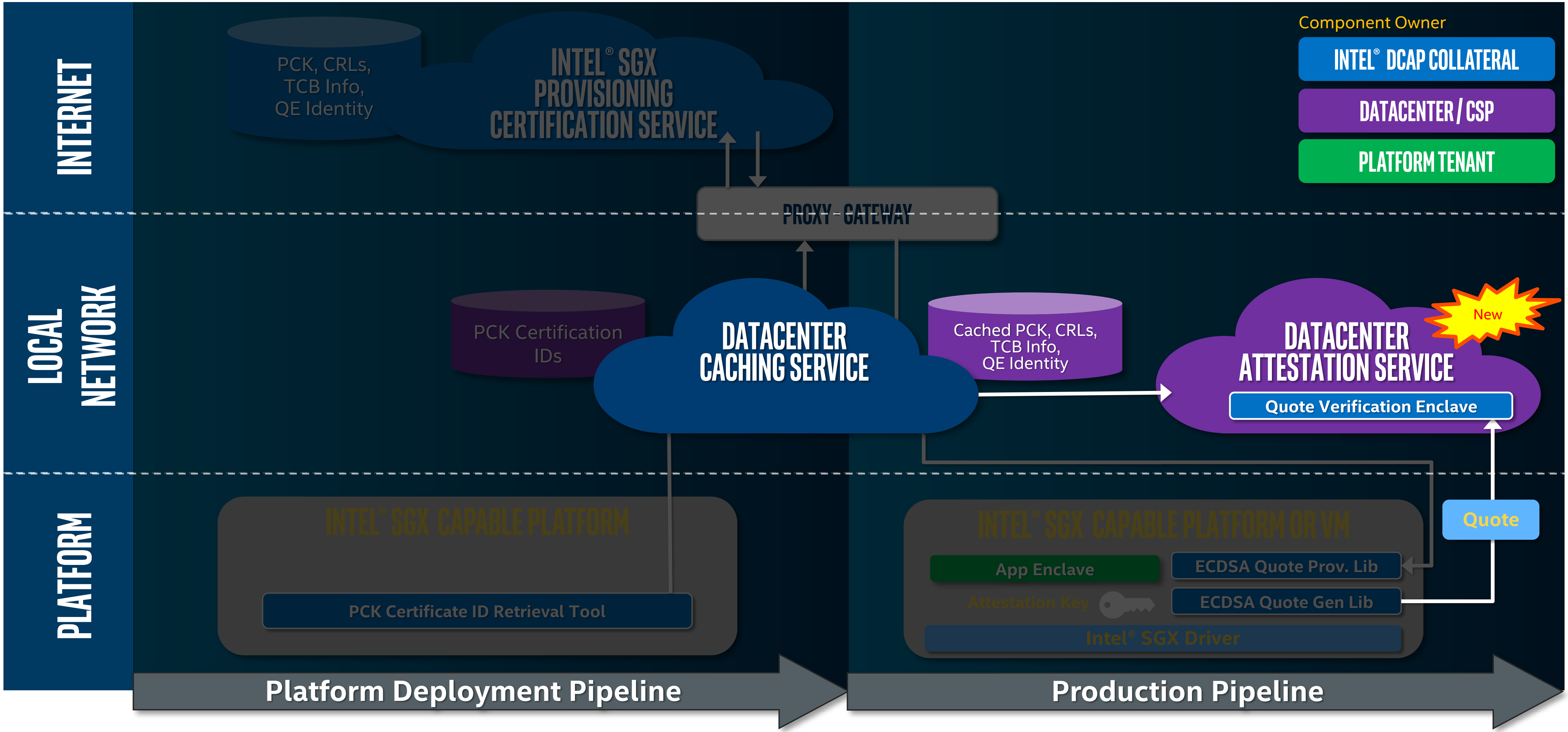
Quote Generation



Quote & TCB Verification



Quote & TCB Verification



DCAP 1.3 Enhancements

New

Intel SGX Provisioning Certificate Service (PCS) v2

- Identifies which CVEs are addressed by each new TCB

Intel SGX ECDSA DCAP Quote Verification Library - New

- Supports new v2 verification
- API supports enclave based verification and untrusted verification
- API support applying a 3rd party quote verification policy
- Intel signed Quote Verification Enclave (QVE)
  - Incorporates new Quote Verification Library
  - Keeps 3rd party verifiers out of the SGX Attestation TCB
- Released with existing DCAP packages.

Multi-Package SGX

Application Isolation through changes in memory architecture & SGX ISA

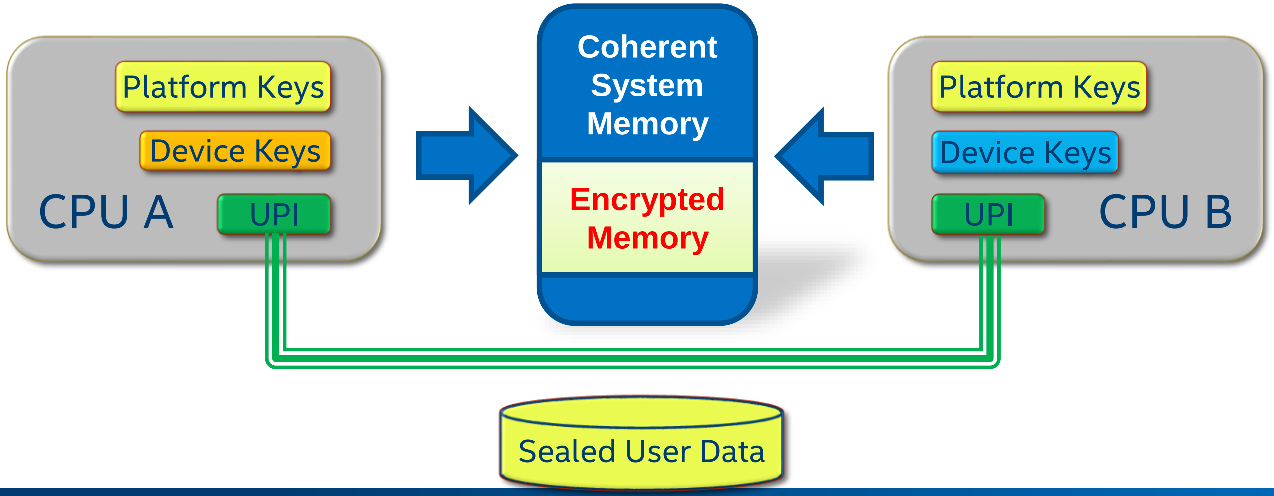
- Launch Control
- Enhanced Key Separation
- Enclave Dynamic Memory Management

Multiple devices Single Keying Hierarchy

- Seal Keys
- Attestation Keys & 3rd Party Service

Lots of Protected Memory

Encryption between packages



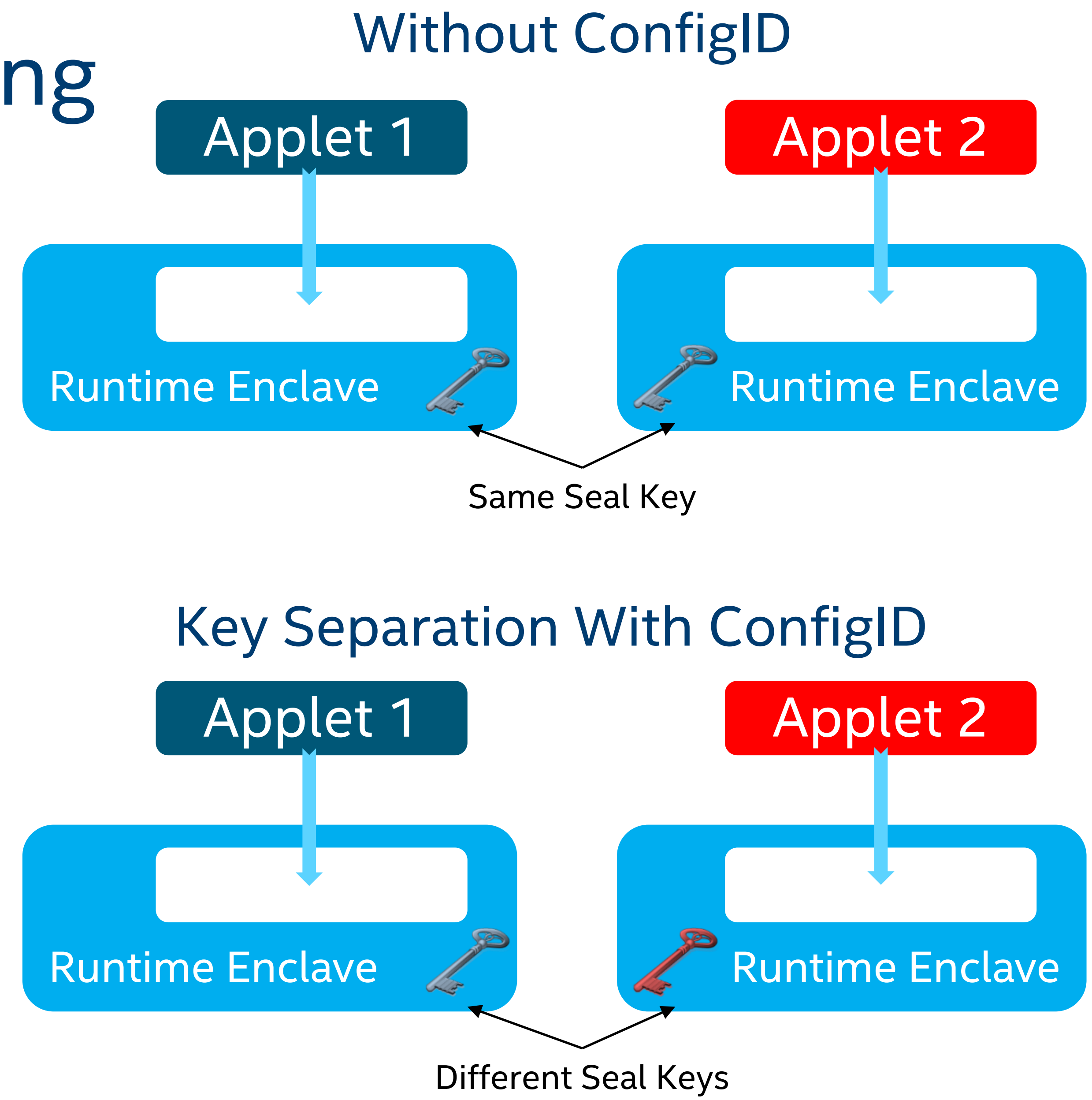
Key Separation and Sharing

Enclaves that load additional logic have keys based only on the loader code.

- Example: Java, JS, C#, Python enclaves

ConfigID allows Enclave Creator to specify an immutable value which can be bound to the additional content

Allows different keys to be created for enclave instances

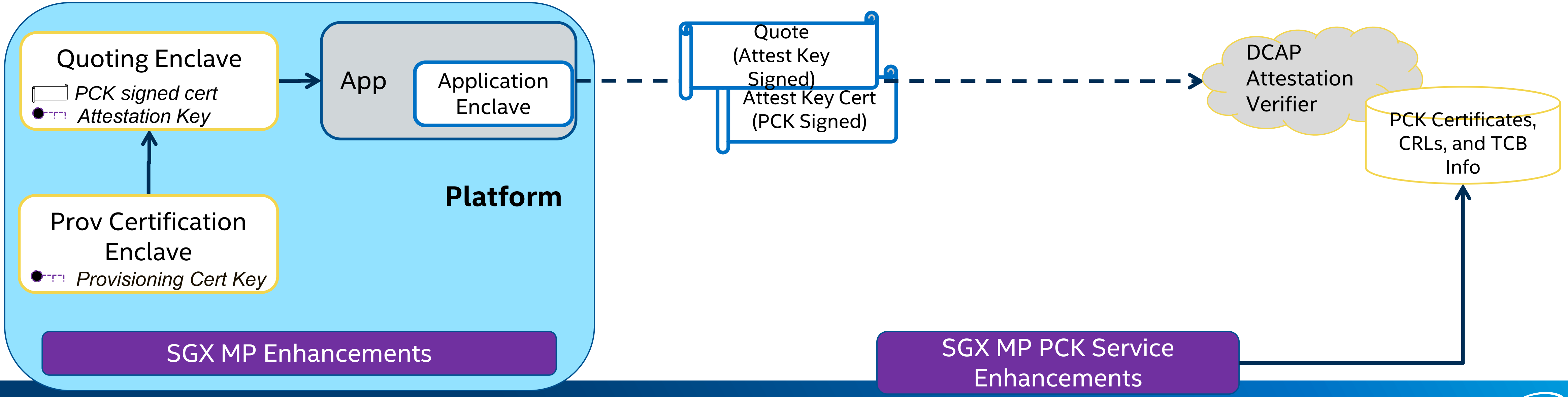


Extending Attestation to Multi-Socket Servers

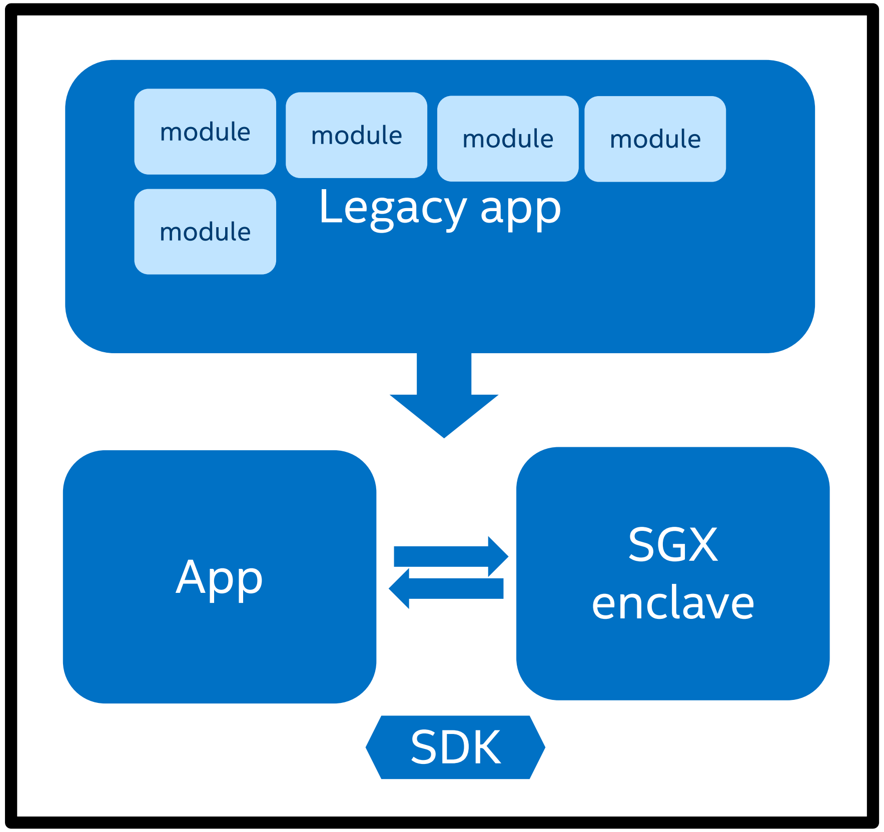
To extend the architectural model from single to multiple sockets:

- Provide software with consistent user keys across on all socket (ex. Seal keys).
- Establish attestation keys that represent the entire platform.

Intel® SGX Multi-socket extensions result in standard DCAP PCK certificates, enabling DCAP software and infrastructure reuse.



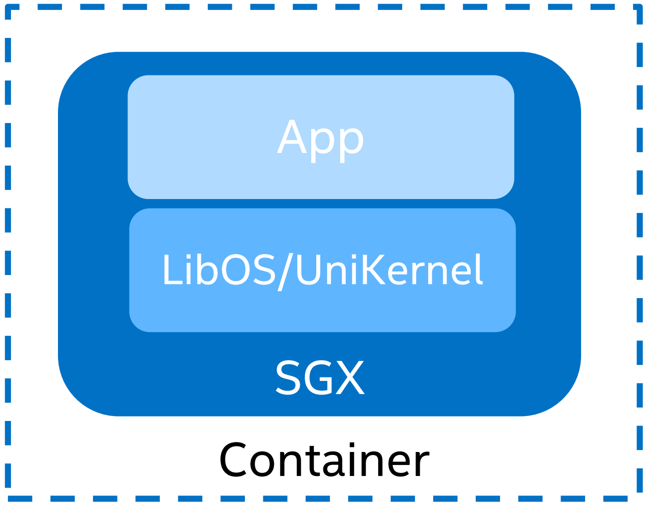
NOW....



Today you can build you own apps using the SDK... best TCB requires some expertise

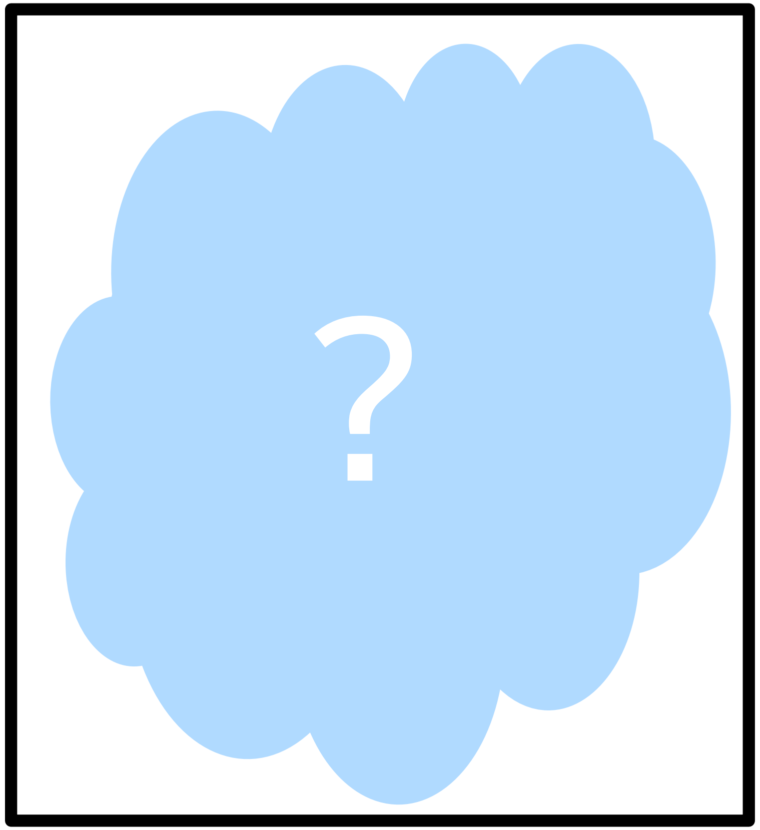
NEXT....

Fully Containerized apps based on LibOS concepts and Unikernel concepts



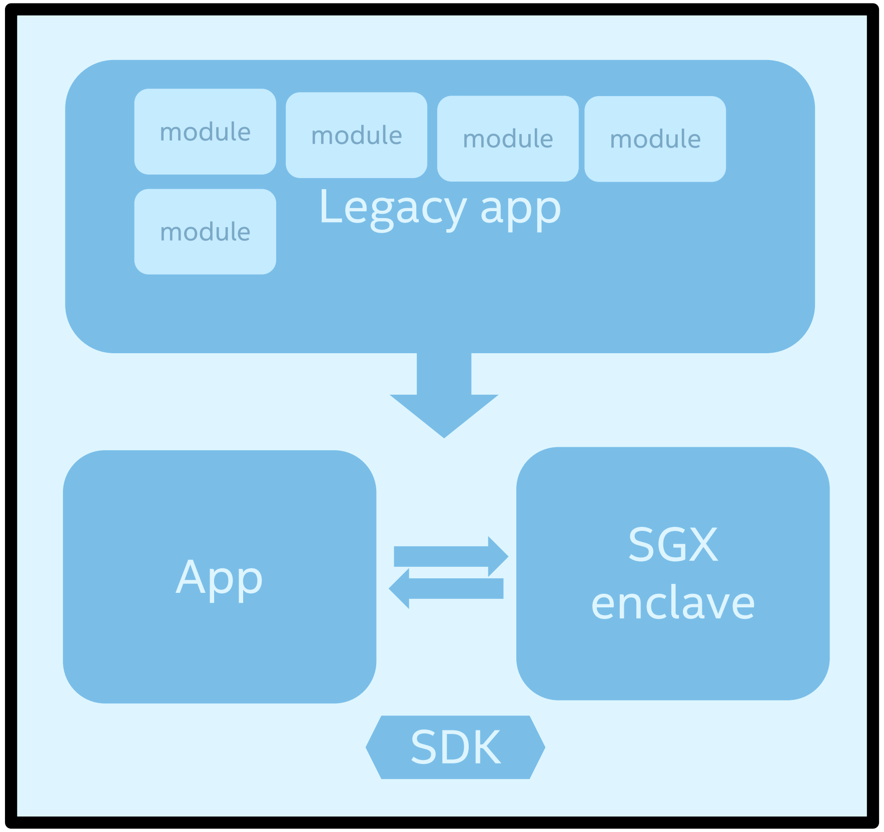
Isolated containerization of apps is fast gaining traction

FUTURE!



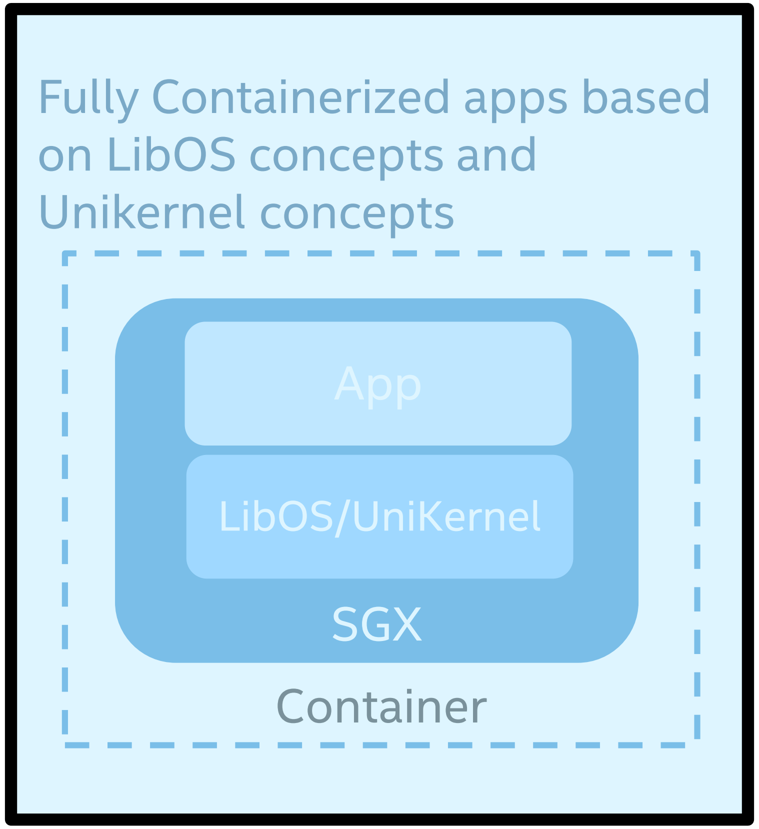
Let’s talk about this a little later...

NOW....



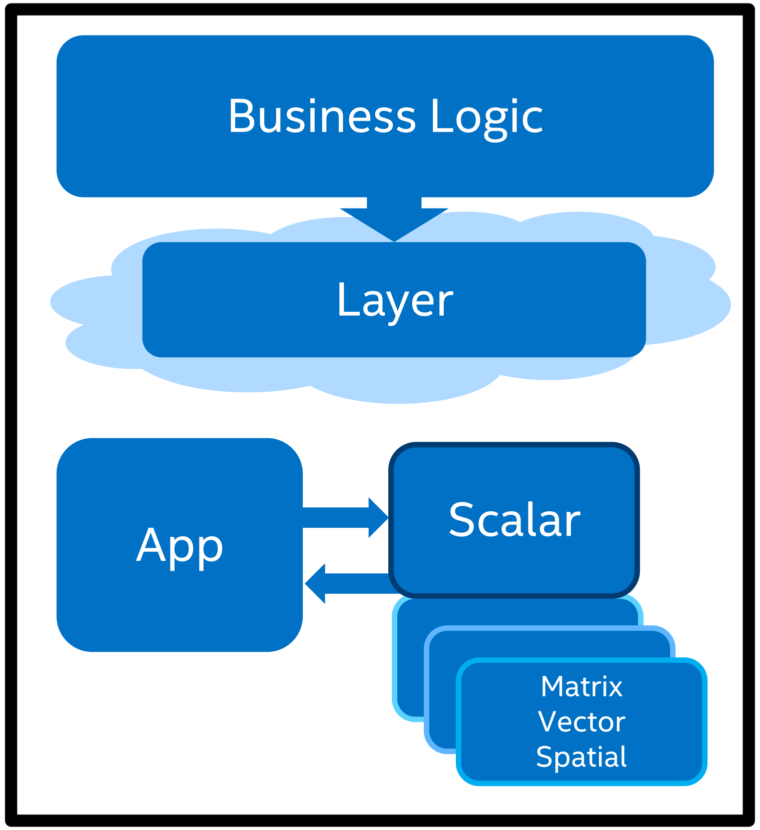
Today you can build you own apps using the SDK... best TCB requires some expertise

NEXT....



Isolated containerization of apps is fast gaining traction

FUTURE!



Frameworks that allow the programmer to concentrate on the business logic and automates more protection of their code no matter where it runs

Future Generation Challenges

Frameworks building out trust when CSP compiles and distributes code

- How do you convey trust?
- How do you compose multiple TEEs?
- Can you attest these types of environments?

Dealing with Attestation at Scale

- Multiple TCBs in the cloud/across clouds
- Multi-TEE environments w/ differing properties

Summary

Confidential Compute Eco-system

- Creation of Confidential Compute Consortia

Confidential Compute HW needs

- Expansion from single socket to multi-socket systems

Attestation

- DCAP for 3rd party services

Future Challenges

- Composability of TEEs
- Attestation at Scale

intel®

experience
what's inside™