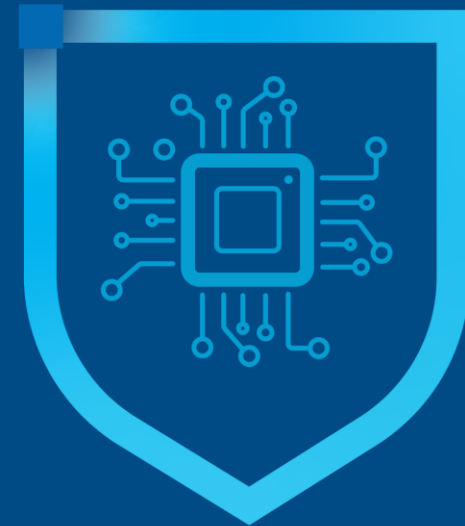


# Intel® TDX Deep Dive

Dr. Benny Fuhry



intel®

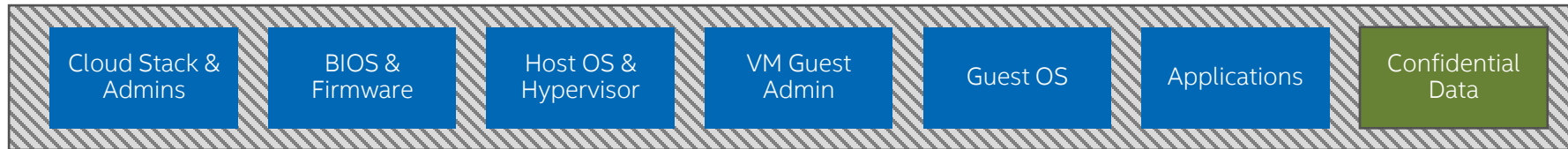


# Intel TDX Overview

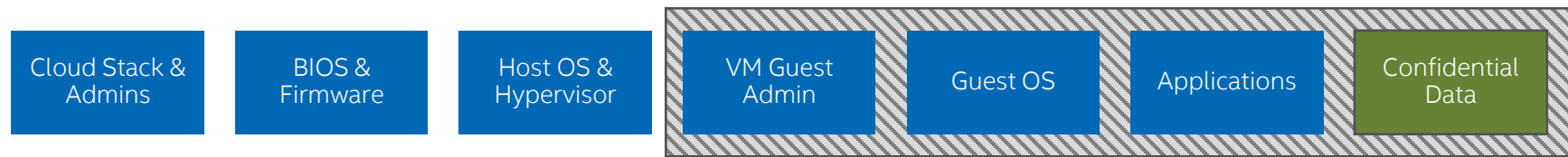
# Trust Boundary of Confidential Computing (CC)

Trust Boundary: Elements with potential to access confidential data

Without Confidential Computing



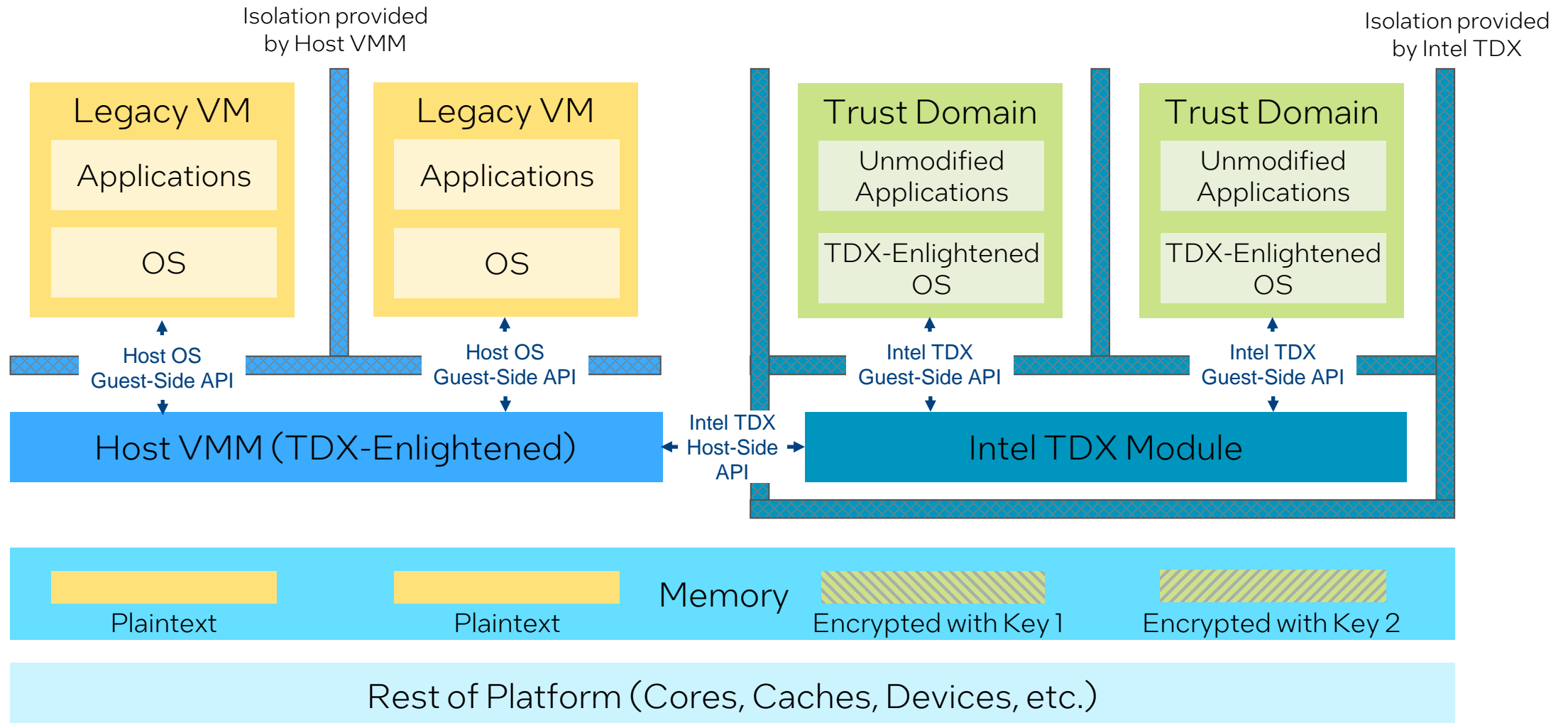
VM Isolation with Intel® TDX



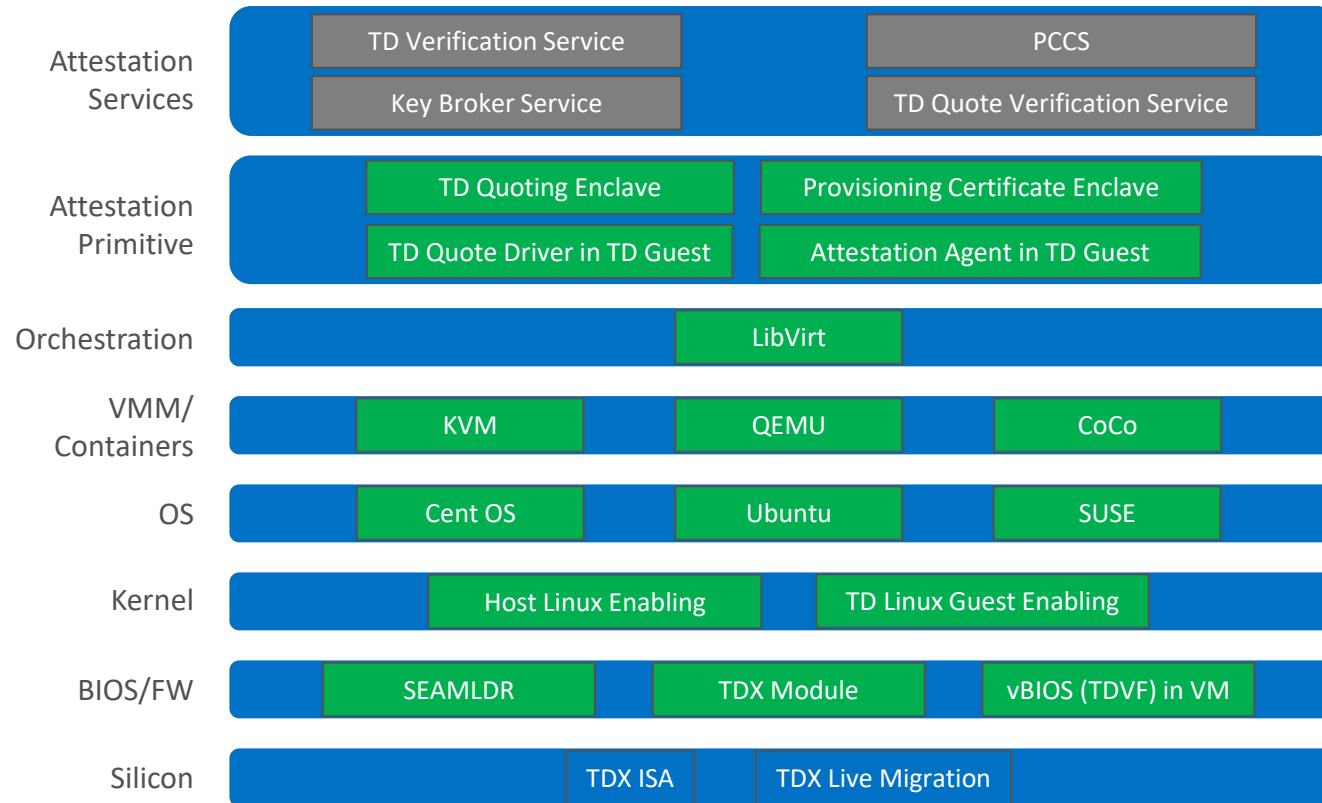
App Isolation with Intel® SGX






# Intel Trust Domain Extensions (Intel TDX) – Overview



# Intel TDX Linux Enabling



-  Open Source
-  Non-Open Source
-  Reference Implementation

# Intel TDX Availability

Intel TDX became available on select 4<sup>th</sup> Gen Intel Xeon Scalable instances through four leading cloud providers

Previews began as early as Q1'23; Check with your provider for their availability dates

Intel TDX became generally available with 5<sup>th</sup> Gen Intel Xeon Scalable processors (code-named Emerald Rapids)



# Intel TDX Details

# Intel TDX – Arch Elements

## CPU-State Confidentiality

TD state managed in CPU-protected memory and invisible to non-TD system SW

## Memory Confidentiality and Integrity

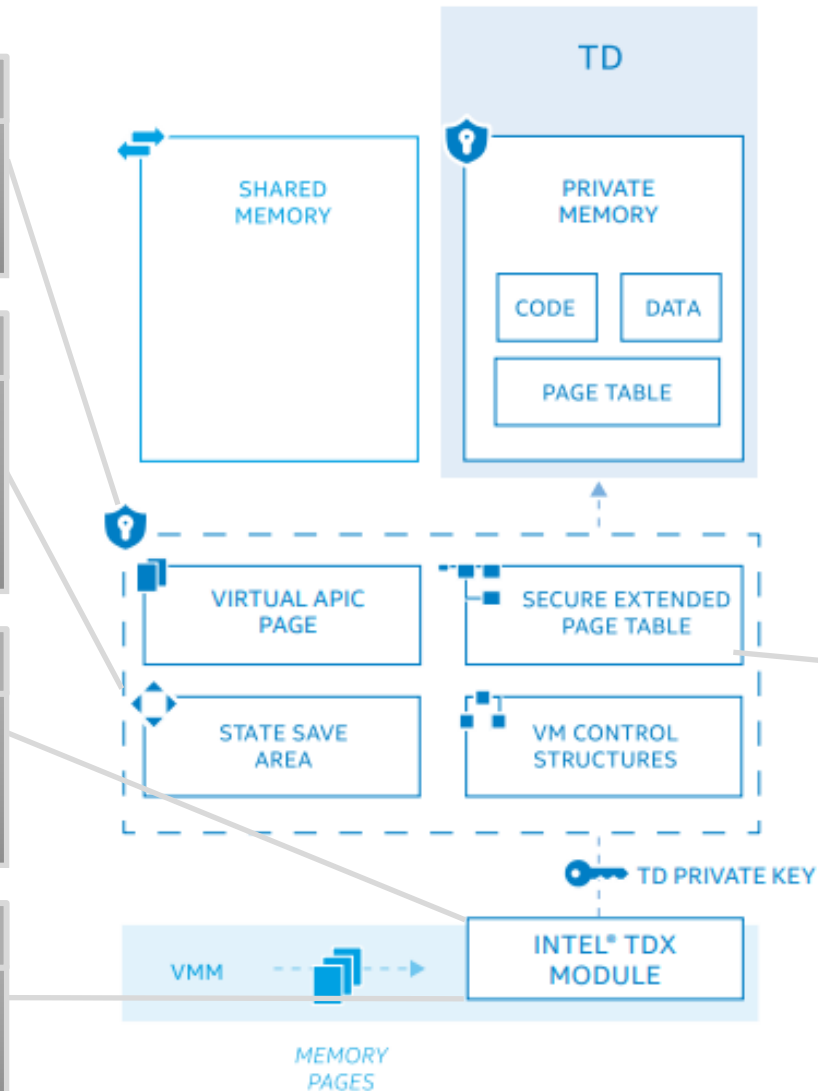
Using access-control and per-TD private key to mitigate VMM attacks from modifying or observing tenant's memory, whether in cache or DDR

## Key Management and Key-ID partitioning

Ability to create, retrieve, use, and manage encryption keys along the lifetime of a TD. Coexist with TMEi-MK usage by host SW.

## Remote Attestation

Authenticate platform and TD image at TD launch time. Leveraging SGX attestation.



## I/O Compatibility

Synthetic and Direct I/O support to shared memory. Support for MMIO emulation.

## Platform Analysis

SW debug/ tuning without loss of confidentiality.

## Memory management

Secure EPT memory mgmt. for private TD memory – to address EPT remap attacks



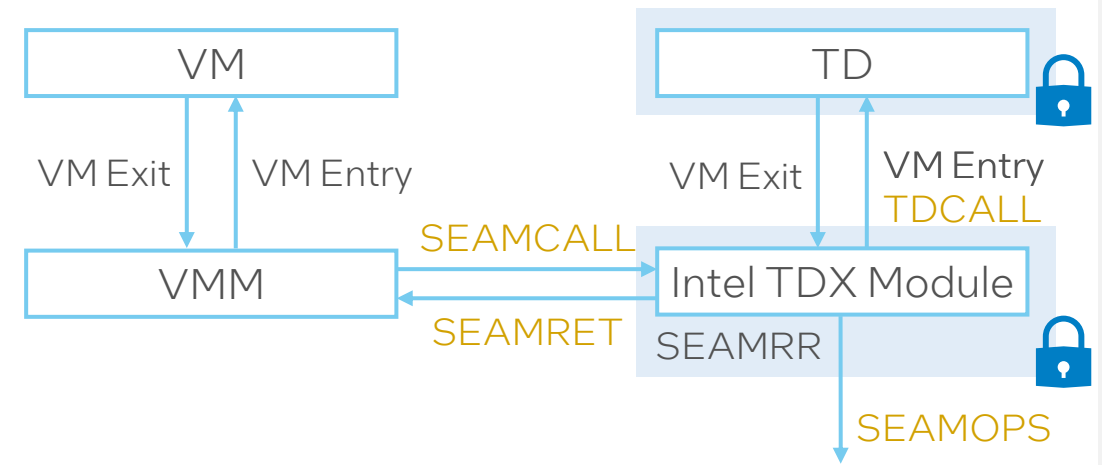
# Intel TDX Module + SEAM

- Intel TDX Module

- Intel-provided and Intel-signed
- SEAM Loader (SEAMLDR) verifies Intel TDX Module and loads it into SEAMRR
- SEAMRR protected with AES-XTS

- Secure Arbitration Mode (SEAM)

- Intel TDX Module operated in SEAM VMX-root mode
- ISA instructions added to enable host & guest interactions: SEAMCALL, SEAMRET, TDCALL, SEAMOPS
- Mode-restricts use of certain ISA instructions

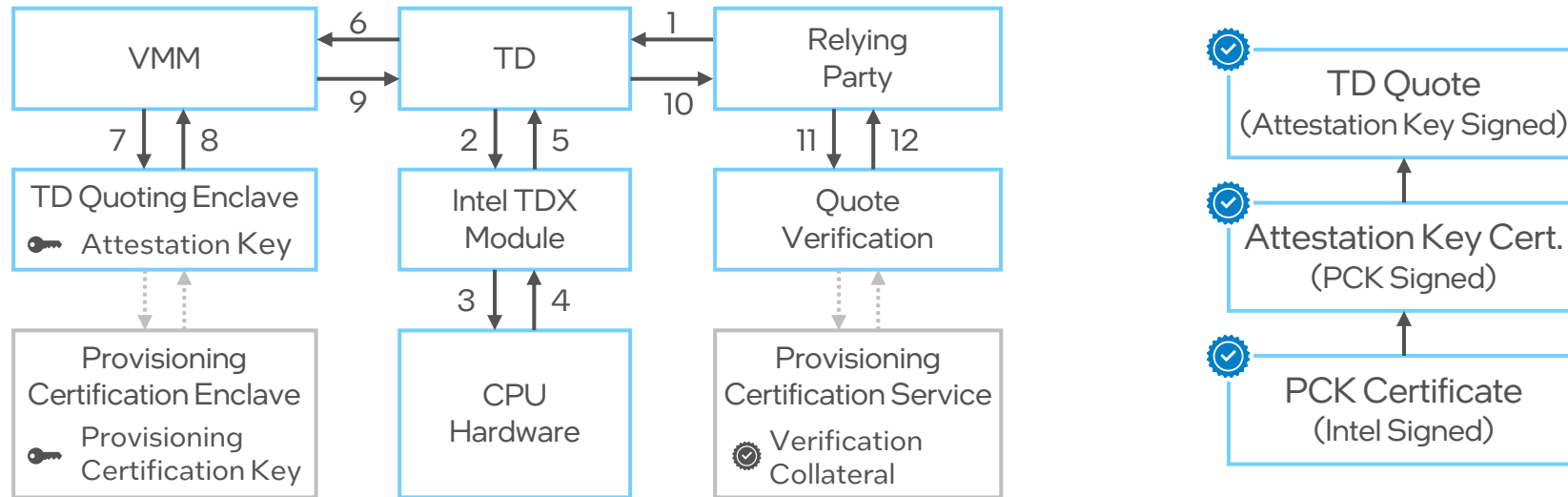


# TDX Remote Attestation

- TD proves to a third/relying party that
  - the booted TD image exactly as expected (MRTD)
  - the measurements created/extended during runtime are as expected (RTMRs)
  - the TD is executed on an Intel TDX-enabled platform
  - the Intel TDX-enabled platform is fully up to date
- Third/relying party can use this proof to decide if TD is trusted

# TDX Remote Attestation

- Process:



- TDX leverages Intel SGX attestation:

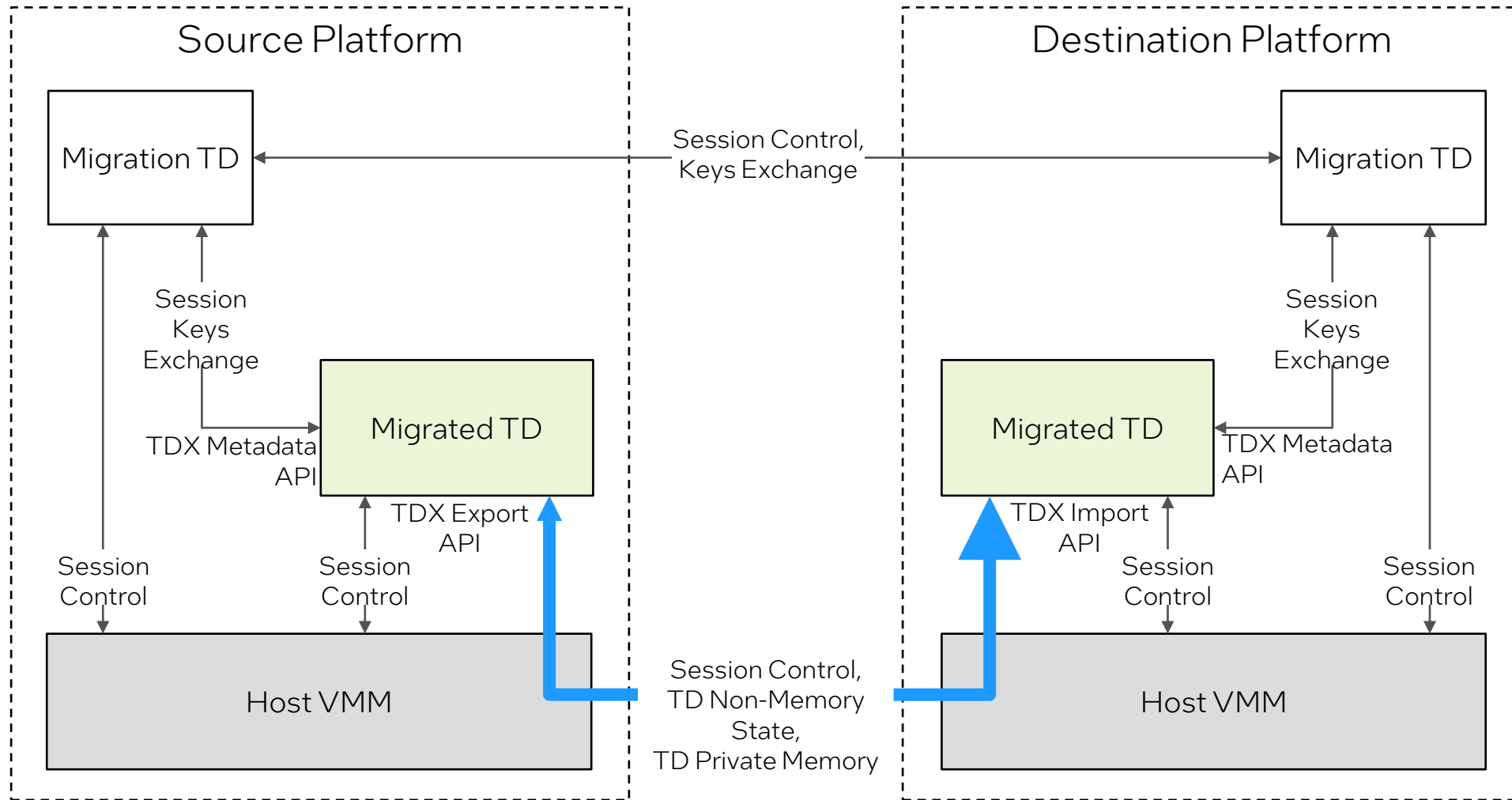
- One set of PCK certificates, distribution, caching services to support SGX & TDX
- Requires SGX be enabled in host for TDX attestation

# Attestation Verification Options

	Cloud Provider's Attestation Service	Application Vendor's Attestation Service	Independent Trust Service (e.g., Intel® Trust Authority)	Build-Your-Own Service with Intel Library
Separation of responsibilities between verifier and infrastructure provider	No	Yes	Yes	Yes
Consistency across Intel SGX and Intel TDX	Yes, if both Intel SGX and TDX offered	Yes, if both Intel SGX and TDX supported	Yes	Yes
Consistent service across on-prem, hybrid, multi-cloud, and edge deployments	No	Possible, but limited to specific application	Yes	Yes
Development effort	Low	Low	Low	Medium

# Upcoming Features

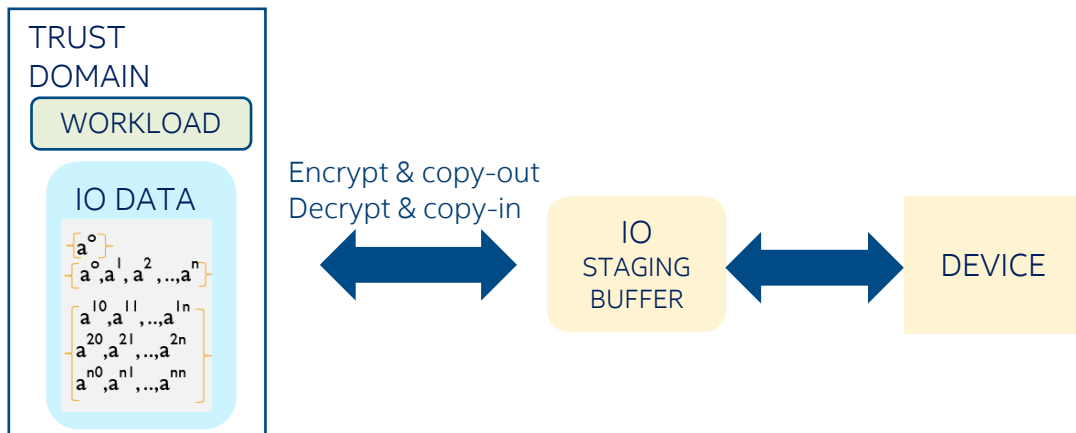
# TD Migration



# Intel TDX Connect

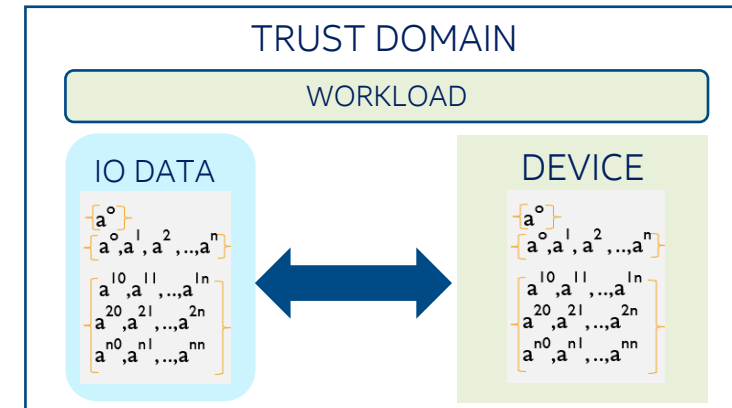
Goal: Enable heterogenous confidential computing with secure, efficient, and low-overhead data movement to/from devices

## TDX 1.0/1.5



- No devices trusted by any TD
- Devices cannot access TD private memory
- Overheads for (secure) data movement

## Intel TDX Connect



- ✓ TD trust can be extended to trusted
- ✓ Trusted devices can access TD private memory
- ✓ Efficient, low-overhead data movement (PCIe, CXL)

# TDX White Papers and Specifications

Overview Documentation Support

## Browse Intel TDX Documentation

Find documentation and explore resources designed for easy access and hands-on learning.  
Jump to: [Architecture](#) | [Source Code](#) | [Security Guidance](#)

### Intel TDX Architecture

#### Common Intel TDX White Papers and Specifications

Document	Description	Last Updated
<a href="#">Intel® Trust Domain Extensions (Intel® TDX)</a>	An overview of the Intel TDX technology.	February 2023
<a href="#">Intel CPU Architectural Extensions Specification</a>	A specification of Intel CPU architectural support for Intel TDX.	May 2021
<a href="#">Intel TDX Loader Interface Specification</a>	A specification of how a virtual machine manager (VMM) loads the Intel TDX Module on a platform.	March 2022
<a href="#">Intel TDX Virtual Firmware Design Guide</a>	A guide on how to design and implement a virtual firmware for a trust domain.	December 2022

#### Intel TDX 1.0

Document	Description	Last Updated
<a href="#">Intel TDX Module 1.0 Specification</a>	Architecture and Application Binary Interface (ABI) specification of the Intel TDX module	February 2023
<a href="#">Intel TDX Guest-Hypervisor Communication Interface</a>	Specification of the software interface between the guest operating system (tenant) and the VMM required to enable Intel TDX 1.0	March 2023

<https://www.intel.com/content/www/us/en/developer/tools/trust-domain-extensions/documentation.html>



# Legal Disclaimer

Intel® technologies may require enabled hardware, software, or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

©Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

intel®