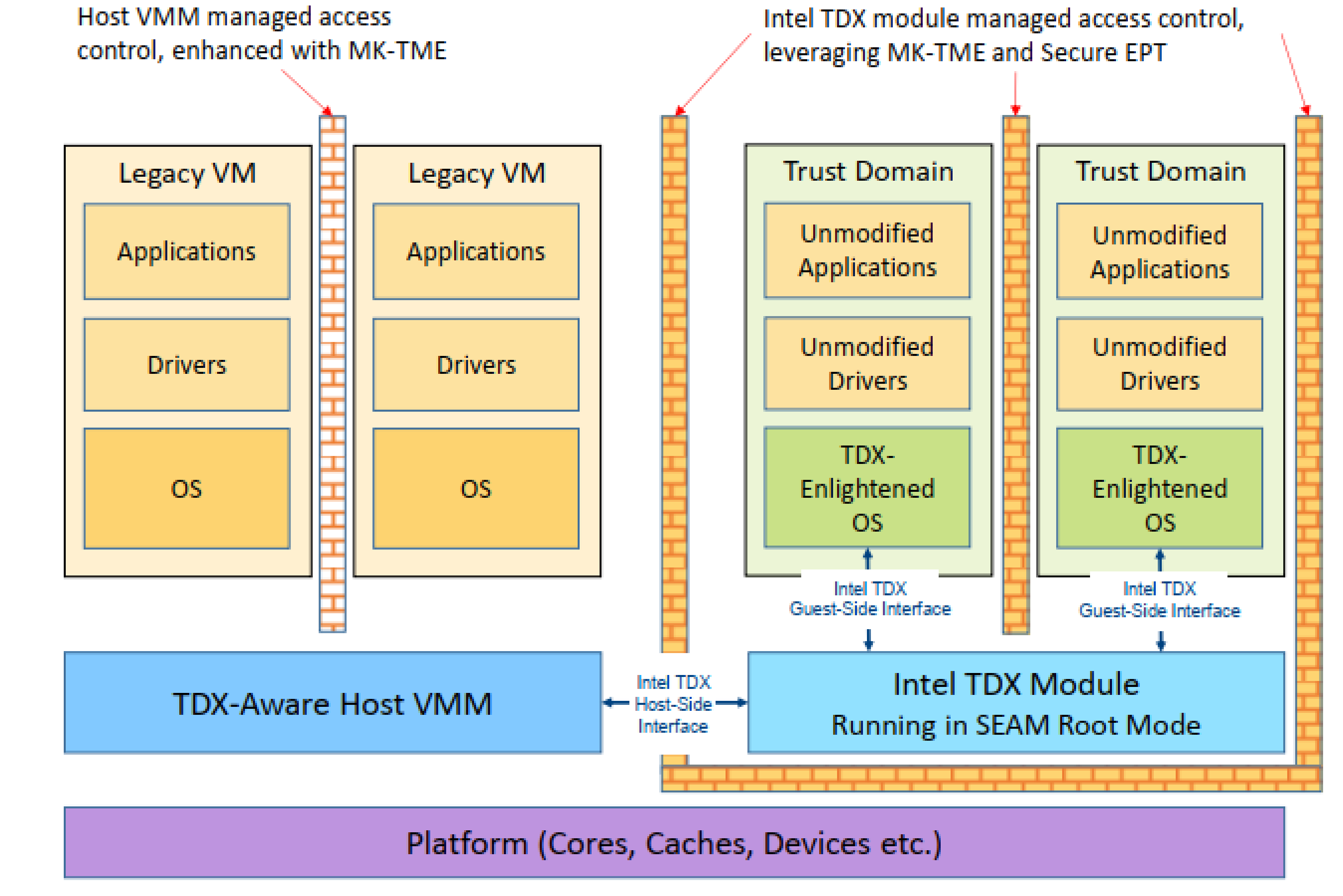
Intel TDX技术解析以及社区演进状态

SATG/SSE/OSV & CSP Engineering
2023 ww41 Fan Du

Intel Trusted Domain eXtension Overview

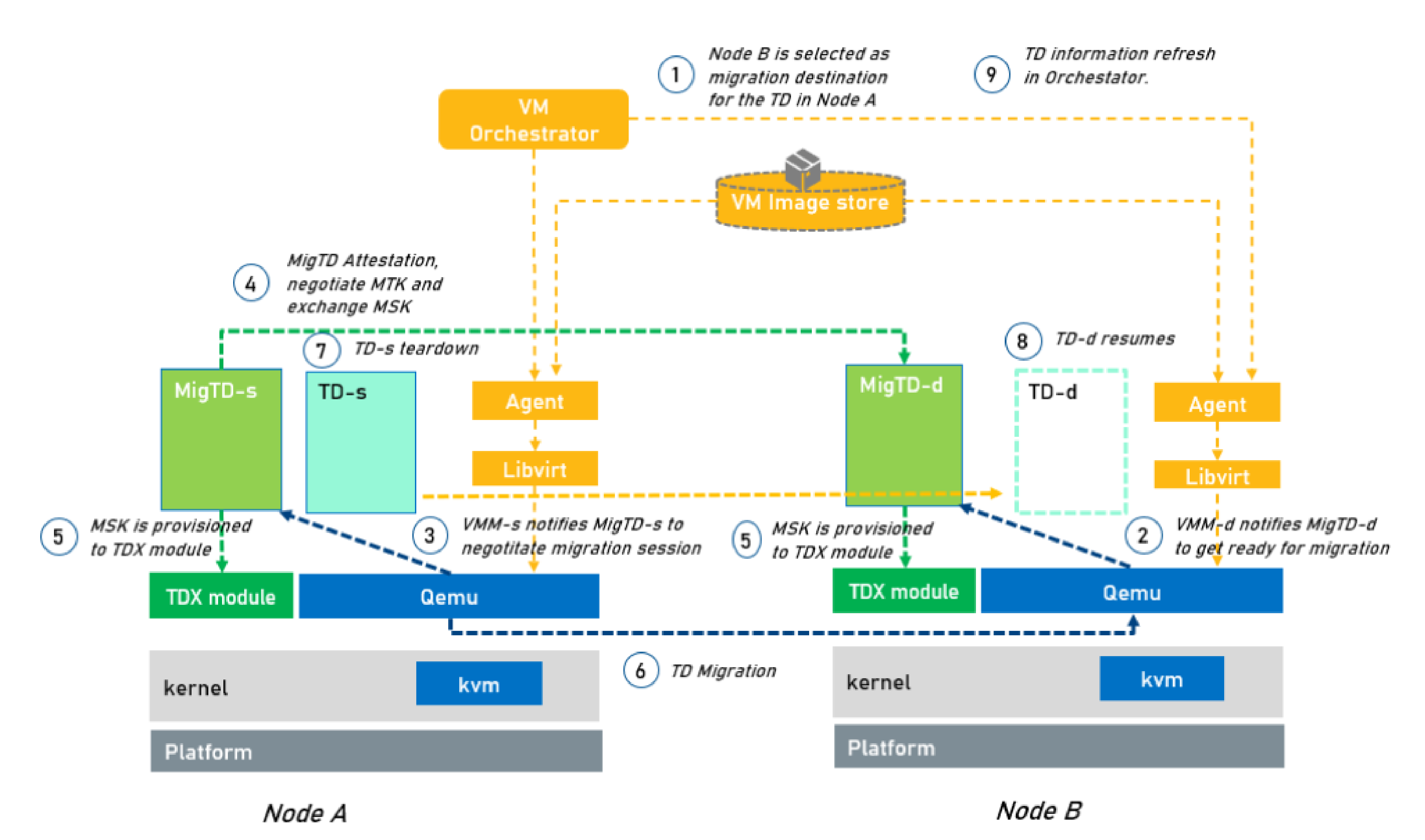
- TDX – an extension of VMX and MKTME technologies to isolate CSP/VMM from trust computing base by protecting TD guest memory, CPU state as well as the link b/w TD guest and device.
- TDX Tech Roadmap
  - ➢ *TDX foundation*
  - ➢ *TDX Live Migration, TD Preserving*
  - ➢ *TDX connect , TD Partitioning*



Host VMM managed access control, enhanced with MK-TME
Intel TDX module managed access control, leveraging MK-TME and Secure EPT
Legacy VM
Applications
Drivers
OS
Legacy VM
Applications
Drivers
OS
Trust Domain
Unmodified Applications
Unmodified Drivers
TDX-Enlightened OS
Intel TDX Guest-Side Interface
Trust Domain
Unmodified Applications
Unmodified Drivers
TDX-Enlightened OS
Intel TDX Guest-Side Interface
TDX-Aware Host VMM
Intel TDX Host-Side Interface
Intel TDX Module Running in SEAM Root Mode
Platform (Cores, Caches, Devices etc.)

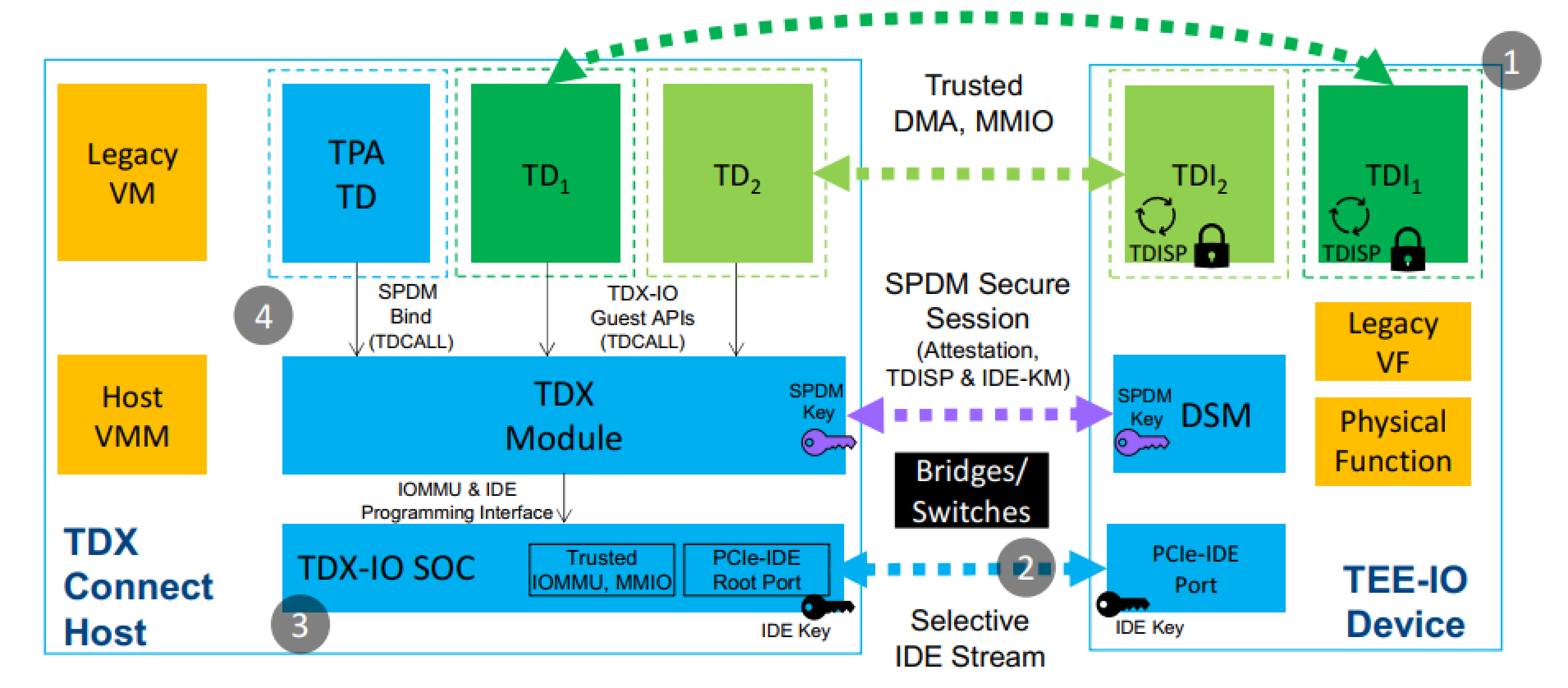
TDX Portal Link (Spec, TDX FW code)

TDX Live Migration



1 Node B is selected as migration destination for the TD in Node A
9 TD information refresh in Orchestator.
VM Orchestrator
VM Image store
4 MigTD Attestation, negotiate MTK and exchange MSK
7 TD-s teardown
8 TD-d resumes
MigTD-s
TD-s
Agent
Libvirt
MigTD-d
TD-d
Agent
Libvirt
5 MSK is provisioned to TDX module
3 VMM-s notifies MigTD-s to negotitate migration session
5 MSK is provisioned to TDX module
2 VMM-d notifies MigTD-d to get ready for migration
TDX module
Qemu
TDX module
Qemu
6 TD Migration
kernel
kvm
kernel
kvm
Platform
Platform
Node A
Node B

TDX Connect


Trusted
DMA, MMIO
1
Legacy VM
TPA TD
TD_1
TD_2
TDI_2
TDISP
TDI_1
TDISP
SPDM Secure Session
(Attestation, TDISP & IDE-KM)
4
SPDM Bind (TDCALL)
TDX-IO Guest APIs (TDCALL)
Host VMM
TDX Module
SPDM Key
SPDM Key
DSM
Legacy VF
Physical Function
Bridges/ Switches
IOMMU & IDE Programming Interface
TDX-IO SOC
Trusted IOMMU, MMIO
PCIe-IDE Root Port
2
PCIe-IDE Port
IDE Key
IDE Key
3
TDX Connect Host
Selective IDE Stream
TEE-IO Device

TDX Feature Break Down

Priority	TDX Host	Upstream Status/commits	TDX Guest	Upstream Status/commits	Deliverables
P1 (Must-to-have)	KVM Foundation	v15/113	Core support	v5.19/30	• TDX basic support – TD creation • Facilitate workload evaluation • Intercept general request from customer.
	TDX Module Init	v12/22	Attestation: GetReport	v6.2/3	
	UPM	RFC v11/29 RFC v4/10			
P2 (Add-on)	EPT Huge Page	RFC v4/16	Lazy accept	v6.5/9	• Enhanced features to reach production requirement.
			Attestation: GetQuote	v3/3	
P3 (In-planning)	TD preserving	Internal Tree	Hardening	Internal Tree	• Enhanced features to meet production requirement.
	Live Migration	Internal Tree			

Qemu support depends on kernel side TDX support to be upstreamed.
Qemu TDX v1 submission to community in Aug’2022.
TDX host support trending v6.8 merge window.

Local OSV TDX enabling Opens

1. TDX intercept scope (Target release)

    v5.10 LTS vs v6.6 LTS

2. Goal: Tech preview or production

    Kernel & Qemu vs Full Stack

3. TDX features list for inclusion

    Community patchset vs TDX internal feature intel®

Intel Xeon Security Roadmap

	Whitley	Eagle Stream		Birch Stream
	Ice Lake	Sapphire Rapids	Emerald Rapids	Granite Rapids/Sierra Forest
Harden Platform	Root of trust and resiliency: Trusted BIOS/firmware startup, secure recovery and debug			
	• Platform Firmware Resilience (PFR) 2.0: ECDSA-256	• PFR 3.0: SPDM 1.0 attestation support, ECDSA-384		• CPU SPDM 1.0 Attestation • PFR 4.0 SPDM 1.2 and RSA 3K support
				Physical hardening: Protection against physical attacks
				• Link Protection for PCIe, UPI, CXL
	SW hardening: HW enforced execution control			
	• User Mode Access Prevention (UMIP) • EPT-Sub Page Permissions	• Hypervisor-managed Linear Address Translation (HLAT) • Control flow Enforcement Tech (CET) • VM Bus Lock Detection • Protection Keys-Supervisor Mode		• Linear Address Space Separation (LASS) - *SRF* • Linear Address Masking (LAM) - *SRF*
Protect Data	Memory encryption	Cryptographic workload isolation and integrity for Virtualized Environments		
	• Total Memory Encryption (TME) • Multi-key TME(MKTME) - 64 Keys	TDX 1.0: • Fuse choice for Logical Integrity (LI) or Crypto Integrity(CI) • 128 MKTME keys (PA = 32TB)	TDX 1.5: • BIOS choice for LI or CI • 128 MKTME keys • VM Migration, TD Preserving	TDX 2.0: • 2048 MKTME keys (PA=2TB) • AES-256 encryption
	Cryptographic workload isolation and integrity for Applications and Bare Metal Environments			
	Intel® SGX 1.0: • Trusted Environment Mode • Up to 512GB Enclave Page Cache	Intel® SGX 2.0: • Cryptographic integrity protection		
	Acceleration/Hardening for cryptographic workloads			
	• Symm encr: Vector AES • Asym encr: VPMADD52 • Hashing: SHA2-256	Intel® Quick Assist Technology (QAT): CPU integration + Key Protection Tech		