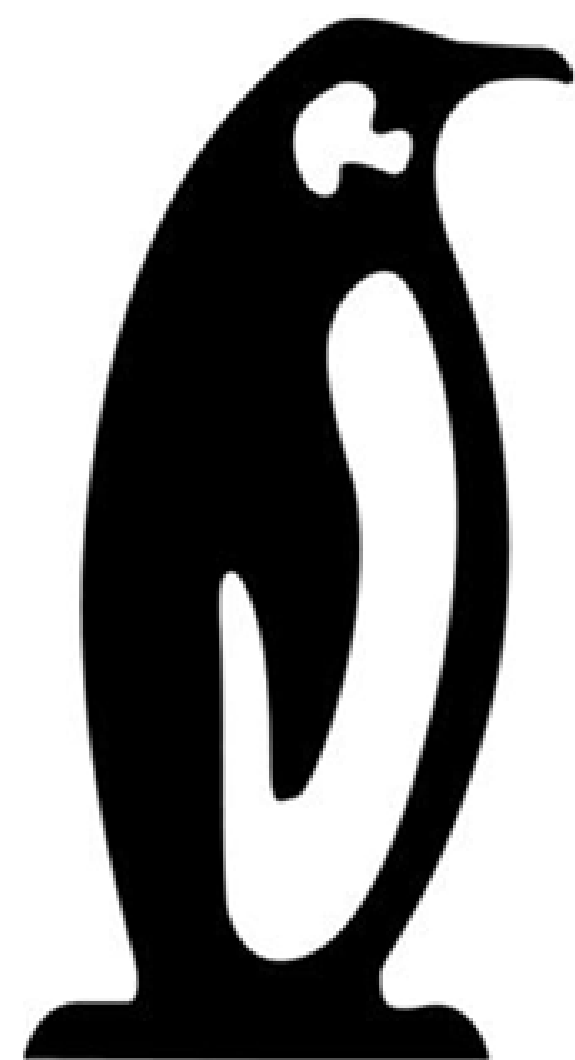




東京 **2025**

**LINUX
PLUMBERS
CONFERENCE**

TOKYO, JAPAN / DECEMBER 11-13, 2025

Confidential Devices (TEE I/O): A series of modest proposals

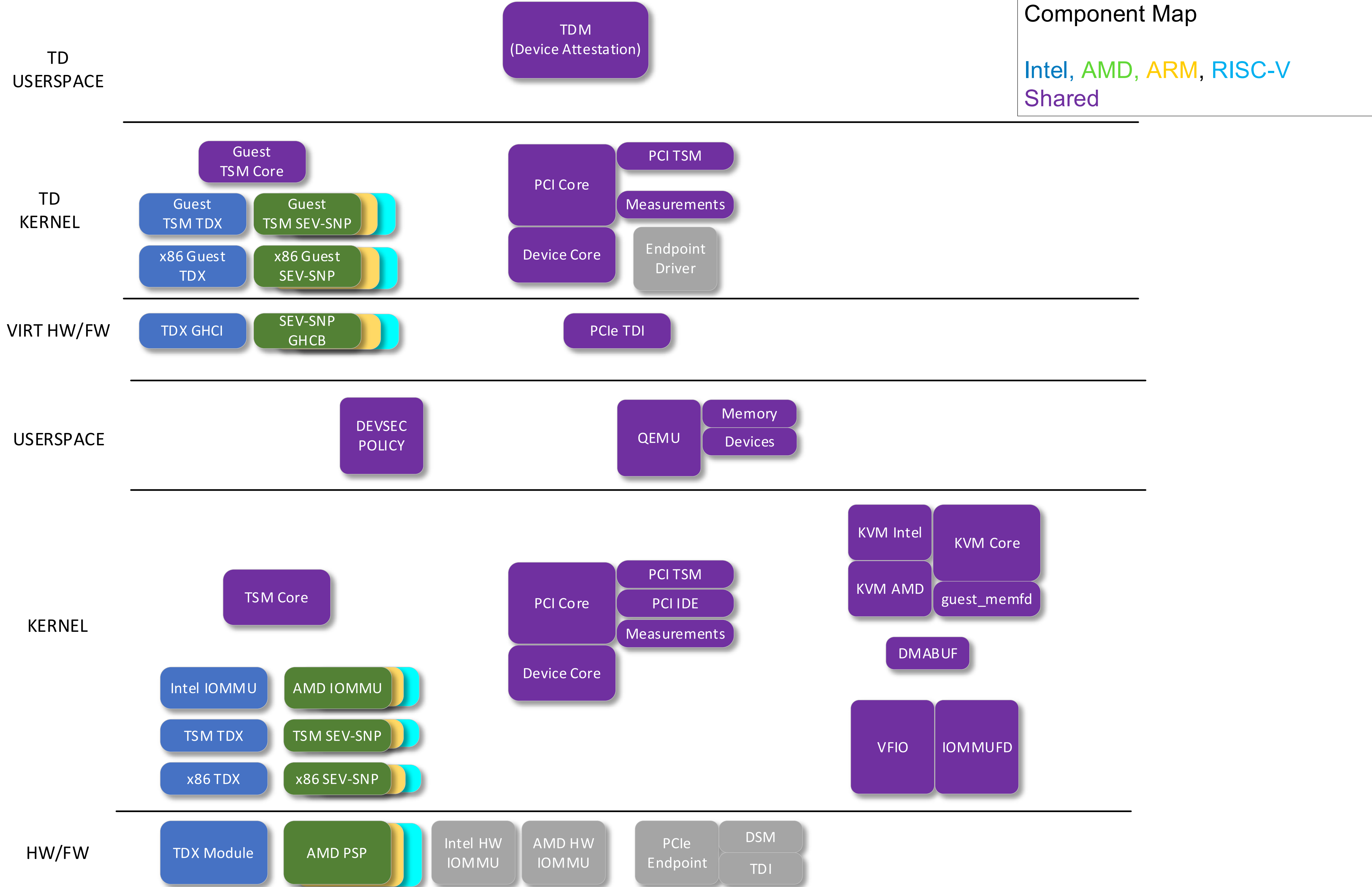
Confidential Devices: TEE I/O

Problem statement

Where the effort stands?

Where is the effort going next?

Discussion



Component Map

Intel, AMD, ARM, RISC-V
Shared

TD
USERSPACE

TDM
(Device Attestation)

TD
KERNEL

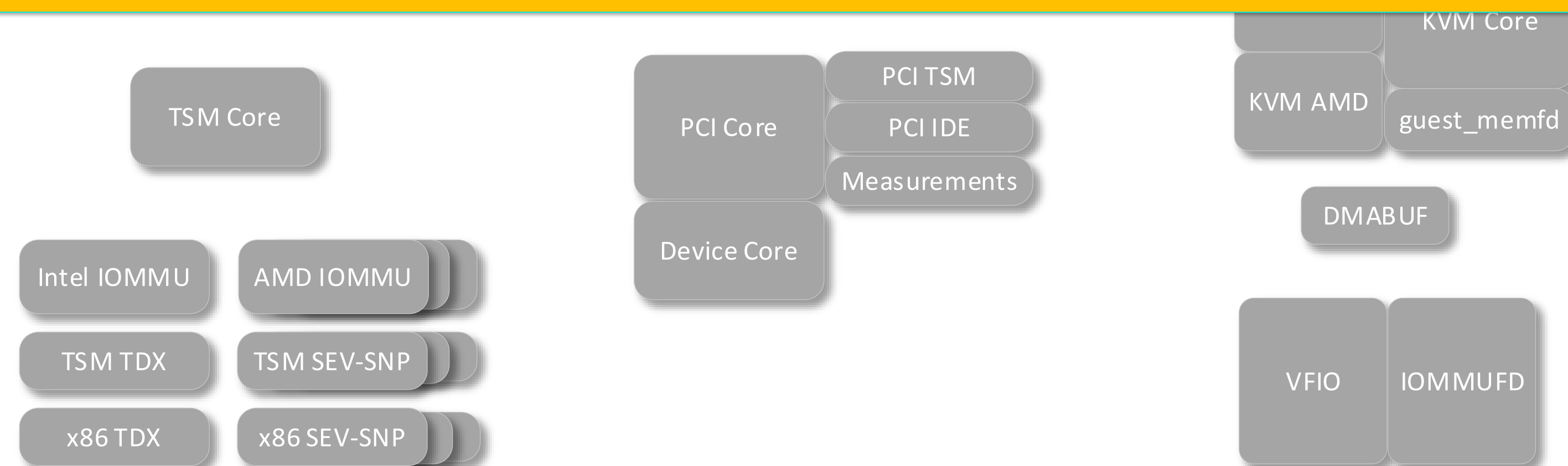


VI

U

The only path to bother this many subsystem, this significantly is through multi-architecture consensus

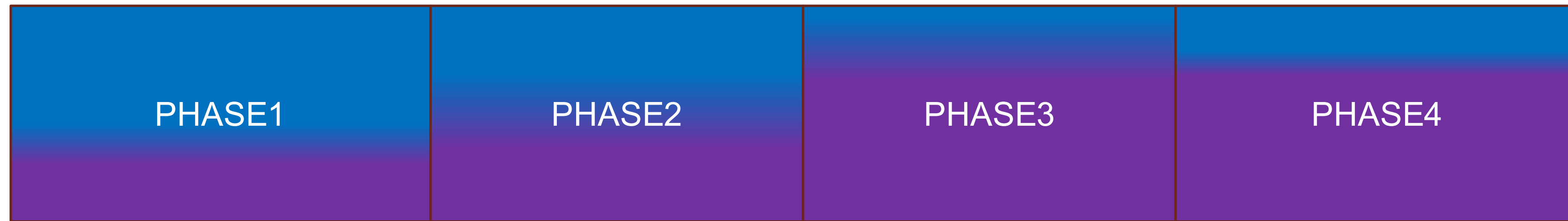
KERNEL



HW/FW



Phase Timeline

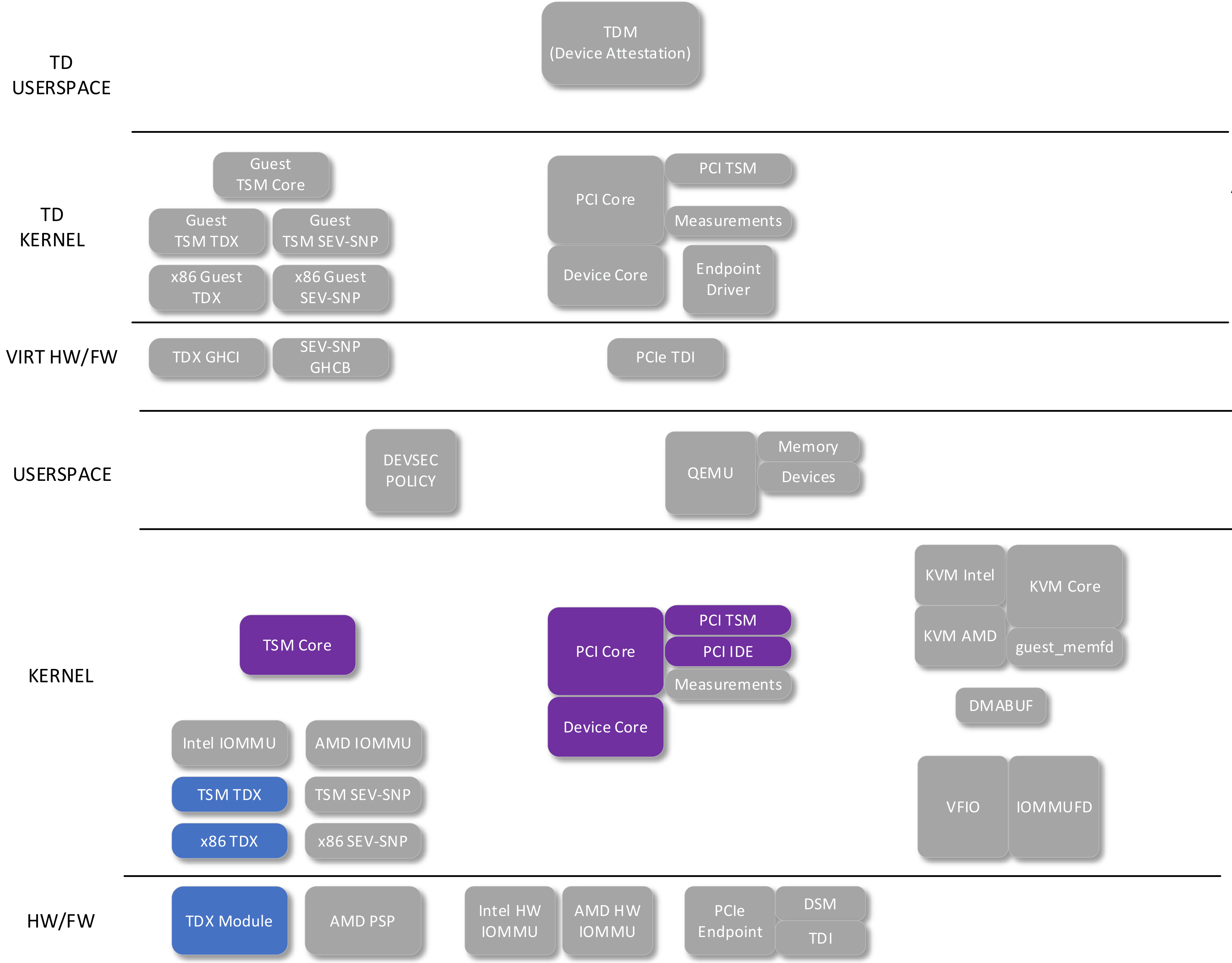


Phase1: Device Authentication and Link Encryption (host-side)

Phase2: Device Lock and Accept (guest-side)

Phase3: Private DMA and MMIO setup (host-side)

Phase4: Attestation



PHASE1

Device Authentication and Link Encryption

TD
USERSPACE

TDM
(Device Attestation)

PHASE2

TD
KERNEL

Guest
TSM Core

Guest
TSM TDX

Guest
TSM SEV-SNP

x86 Guest
TDX

x86 Guest
SEV-SNP

PCI Core

PCI TSM

Measurements

Device Core

Endpoint
Driver

VIRT HW/FW

TDX GHCI

SEV-SNP
GHCB

PCIe TDI

USERSPACE

DEVSEC
POLICY

QEMU

Memory
Devices

KERNEL

TSM Core

Intel IOMMU

AMD IOMMU

TSM TDX

TSM SEV-SNP

x86 TDX

x86 SEV-SNP

PCI Core

PCI TSM

PCI IDE

Measurements

Device Core

KVM Intel

KVM Core

KVM AMD

guest_memfd

DMABUF

VFIO

IOMMUFD

HW/FW

TDX Module

AMD PSP

Intel HW
IOMMU

AMD HW
IOMMU

PCIe
Endpoint

DSM
TDI

TD
USERSPACE

TDM
(Device Attestation)

PHASE3

TD
KERNEL

Guest
TSM Core

Guest
TSM TDX

Guest
TSM SEV-SNP

x86 Guest
TDX

x86 Guest
SEV-SNP

PCI Core

PCI TSM

Measurements

Device Core

Endpoint
Driver

VIRT HW/FW

TDX GHCI

SEV-SNP
GHCB

PCIe TDI

USERSPACE

DEVSEC
POLICY

QEMU

Memory
Devices

KERNEL

TSM Core

PCI Core

PCI TSM

PCI IDE

Measurements

Device Core

KVM Intel

KVM Core

KVM AMD

guest_memfd

DMABUF

VFIO

IOMMUFD

Intel IOMMU

AMD IOMMU

TSM TDX

TSM SEV-SNP

x86 TDX

x86 SEV-SNP

HW/FW

TDX Module

AMD PSP

Intel HW
IOMMU

AMD HW
IOMMU

PCIe
Endpoint

DSM
TDI

TD
USERSPACE

TDM
(Device Attestation)

PHASE4

Attestation

TD
KERNEL

Guest
TSM Core

Guest
TSM TDX

Guest
TSM SEV-SNP

x86 Guest
TDX

x86 Guest
SEV-SNP

PCI Core

PCI TSM

Measurements

Device Core

Endpoint
Driver

VIRT HW/FW

TDX GHCI

SEV-SNP
GHCB

PCIe TDI

USERSPACE

DEVSEC
POLICY

QEMU

Memory

Devices

KERNEL

TSM Core

Intel IOMMU

AMD IOMMU

TSM TDX

TSM SEV-SNP

x86 TDX

x86 SEV-SNP

PCI Core

PCI TSM

PCI IDE

Measurements

Device Core

KVM Intel

KVM Core

KVM AMD

guest_memfd

DMABUF

VFIO

IOMMUFD

HW/FW

TDX Module

AMD PSP

Intel HW
IOMMU

AMD HW
IOMMU

PCIe
Endpoint

DSM

TDI

Discussion

- Phase2: Lock preparation drivers
- Phase3: DMA-BUF for Private MMIO
- Phase3: IOMMUFD BIND ABI
- Phase4: Attestation

Get Involved!

List: linux-coco@lists.linux.dev

(<https://subspace.kernel.org/lists.linux.dev.html>)

Discord: <https://discord.gg/2rb53MXB> #devsec

Call: CCC TAC Subcommittee: Linux Kernel Special Interest Group
(to be renamed: OS Arch Special Interest Group)

Git: <https://git.kernel.org/pub/scm/linux/kernel/git/devsec/tsm.git>
#staging





東京 **2025**

LINUX PLUMBERS CONFERENCE

TOKYO, JAPAN / DECEMBER 11-13, 2025

