Qualcomm

SoC peripheral TDISP

David Hartley

Qualcomm Germany GmbH

Linux Plumbers Conference, September 2024

SoC vs external peripherals

SoC peripherals

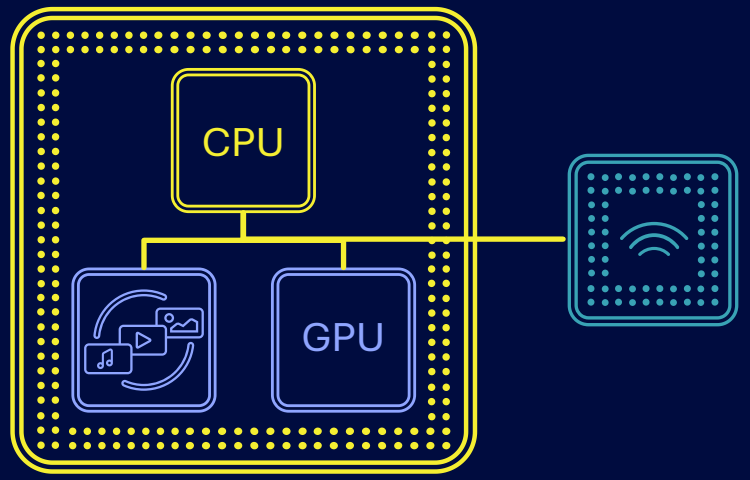
Connection security
- Fixed endpoints
- Internal isolation

Optimization scope
- Additional DMA interfaces
- Wired interrupts
- Shared dependencies

External peripherals

Standard links (e.g. PCIe)
- Endpoint enumeration
- Interface identification
- Link protection (IDE)
- Virtualization
- Confidential compute (TDISP)

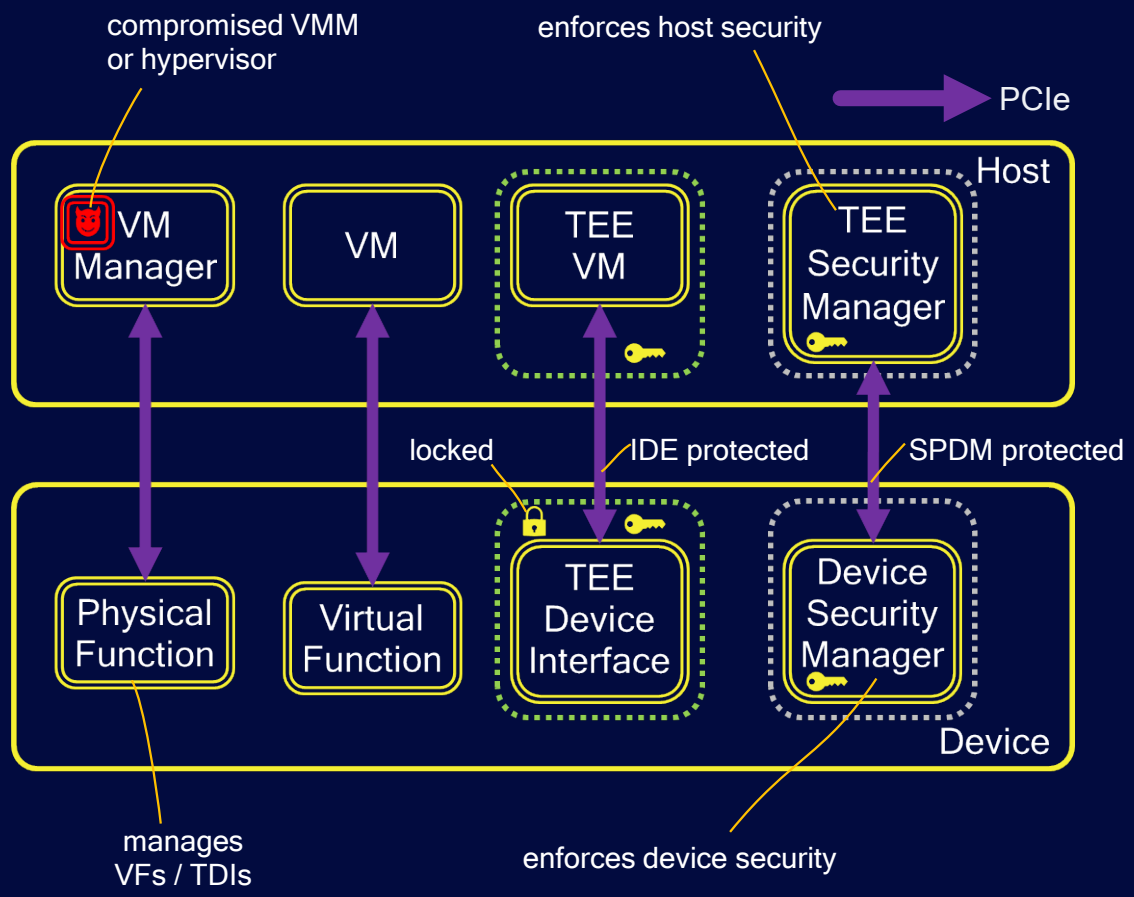
SW support
- Across multiple OS



TEE: Trusted Execution Environment
TDISP: TEE Device Interface Security Protocol
SPDM: Security Protocol and Data Model
IDE: Integrity and Data Encryption

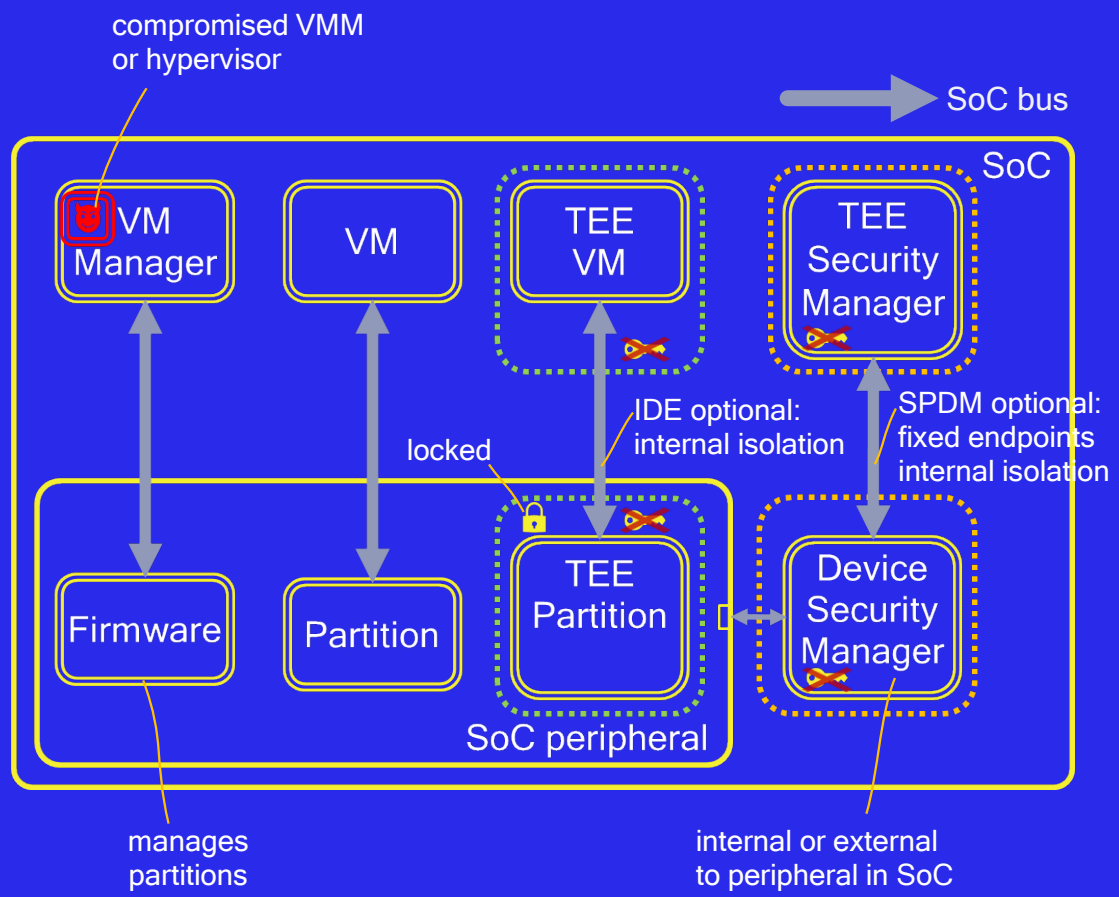
PCIe TDISP

Structure



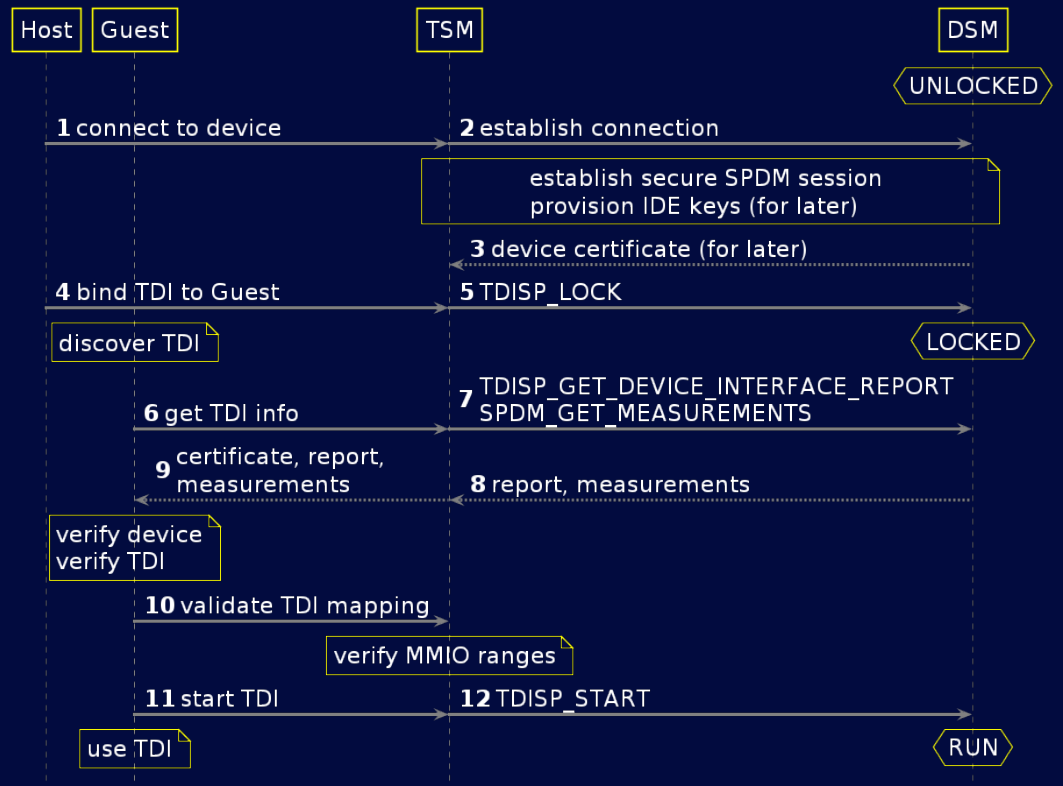
SoC peripheral TDISP

Structure



PCIe TDISP

Flow

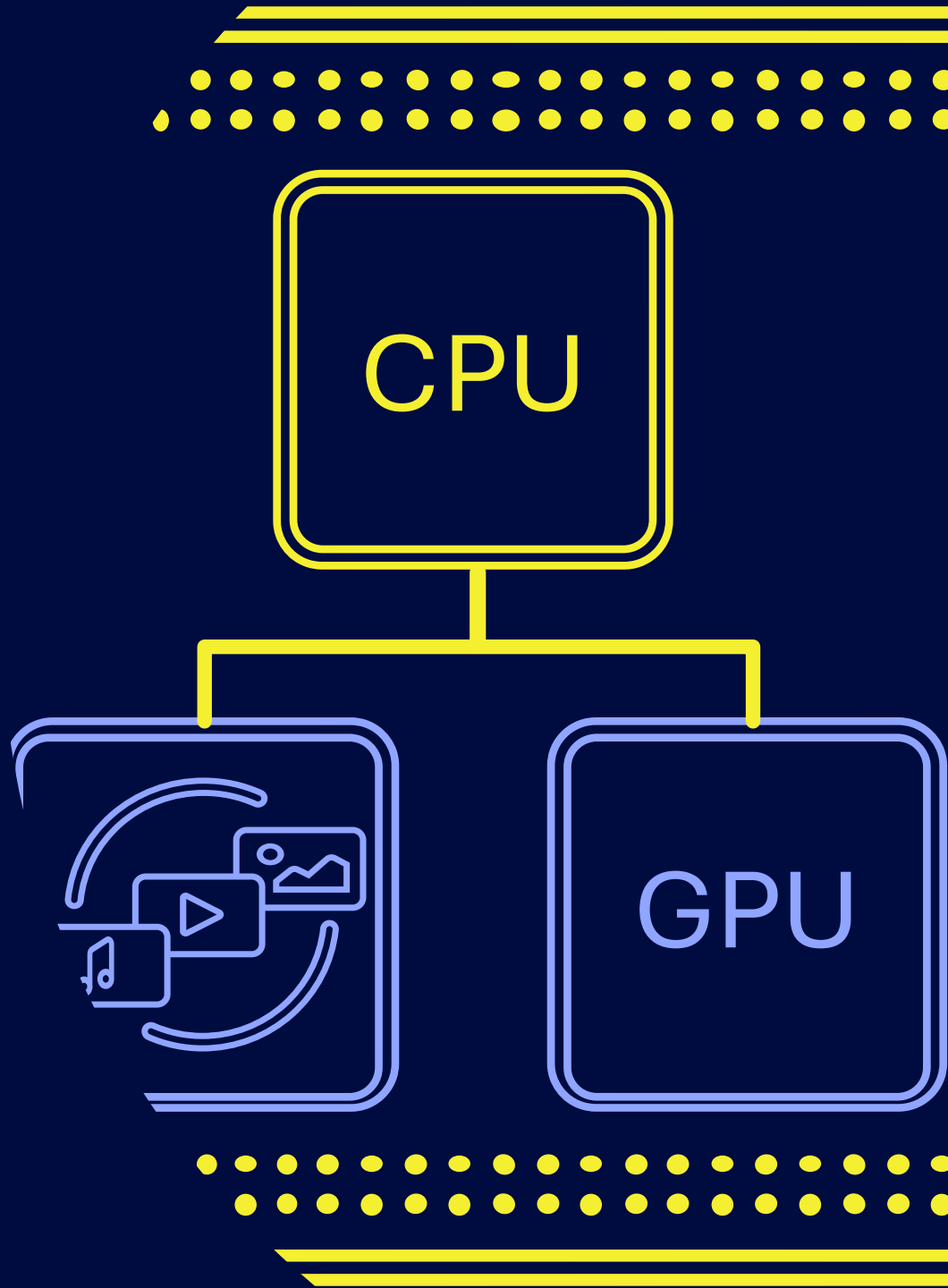


SoC peripheral TDISP

Flow

Support needed for confidential compute with SoC peripherals

- Generalise Linux TSM ops and TDISP protocol
- Allow arch-specific and SoC-specific interfaces, reports and measurements



Thank you

Follow us on:

For more information, visit us at qualcomm.com & qualcomm.com/blog