

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



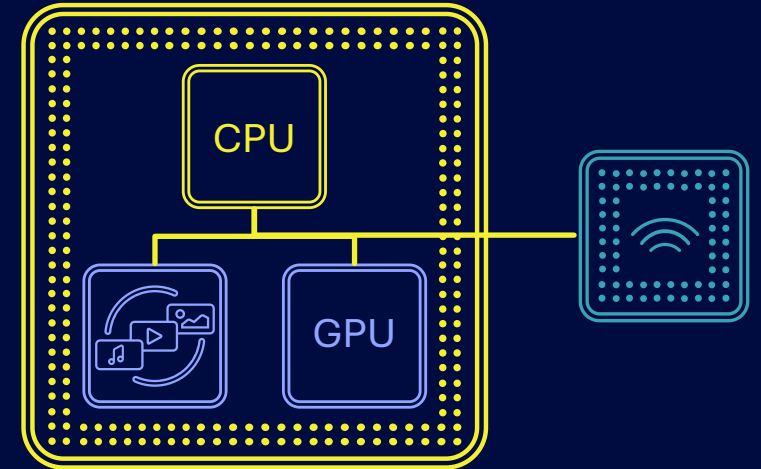
External peripherals

Standard links (e.g. PCIe)

- Endpoint enumeration
- Interface identification
- Link protection (IDE)
- Virtualization
- Confidential compute (TDISP)

SW support

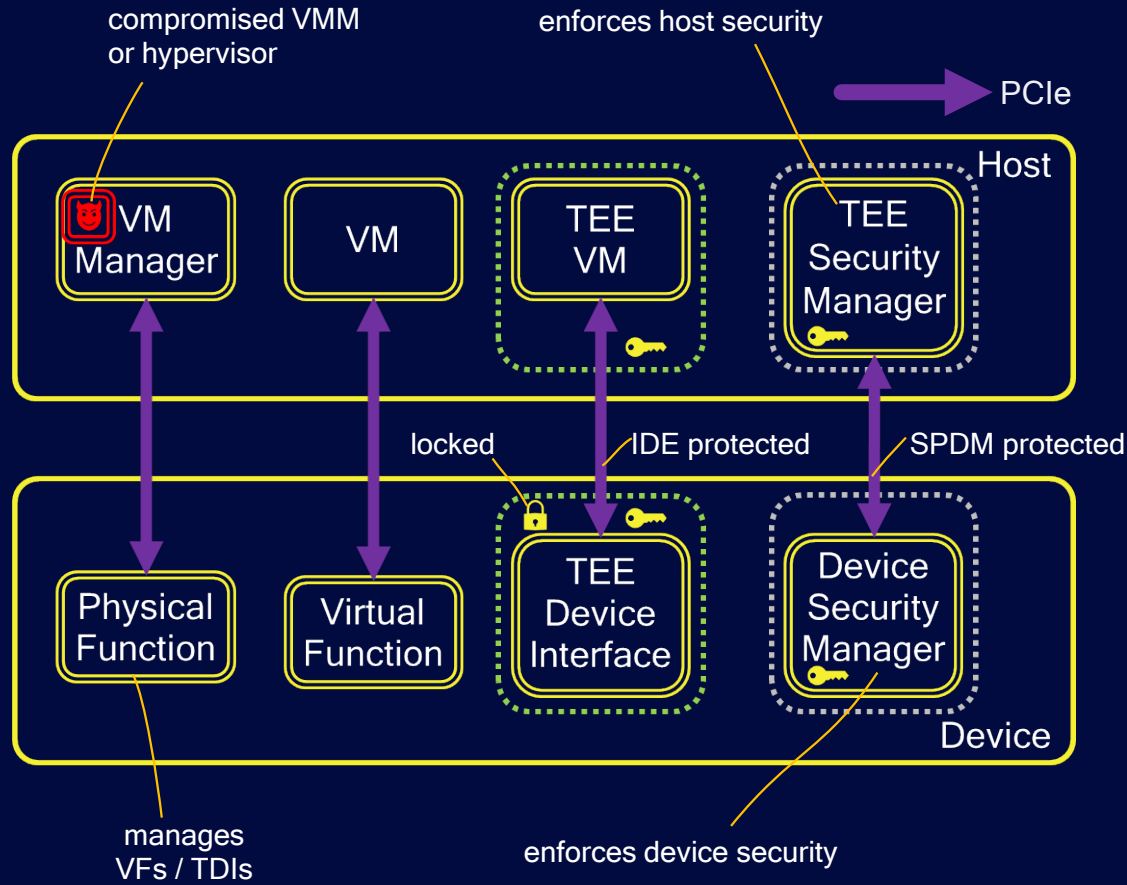
- Across multiple OS



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

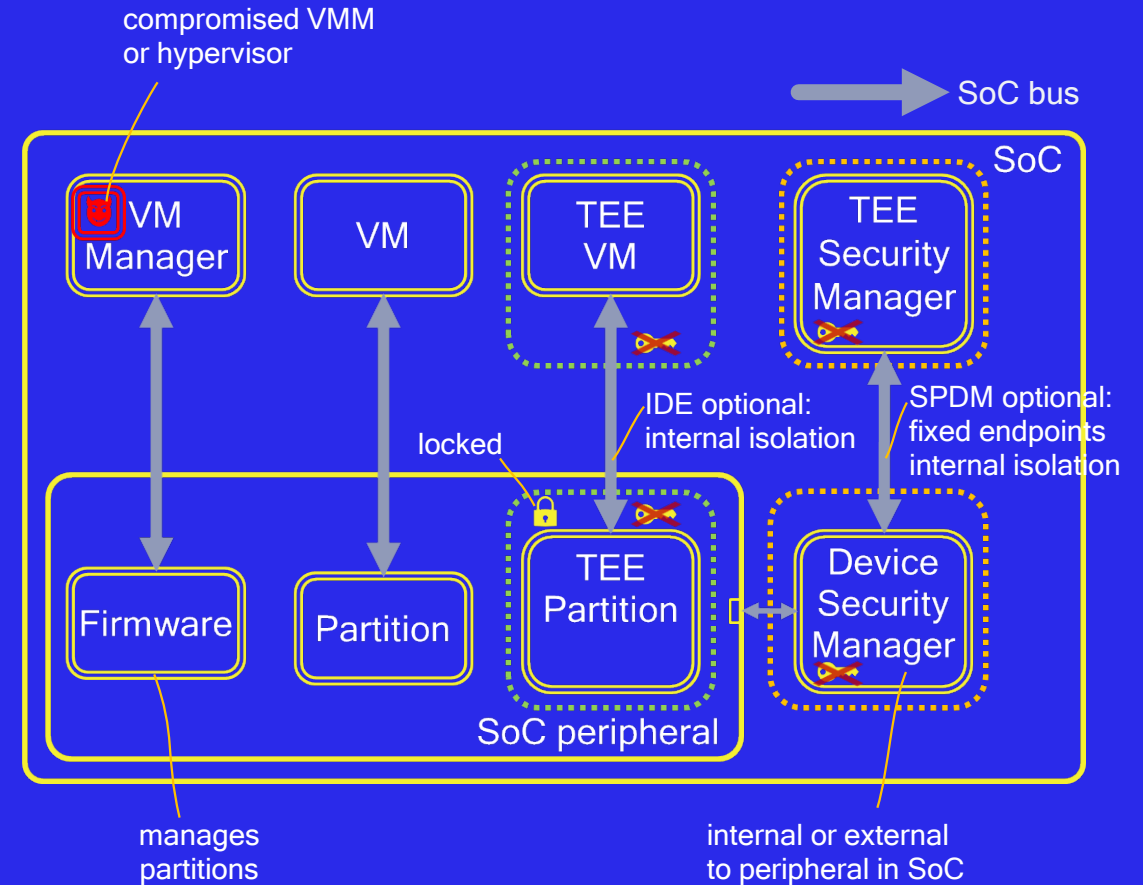
PCIe TDISP

Structure



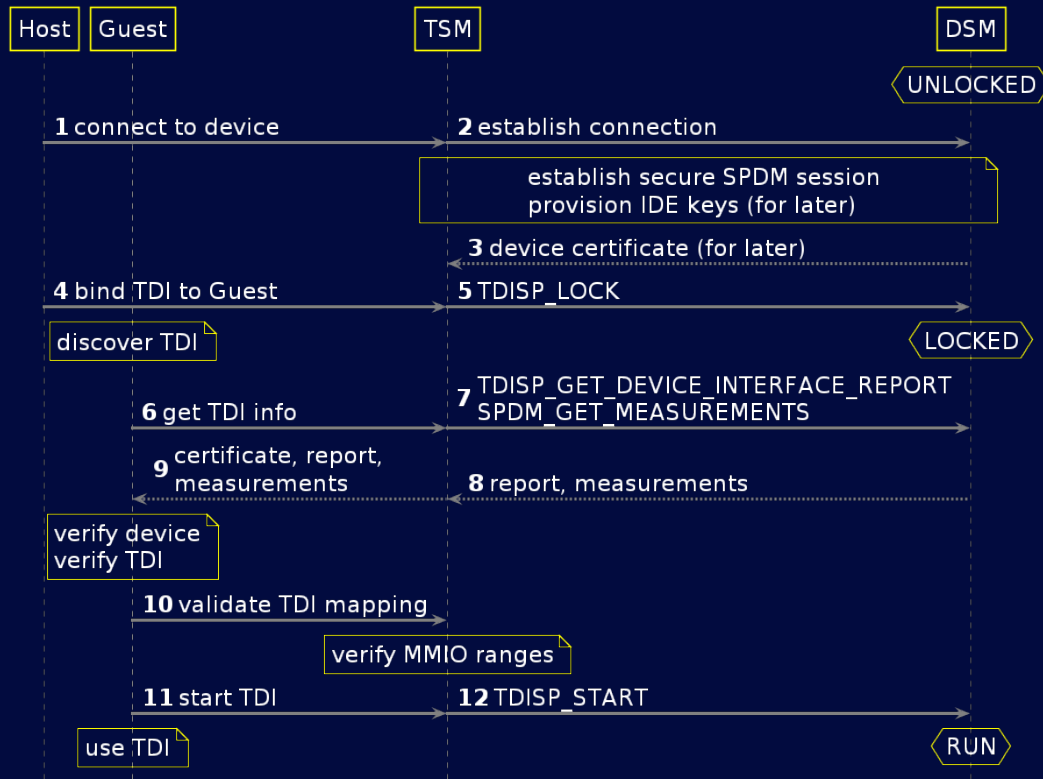
SoC peripheral TDISP

Structure



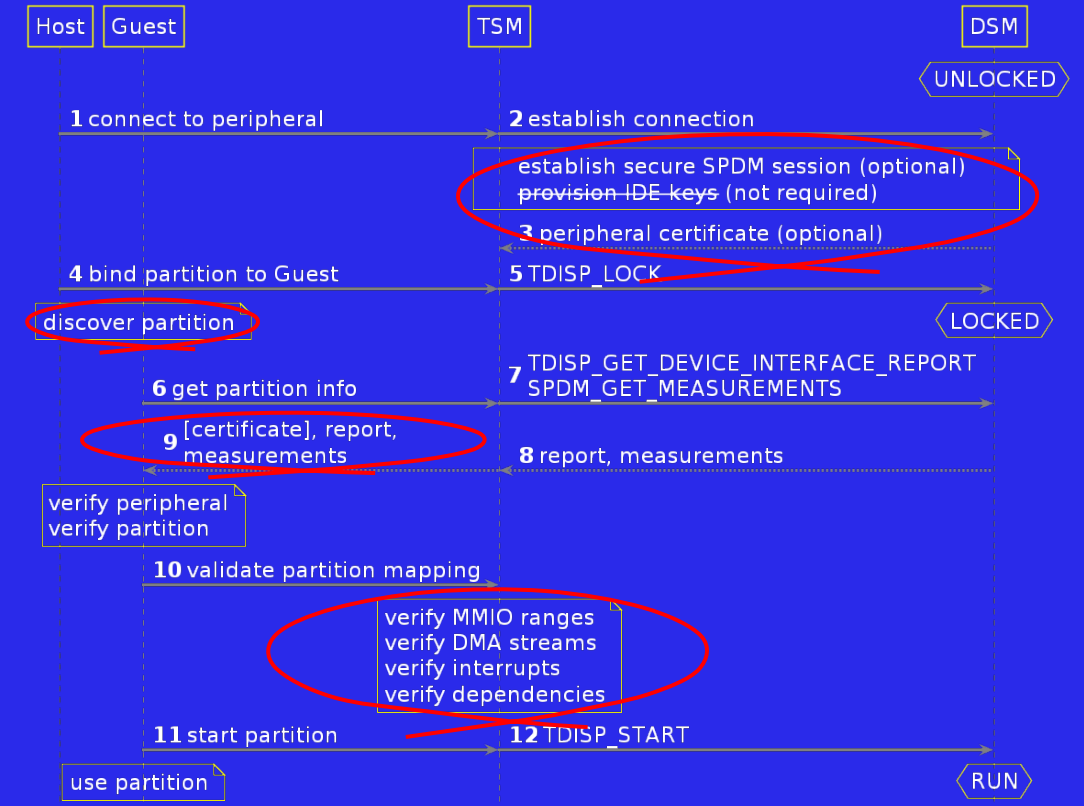
PCIe TDISP

Flow



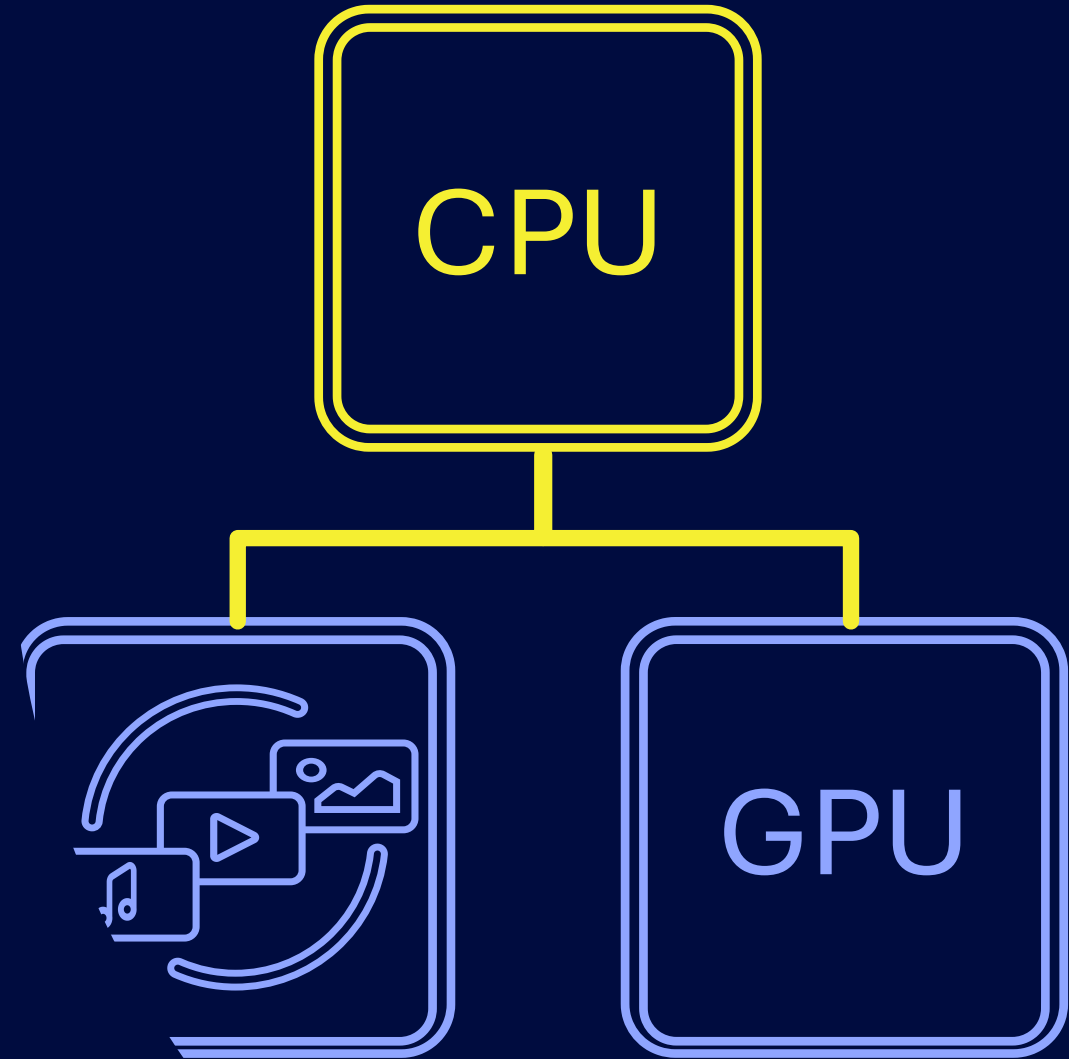
SoC peripheral TDISP

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

Nothing in these materials is an offer to sell any of the components or devices referenced herein.

© Qualcomm Technologies, Inc. and/or its affiliated companies. All Rights Reserved.

Qualcomm and Snapdragon are trademarks or registered trademarks of Qualcomm Incorporated. Other products and brand names may be trademarks or registered trademarks of their respective owners.

References in this presentation to “Qualcomm” may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes our licensing business, QTL, and the vast majority of our patent portfolio. Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of our engineering, research and development functions, and substantially all of our products and services businesses, including our QCT semiconductor business.

Snapdragon and Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries. Qualcomm patented technologies are licensed by Qualcomm Incorporated.

Follow us on: [in](#) [X](#) [@](#) [v](#) [f](#)

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

