SPDM Broker

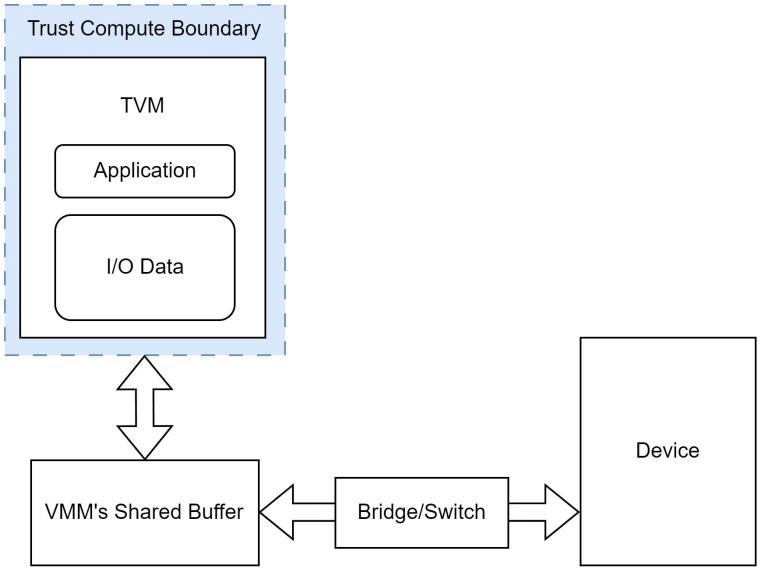
Julian Pritzi
Chair of Distributed Systems & Operating Systems

Outline

- Intel TDX TEE-I/O
  - Motivation
  - Overview
- SPDM Broker
  - Design
  - Attestation
  - Secure MMIO and DMA

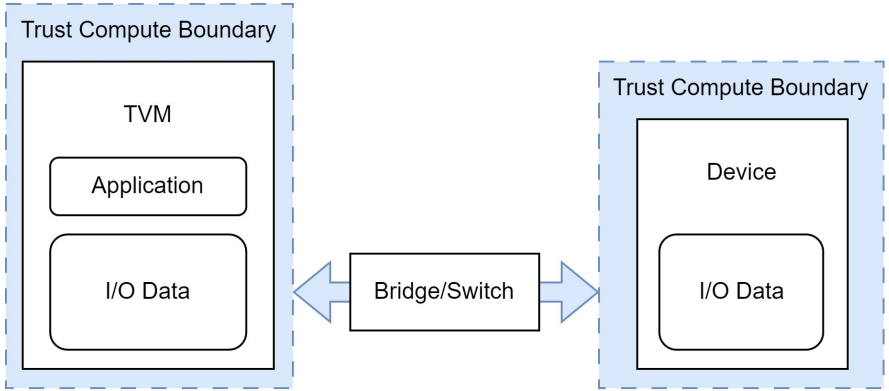
Intel TDX

- Isolated TEE VMs (TVMs)
- Untrusted VMM and devices
- How to securely use untrusted devices?
  - Encrypt data in shared buffer
  - Not possible for all types of devices



Intel TDX TEE I/O

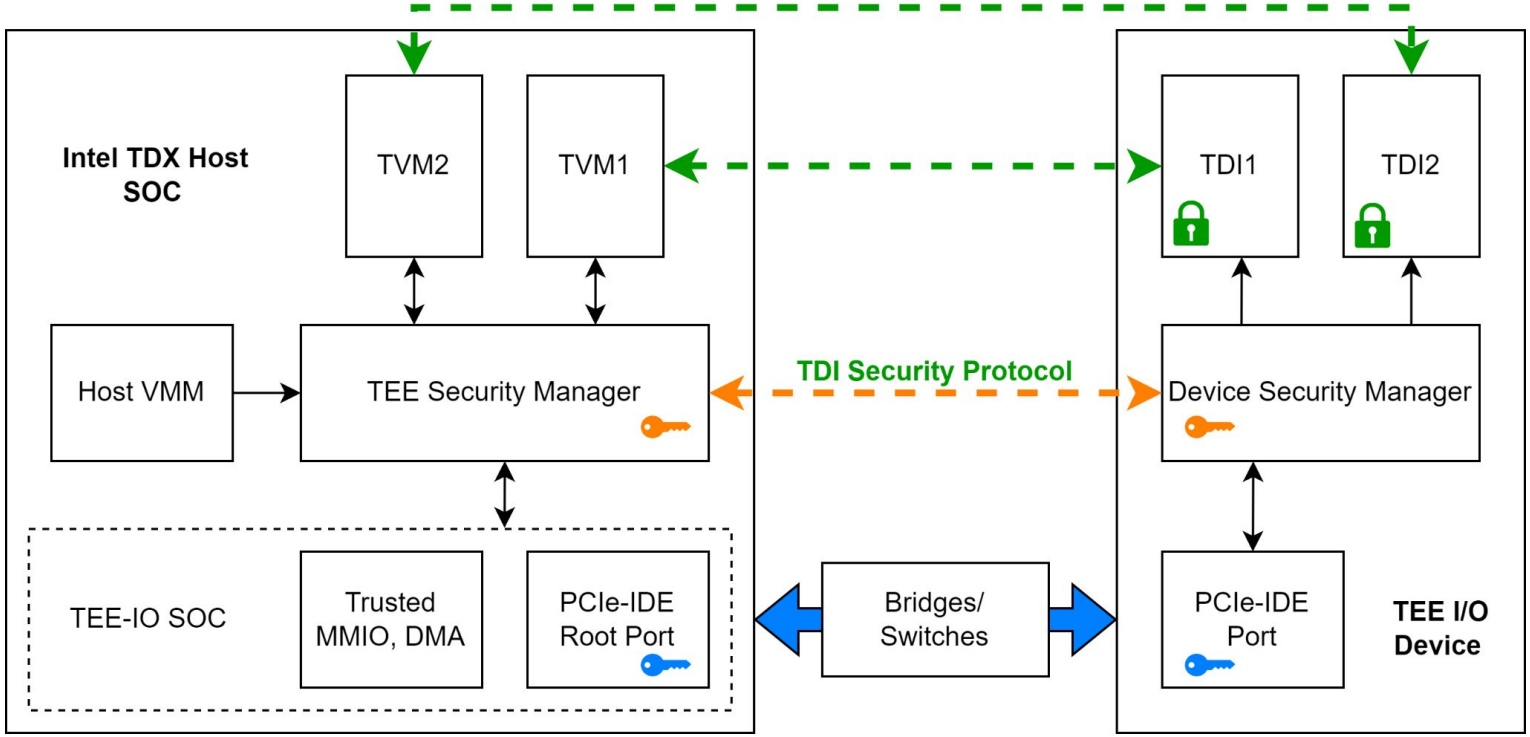
- Remove shared buffers
- Remove device specific proprietary protocol
- Using the following protocols:
  - SPDM
  - TDISP
  - PCIe IDE



Intel TDX TEE I/O - Protocols

- Security Protocol and Data Model (SPDM)
  - Authentication and provisioning of hardware identities
  - Measurements for firmware identities
  - Secure session key exchange protocol
  - In TEE I/O: Software channel for configuration of the device
- Integrity & Data Encryption (IDE)
  - Confidentiality
  - Integrity
  - Replay protection
- TEE Device Interface Security Protocol (TDISP)
  - Manages TVM to TEE Device Interface (TDI) assignment

Intel TDX TEE I/O - In detail



Intel TDX TEE I/O

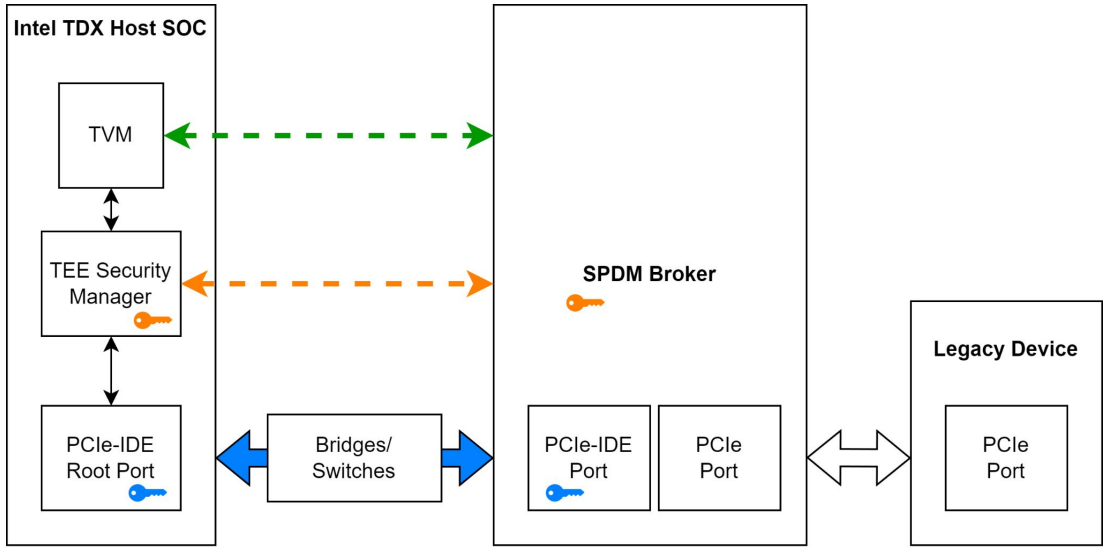
- Requires TEE I/O compatible devices
  - At least one TDI
  - Device Security Manager
  - support for selective IDE on the PCIe link

- What about devices without TEE I/O support?

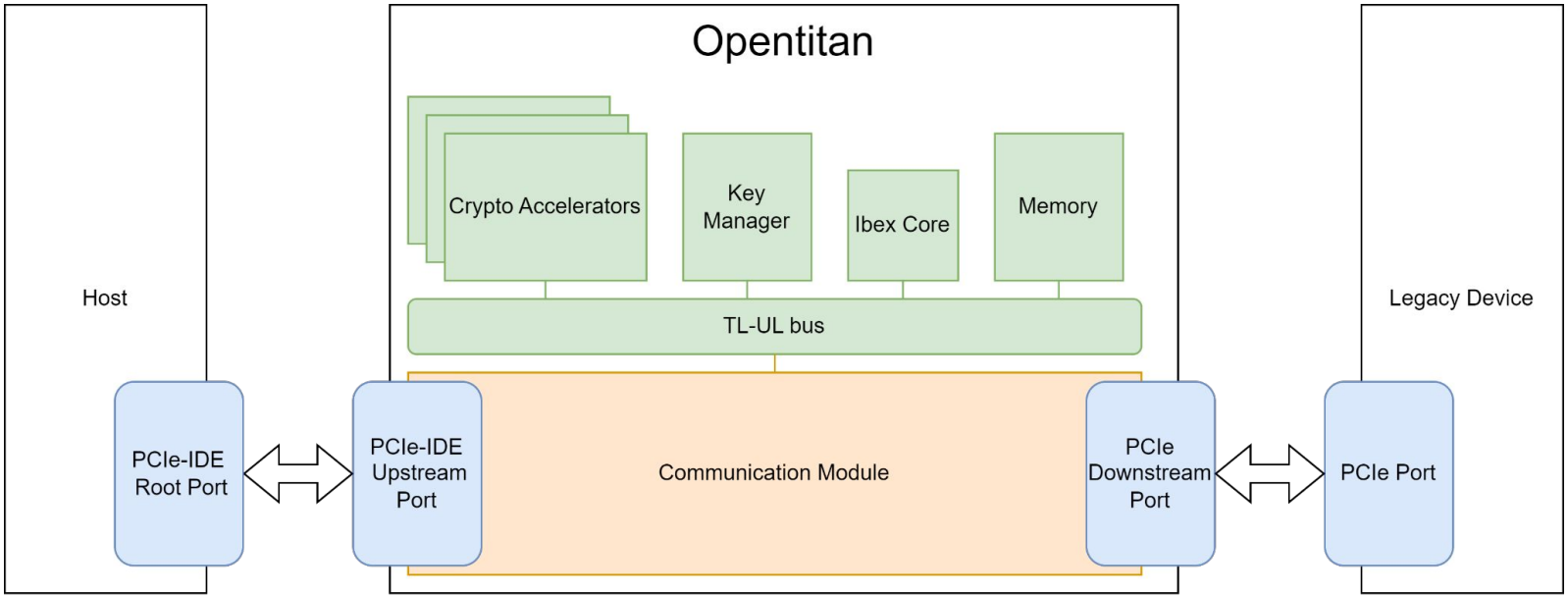
SPDM Broker: mix of PCIe switch and TEE I/O compatible device

SPDM Broker

- Sits between legacy device and host SOC
- Transparent to device
- Security guarantees for TVM ⇔ SPDM Broker
- No protection for SPDM Broker ⇔ device



SPDM Broker design



SPDM Broker requirements

- support for SPDM protocol
- support for TDISP
- support for IDE_KM
- PCIe port supporting IDE and DOE

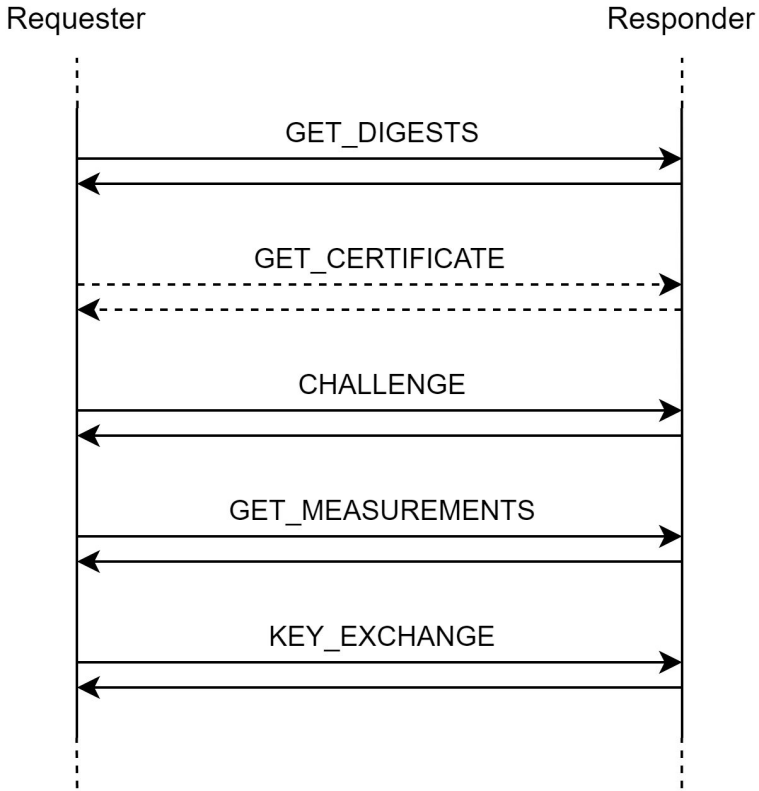
Is Opentitan a good fit for these requirements?

Functionality required for the protocols

- asymmetric cryptography algorithms
  - ECC with the NIST P256 curve ⇒ Opentitan Big Number Accelerator
- hash & measurement algorithm
  - SHA256 ⇒ Opentitan HMAC accelerator
- symmetric encryption using AES GCM
  - extend Opentitan aes accelerator's CTR mode
- compatibility with Device Identifier Composition Engine (DICE)
  - provided by Opentitan Key Manager & identities and root keys strategy

Attestation

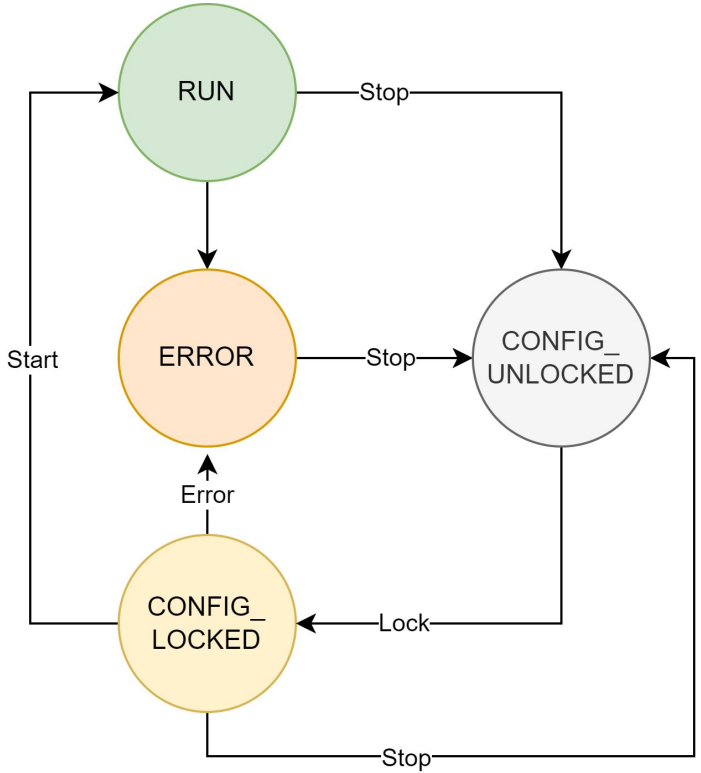
- Certificates and keys stored in opentitan
- Keys protected using Opentitan's Key Manager
- SPDM Measurements include hash of some standard device registers
  - Device ID
  - Vendor ID
  - Subsystem (Vendor) ID



SPDM attestation & key exchange

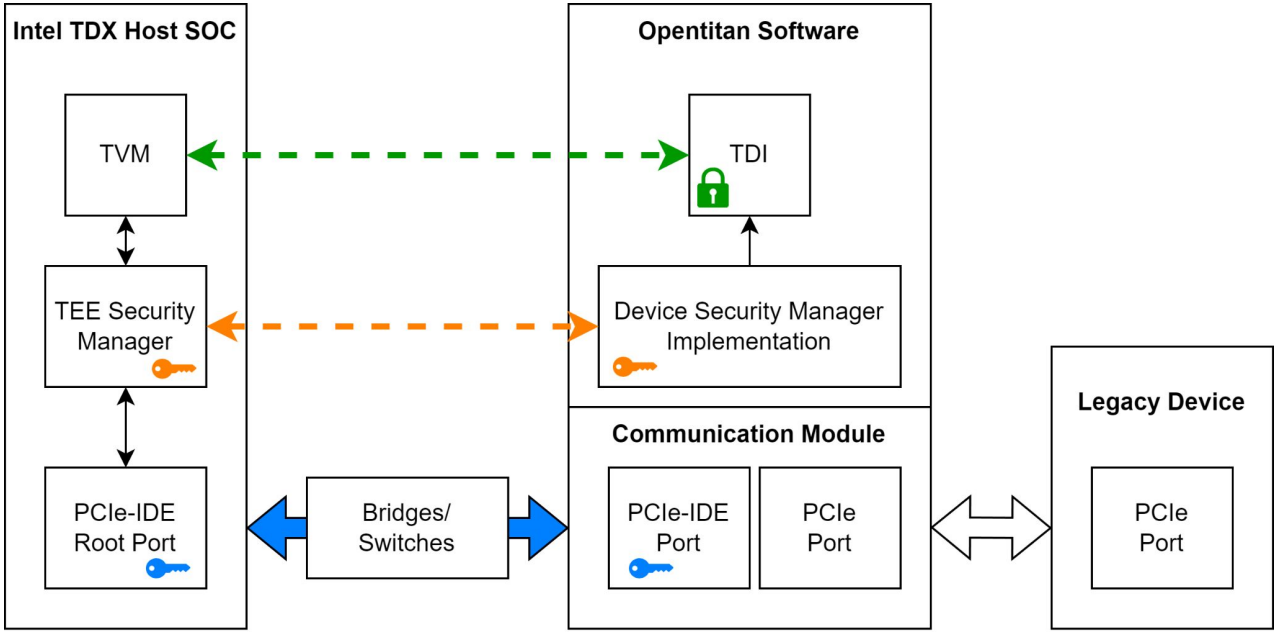
Secure MMIO and DMA

- One TDI for entire device
- Opentitan manages the TDI structure in memory according to the TDISP
- MMIO and DMA are validated against the TDI before forwarding to the device



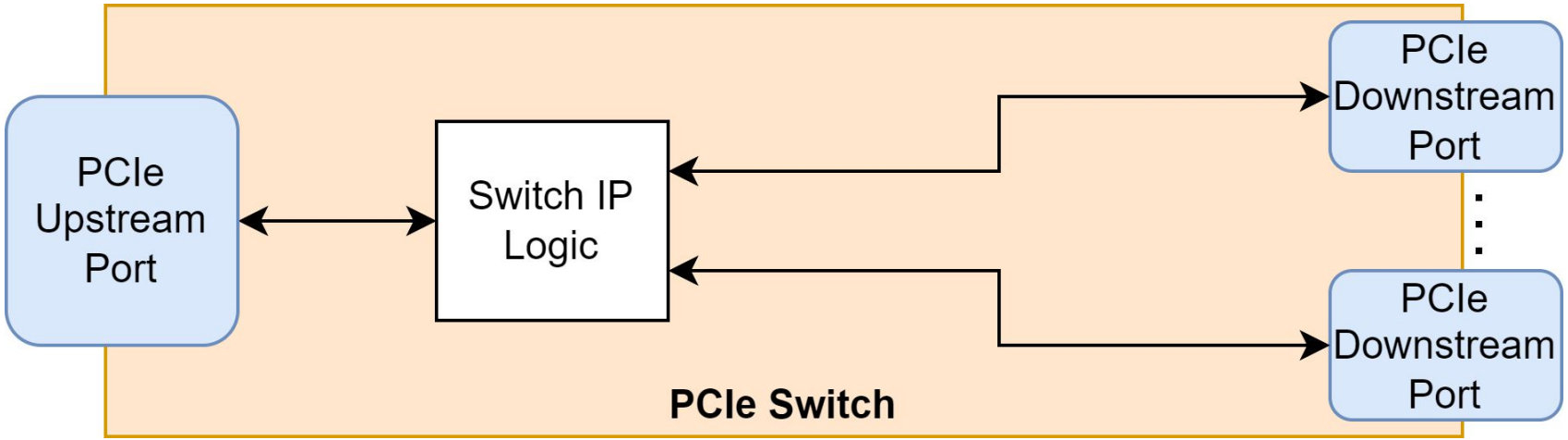
TDI configuration state transitions

SPDM Broker Overview



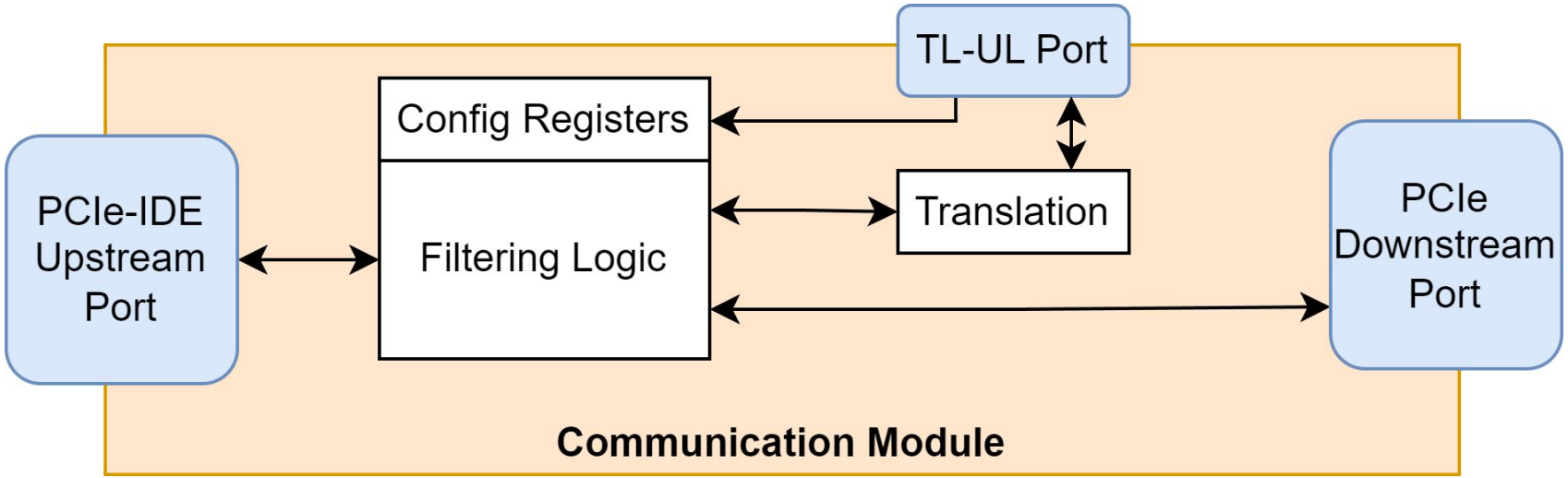
Communication Module

- Similar to PCIe Switch
  - Upstream port
  - Multiple downstream ports
  - Switching logic



Communication Module

- Filter for determining destination
  - Data Object Exchange for SPDM ⇒ TL-UL
  - Trusted MMIO & DMA access checked against filter configuration registers



Performance Estimates

- Opentitan is a potential bottleneck
  - Certificate verification: ~7ms
  - Measurement generation & signing: ~10ms
  - Encryption/Decryption of 1 KB: ~24ms ⇒ ~43kB/s
- Opentitan is only needed for configuration (SPDM, TDISP, IDE_KM)
- Performance critical MMIO and DMA access is handled by the communication module
  - Only forwarded to Opentitan if filter logic detects an invalid access

Summary

Providing TEE I/O support for legacy devices using a transparent hardware module.