TEE-I/O with TDISP and SPDM

CCC Attestation - 20230620

sameo@rivosinc.com

Rivos

I/O Virtualization

Paravirtualized (e.g. virtio)

Guest shares memory with the host VMM

Host must be trusted (VMM emulates devices)

Ubiquitous

Reduced performance

Direct Device Assignment

Device directly accesses guest memory

Host must be trusted (VMM builds IO mappings)

Limited scalability

Bare metal performance

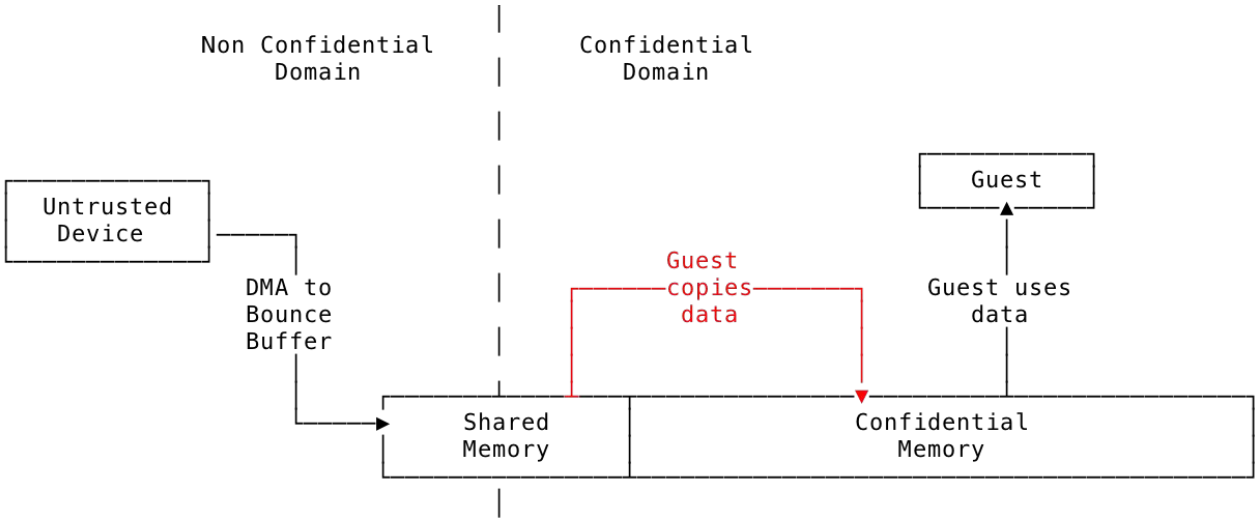
Confidential Computing Paravirtualization

Guest and host share memory bounce buffers

Guest copies from shared to confidential memory

Guest hardening

Performance is reduced further



Confidential Computing Direct Device Assignment

Let devices directly access guest confidential memory

Establish assigned devices' trustworthiness

Keep the host VMM out of the trust boundary

Maintain bare metal performance

TEE-I/O

A PCI-SIG defined architecture for:

- **Establishing trust between a physical PCI device and a confidential guest**
- **Securing the I/O path between the host and the device**
- **Attaching and detaching a PCI device to a confidential guest in a trusted manner**

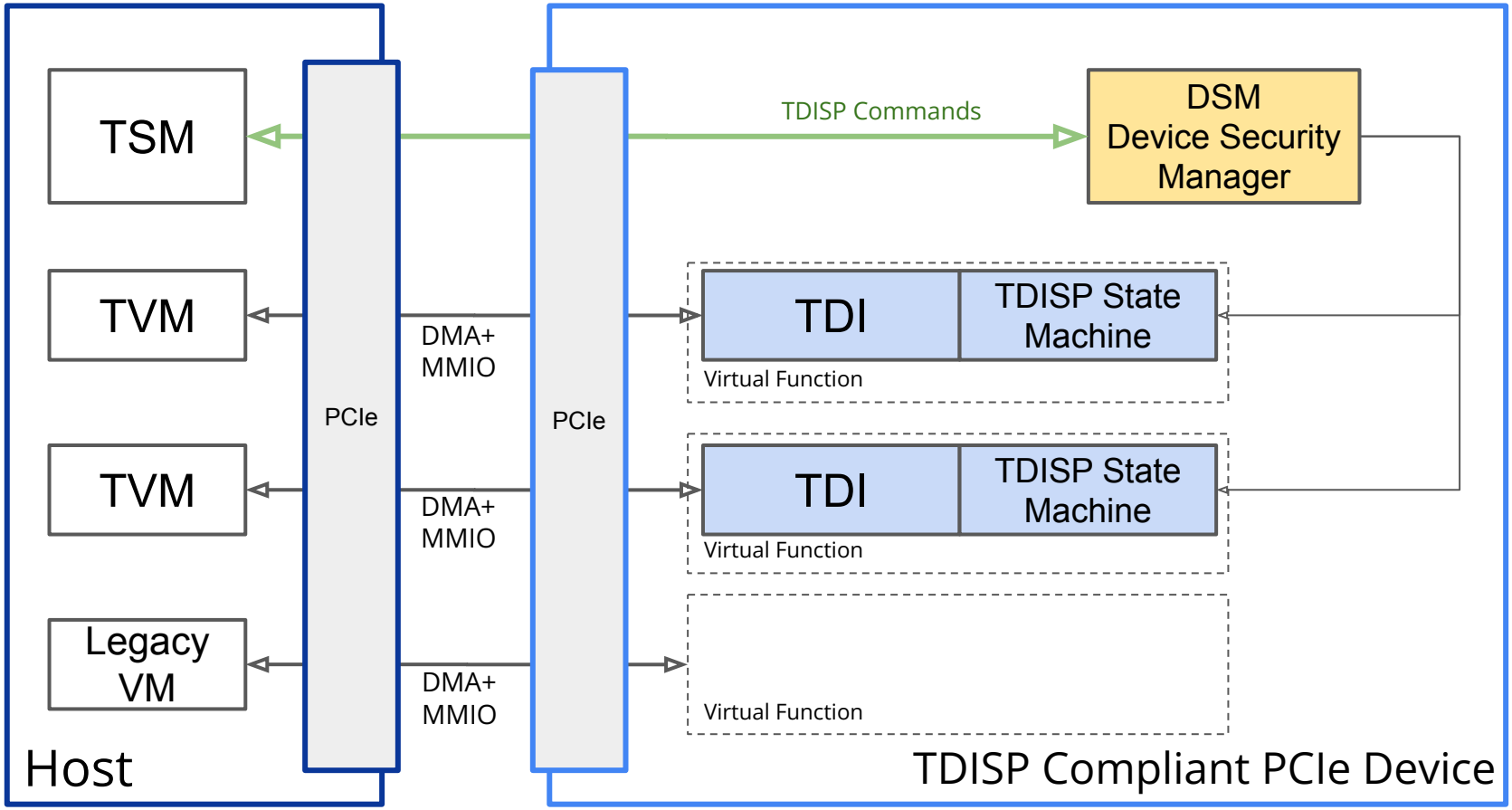
Built on top of the TDISP and SPDM protocols

TDISP - TEE Device Interface Security Protocol

- **Securely assign and reclaim devices to and from a confidential guest**
- **Secure the I/O path between an assigned PCI device and the guest**
  - Both MMIO and DMA paths
- **Defines a set of isolation and security requirements**
  - Assigned devices must protect confidential data that they hold or transfer
  - Assigned devices follow different security restrictions depending on their TDISP state
    - TDISP State Machine
  - Enforced by a Device Security Manager (DSM)
    - A piece of software running in the device
- **Provides the guest with**
  - Device certificate chain
  - Device attestation report
  - Device interface report (e.g. MMIO ranges)

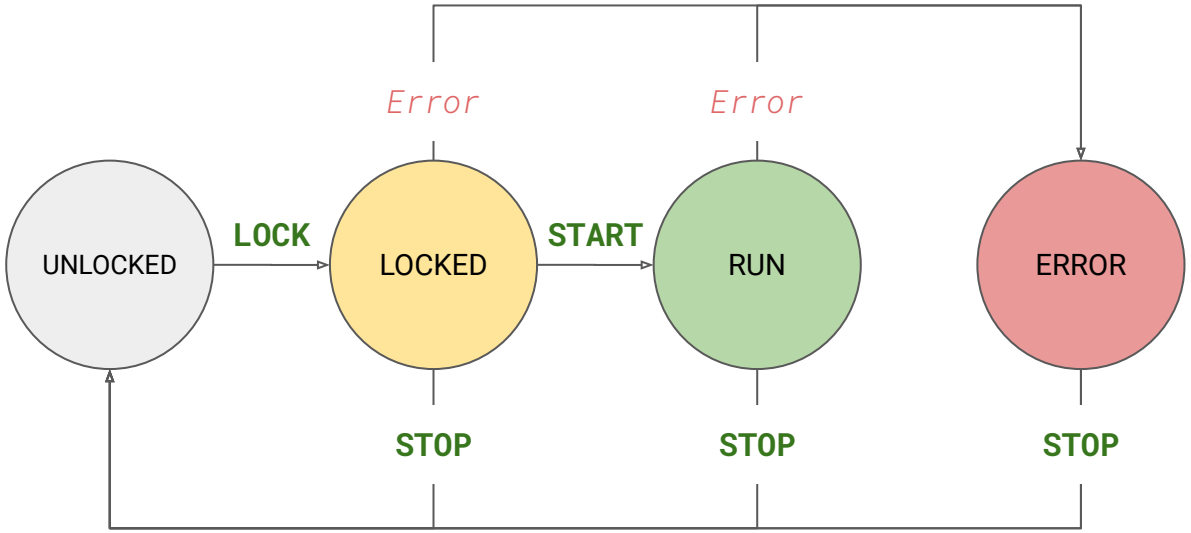
TDISP Terminology

Acronym	Definition	Description and example
TSM	TEE Security Manager	Intel TDX, AMD PSP
TVM	TEE Virtual Machine	Confidential VM
TDI	TEE Device Interface	The unit of assignment for a TEE-IO PCI device. E.g. a PCI Physical (PF) or Virtual Function (VF).
DSM	Device Security Manager	A logical/software entity running on the device. The TDISP security policy enforcer on the device, the TSM's peer in the device.


TSM
TVM
TVM
Legacy VM
Host
PCIe
DMA+ MMIO
DMA+ MMIO
DMA+ MMIO
PCIe
TDISP Commands
DSM Device Security Manager
TDI
TDISP State Machine
Virtual Function
TDI
TDISP State Machine
Virtual Function
Virtual Function
TDISP Compliant PCIe Device

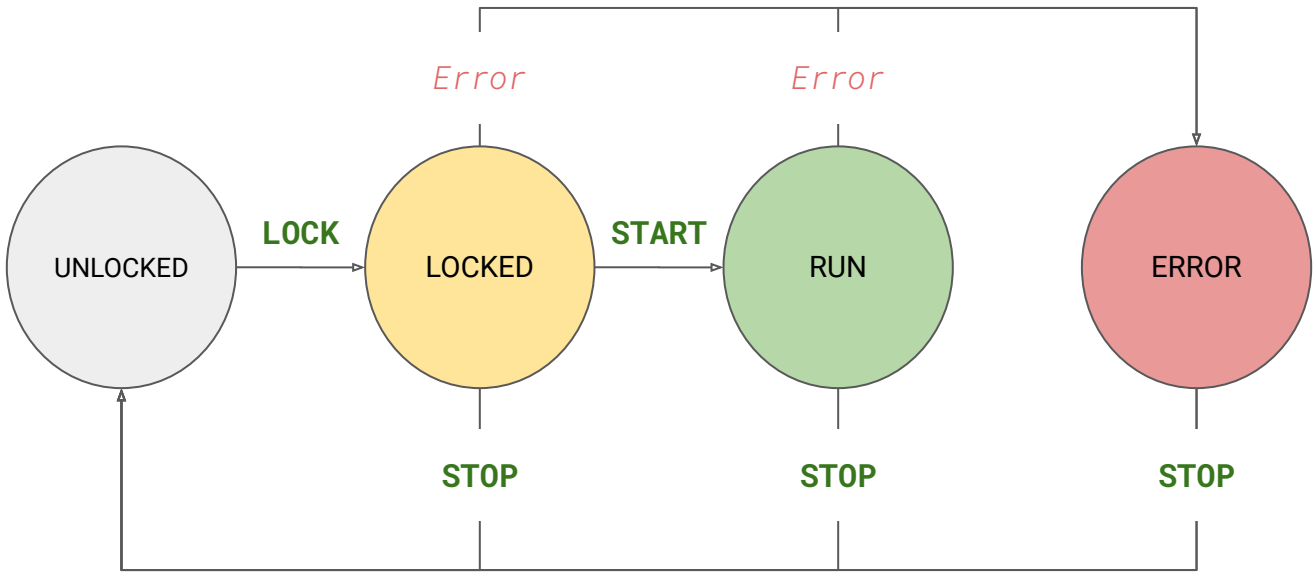
TDISP State Machine

- **One state machine per TDI**
- **State transitions**
  - TDISP command from the host
  - Device or function reset
  - Error condition

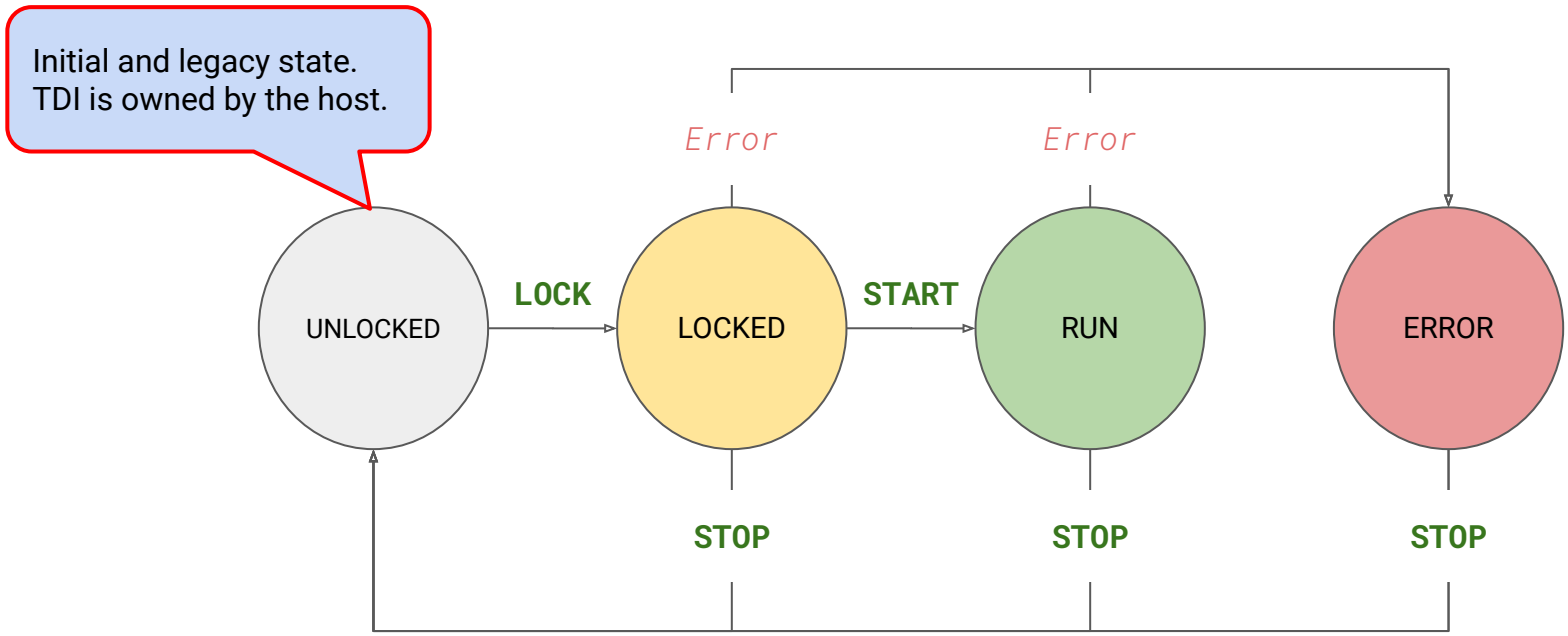


State	Device Config Changes?	DMA/MMIO	Device hold confidential data?	Usage
UNLOCKED	Yes	Yes - Not Confidential	No	Legacy
LOCKED	No	No	No	Verification by TVM
RUN	No	Yes - Confidential	**Yes**	TDI in use by guest
ERROR	No	No	**Yes**	Fatal Error - Confidential data wiped

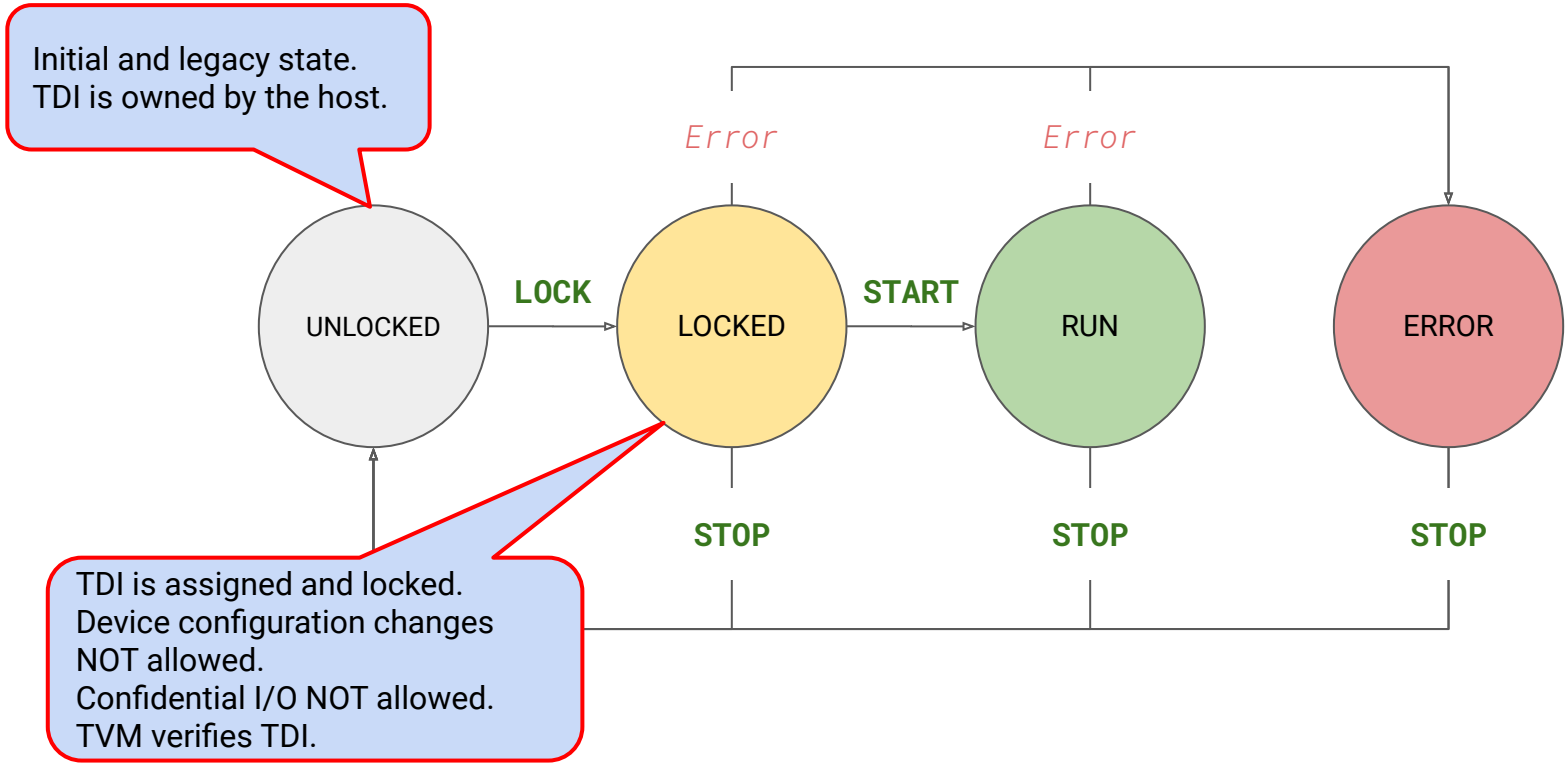
TDISP State Machine



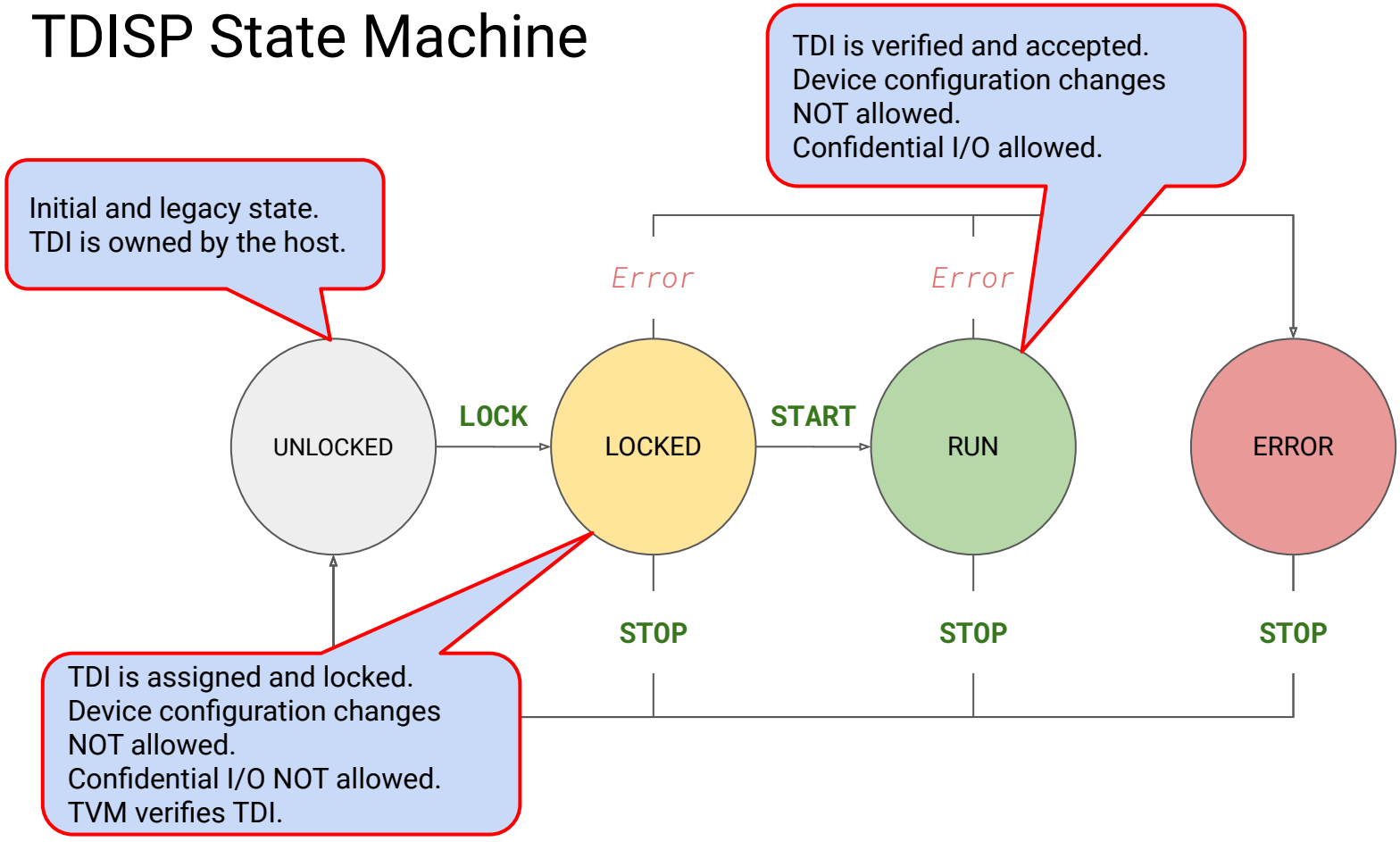
TDISP State Machine



TDISP State Machine

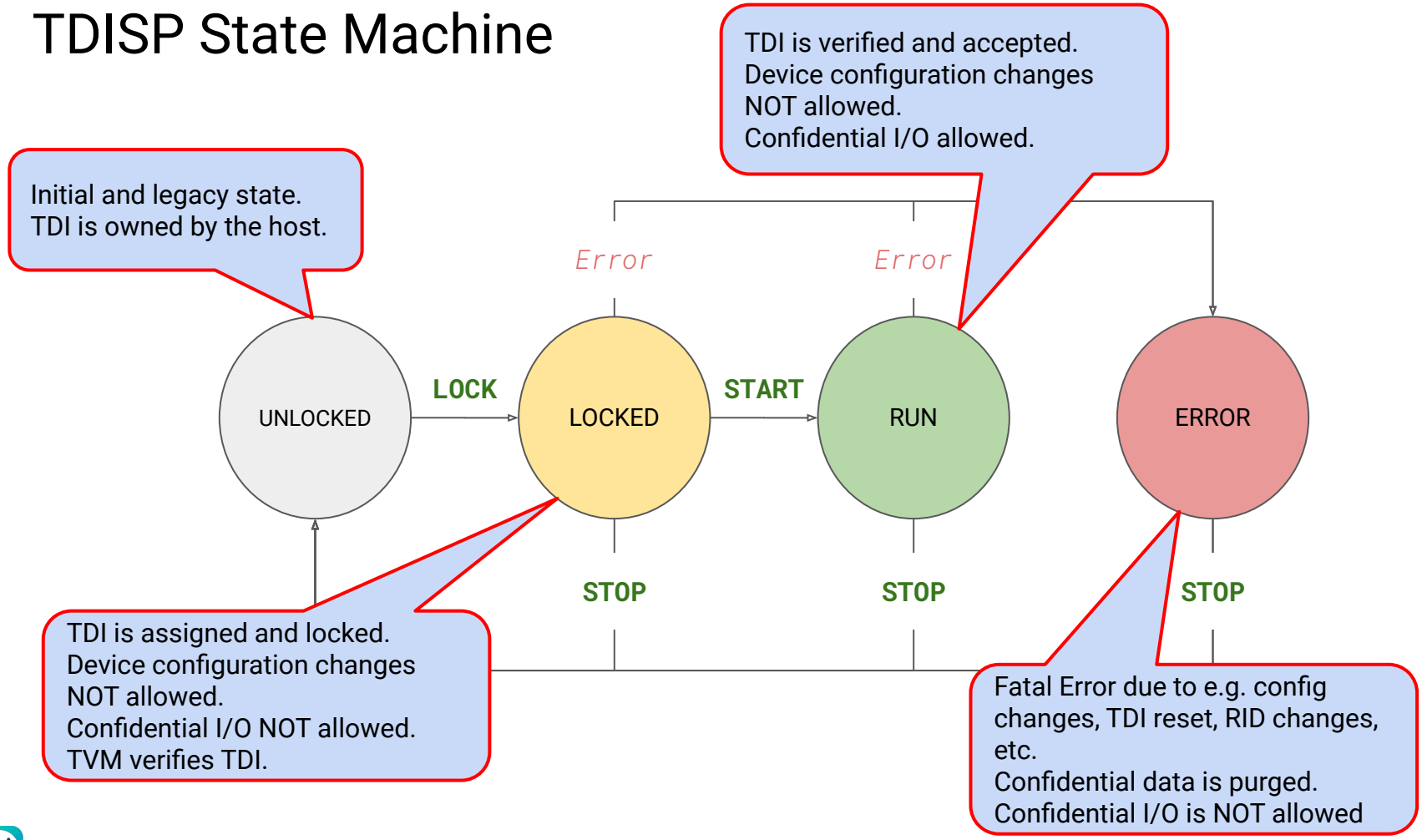


TDISP State Machine



Rivos

TDISP State Machine



Rivos

TDISP State Machine

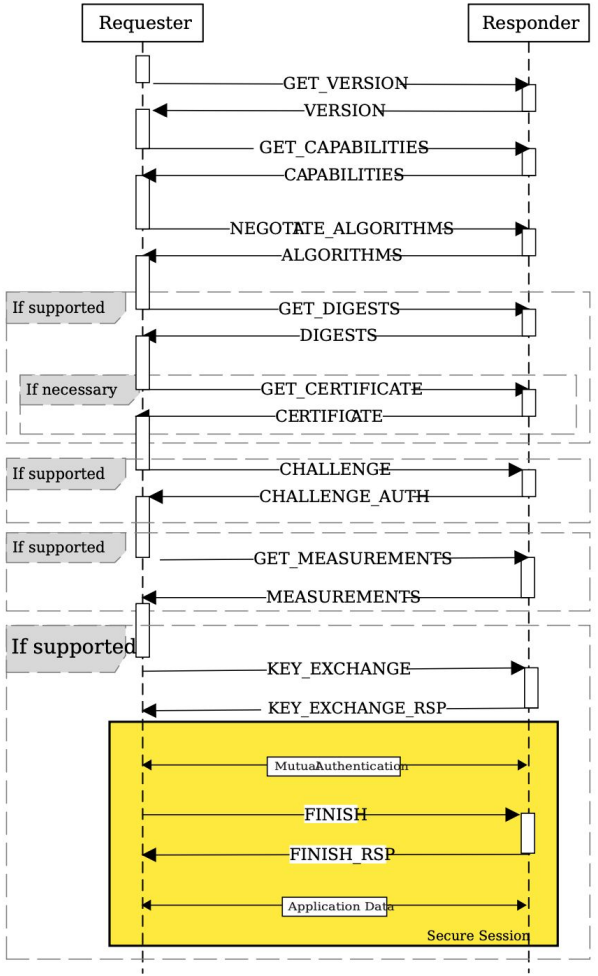
- **LOCKED**
  - Triggered by the TSM, when the host attempts to assign the TDI
  - Guest verifies the TDI
    - Are MMIO ranges set according to the TDI interface report?
    - Is the physical link secured (PCIe IDE)?
    - Is the device trustworthy?
    - Yes, Yes and Yes → Accept TDI → Transition to RUN
- **RUN**
  - Guest explicitly accepts the device and notifies the TSM
  - Transition from LOCKED to RUN triggered by the guest, through the TSM

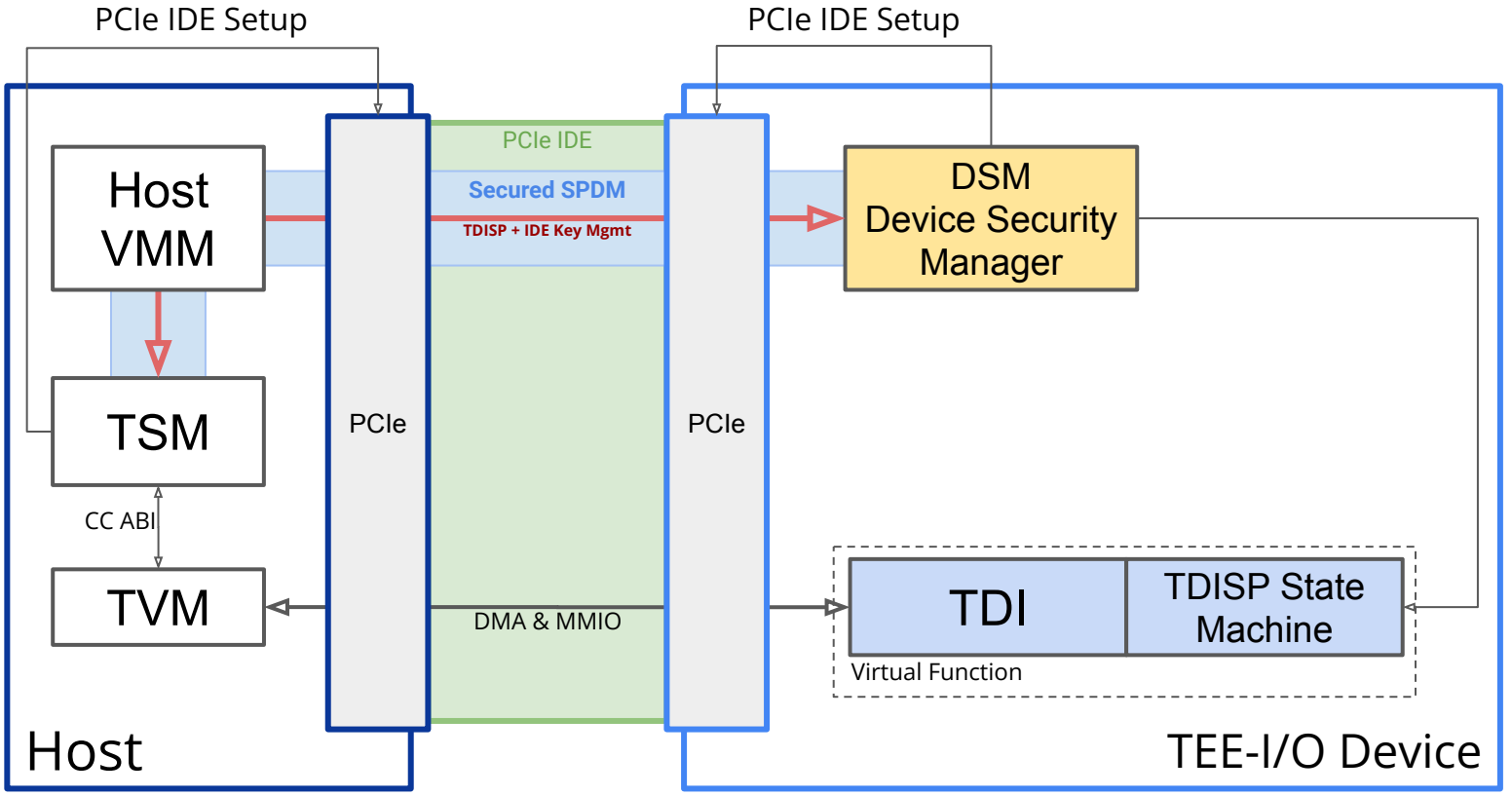
TDISP and SPDM

- **How can a TVM trust a device?**
- **How can TDISP commands be securely transported?**
- **DMTF Secure Protocol and Data Model (SPDM)**
- **SPDM provides**
  - Device attestation and authentication
  - Secure communication channel through an untrusted proxy (e.g. the host VMM)

TDISP and SPDM

- **TDISP requires SPDM**
- **TSM is the requester, DSM is the responder**
- **TSM authenticates the device**
  - GET_CERT + CHALLENGE
- **Secured SPDM session established between the TSM and the DSM (DHE)**
  - Untrusted host is the proxy
  - One SPDM session per device, for all TDIs.
- **TDISP requests and responses transported over Secured SPDM**
  - PCIe IDE Key Management as well




PCIe IDE Setup
PCIe IDE Setup
Host
VMM
TSM
CC ABI
TVM
PCIe
PCIe IDE
Secured SPDM
TDISP + IDE Key Mgmt
DMA & MMIO
PCIe
DSM
Device Security
Manager
TDI
TDISP State
Machine
Virtual Function
Host
TEE-I/O Device

Device Attestation

- **SPDM provides the device attestation Evidence**
  - GET_CERTIFICATE response
    - Device certificate chain
    - DICE devices may include DiceTcbInfo or CWT extensions
  - GET_MEASUREMENTS response
    - Device replies with multiple measurement blocks
    - DMTF specific format
- **TSM and DSM are the attesters**
- **Local Attestation**
  - TVM is the Verifier
    - Static or runtime provisioning
- **Remote Attestation**
  - As part of the TVM attestation