Overcoming Verification Hurdles in IDE and TDISP Systems

Gaurav Manocha
Sr Staff Engineer
Synopsys

Agenda

- IDE:
  - What is IDE and Why?
  - IDE Streams
  - Encryption using IDE
  - TLP Aggregation
  - Verification Scenarios

- TDISP:
  - Why TDISP
  - Architecture
  - State Machine
  - Verification Scenarios

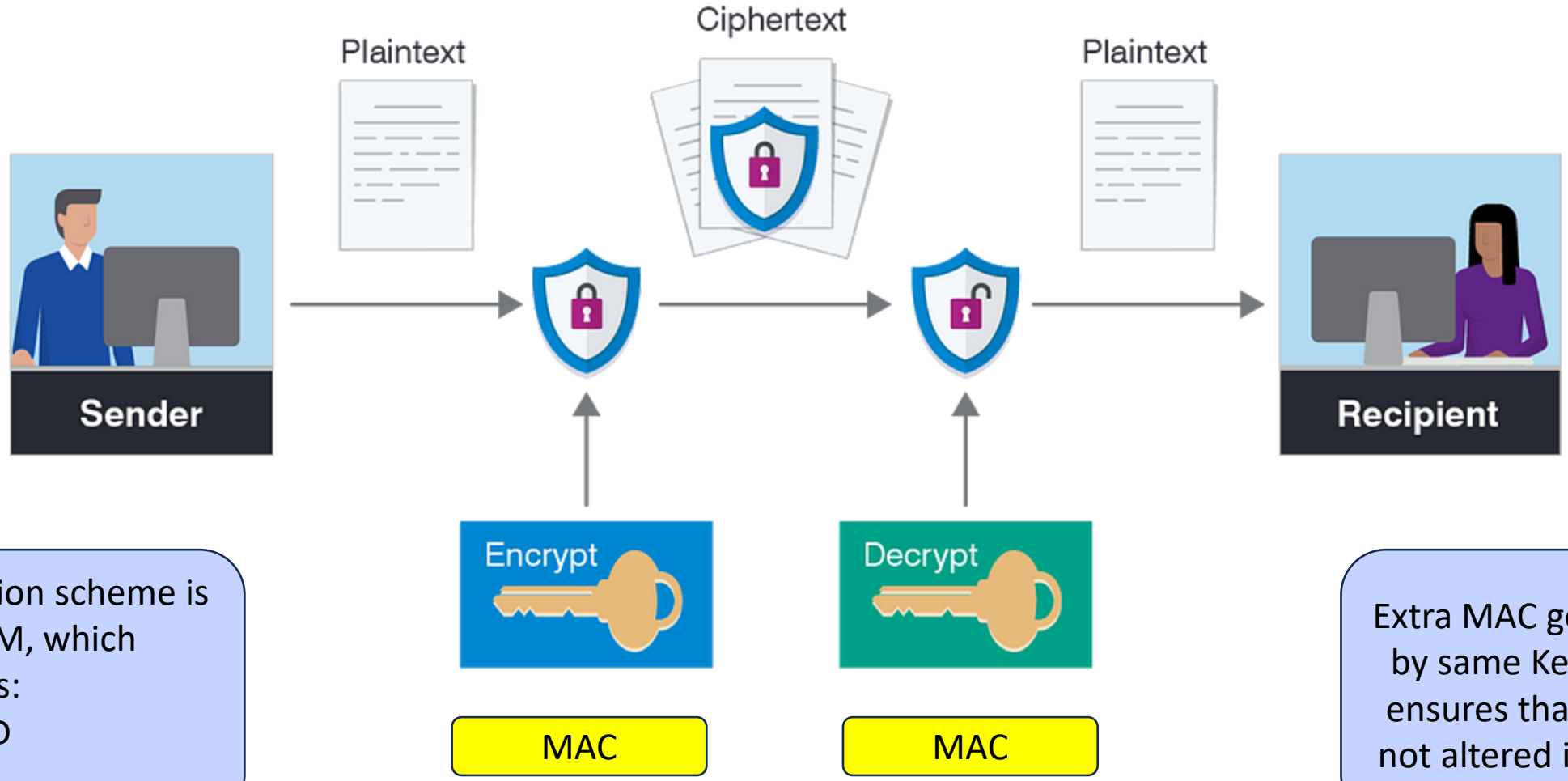
IDE

Integrity & Data Encryption

What is IDE

- IDE is a security feature which provides:
  - Confidentiality
  - Integrity
  - Replay protection of TLPs
- Provides security against various kinds of physical attacks such as
  - purpose-built interposers
  - malicious Extension Devices like switch or Retimer
- IDE Key Management used to setup Keys
- IDE KM is protected by SPDM Secure Session

IDE Flow



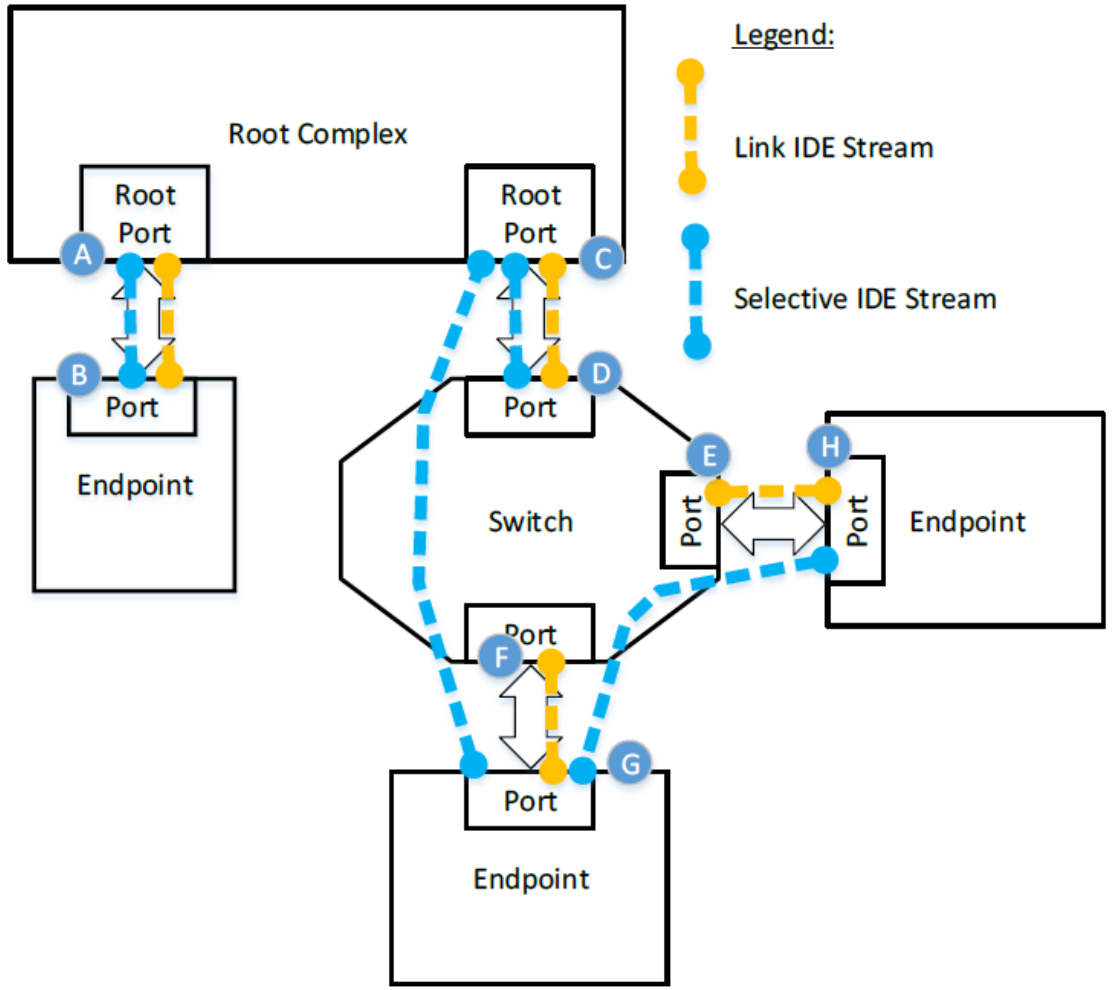
Encryption scheme is AES-GCM, which provides:

- AEAD
- MAC

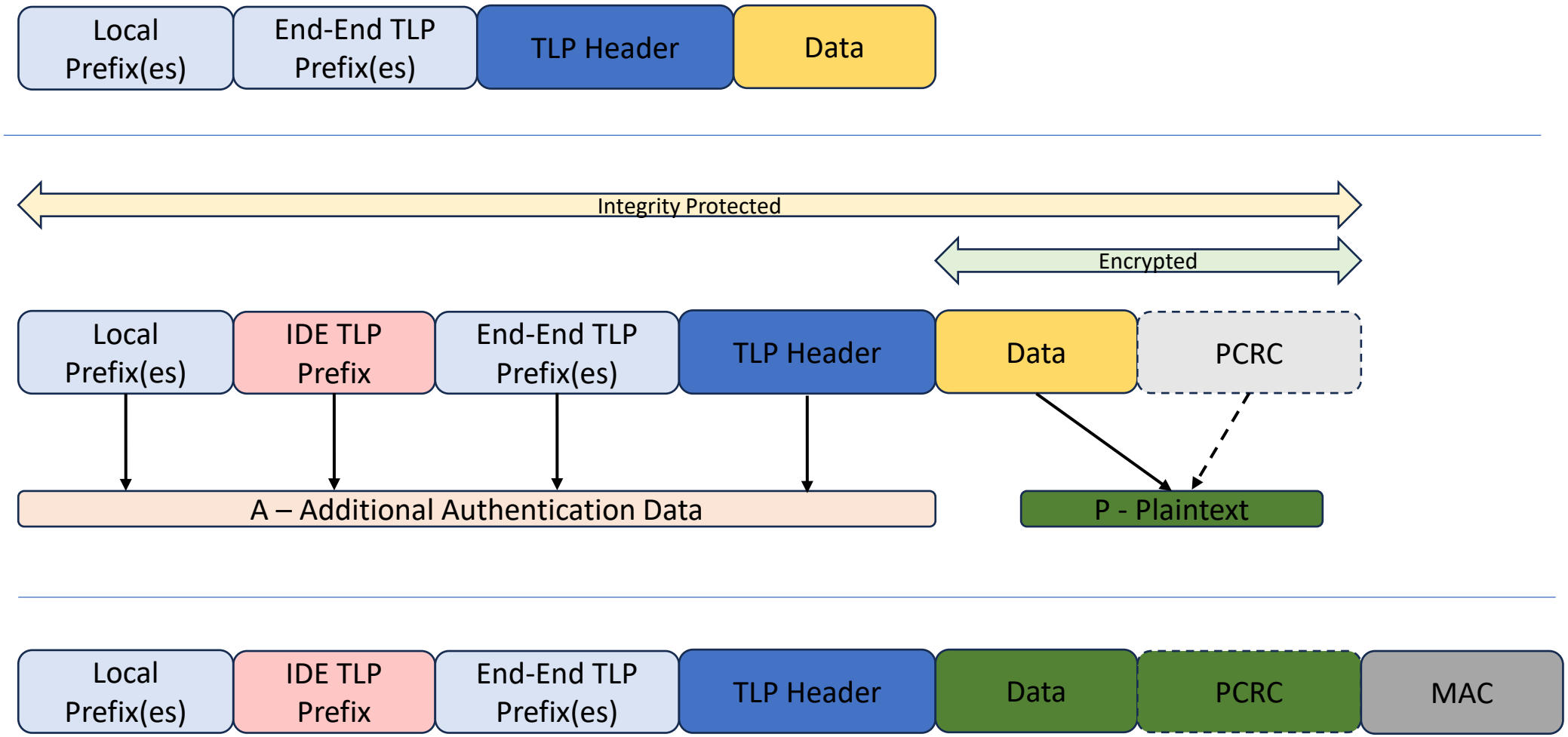
Extra MAC generated by same Key which ensures that data is not altered in transit

IDE Streams

- Link IDE Stream
  - Secure IDE TLPs between two directly connected ports
  - All TLPs are encrypted
- Selective IDE Stream
  - Secure IDE TLPs between two ports flow through switches/bridges
  - Only selective TLPs encrypted based on:
    - Address range
    - Routing ID range



TLP Encryption using IDE



TLP Aggregation

- To reduce per-TLP overhead for IDE TLP MAC
- Can be applied to TLPs withing same stream and Sub-stream
- Permitted to transmit other TLPs that are not part of Sub stream between TLPs of aggregated unit

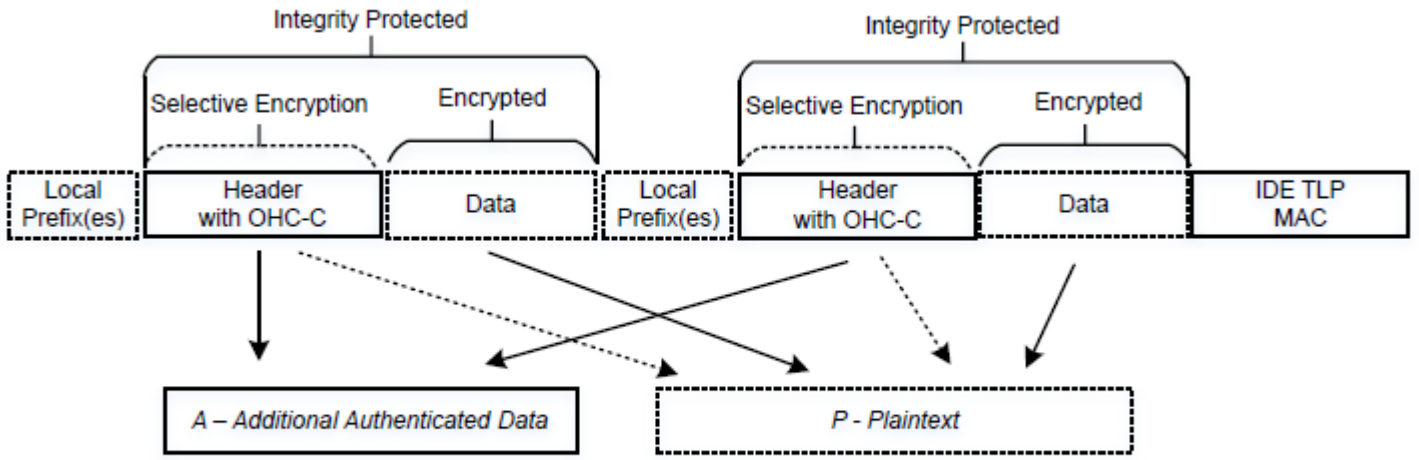


Figure 6-73 IDE TLP – Example Showing Aggregation of Two TLPs for a Selective IDE Stream (Flit Mode) §

IDE Verification Scenarios

- Aggregation
  - Validate that TLPs from an aggregated unit are correctly interleaved with IDE and non-IDE TLPs from other Streams without violating ordering or integrity constraints
- K Bit Toggling
  - Validate K Bit functionality and ensure that only intended sub stream utilizes updated key after toggling K Bit for that specific sub stream
- Selective IDE Rules
  - Only particular TLP types are permitted for a Selective IDE Stream
  - Ensure that IO Read/Write TLPs are not generated or accepted for Selective IDE Streams, as these TLP types are explicitly disallowed

TDISP

TEE Device Interface Security Protocol

What is TDISP

- TEE Device Interface Security Protocol (TDISP)
  - Specialized protocol builds on IDE to enable secure, authenticated, and isolated communication between TEEs and PCIe devices
  - Implement Security measures to isolate TVM
  - Secure confidential data of TDI

- How it is different from IDE:
  - IDE secures data path between two ports
  - TDISP goes beyond IDE by securing device-specific control interfaces and not only just data paths
  - Ensures only authorized TEEs can access or control specific device functions

- Legend:
  - TEE : Trusted Execution Environment
  - TDI : TEE Device Interface
  - TVM: Trusted Execution Environment VMs

Architecture of TDISP

- TSM:
  - Provide interfaces to the VMM to assign memory and TDI resources to TVMs
  - Implements the security mechanisms
  - Manage TDI states
  - Establishing IDE encryption keys
- DSM:
  - Authentication of device
  - IDE key configuration
  - TDI management & tracking
  - Isolate TVM provided data from entities not in the TCB

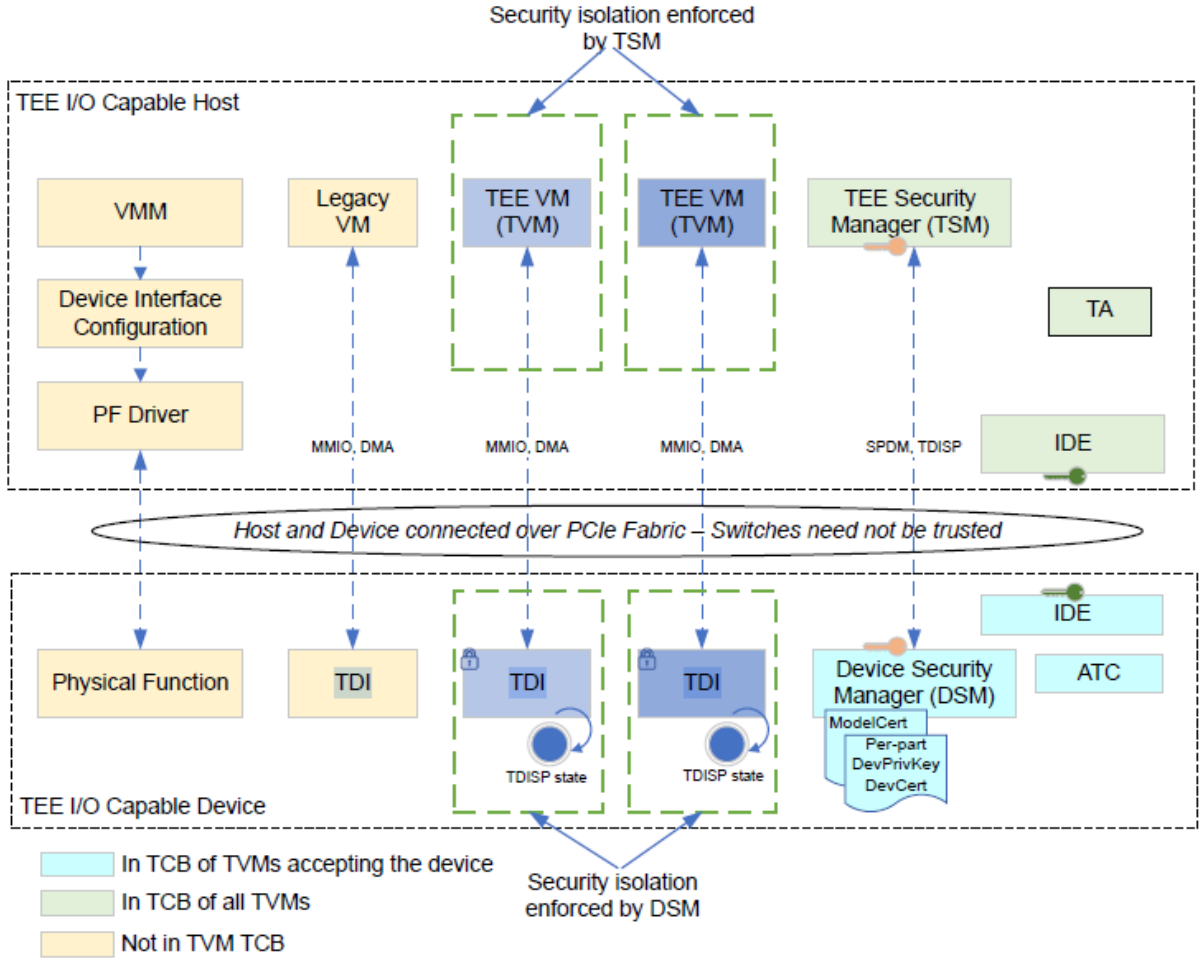


Figure 11-2 TDISP Host/Device Reference Architecture §

State Machine of TDISP

- CONFIG_UNLOCKED:
  - Default State
  - VMM configures TDI to be assigne to TVM
- CONFIG_LOCKED:
  - VMM requests TSM to lock TDI
- RUN:
  - TDI resources are operational and permitted to be managed by TVM
- ERROR:
  - Move to this state in case of any security breach

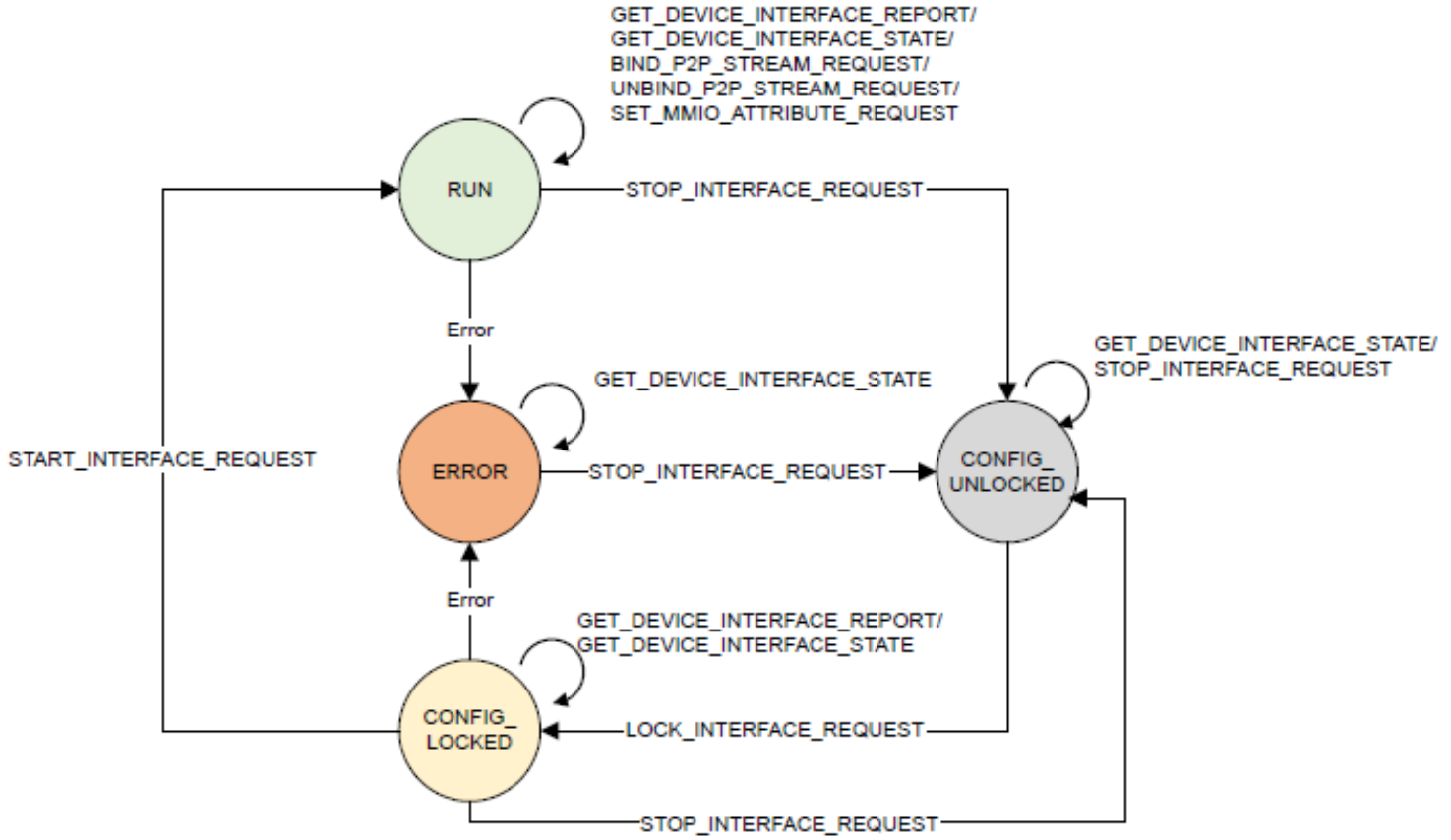


Figure 11-5 TDISP State Machine §

TDISP Verification Scenarios

- DSM Tracking: Cfg Space Registers
  - Validate that any attempt to modify configuration space registers (e.g., Device Control/2/3) while the TDI is in CONFIG_LOCKED or RUN state results in the TDI transitioning to an error state

- Function Level Reset (FLR) – Validate transition to ERROR state
  - FLR on VF transitions corresponding TDI to ERROR state
  - FLR on PF transitions all VF TDIs from CONFIG_LOCKED or RUN to ERROR state

- TEE_MEM/NON_TEE_MEM Rules: Validate below
  - For Non-TEE-MEM, TLPs are processed normally regardless of TDI state or T-bit
  - For TEE-MEM, only T-bit set TLPs are processed in RUN state; others must be Dropped or Completed with UR

Summary

- IDE
  - Ensures data confidentiality and integrity across PCIe/CXL links
  - Operates per Traffic Class (TC) and stream
  - Enforced via stream associations using Stream IDs
  - Secured using SPDM session and negotiated keys

- TDISP
  - Goes beyond IDE by securing device-specific control interfaces (not just data paths)
  - Integrates with IDE + SPDM to create complete secure PCIe/CXL communication flow
  - Enforces runtime checks and transitions via a well-defined TDISP state machine
  - Guarantees only authorized TEEs can control or access device functions (via TDIs)

References

- PCIe® 7.0 Specification, Version 0.9
- IDE and TDISP: An Overview of PCIe® Technology Security Features | PCI-SIG