CXL Security Stack Verification and its Challenges

Richa Gupta

Senior Engineering Manager, Siemens EDA

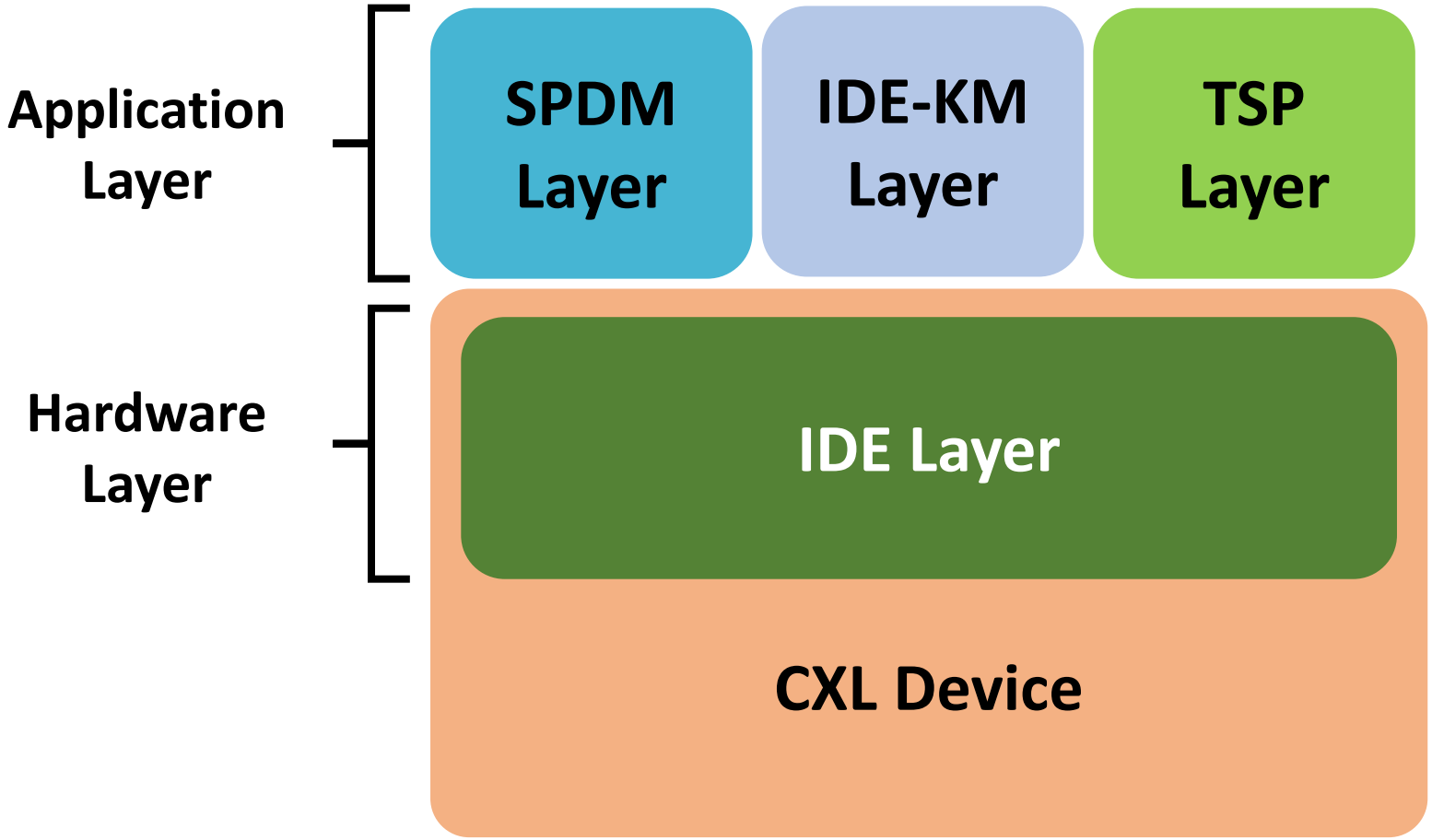
Agenda

- Security Overview
- Security Stack Structure
- Security Process Flow
- Challenging Verification Scenarios
- Summary

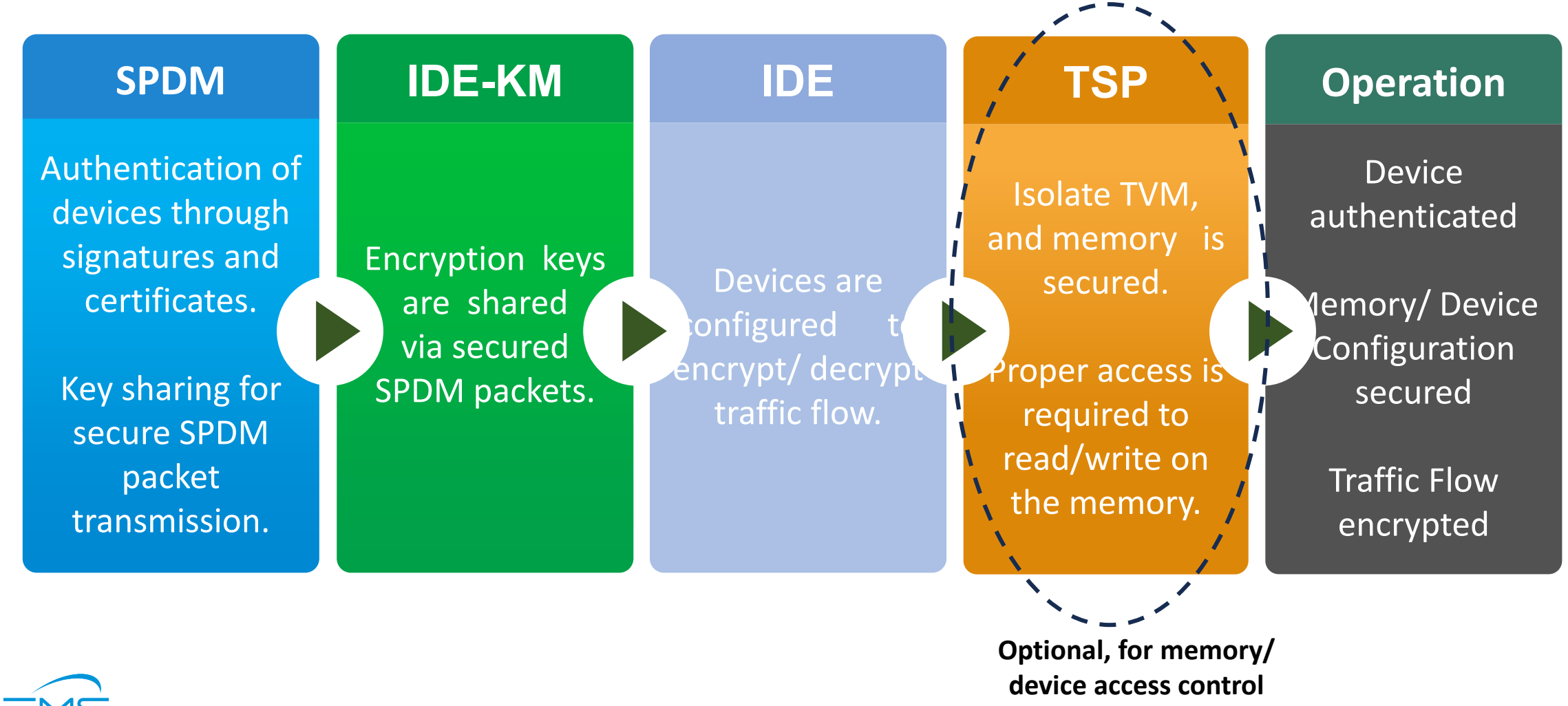
Security Overview

CMA	Authentication Establish trust relationship
IDE-KM	Sharing of Encryption keys via secured environment
IDE	Secure Data path between Host and Device Provide encryption
TSP	Implement Security mechanism to isolate TVM Secure confidential data of CXL Memory Device

Security Stack Structure



Security Process Flow



Challenging Verification Scenarios

- Reset:
  - Conventional Reset: IDE Insecure, Terminate SPDM session
  - CXL Reset : IDE Insecure, TSP in Config Locked moves to ERROR state
  - FLR : No effect on CXL.Cachmem IDE state or CXL.cachemem keys or TSP state
- IDE.Start after Conventional Reset:
  - Scenario:
    - Program the keys and send K_SET_GO.
    - Conventional Reset.
    - Send IDE.start without re-programming the keys Or, sending K_SET_GO again.
- IDE.Start on an active stream without reprogramming the keys

Challenging Verification Scenarios

- Initiate CXL_IDE_KM messages interleaved with IDE_KM messages to configure both CXL.IO and CXL.Cachemem keys. Then initiate CXL.cachemem and CXL.io traffic and check for write read data matching.
- Send K_SET_GO in an IDE stream already active with different value of IDE mode

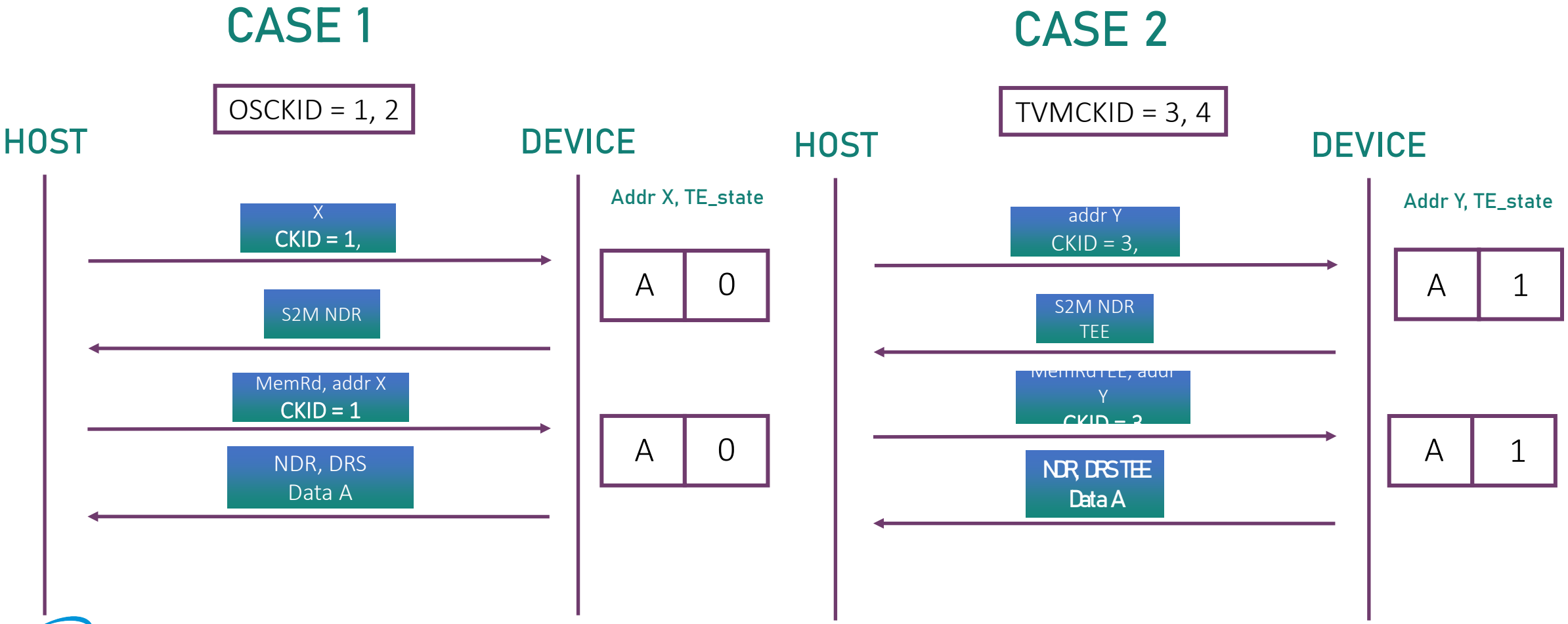
Challenging Verification Scenarios

- It is also permissible for the transmitter to send an IDE.Start after the MAC epoch ends but before the corresponding MAC header is transmitted. In this scenario, the receiver must use the old keys to decrypt the message and to check the MAC.
  - Scenario:
    - Transmit a Mac Epoch
    - Switch the keys by sending IDE.Start.
    - Transmit MAC for previous Epoch – should be encrypted/decrypted using new keys

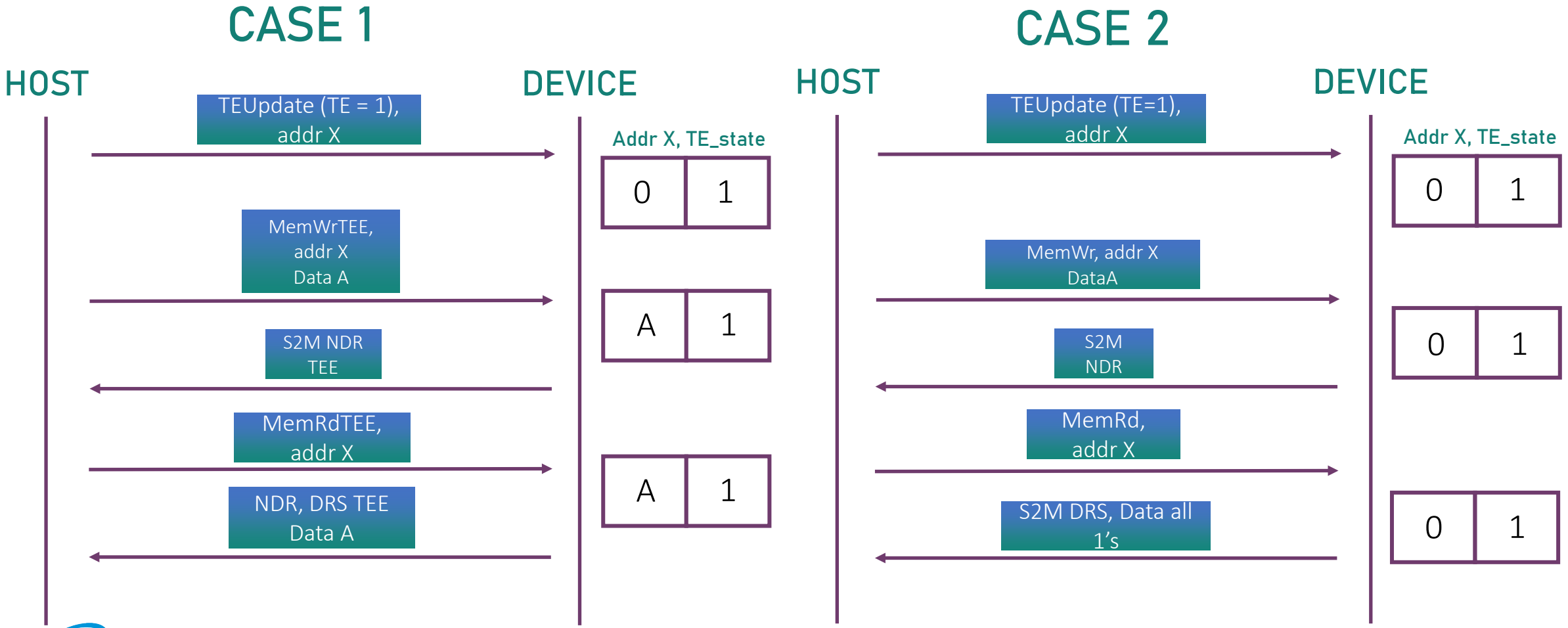
Challenging Verification Scenarios

- Memory Encryption:
  - Initiator based Encryption:
    - Send partial write request through TVM with TEE opcode –Underfill Read
    - Send MemRDTEE on same address

Target based Encryption – CKID



TSP Explicit In-Band TE State Change – Read/Write access control:



Avery CXL Security Verification Modes

- **Front-door mode**: Normal mode where SPDM is active
  - Full SPDM and IDE Key Management process to configure keys
- **Back-door mode**: SPDM disabled
  - Use backdoor APIs to configure IDE keys
  - Use backdoor APIs to move configure TSP and move to a particular state

Avery VIP- CXL Security Assertions/CTS

Feature	CXL.IO Assertions	CXL.IO CTS	CXL Assertions (CM+ IO)	CXL CTS (CM + IO)
DOE	22	34	42	50
SPDM	90	50	97	64
IDE	70	119	125	151
TDISP/TSP	30	127	66	20
Total	**212**	**330**	**379**	**312**

Summary

- Challenging Verification Scenarios:
  - Reset – Conventional Reset, CXL Reset and FLR.
  - IDE.Start while in Secure/Insecure state without re-initiating KEY_PROG and K_SET_GO
  - Interleaving CXL_IDE_KM with IDE_KM messages
  - K_SET_GO in Secure state with IDE mode different than already enabled
  - IDE.Start before MAC of Epoch
  - TSP Memory Encryption – Initiator and Target based
  - TSP Explicit In-Band TE State Change – Read/Write access control

Thank You !

Visit us at booth #(Siemens)
for more information