# Enhancing Security in CXL: IDE and TSP Verification

Heetashi Arora
Lead Member of Consulting Staff
Siemens EDA

# Agenda

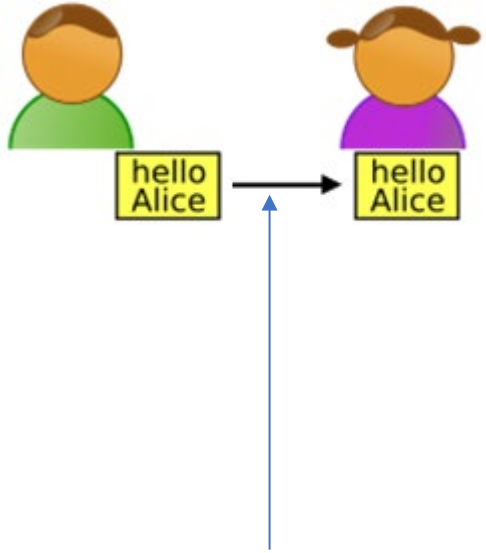
- Security Stack : IDE and TSP Roleplays
  - Requirements
  - Why IDE
  - Encryption/Decryption
  - TSP Architecture
- Verification Scenarios
  - Invalid Keys
  - Retry Scenario
  - TSP: Set Target TE State
  - TSP: Rules to Maintain the Security of Memory Data

# Requirements

| | |
|---|---|
| CMA | Authentication<br>Establish trust relationship |
| IDE | Secure Data path between host and device<br>Provide encryption |
| TSP | Implement Security mechanism to isolate TVM<br>Secure confidential data of CXL Memory Device |

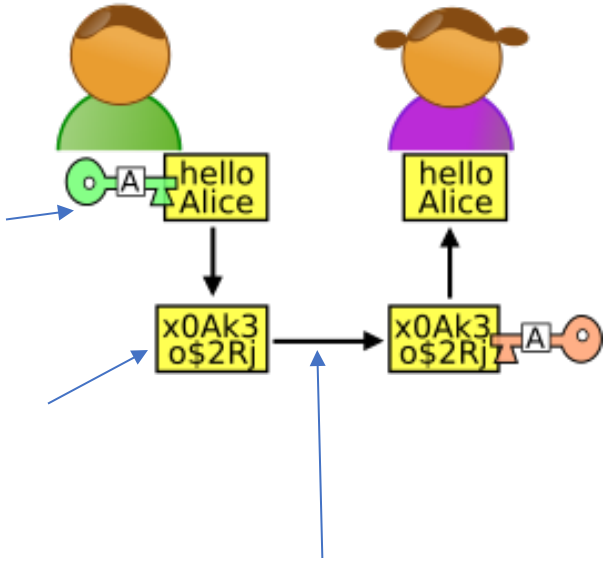
# Why IDE ?

## Without Encryption



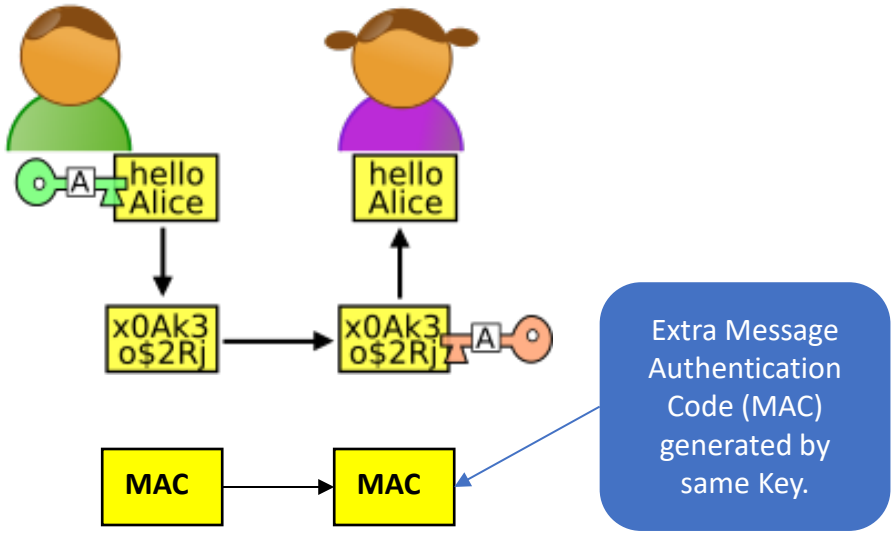

- Can be read by Attacker.
- Can be modified by Attacker.

## Data Encryption




- Can be modified by Attacker.

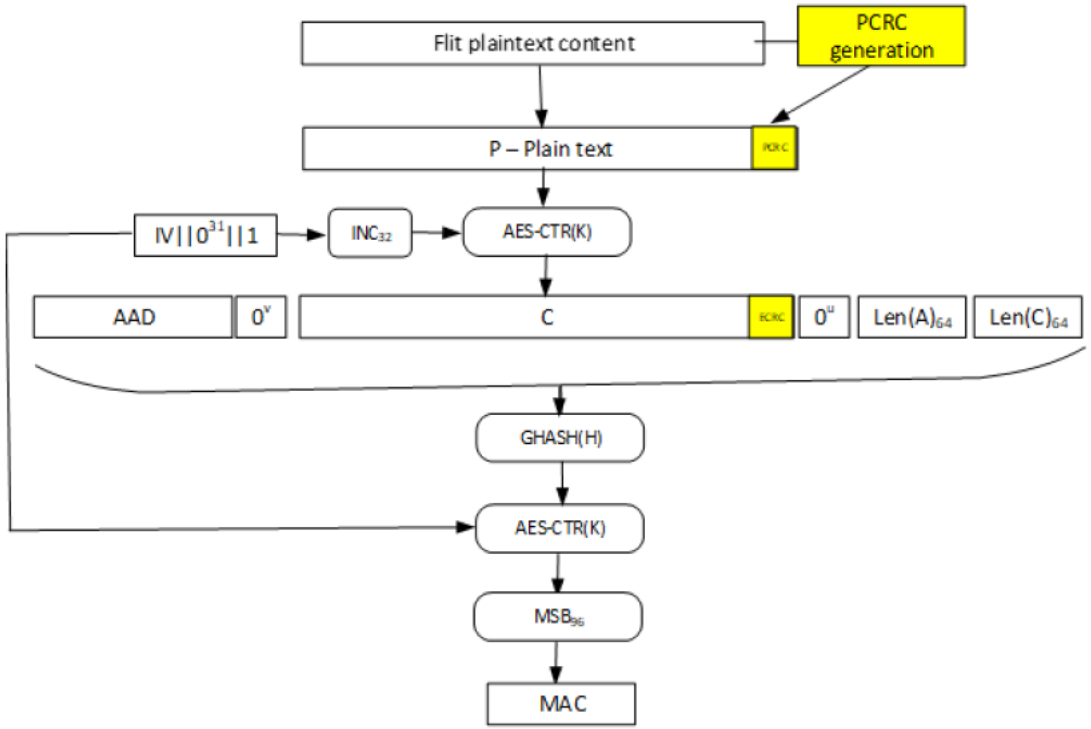
## Integrity & Data Encryption



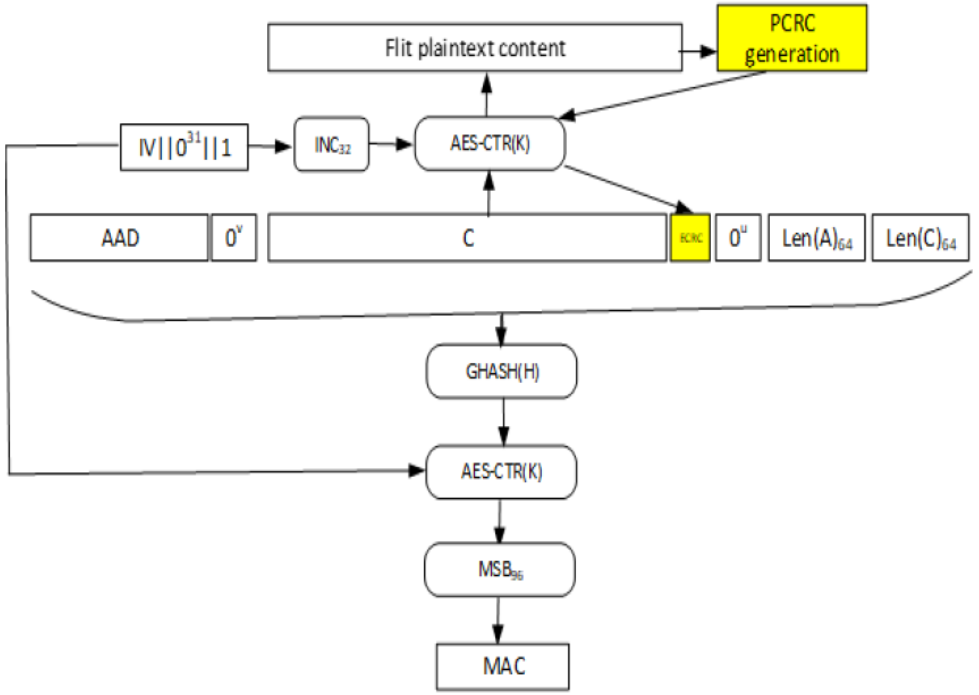

- With the help of MAC, it can be recognized whether message is modified or not.

# CXL Flit Encryption/Decryption

## Encryption



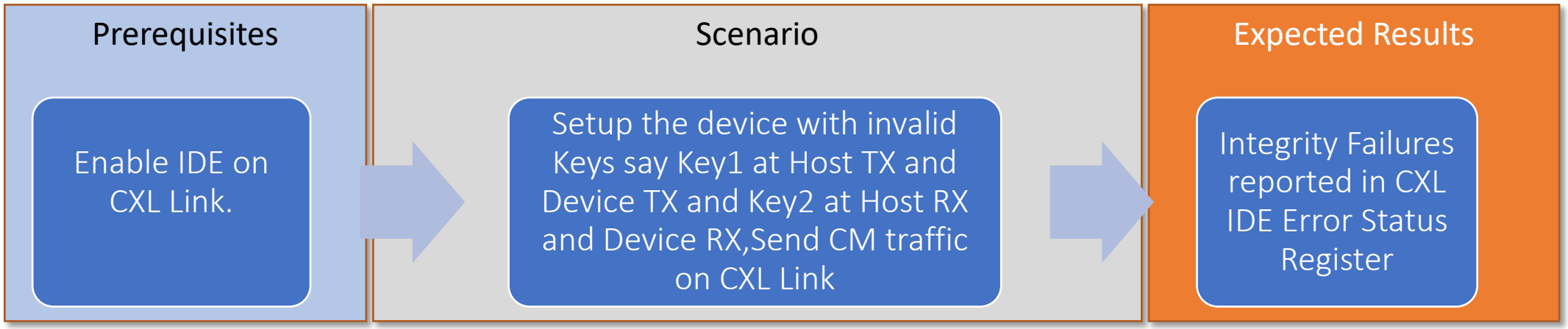

## Decryption



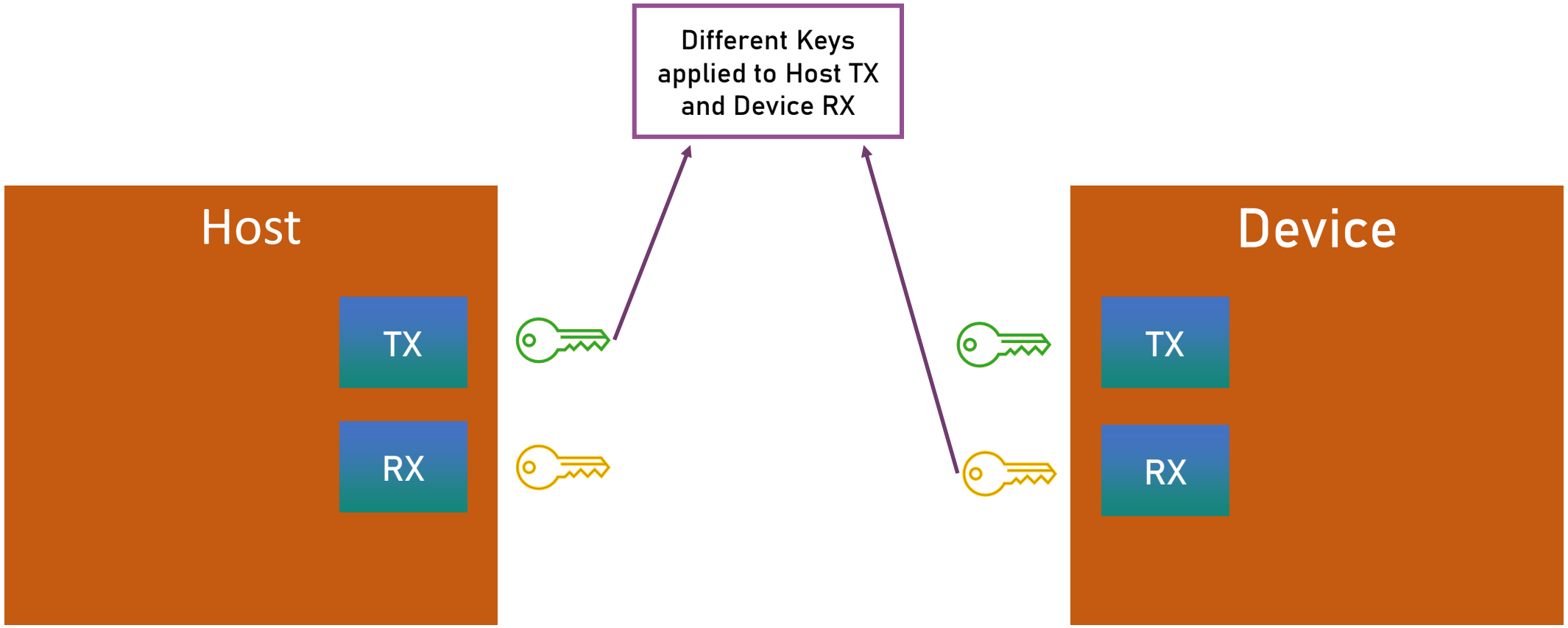
# Verification Scenarios

Securing the Link

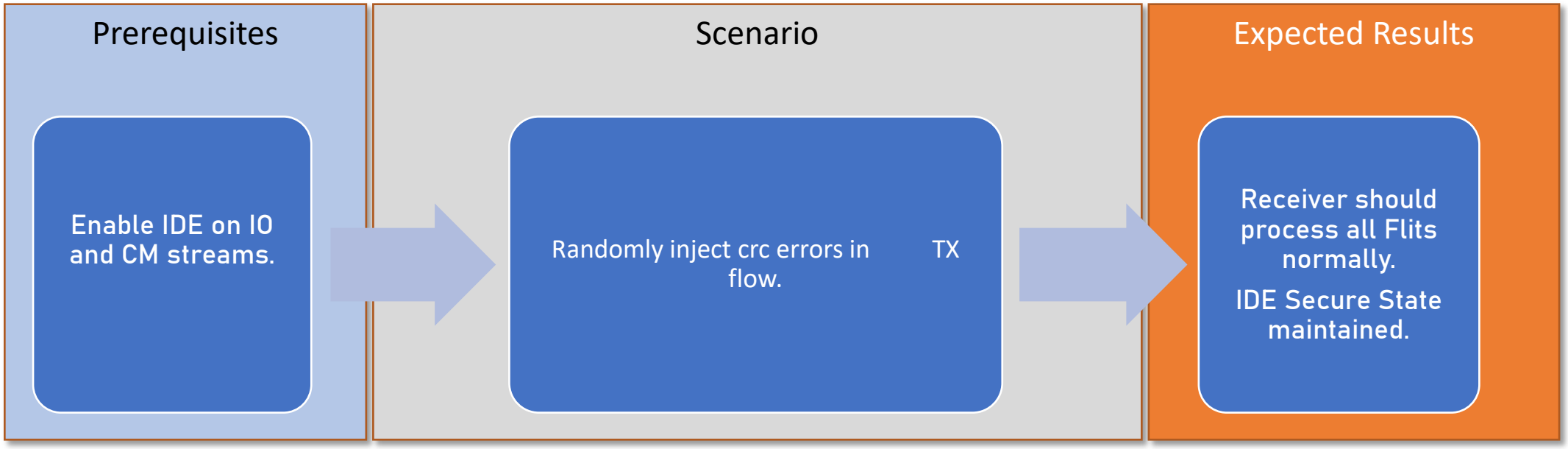
# Invalid Keys



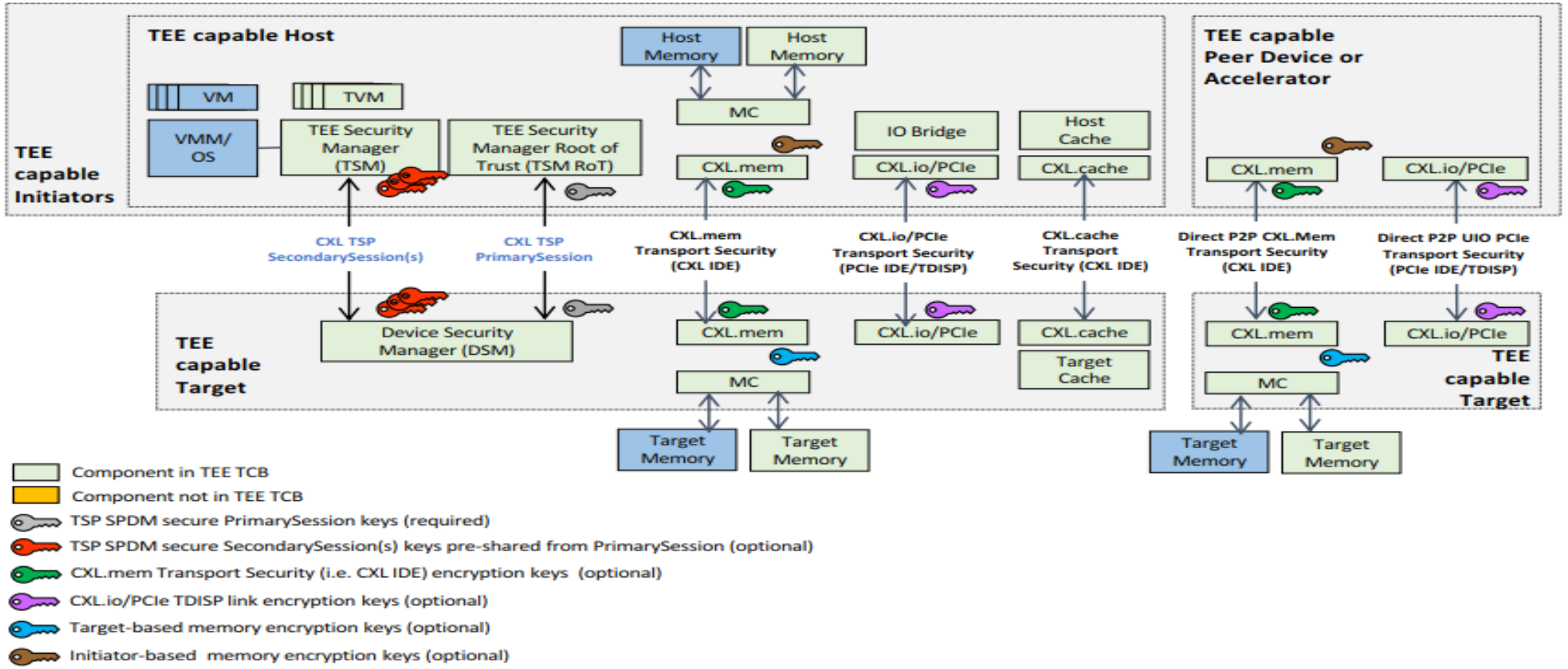
# Invalid Keys



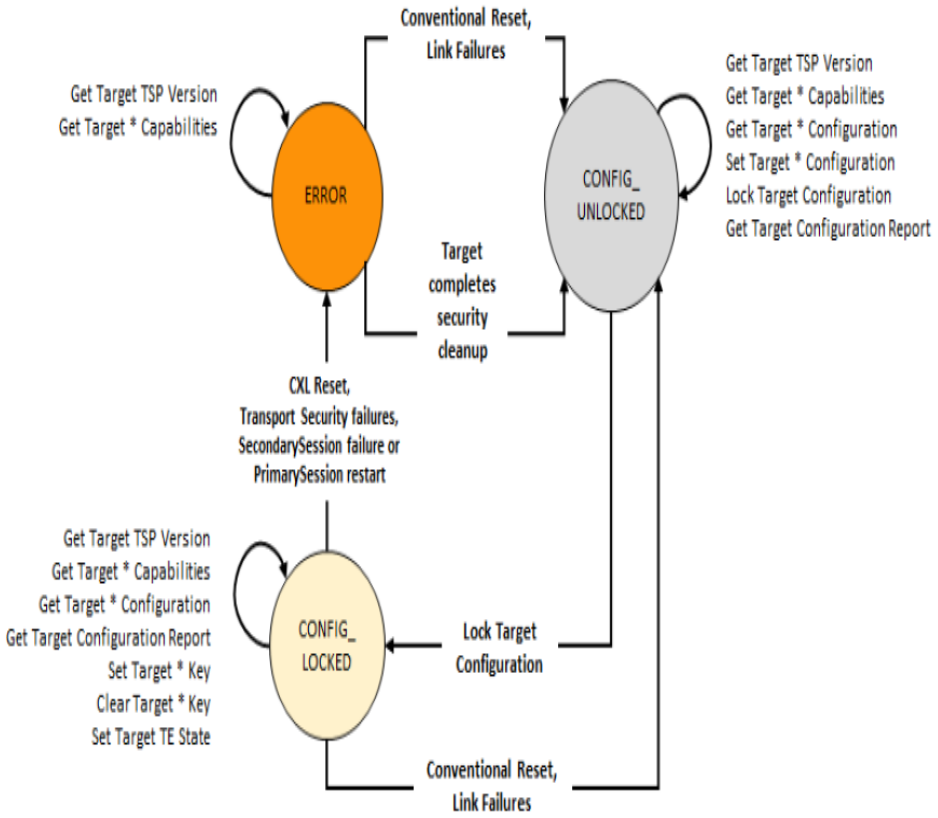
# Retry



# Architecture



# Target TSP Security States




## CONFIG_UNLOCKED :

- Default state.
- VMM configures the Mem Device to be assigned to a TVM.
- VMM requests the TSM to lock the Device.

## Config_LOCKED

- Device memory resources are operational and permitted to be accessed and managed by the TVM.

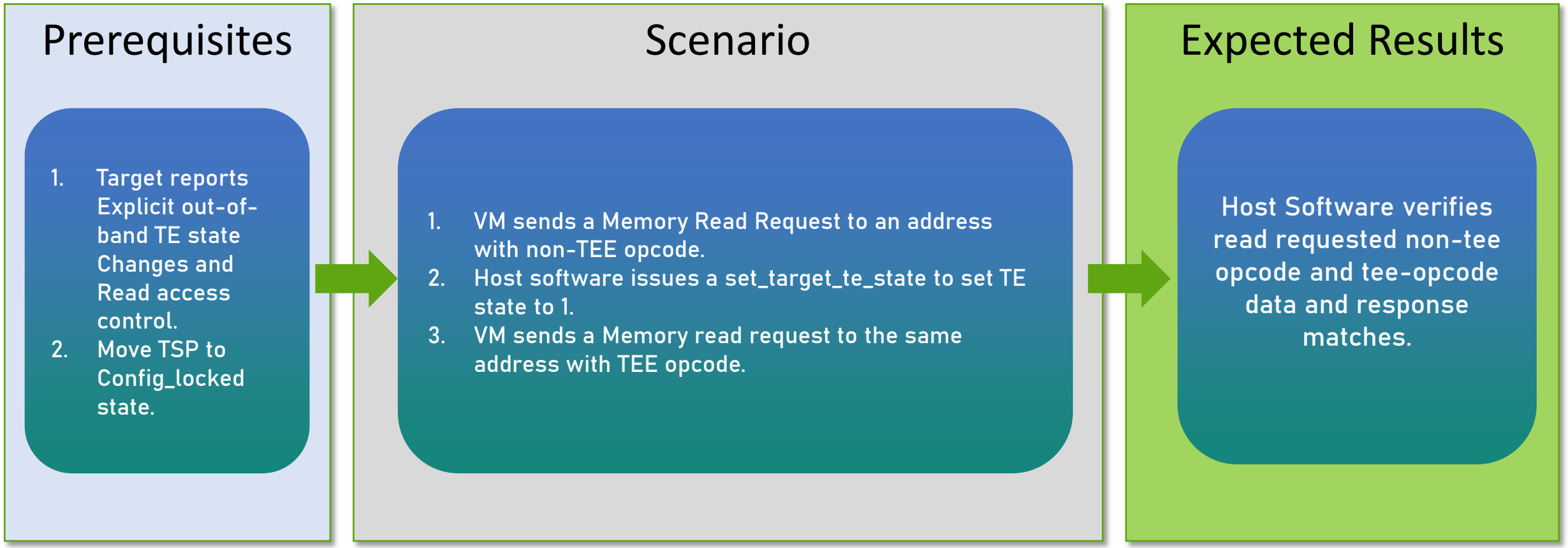
## ERROR

- Move to this state in case of any security breach.
- Device must not expose confidential TVM data.

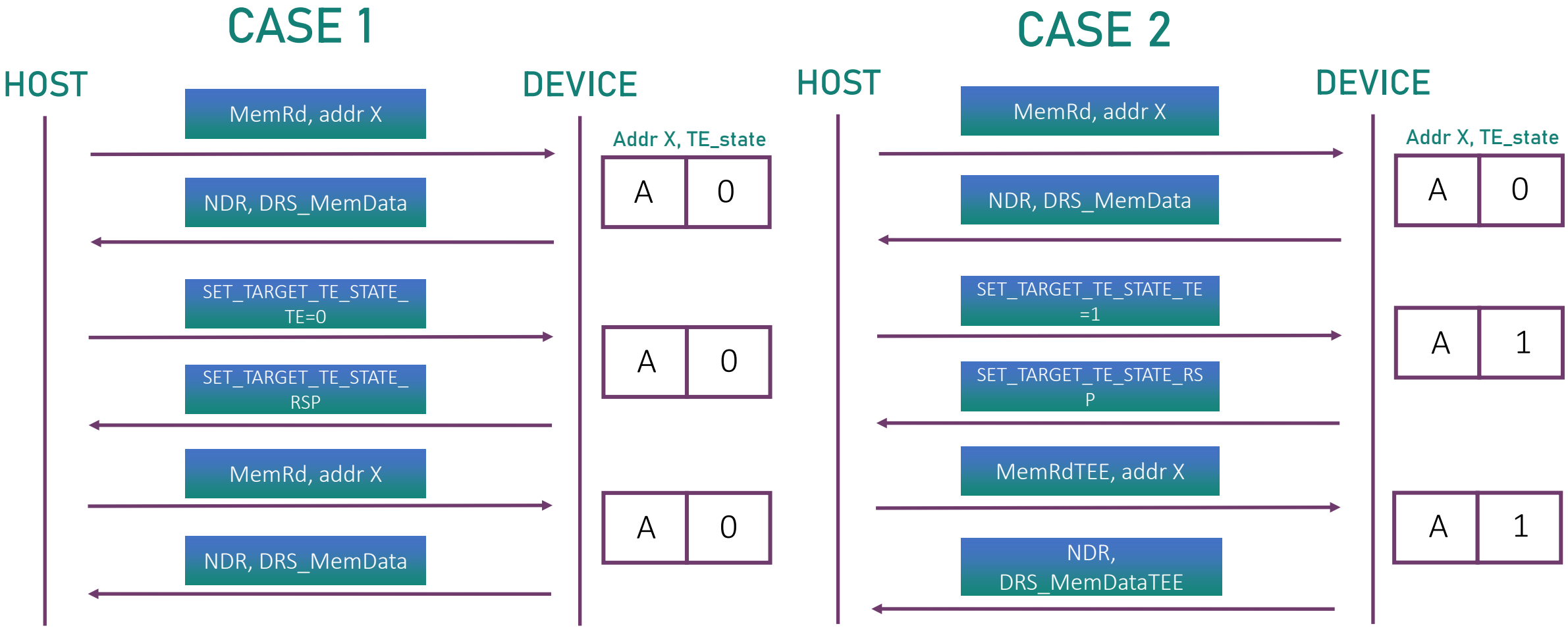
# Verification Scenarios

Securing the Memory

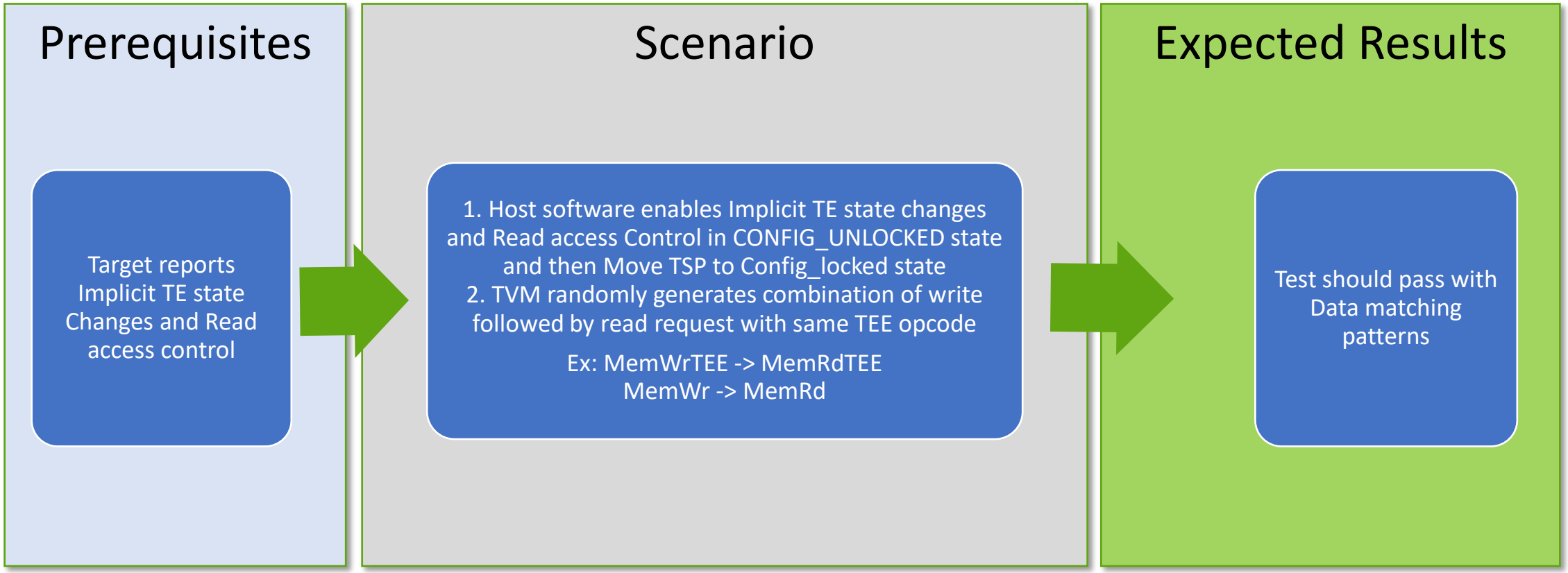
# SET_TARGET_TE_STATE

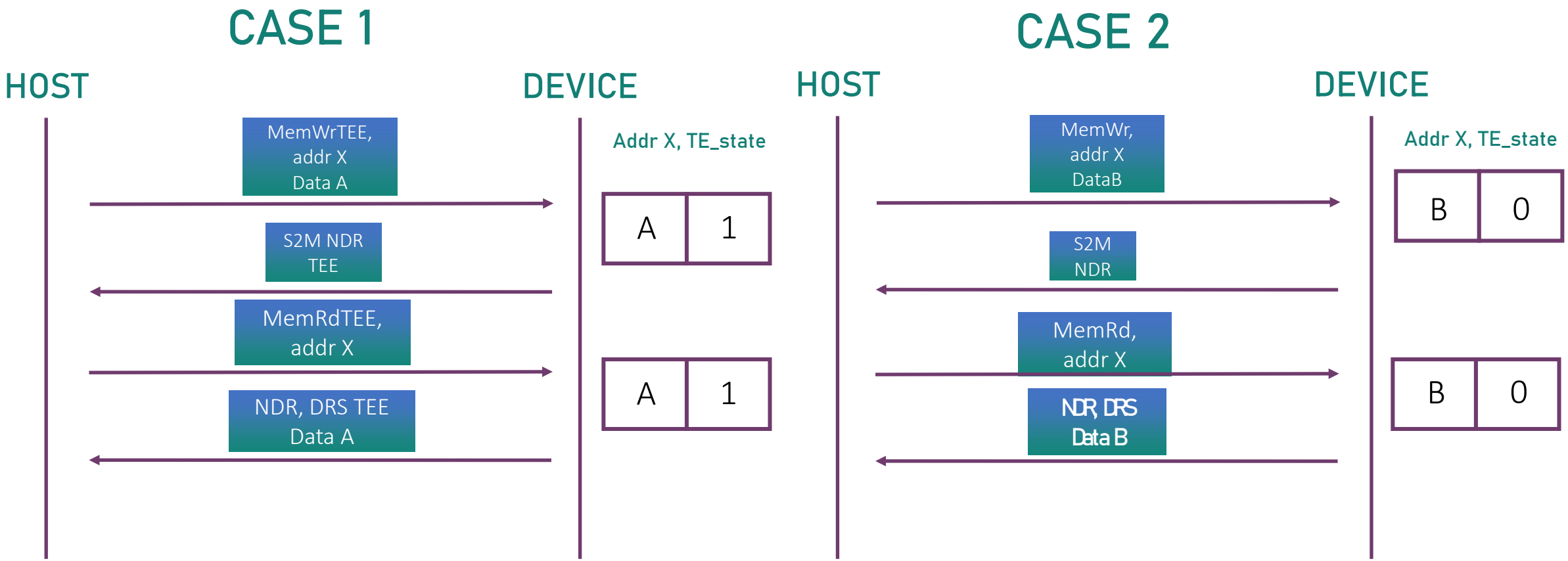


# SET_TARGET_TE_STATE



# Implicit + Read Access Control



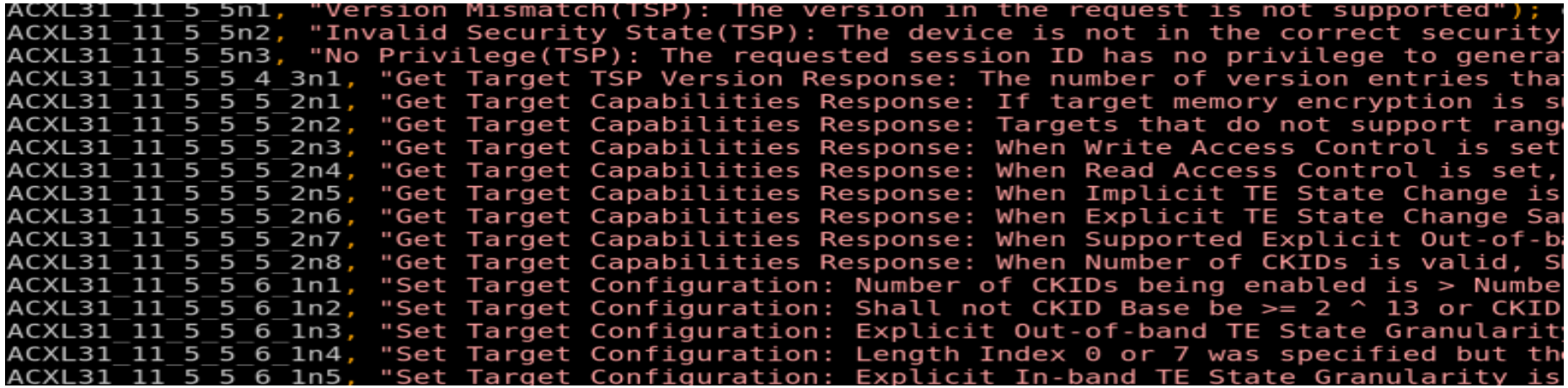


# Protocol Compliance Test - Modes

- Front door Mode
  - Full Security Stack is Active
  - Callbacks for easily achieving the scenarios
    - Based on encryption flows
    - TSP Commands
- Backdoor Mode
  - Provides layer wise configurability
  - Callbacks/API's for
    - Flow Configurations
    - TSM/DSM State controls

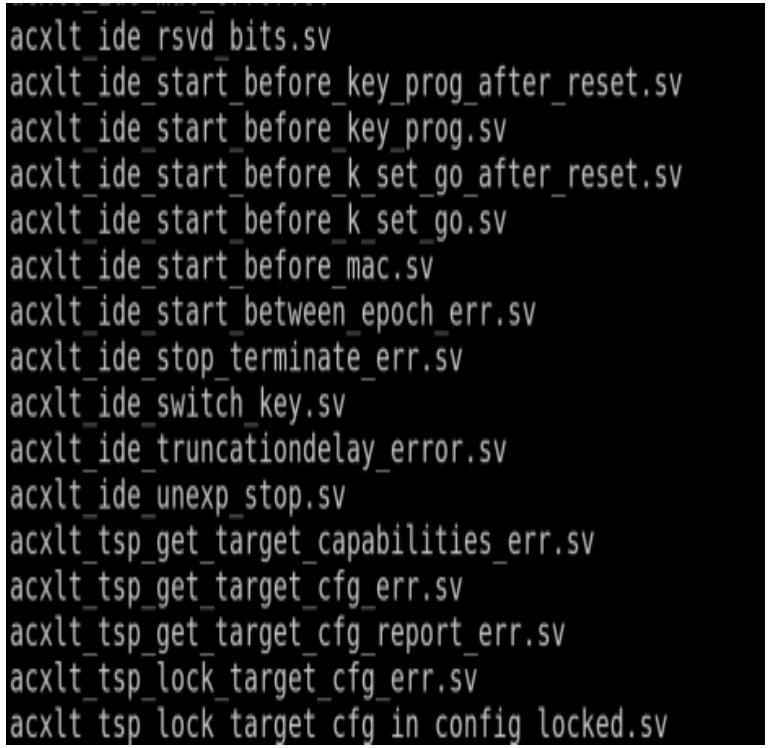
# Protocol Compliance – Protocol Suite

- Exhaustive Protocol Suite
  - 2000+ checklist items built into BFM and Test Suite
  - 500+ checklist items for Full Security Stack
  - Checklist derived based on spec



# Stimuli / Testing – Compliance Suite

- Transport Independent Stimulus Library
  - 300+ Off-the-shelf compliance tests for Security Stack
- Highly Configurable Requests Structure
  - Specification defined fields are directly accessible
- Randomization of Stimulus
  - Corner cases and unexpected scenarios
- Automating Request Creations, Real time scenarios
  - Constraints, APIs
  - Minimized user input for stress-testing
- Error Injection
  - Can be easily achievable through callbacks and APIs



# Stimuli/Testing – Transaction Mode

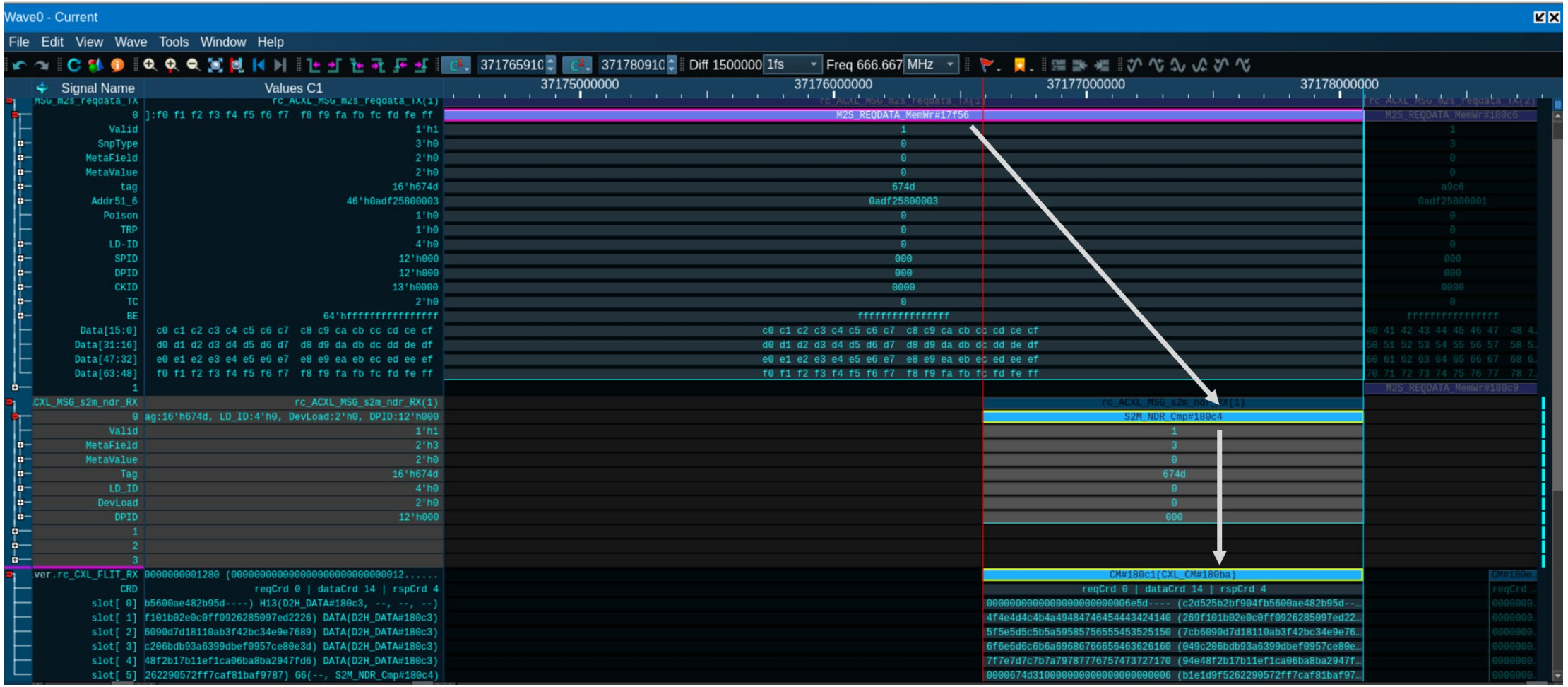
- Encrypted Flit Spec relation

```
| => 2427000 CM_PROT#6af6(M2S_REQ_MemInvNT#67ea, M2S_REQ_MemInv#67eb, M2S_REQ_MemRdData#67ec, M2S_REQ_MemSpecRd#67ed, M2S_REQ_MemInv#67ee, M2S_REQ_MemRd#67f0,
| reqCrd 0, dataCrd 19, rspCrd 1d
| 34e4c0aa684cd6201b2337635fe4---- (000000033be18f0adc9cf6e13134----) H4(M2S_REQ_MemInvNT#67ea)
| 1eafb6e893ba94a84210878d14456c69 (000000000006276e550fedd6c170014) G4(M2S_REQ_MemInv#67eb)
| 47a81b307d58420edefc935ee6c86312 (0000000000001e9bb83b883f90ba3054) G4(M2S_REQ_MemRdData#67ec)
| d3724c7414d5690a2c8e438aa7ddc9ac (00000000000000000000000000000000)
| be6ee0eaa7f886414fedcf1f66a4c35b (000000000000888bc9af3c61fdcff114) G4(M2S_REQ_MemSpecRd#67ed)
| a7f4c7769de9ea5fcb2d401272539c66 (00000000000000000000000000000000)
| 8bd40e732c28e2a038a0fa0d9cb7bd6a (00000000000000000000000000000000)
| 8e2c51ac1fe610a63ecf8e162fac9d86 (00000000000000000000000000000000)
| 4c86db8a3550ac52c5750e9bf23a7b81 (000000000001f93bb3c96c45f4b68014) G4(M2S_REQ_MemInv#67ee)
| 817972d1b2fdb742a6e360fd520e68f6 (0000000000005a620c50fa4946f70034) G4(M2S_REQ_MemRd#67f0)
| 9fcf47dce4bc6fca4c4393a3c5328503 (0000000000343216e36427e1d813134) G4(M2S_REQ_MemInvNT#67f4)
| e7deede40af5d19356dbde23cd1cfab0 (00000000000000000000000000000000)
| 326cb097fd1e156d28e8a73dab2e105c (0000000000338f3209b47fb5c9e3054) G4(M2S_REQ_MemRdData#67f7)
| 7cc82eb6e02e296834bf4d28d83600a5 (00000000000000000000000000000000)
| 876396f1db3041102067b476ebb17c88 (00000000000000000000000000000000)
| 00000000000000000000000000007720 (00000000000000000000000000007720)
| (user dropped at tx_flit_exit_dll)
| MAC_EPOCH#6af3(mac 1823d3c0d44ea82bc85d5d47, pcrc disabled, key 0000000000000000000000000000000000000000000000000000000000000000, iv 00000000000000000000
```

# Transaction Recording

- Comprehensive Command Coverage
  - Each CXL transaction in the waveform captures the full lifecycle of an CXL Request/Flit—from initiation to completion
- CXL Transactions Mapping
  - Parent CXL transactions are linked to related child transactions such as MemRd/NDR-DRS data transfers

# Transaction Recording



# Questions?