

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

Establish trust relationship



IDE

Secure Data path between host and device

Provide encryption



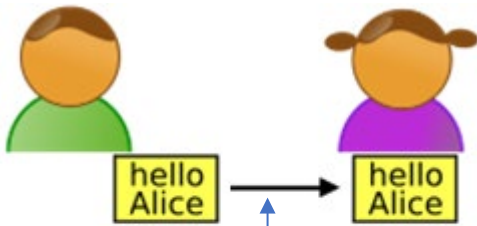
TSP

Implement Security mechanism to isolate TVM

Secure confidential data of CXL Memory Device

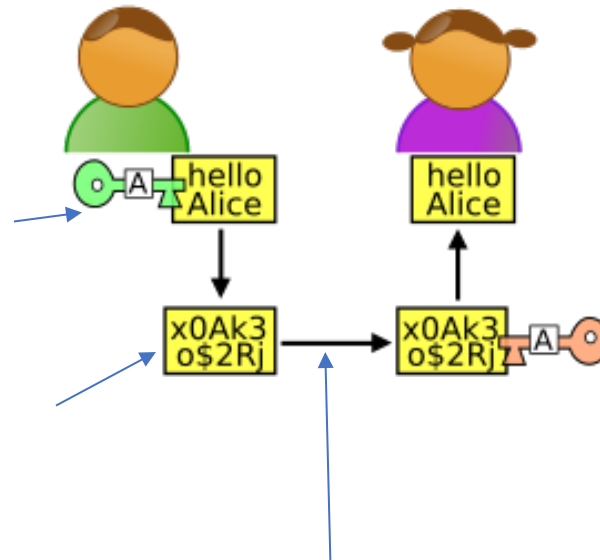
Why IDE ?

Without Encryption



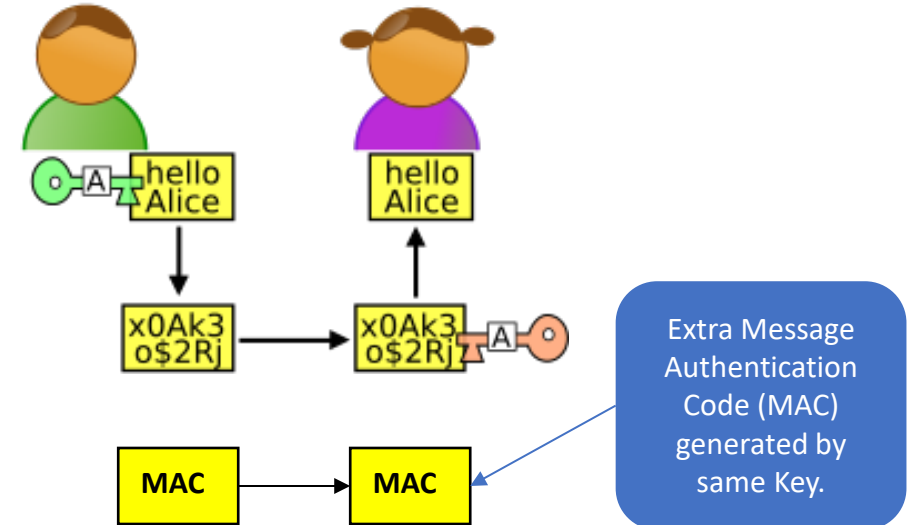
- Can be read by Attacker.
- Can be modified by Attacker.

Data Encryption



- Can be modified by Attacker.

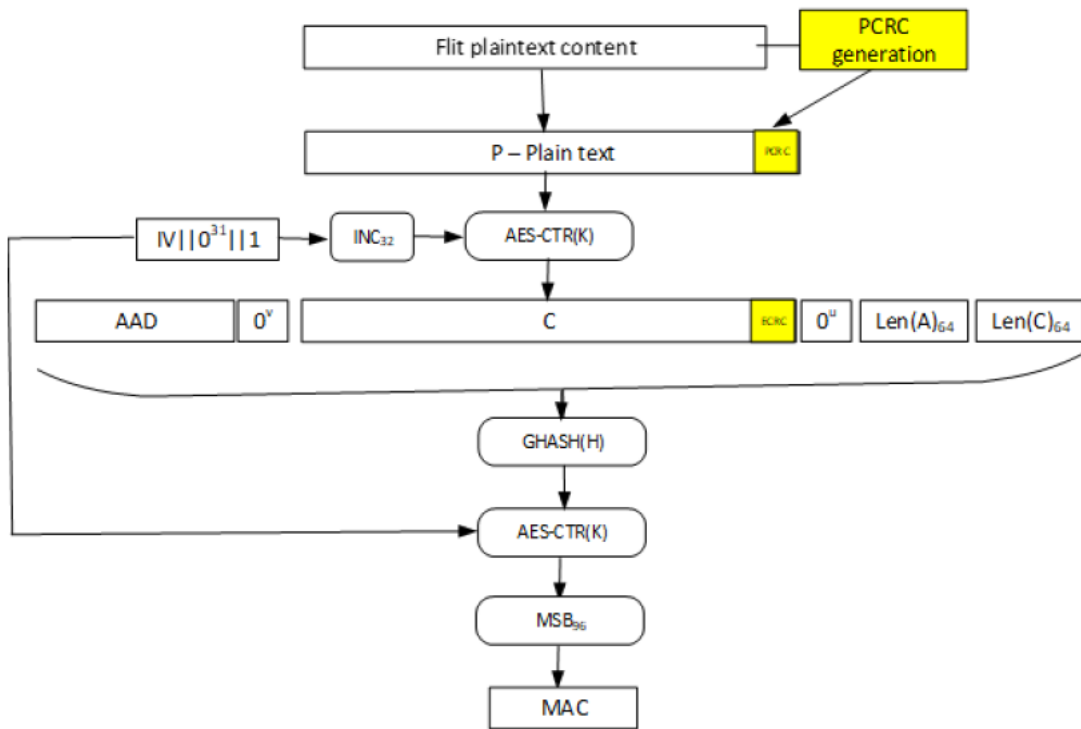
Integrity & Data Encryption



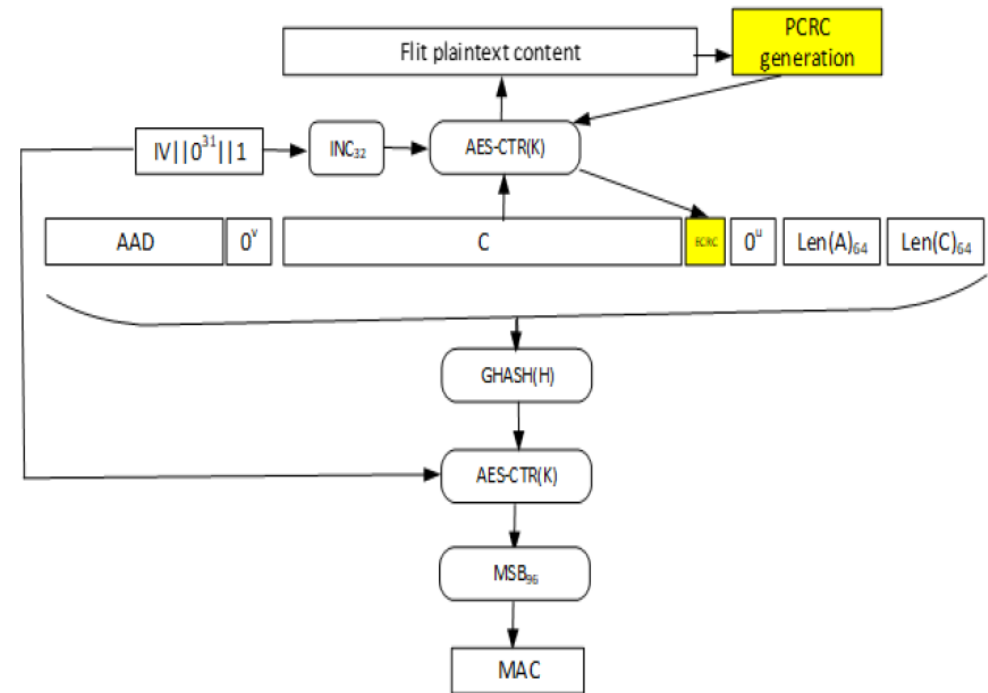
- With the help of MAC, it can be recognized whether message is modified or not.

CXL Flit Encryption/Decryption

Encryption



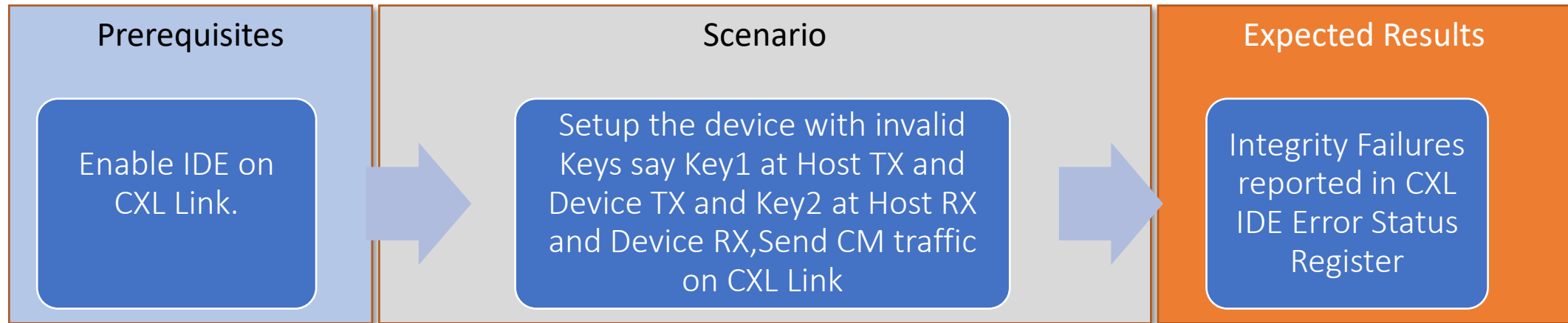
Decryption



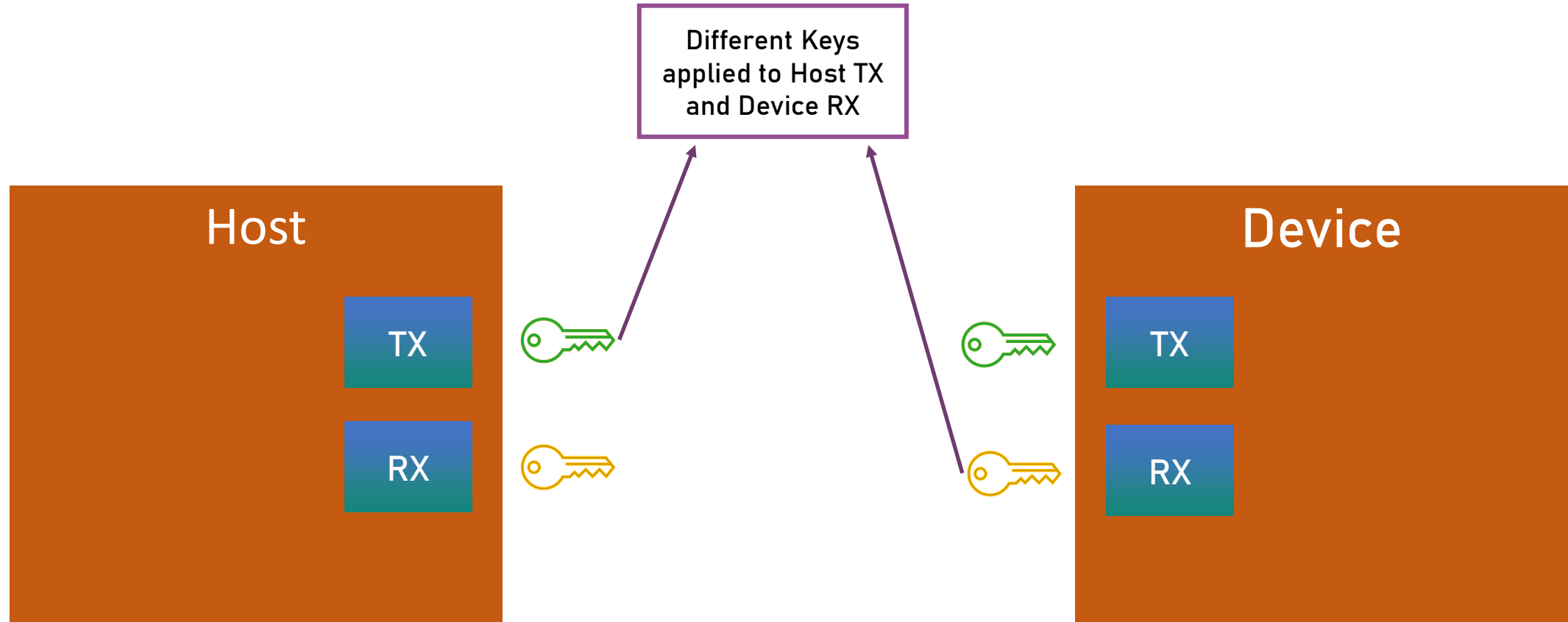
Verification Scenarios

Securing the Link

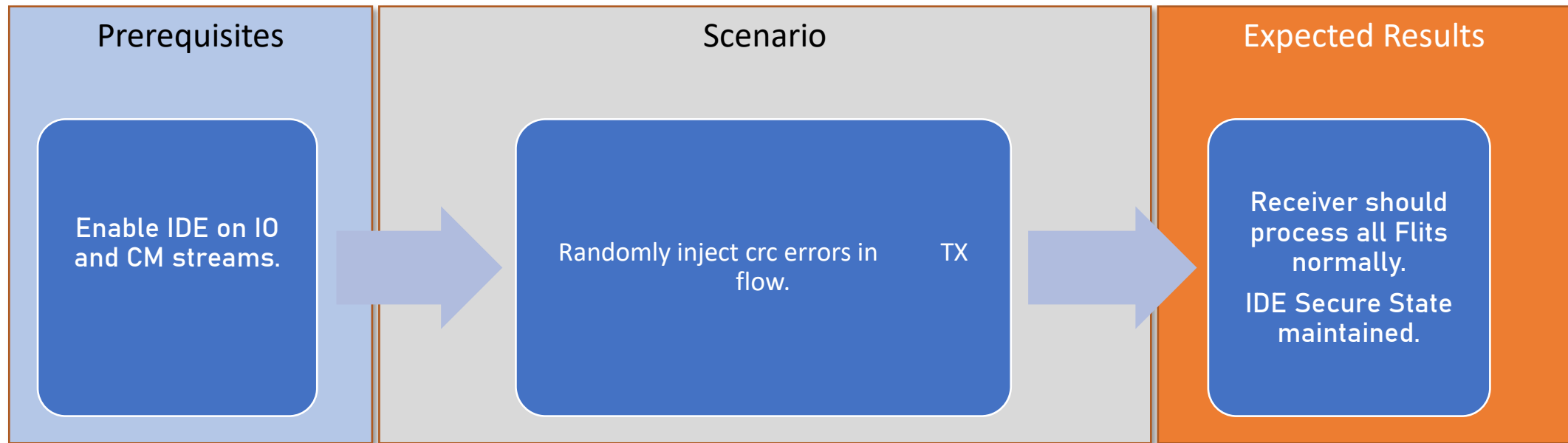
Invalid Keys

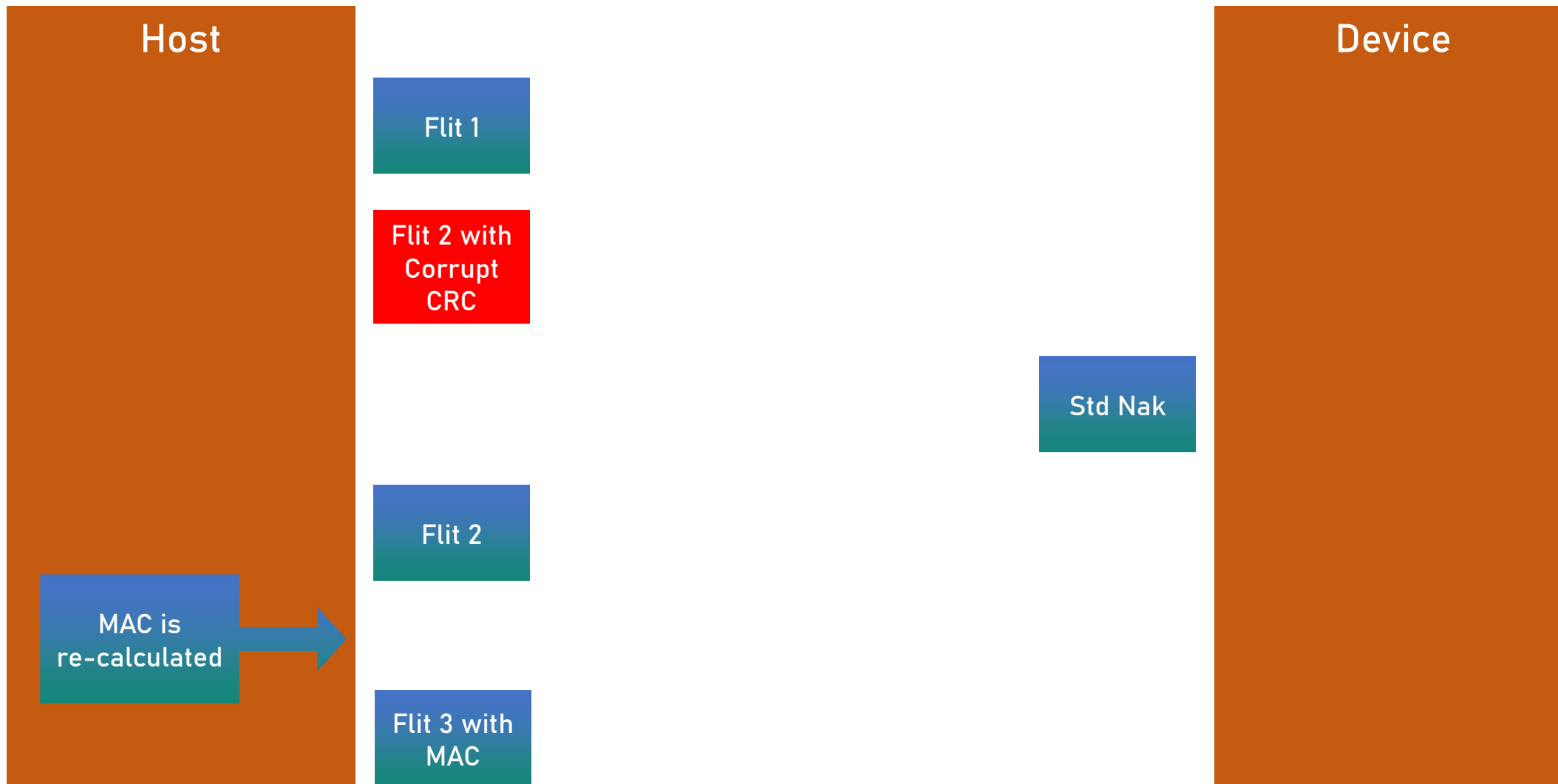


Invalid Keys

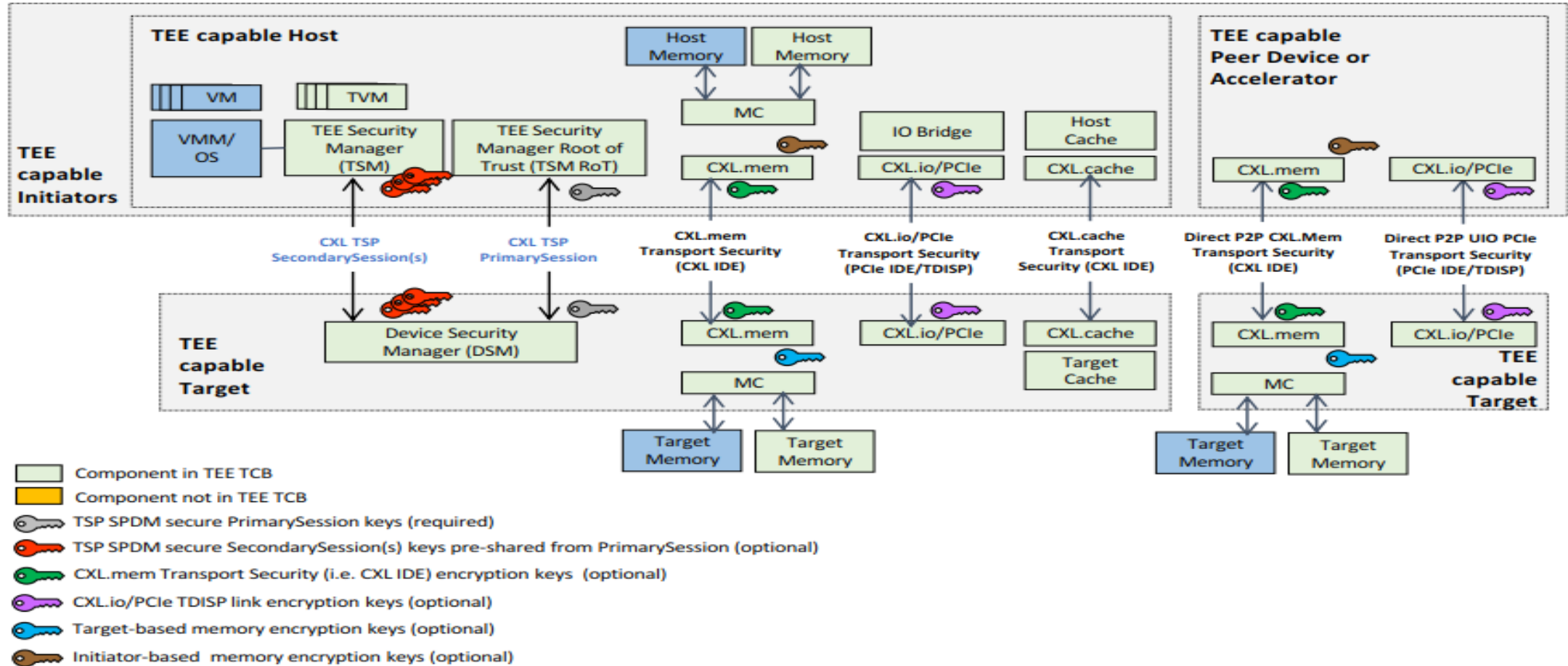


Retry

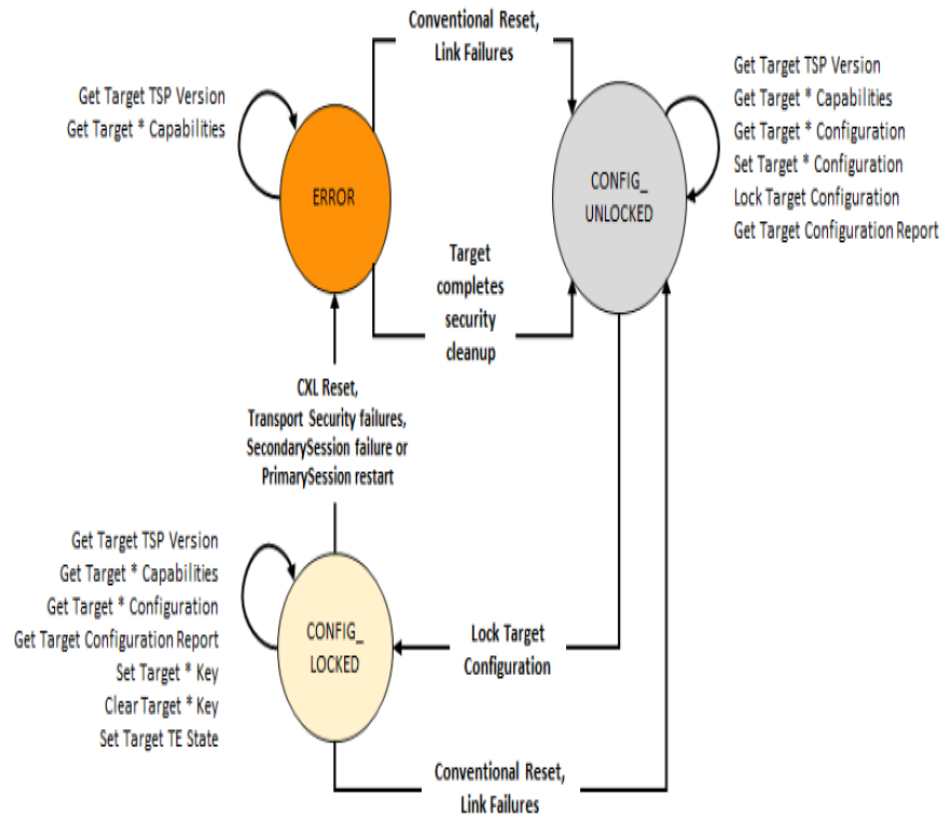




Architecture



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

Prerequisites

1. Target reports Explicit out-of-band TE state Changes and Read access control.
2. Move TSP to Config_locked state.

Scenario

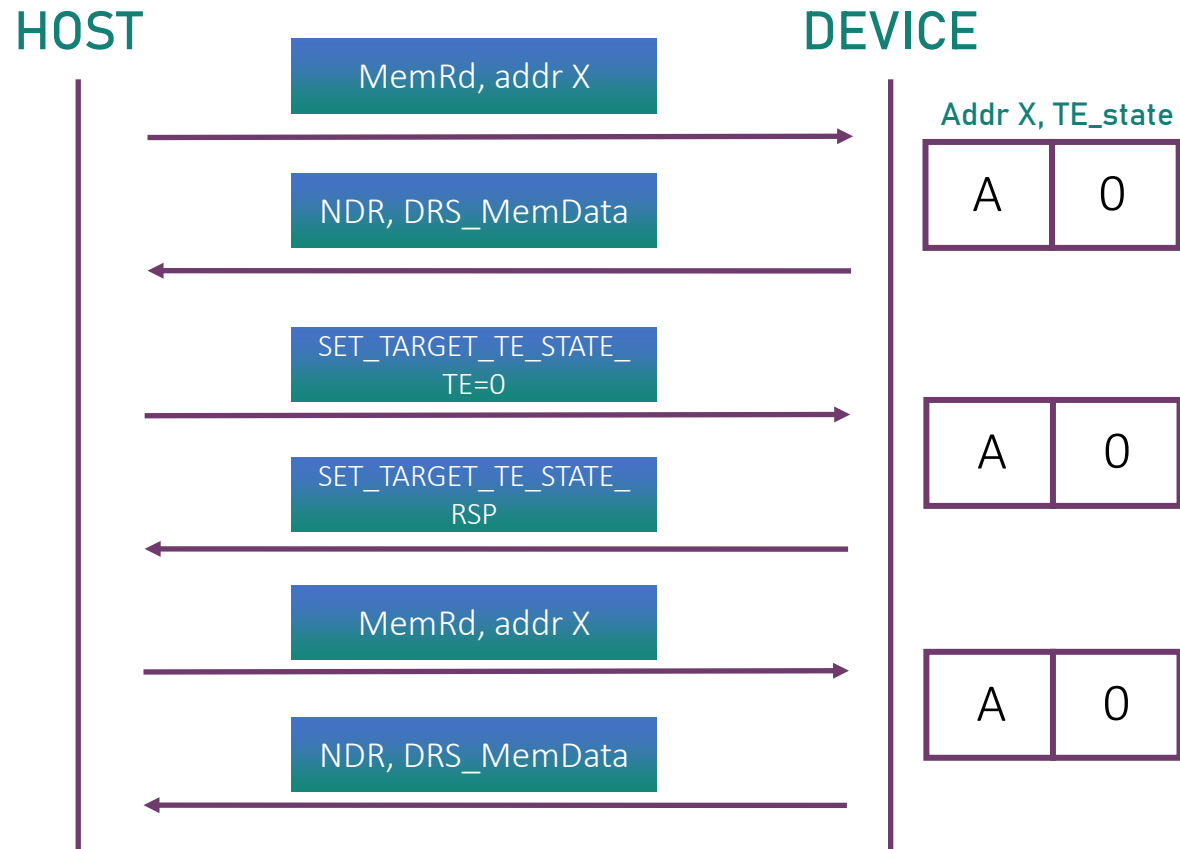
1. VM sends a Memory Read Request to an address with non-TEE opcode.
2. Host software issues a set_target_te_state to set TE state to 1.
3. VM sends a Memory read request to the same address with TEE opcode.

Expected Results

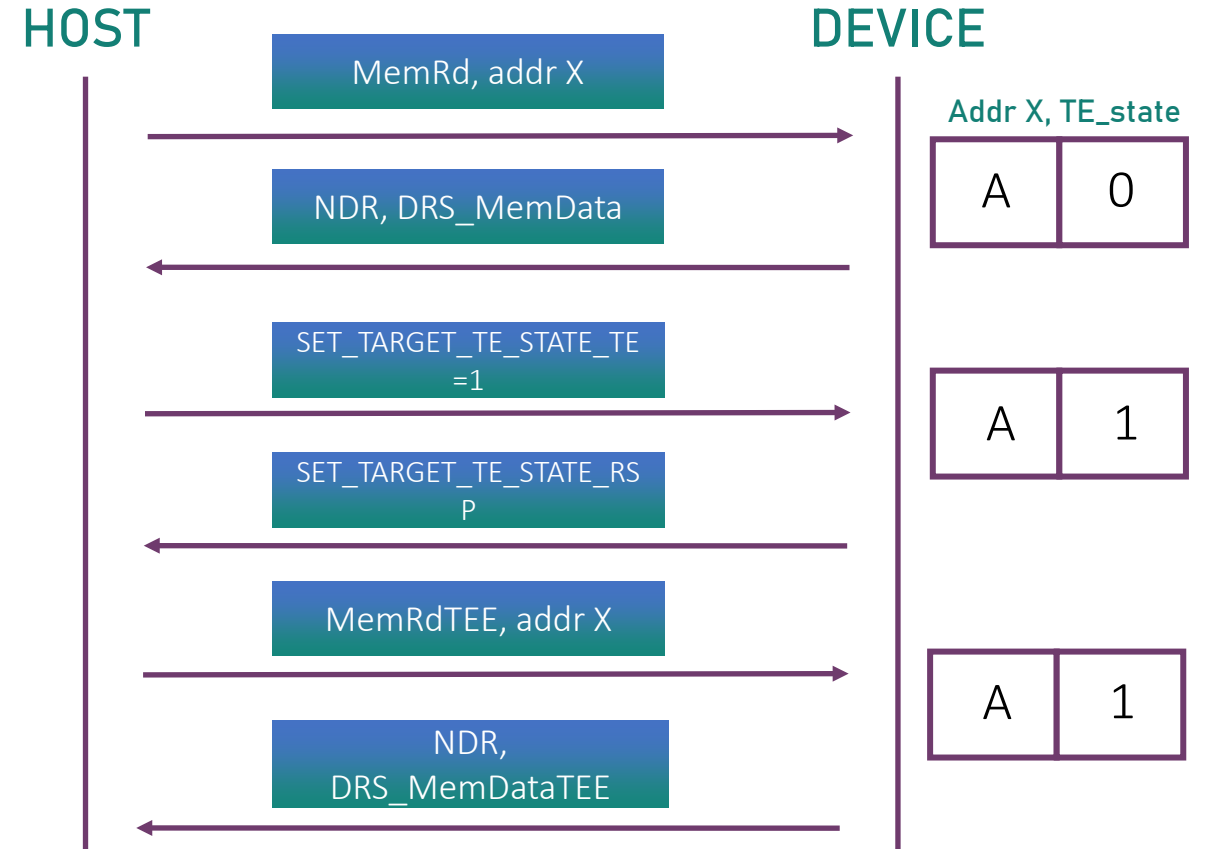
Host Software verifies read requested non-tee opcode and tee-opcode data and response matches.

SET_TARGET_TE_STATE

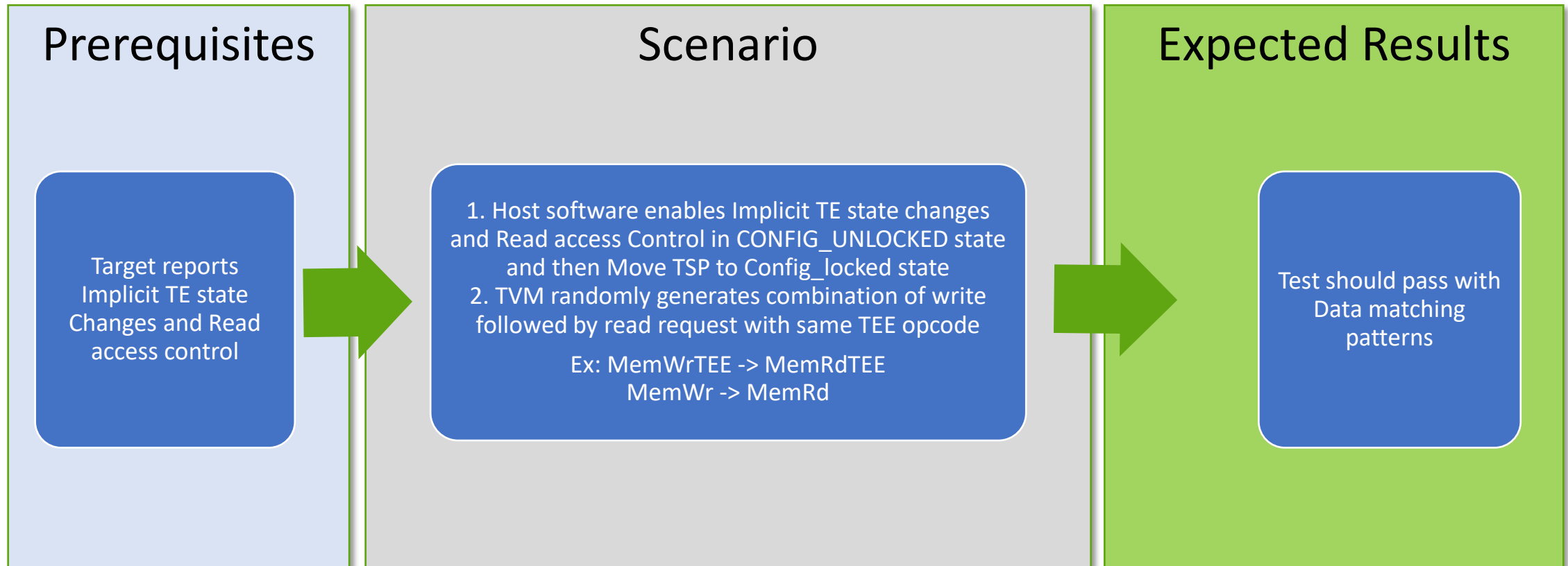
CASE 1



CASE 2



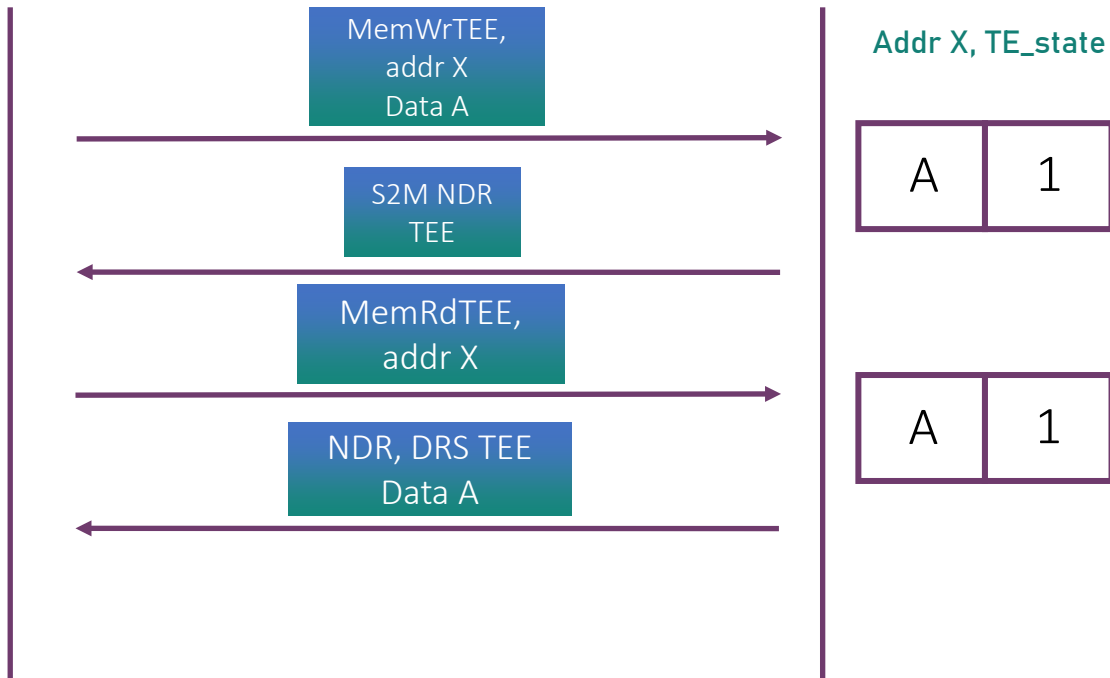
Implicit + Read Access Control



CASE 1

HOST

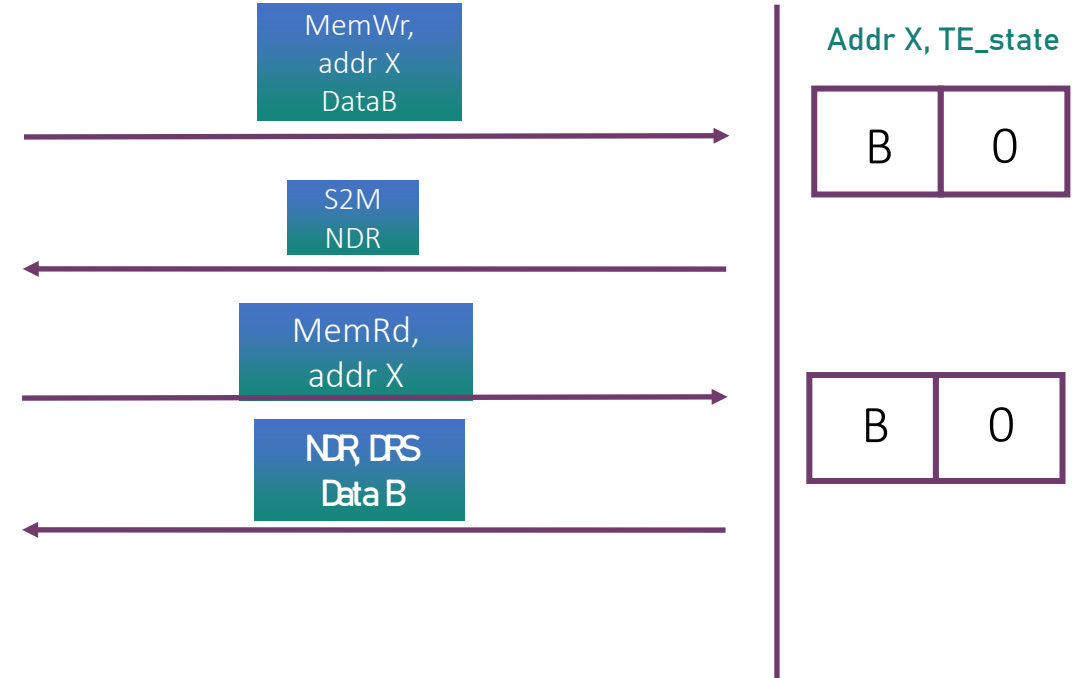
DEVICE



CASE 2

HOST

DEVICE



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

```
ACXL31_11_5_5n1, "Version Mismatch(TSP): The version in the request is not supported");
ACXL31_11_5_5n2, "Invalid Security State(TSP): The device is not in the correct security
ACXL31_11_5_5n3, "No Privilege(TSP): The requested session ID has no privilege to genera
ACXL31_11_5_5_4_3n1, "Get Target TSP Version Response: The number of version entries tha
ACXL31_11_5_5_5_2n1, "Get Target Capabilities Response: If target memory encryption is s
ACXL31_11_5_5_5_2n2, "Get Target Capabilities Response: Targets that do not support rang
ACXL31_11_5_5_5_2n3, "Get Target Capabilities Response: When Write Access Control is set
ACXL31_11_5_5_5_2n4, "Get Target Capabilities Response: When Read Access Control is set,
ACXL31_11_5_5_5_2n5, "Get Target Capabilities Response: When Implicit TE State Change is
ACXL31_11_5_5_5_2n6, "Get Target Capabilities Response: When Explicit TE State Change Sa
ACXL31_11_5_5_5_2n7, "Get Target Capabilities Response: When Supported Explicit Out-of-b
ACXL31_11_5_5_5_2n8, "Get Target Capabilities Response: When Number of CKIDs is valid, S
ACXL31_11_5_5_6_1n1, "Set Target Configuration: Number of CKIDs being enabled is > Numbe
ACXL31_11_5_5_6_1n2, "Set Target Configuration: Shall not CKID Base be  $\geq 2^{13}$  or CKID
ACXL31_11_5_5_6_1n3, "Set Target Configuration: Explicit Out-of-band TE State Granularit
ACXL31_11_5_5_6_1n4, "Set Target Configuration: Length Index 0 or 7 was specified but th
ACXL31_11_5_5_6_1n5, "Set Target Configuration: Explicit In-band TE State Granularity is
```

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

```
acxlt_ide_rsvd_bits.sv
acxlt_ide_start_before_key_prog_after_reset.sv
acxlt_ide_start_before_key_prog.sv
acxlt_ide_start_before_k_set_go_after_reset.sv
acxlt_ide_start_before_k_set_go.sv
acxlt_ide_start_before_mac.sv
acxlt_ide_start_between_epoch_err.sv
acxlt_ide_stop_terminate_err.sv
acxlt_ide_switch_key.sv
acxlt_ide_truncationdelay_error.sv
acxlt_ide_unexp_stop.sv
acxlt_tsp_get_target_capabilities_err.sv
acxlt_tsp_get_target_cfg_err.sv
acxlt_tsp_get_target_cfg_report_err.sv
acxlt_tsp_lock_target_cfg_err.sv
acxlt_tsp_lock_target_cfg_in_config_locked.sv
```

Stimuli/Testing – Transaction Mode

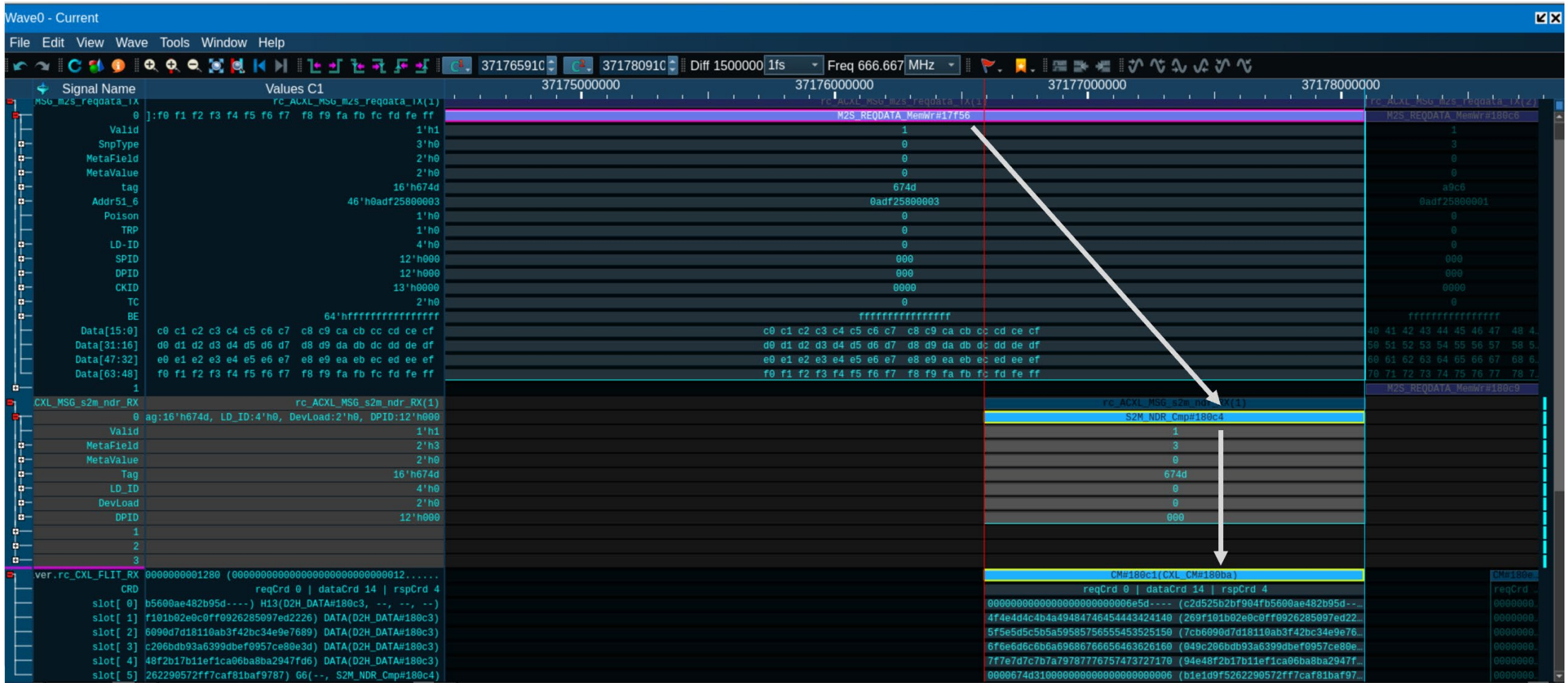
- Encrypted Flit Spec relation

```
=> 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---- (0000000033be18f0adc9cf6e13134----) H4(M2S_REQ_MemInvNT#67ea)
1eafb6e893ba94a84210878d14456c69 (00000000000006276e550fedd6c170014) G4(M2S_REQ_MemInv#67eb)
47a81b307d58420edefc935ee6c86312 (00000000000001e9bb83b883f90ba3054) G4(M2S_REQ_MemRdData#67ec)
d3724c7414d5690a2c8e438aa7ddc9ac (00000000000000000000000000000000)
be6ee0eaa7f886414fedcf1f66a4c35b (0000000000000888bc9af3c61fdcff114) G4(M2S_REQ_MemSpecRd#67ed)
a7f4c7769de9ea5fcb2d401272539c66 (00000000000000000000000000000000)
8bd40e732c28e2a038a0fa0d9cb7bd6a (00000000000000000000000000000000)
8e2c51ac1fe610a63ecf8e162fac9d86 (00000000000000000000000000000000)
4c86db8a3550ac52c5750e9bf23a7b81 (0000000000001f93bb3c96c45f4b68014) G4(M2S_REQ_MemInv#67ee)
817972d1b2fdb742a6e360fd520e68f6 (00000000000005a620c50fa4946f70034) G4(M2S_REQ_MemRd#67f0)
9fcf47dce4bc6fca4c4393a3c5328503 (000000000000343216e36427e1d813134) G4(M2S_REQ_MemInvNT#67f4)
e7deede40af5d19356dbde23cd1cfab0 (00000000000000000000000000000000)
326cb097fd1e156d28e8a73dab2e105c (000000000000338f3209b47fb5c9e3054) 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 0000000000000000000000000000000000000000000000000000000000000000)
```

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?