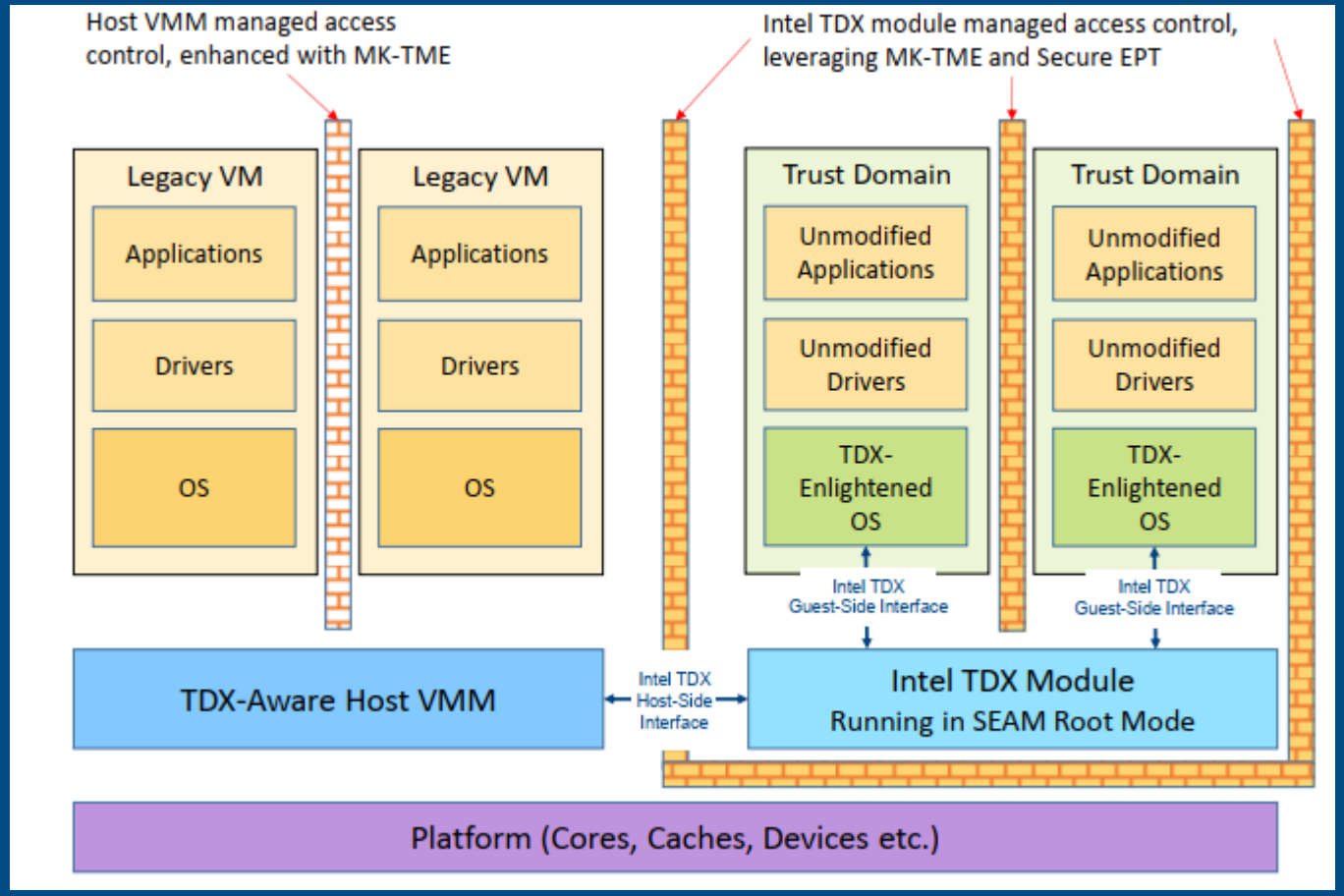
TDX Memory Integrity Protection & Machine Check Handling

SATG/SSE/OSV & CSP Engineering
2023 ww50
Fan Du

Intel Trusted Domain eXtension Overview

- TDX – an extension of VMX and MKTME technologies to isolate CSP/VMM from trust computing base by protecting TD guest memory, CPU state as well as the link b/w TD guest and device.
- TDX Tech Roadmap
  - ***TDX foundation***
  - ***TDX Live Migration, TD Preserving***
  - ***TDX connect , TD Partitioning***



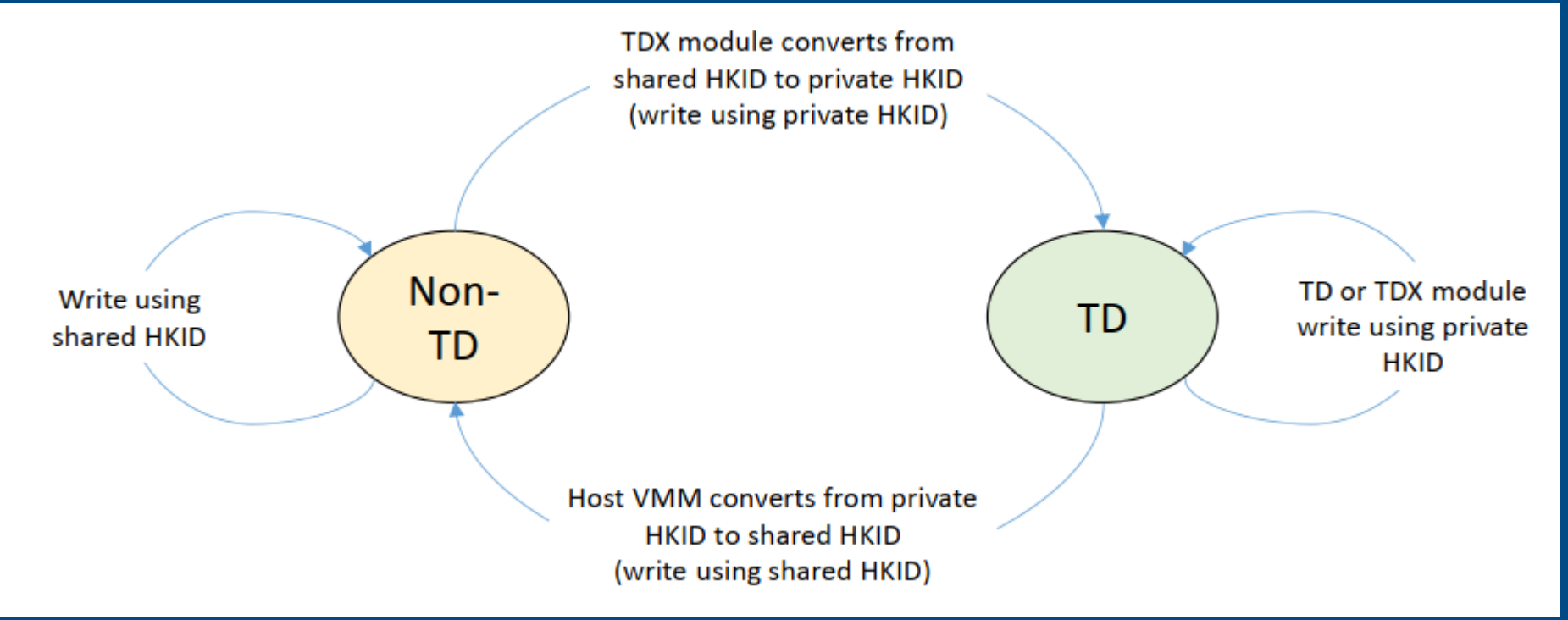
TDX Portal Link (Spec, TDX FW code)

TDX Memory Integrity Objectives

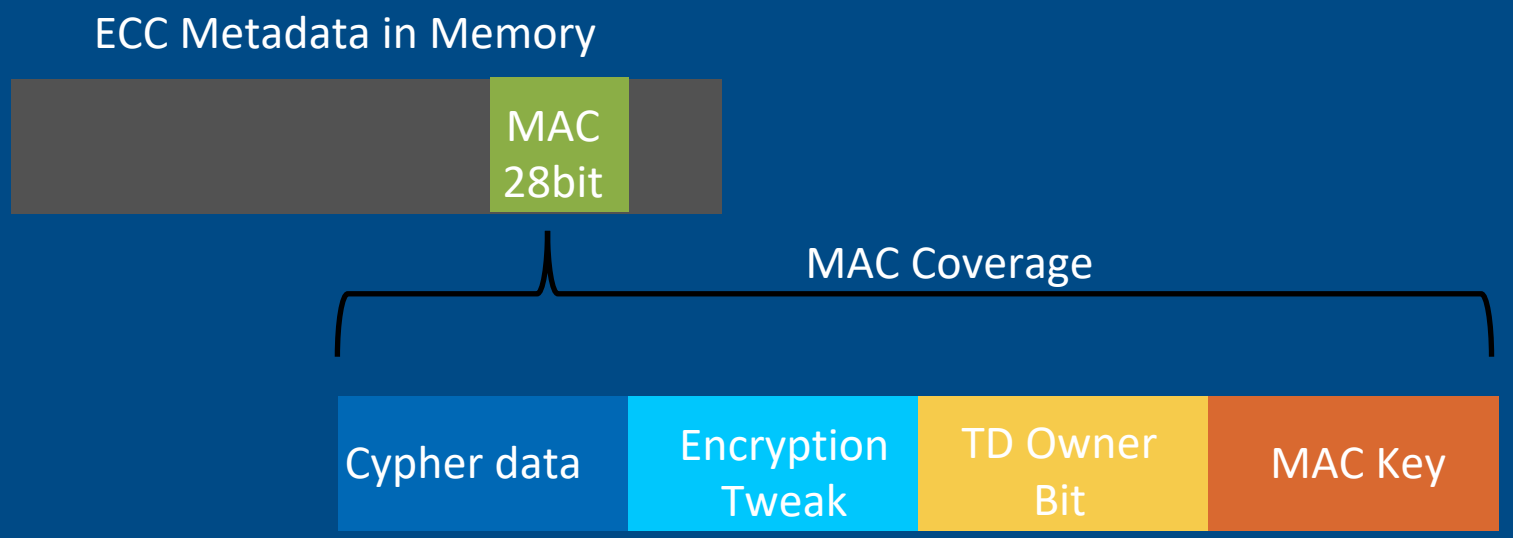
- Detect TD memory corruption before consumption.
- Resistance to brutal force attack
- Anti-dictionary attack:

  Non-TD read TD private memory return ZERO data

TD Owner bit update on write path

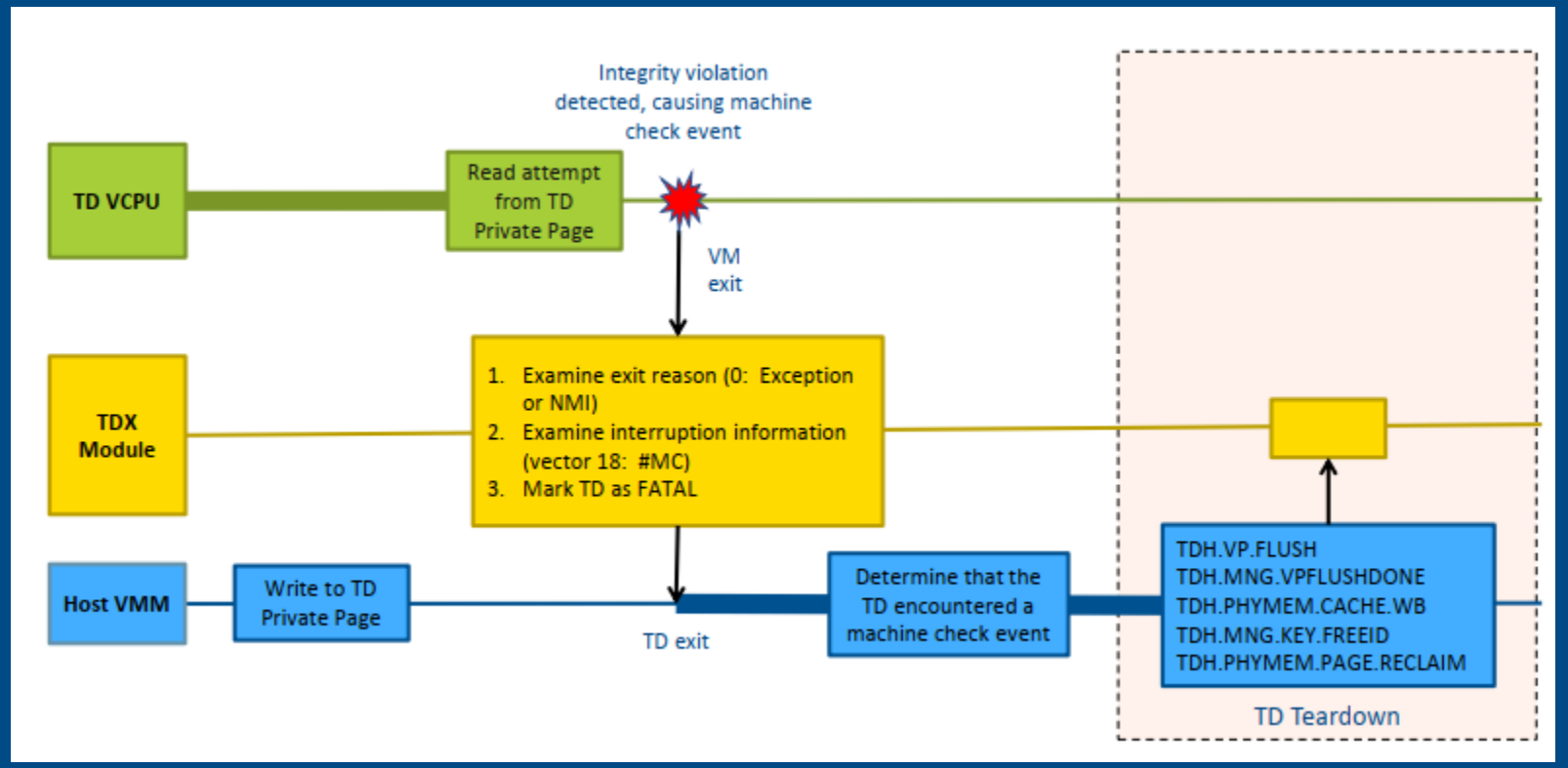


TD Owner bit checking on read path

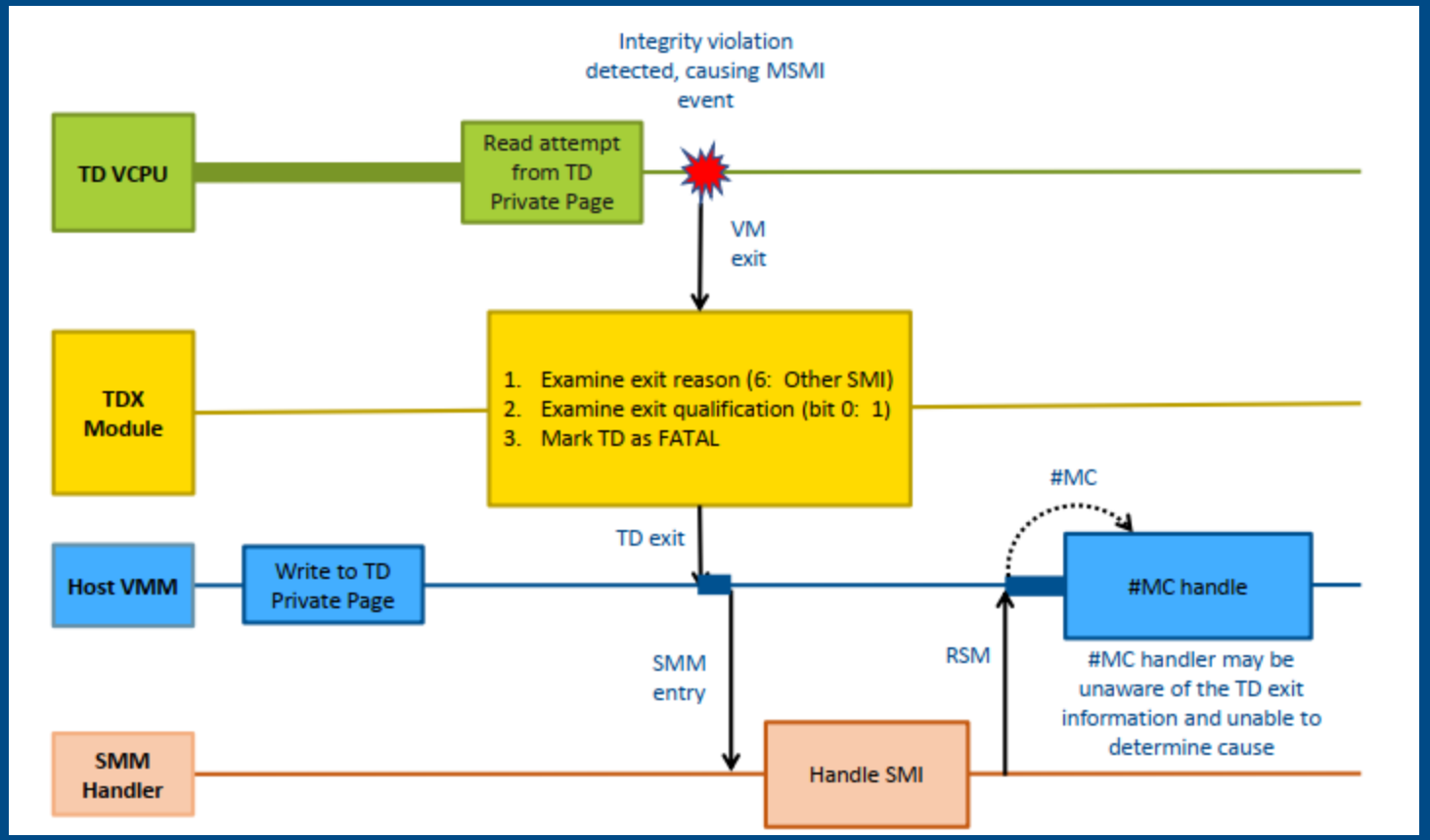


ECC Check -> MAC Check(Poison/Zero data) -> TD Owner Bit check(Poison/Zero data)

Machine Check Handing in TD Context via #MC



Machine Check Handing in TD Context – via MSMI



Machine Check Handing in TDX Module Context

- Unbreakable Shutdown, no further SEAMCALL/TDCALL allowed
- TDX function disable on platform


intel


intel


intel