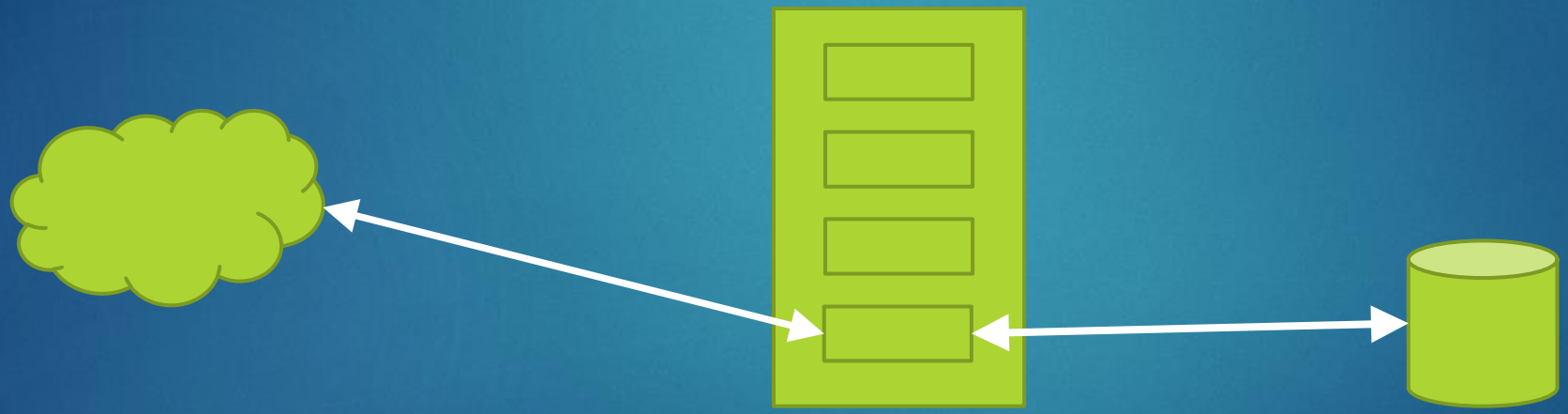
CONFIDENTIAL COMPUTING ACROSS DEVICES

JON LANGE

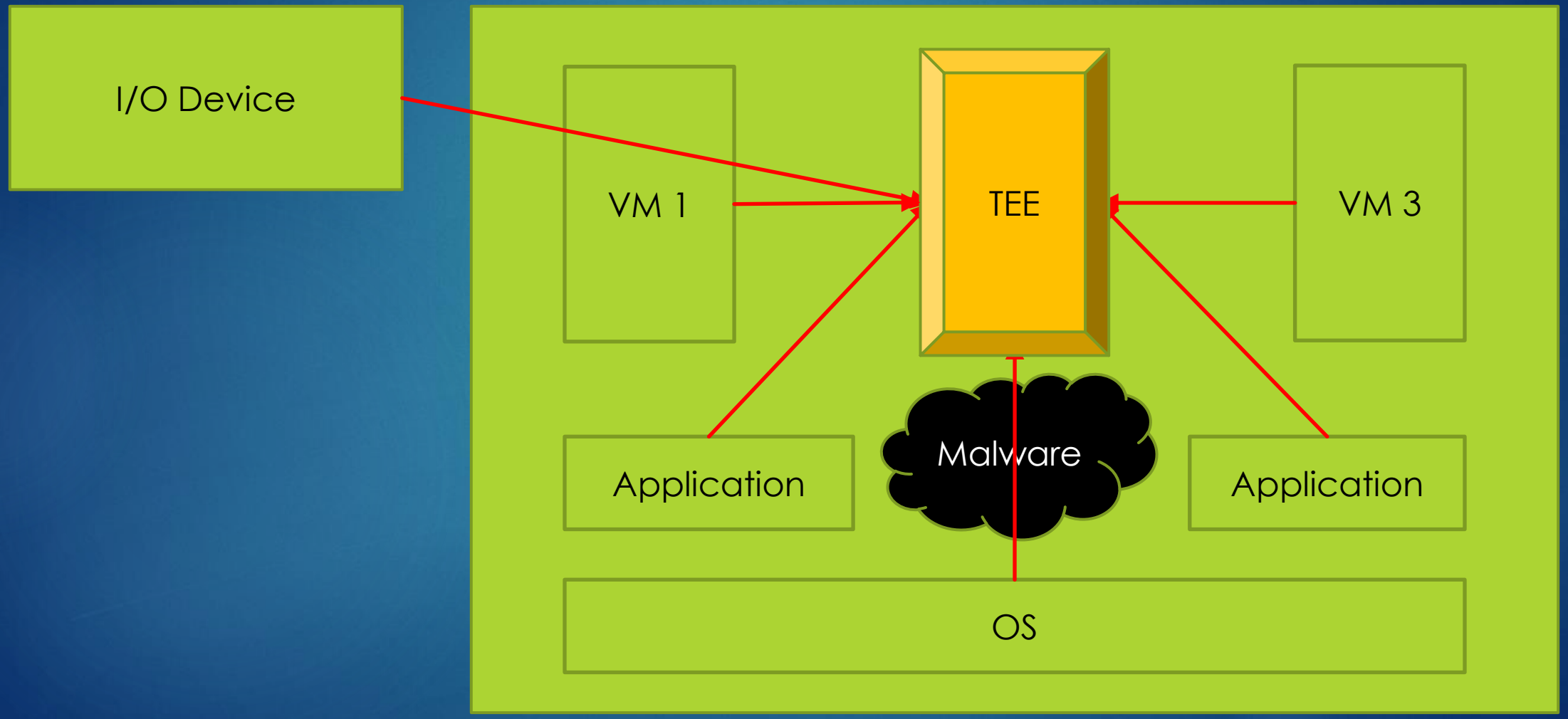
MICROSOFT CORPORATION

What is Confidential Computing?

- Confidential Computing is the **protection** of data **in use** by an **attested**, hardware-based **trusted execution environment (TEE)**.



Why protect data in use?



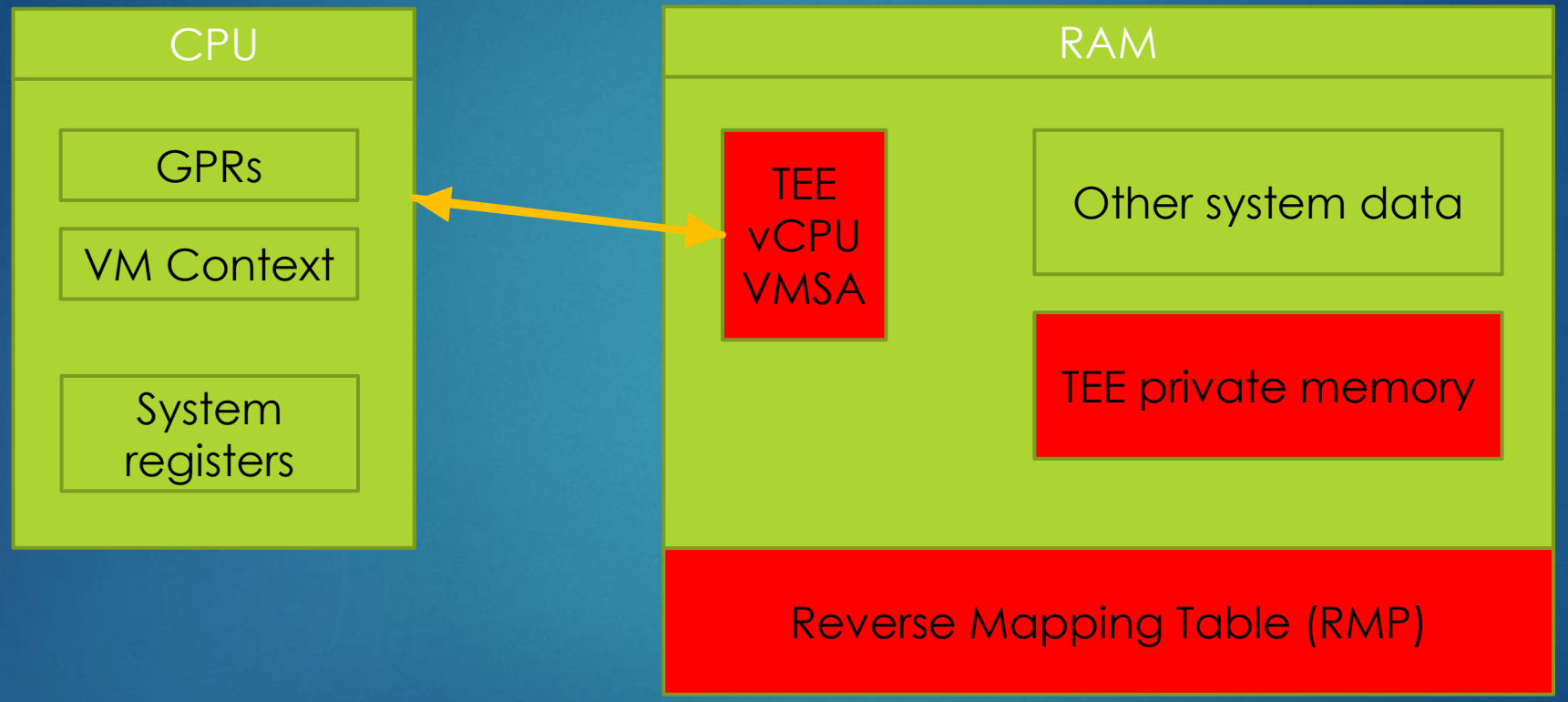
What is a hardware TEE?

- Security Properties: Code and Data
  - Confidentiality
  - Integrity
- Attestability
- Guaranteed by hardware architecture
- Examples
  - Intel SGX
  - AMD SEV-SNP
  - Intel TDX

TEE Example: SEV-SNP

- Reverse Mapping Table (RMP)
  - Stored in RAM
  - Describes VM owner and Guest Physical Address for every 4 KB page
  - Consulted during every memory access
  - Describes all of physical memory
  - Self-protecting
- Virtual Machine Save Area (VMSA)
  - Holds private CPU register state for each vCPU
  - Stored in RAM
  - Protected by the RMP

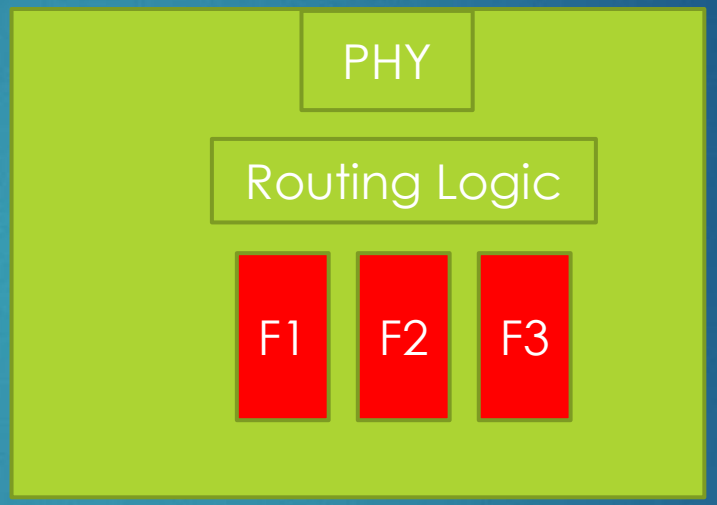
TEE example: SEV-SNP



TEE Attestation

- Platform Report
  - Describes the underlying TEE architecture
  - Describes system-wide posture (firmware, configuration)
  - Describes a public key associated with the TEE architecture
  - Endorsed by a key derived from protected hardware secrets (e.g. fuses)
  - Can be generated once at system startup
- TEE Report
  - Describes the initial content of the TEE as measured by the platform
  - Describes the configuration of the TEE
  - Can describe data provided dynamically by the TEE (e.g. a public key generated by the TEE)
  - Signed by the platform public key
  - Can be generated any time the TEE wants to update the signed data

Peripheral TEE

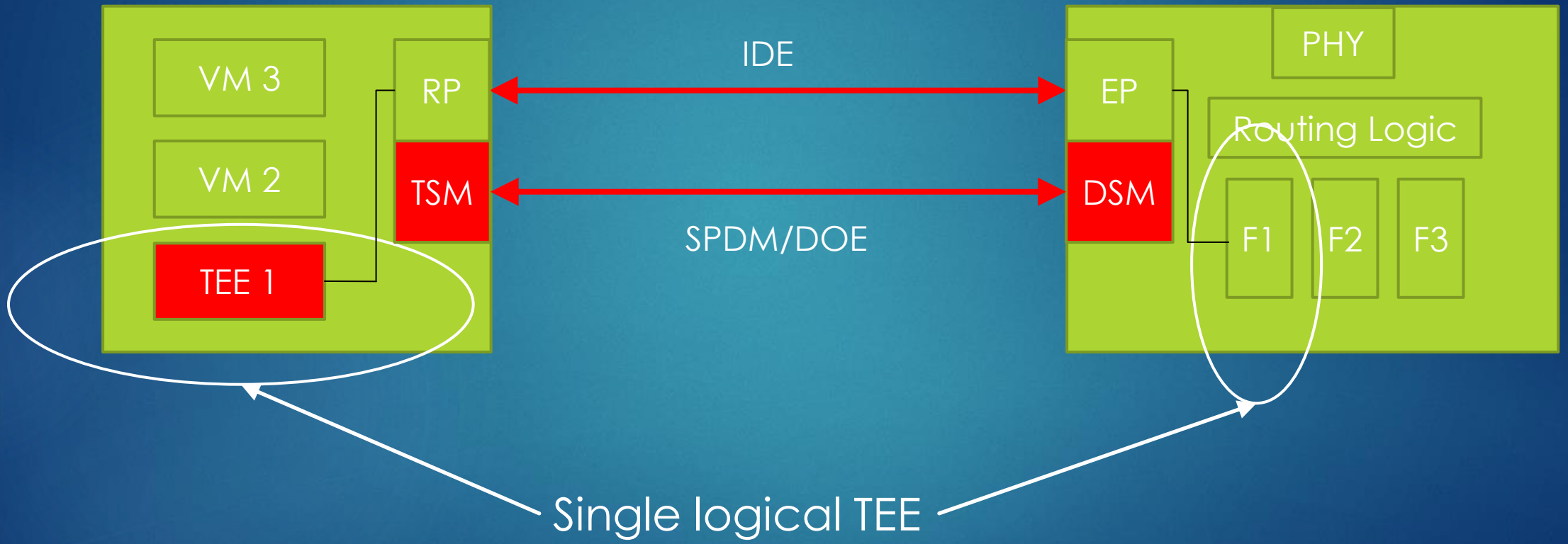


Cross-System TEE Communication

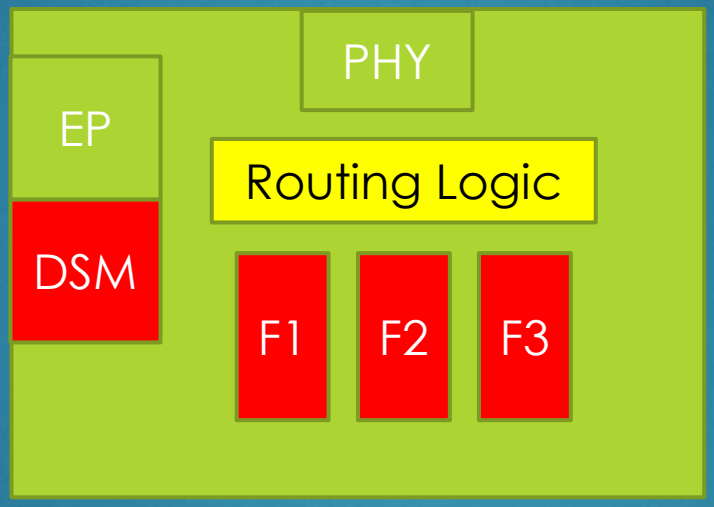
Joining TEEs: PCIe TDISP

- Transport-level encryption: PCIe IDE (Integrity and Data Encryption)
- Attestation: SPDM (Security Protocol and Data Model)
- PCIe TDISP (Trusted Data Interface Security Protocol)
  - Configuration protocol
  - Device interface lifecycle behavior

Joining TEEs: PCIe TDISP



Peripheral Attestation



Questions