SPDM Tool Project Annual Review 2025

Jiewen Yao, Intel

Samuel Ortiz, Rivos Inc

Timothy Prinz, Nvidia

Content

- Intro
- Update
- Plan
- Annual Review

Intro – Background

- Industry trend:
  - Move TEE-TCB from {SOC} only to {SOC + Device}.

- Change and Solution:
  - Host TEE needs to trust and verify the device. (via SPDM protocol)
  - Host SOC and device need a secure way to encrypt PCIe TLP. (via PCIe IDE)
  - Host TEE needs a way to manage the device. (via PCIe TDISP)

- Reference:
  - Making PCI devices ready for confidential computing, OC3, 2023
  - PCIe Base Specification 6.2, January, 2024

Intro – SPDM-RS

- A pure rust version SPDM library
  - https://github.com/ccc-spdm-tools/spdm-rs
  - Following DMTF SPDM 1.2 specification (DSP0274, DSP0277)
  - (SPDM = Security Protocol and Data Model)
- with PCIe IDE_KM and TDISP feature
  - Following PCI-SIG PCIe specification (PCIe 6.2)
  - (IDE KM = Integrity and Data Encryption Key Management Protocol)
  - (TDISP = TEE Device Interface Security Protocol)

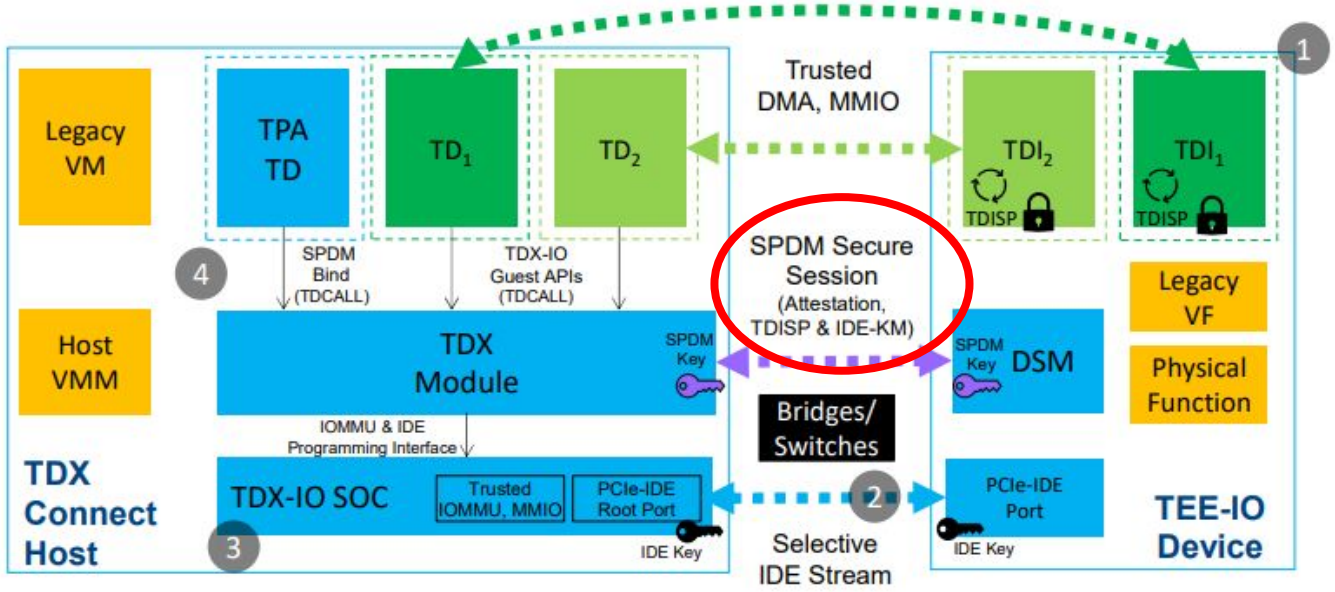
- Support SPDM Requester and SPDM Responder.

- TEE-IO Use Case (see next pages)

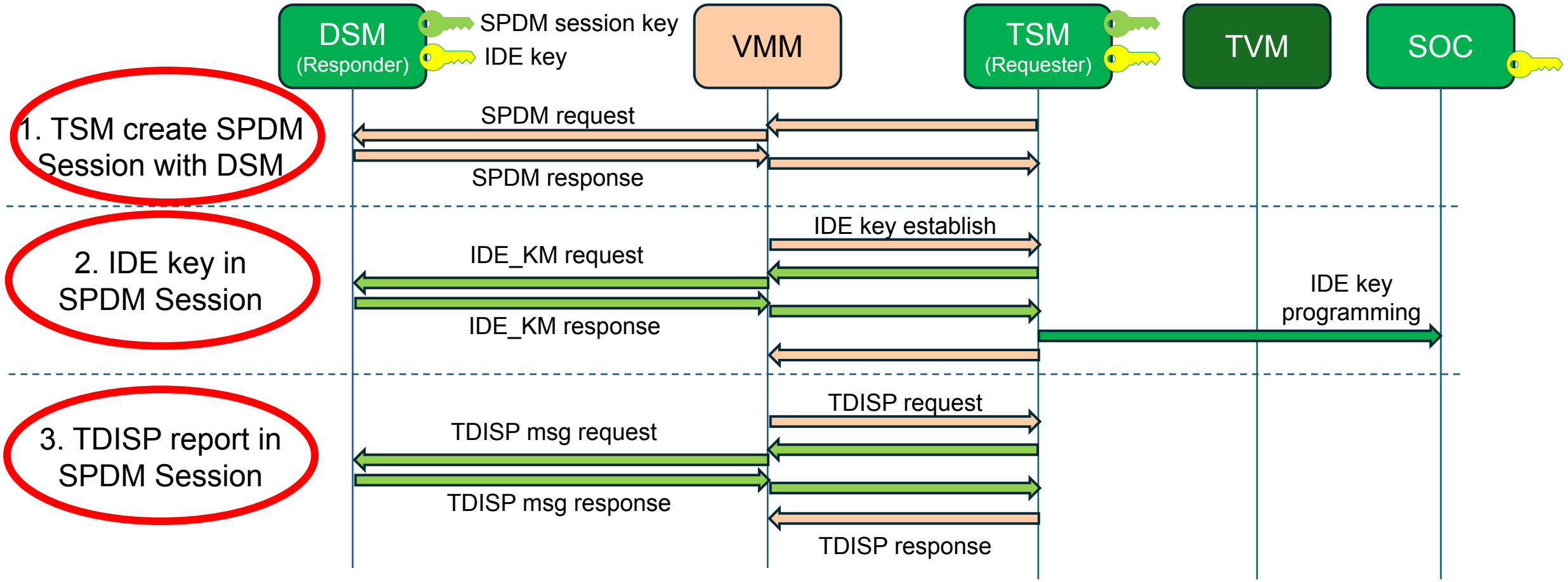
SPDM stack for TSM

- Intel TSM (TDX-module + TPA)
  - Intel® TDX Connect Architecture Specification
  - SPDM Requester
  - SPDM Device Certificate and Measurement Collection
  - SPDM Session with the device, for IDE_KM and TDISP

- SPDM candidate for any other secure TSM.

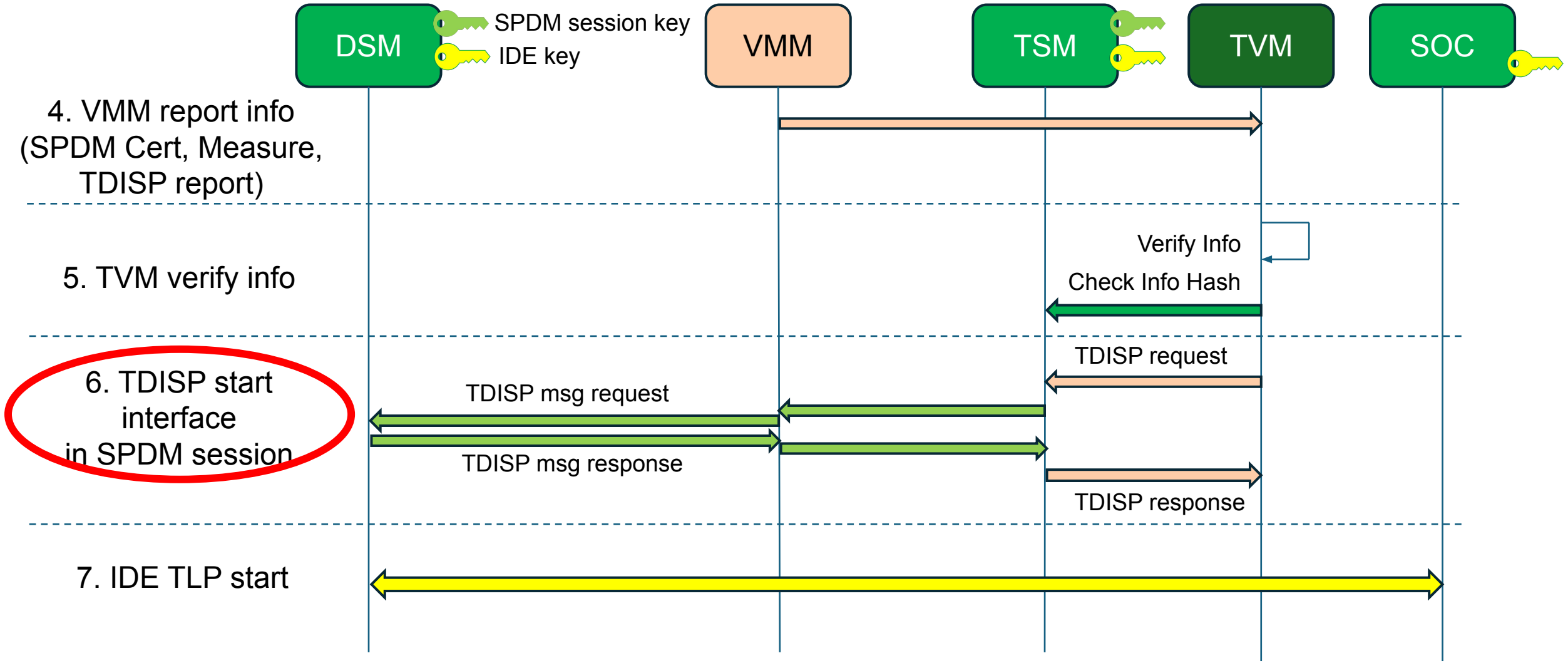


TEE-IO Use Case - Startup

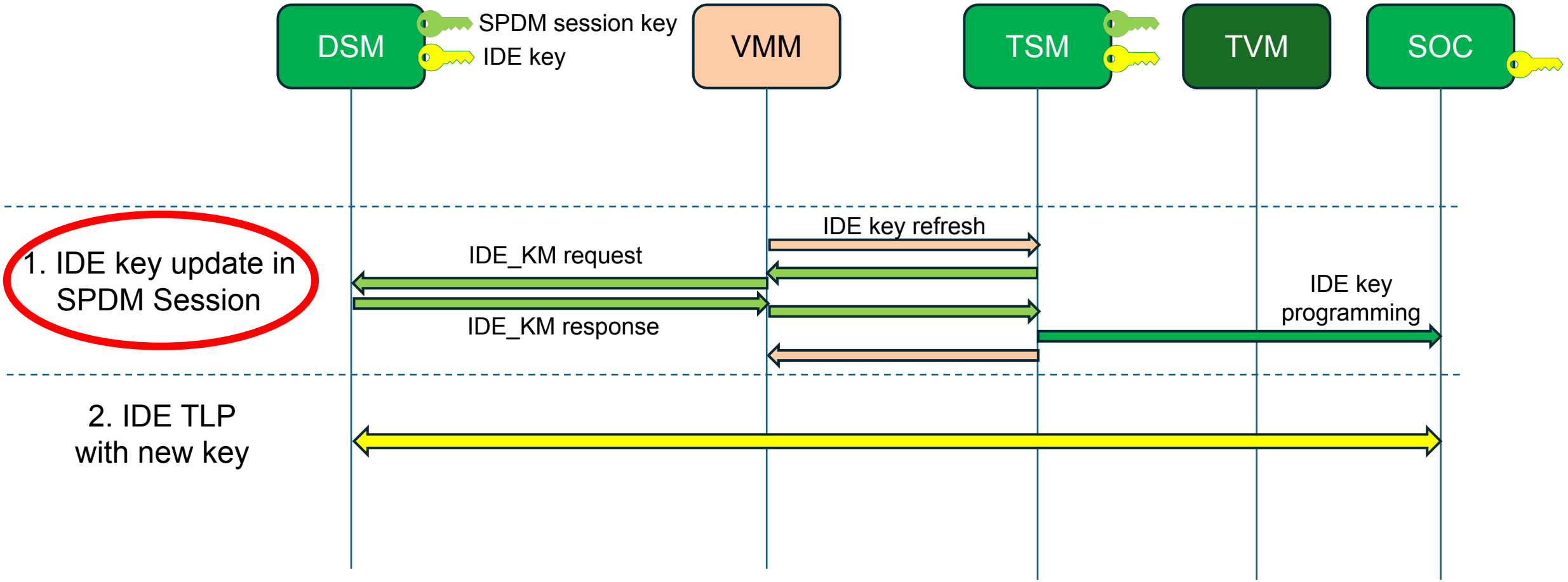


DSM: Device Security Manager
TSM: TEE Security Manager
TVM: TEE Virtual Machine

TEE-IO Use Case - Startup (Cont'd)



TEE-IO Use Case - IDE Key Refresh



Update since adoption

- Upgrading to SPDM 1.3
  - VCA, DIGEST, MEASUREMENT, CHALLENGE, KEY_EXCHANGE, PSK_EXCHANGE
- Adding FIPS self-test.
  - HASH, AEAD (AES-GCM), RSA, ECDSA
- Bug fix
  - Fix bugs in certificate chain verification, key update, etc.
  - Add more unit test.
  - Add more fuzzing test.

Plan

- SPDM version upgrade
  - Add new SPDM 1.3 feature
  - Prepare for SPDM 1.4 – PQC
- FIPS 140-3
  - Add rest FIPS crypto self-test
  - Add SPDM-Key-Exchange self-test
- More Security test
  - 3rd party penetration test (Budget Request)

Adoption in planning

- Intel TDX Connect TSM
- Rivos Salus TSM

Annual Review

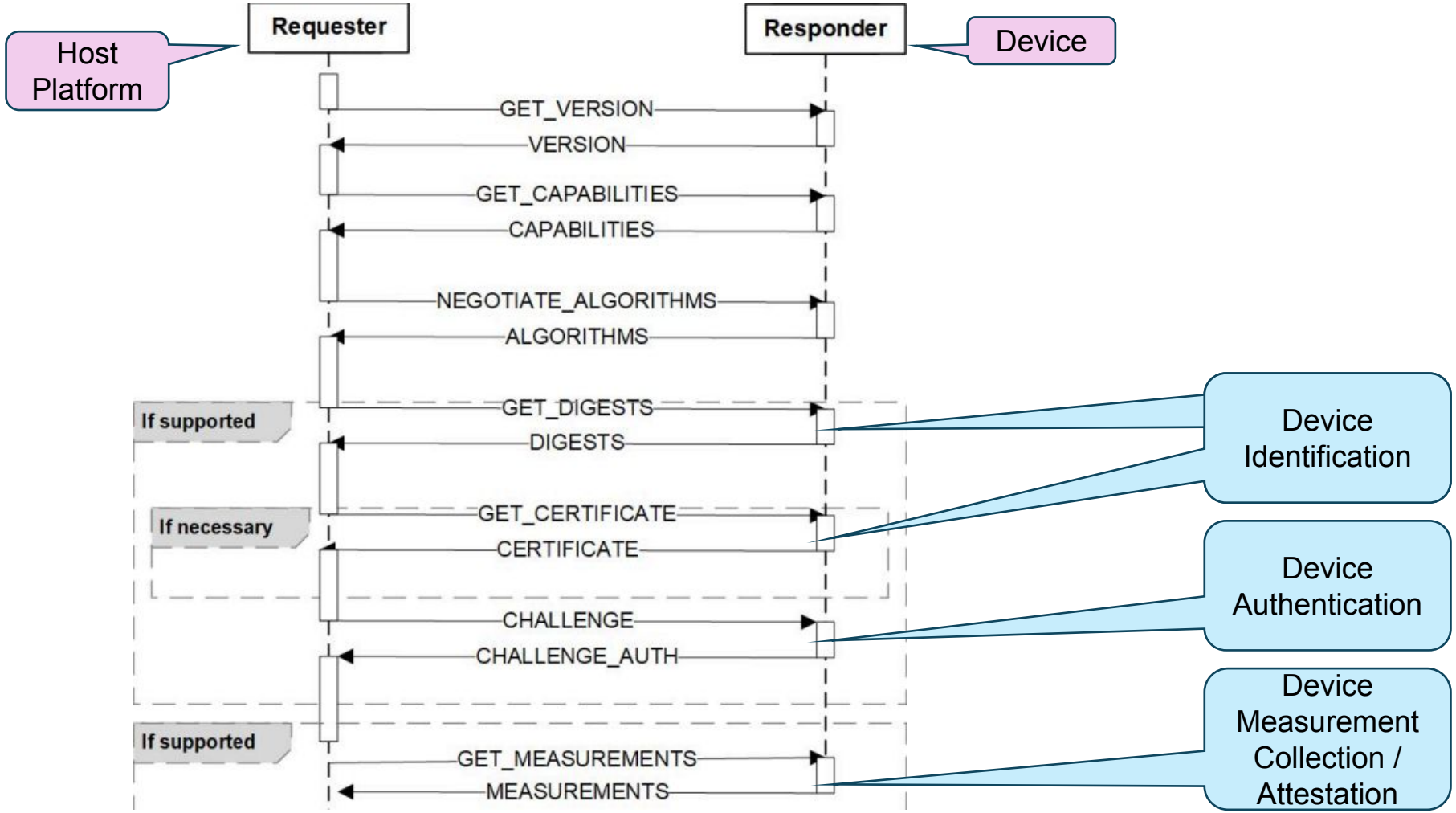
- Charter – No Change
- Project Status – On Track
- Budget – **May request budget for security audit (penetration test).**
- License – No Change
- OpenSSF Best Practices Badge – 97%.

Backup

What is SPDM?

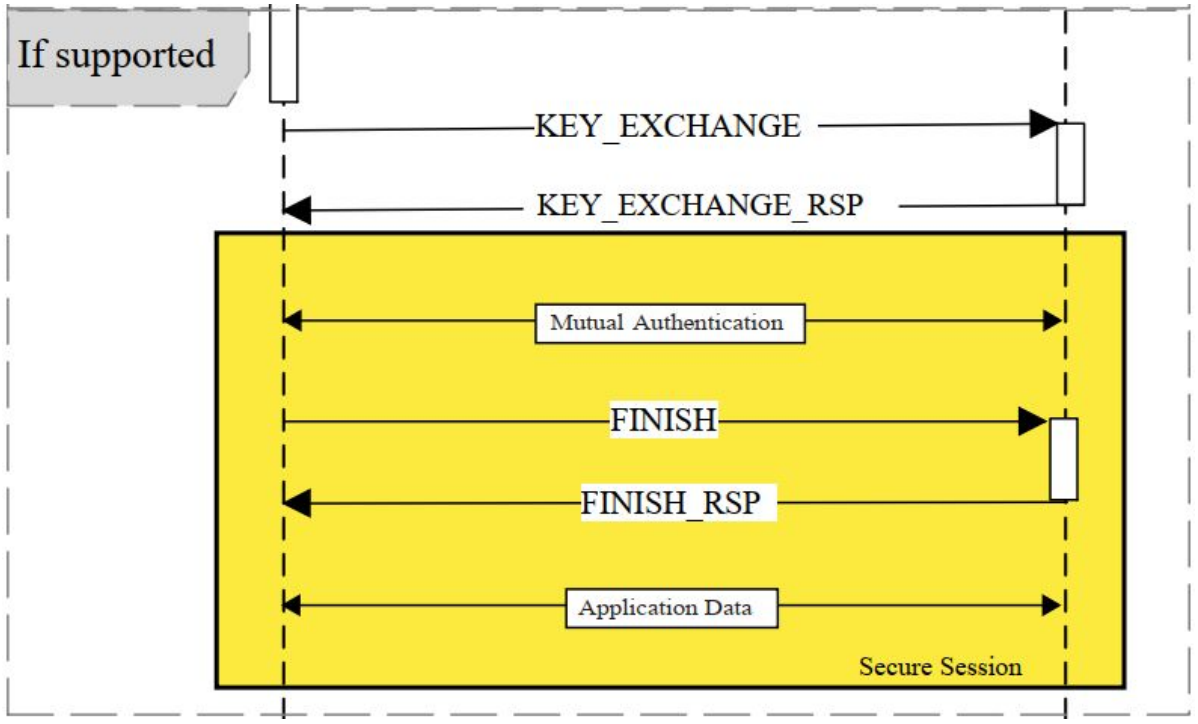
- Security Protocol and Data Model (SPDM)
  - DSP0274 - https://www.dmtf.org/dsp/DSP0274
  - Defined by DMTF SPDM WG - https://www.dmtf.org/standards/spdm
- Version
  - SPDM 1.0 (Dec 2019) – Device Authentication and Measurement.
  - SPDM 1.1 (August 2020) – Device Secure Session Communication.
  - SPDM 1.2 (Dec 2021) – DICE support, Device Provisioning, Message Chunking.
  - SPDM 1.3 (May 2023) – Multiple Key support, Hash Extend Measurement (HEM), Measurement Extension Log (MEL), Async Event.
- Adoption
  - DMTF, PCI/CXL, TCG, MIPI, NVMe, …

SPDM 1.0



* source: SPDM 1.0 specification

SPDM 1.1



Diffie-Hellman (DH) based Key Exchange + (Mutual) Authentication

or

Pre-Shared Key (PSK) based Key Exchange

* source: SPDM 1.1 specification

SPDM use case in Confidential Computing

- A. Device Attestation
  - PCI Component Measurement and Authentication (CMA)
- B. Device Secure Communication
  - PCI Integrity and Data Encryption (IDE) Key Management (KM) – IDE_KM
  - PCI TEE Device Interface Security Protocol (TDISP)
- C. Secure Communication between two TEEs
  - Candiate: TLS, SPDM, …

Rust-SPDM Overview

- The Rust implementation of SPDM protocol.
  - https://github.com/intel/rust-spdm
  - Apache 2.0 License
  - SPDM version 1.2
  - Support SPDM Requester and SPDM Responder
  - Support rust no-std.
  - Use ring/webpki crypto stub by default.
    - rust-mbedtls as backup.
  - Interoprability test with DMTF libspdm sample implementation.