

presented by



Microsoft



Using SPDM in UEFI for Device Attestation

UEFI Fall 2023 Developers Conference & Plugfest

October 9-12, 2023

Presented by:

Jiewen Yao (Intel), Michael Kubacki (Microsoft), Vincent Zimmer (Intel)

Agenda

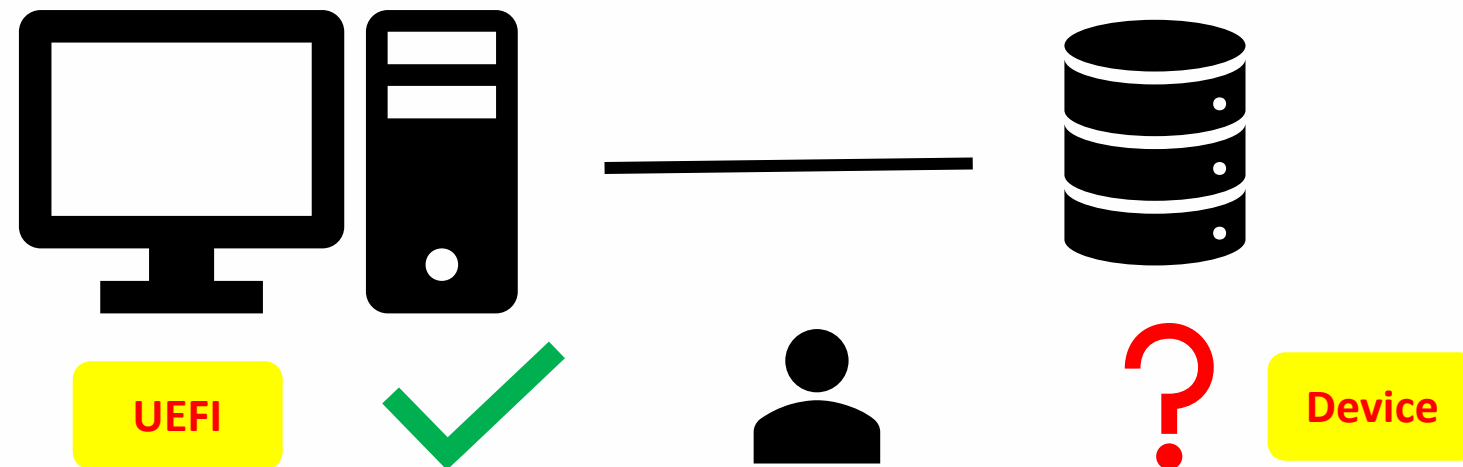


- Problem Statement
- Solution – SPDMM
 - DMTF
 - UEFI
 - TCG
- EDKII - Device Security POC
- Surface Experience
- Demo



Problem Statement

- During System Boot:
 - How I know the **attached devices** on the platform are trusted?
- After System Boot:
 - How I know the system booted with the **known good devices**?



How to extend the trust from the platform to the devices?



Solution

Specification – SPDMM



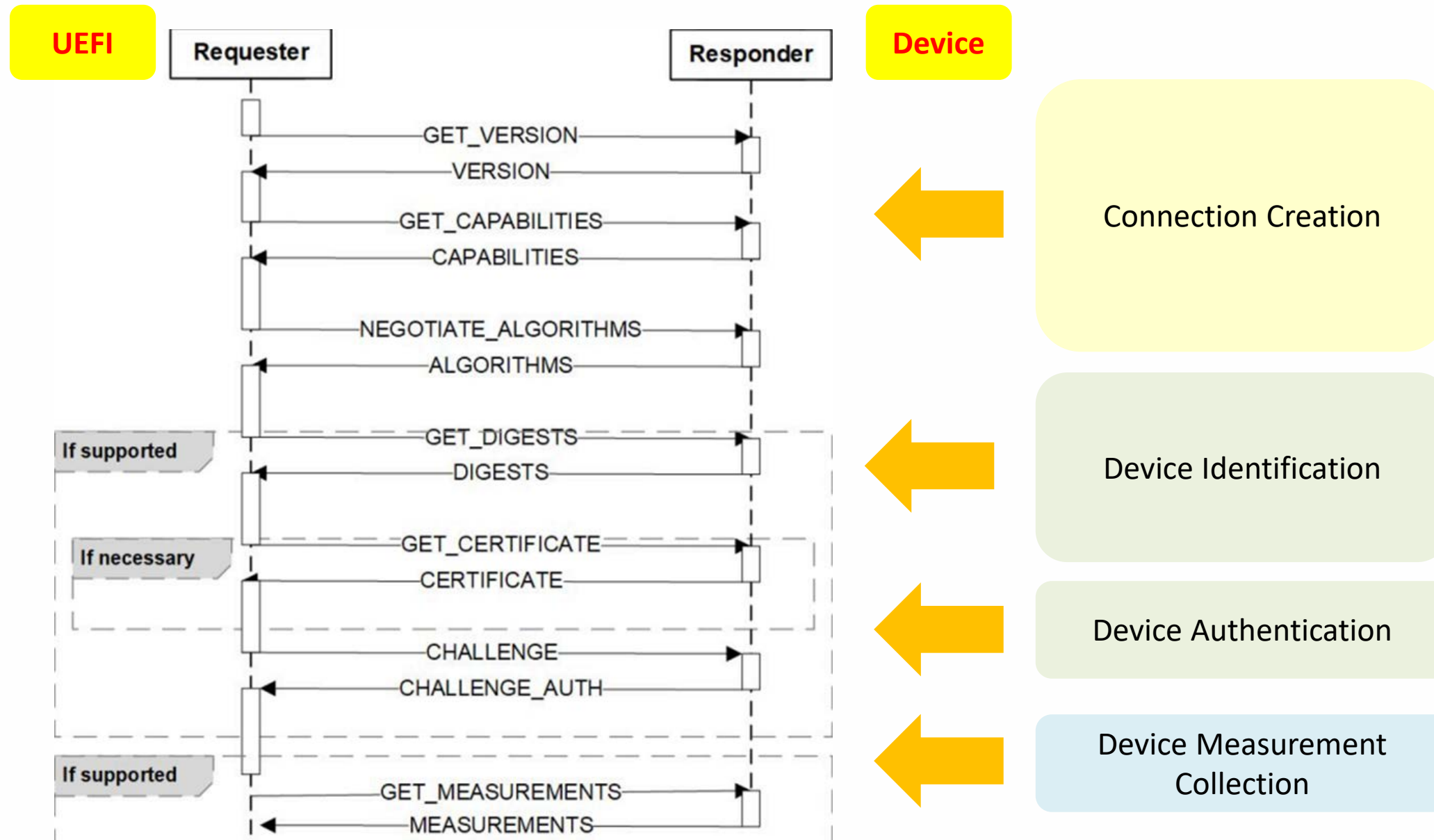
- Security Protocol and Data Model – from DMTF
 - SPDMM 1.0 (2019): **device authentication and measurement collection.**
 - SPDMM 1.1 (2020): secure session, mutual authentication.
 - SPDMM 1.2 (2021): alias certificate, certificate provisioning, message chunking.
 - SPDMM 1.3 (2023): event notification, measurement extension log, multiple key.

Alliance Partners and Adopters



Source: https://www.dmtf.org/sites/default/files/SPDM_1.3_and_Beyond_2023-08.pdf

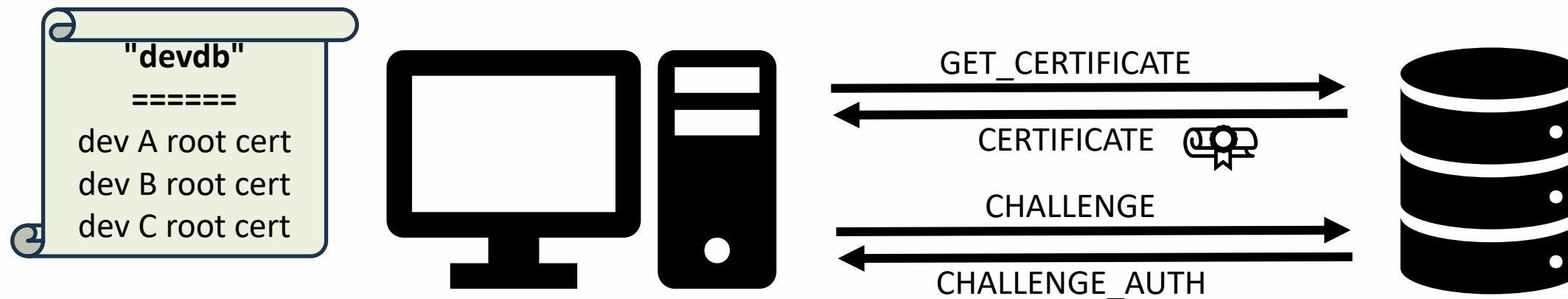
SPDM Attestation and Authentication



Specification – UEFI



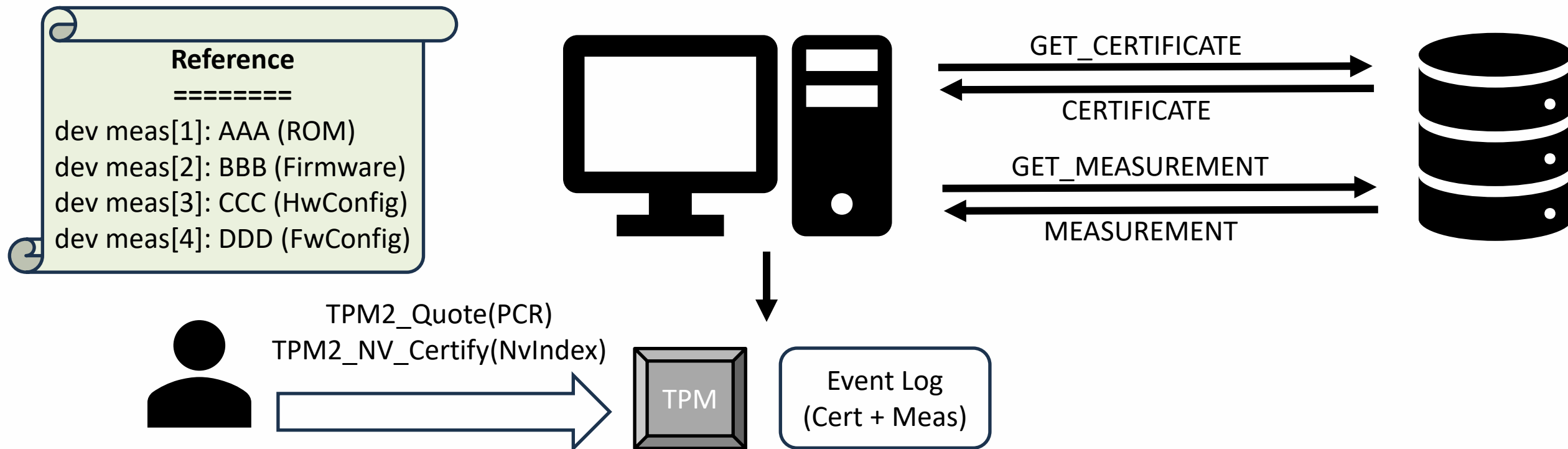
- UEFI 2.10 adds **Device Authentication**.
 - L"devdb": device security database -> device trust anchor
 - L"devAuthBoot": enable/disable device authentication.
 - UEFI may
 - Get device certificate and challenge the device.
 - Check if the device cert is endorsed by the device trust anchor.
 - Ignore/Disable the device in case of failure.



Specification – TCG PC Client PFP



- PC Client PFP 1.06 (draft) adds **device measurement**
 - SPDM Device Measurement => TPM PCR + EventLog (class data)
 - SPDM Device Certificate => TPM NvIndex + EventLog (instance data)
 - SPDM Device Auth Nonce => TPM NvIndex + EventLog (dynamic data)



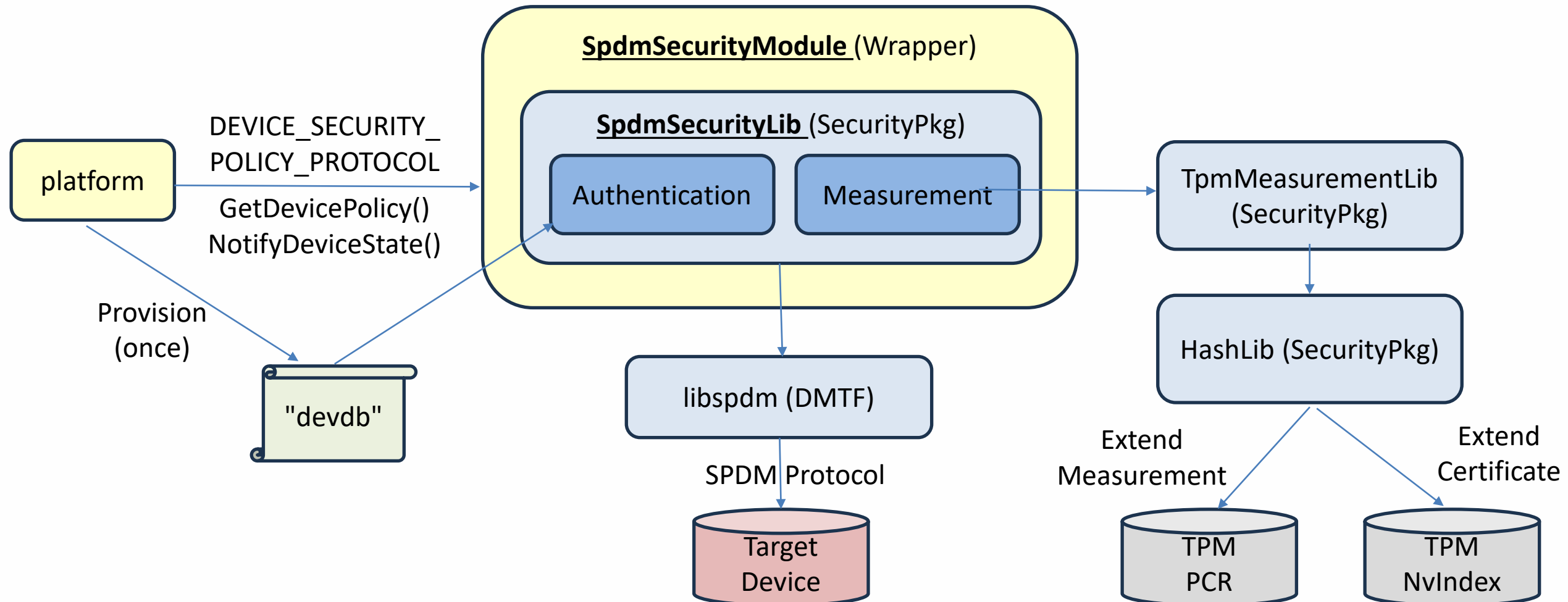


Implementation POC

EDKII – Device Security POC



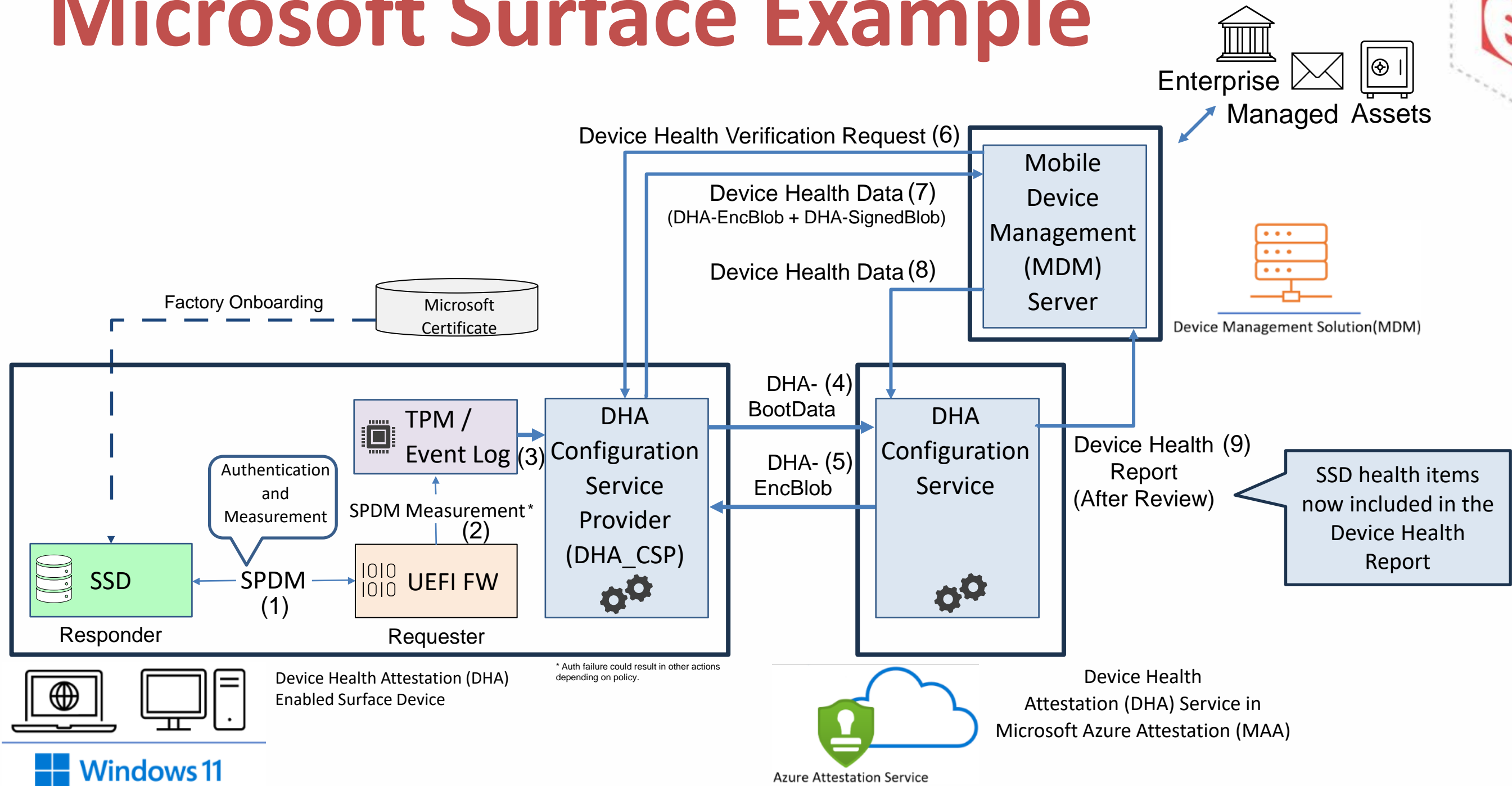
- EDKII Staging – DeviceSecurity Branch





Use Case

Microsoft Surface Example





Demo

Reference



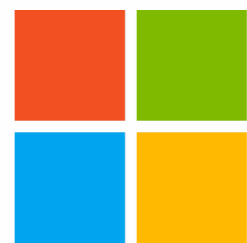
- DMTF, SPDM Specification 1.3
 - <https://www.dmtf.org/dsp/DSP0274>
- UEFI, UEFI Specification 2.10 – Device Authentication
 - https://uefi.org/specs/UEFI/2.10/32_Secure_Boot_and_Driver_Signing.html#device-authentication
- TCG, PC Client Platform Firmware Profile (PFP) Specification 1.06 (Draft),
 - https://trustedcomputinggroup.org/wp-content/uploads/TCG-PC-Client-Platform-Firmware-Profile-Version-1.06-Revision-49_31July2023.pdf
- Jiewen Yao, Xiaoyu Ruan, "An open source SPDM implementation for secure device communication", OSFC, 2020,
 - <https://cfp.osfc.io/osfc2020/talk/ECQ88N/>
- Amy Nelson, Jiewen Yao, Vincent Zimmer, "Traceable Firmware Bill of Materials Overview", UEFI Webinar, 2021
 - <https://uefi.org/sites/default/files/resources/Traceable%20Firmware%20Bill%20of%20Materials%20-%2020211207%20-%200007.pdf>
- DMTF, SPDM sample implementation and emulator
 - <https://github.com/DMTF/libspdm>, <https://github.com/DMTF/spdm-emu>
- EDKII, Device Security POC
 - <https://github.com/tianocore/edk2-staging/tree/DeviceSecurity>
- Microsoft, Device Health Attestation
 - <https://learn.microsoft.com/en-us/windows-server/security/device-health-attestation>
 - <https://learn.microsoft.com/en-us/windows/client-management/mdm/healthattestation-csp>



Thanks for attending the UEFI Fall 2023
Developers Conference & Plugfest

For more information on UEFI Forum and UEFI
Specifications, visit <http://www.uefi.org>

presented by



Microsoft