presented by

SECURE CONNECTIONS
FOR A SMARTER WORLD

Capsule update with MM

Fall 2018 UEFI Plugfest

October 15 – 19, 2018

Presented by:

Meenakshi Agrawal (NXP Semiconductor)

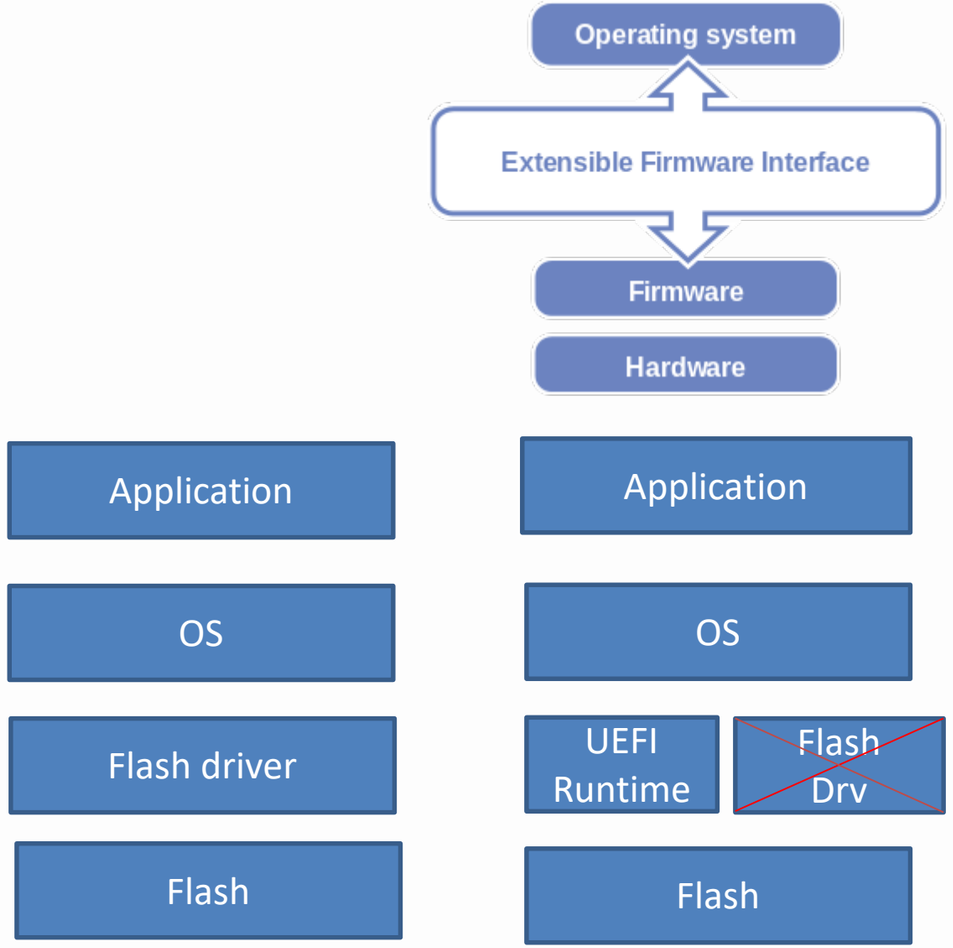
Udit Kumar (NXP Semiconductor)

Agenda

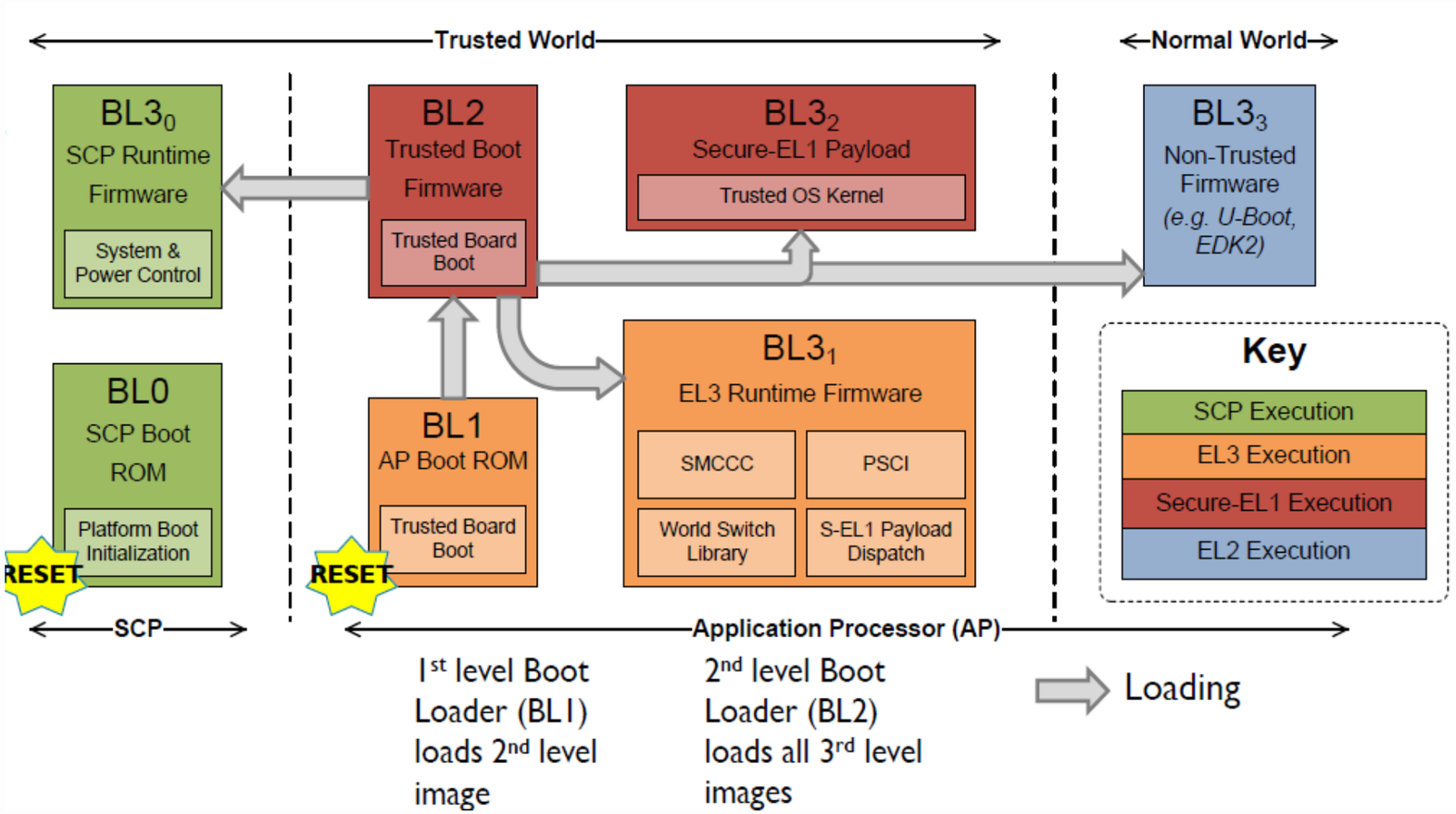
- Introduction
- Arm® boot flow
- Capsule Structure
- Updating capsule with MM
- Advantage
- Questions

Introduction

- Why we need capsule update
  - New features
  - Bug fixes
- How to update firmware
  - OS
  - UEFI Runtime
  - Some Service processor
- Thing to take care
  - Security
  - Reliability



Arm Boot flow

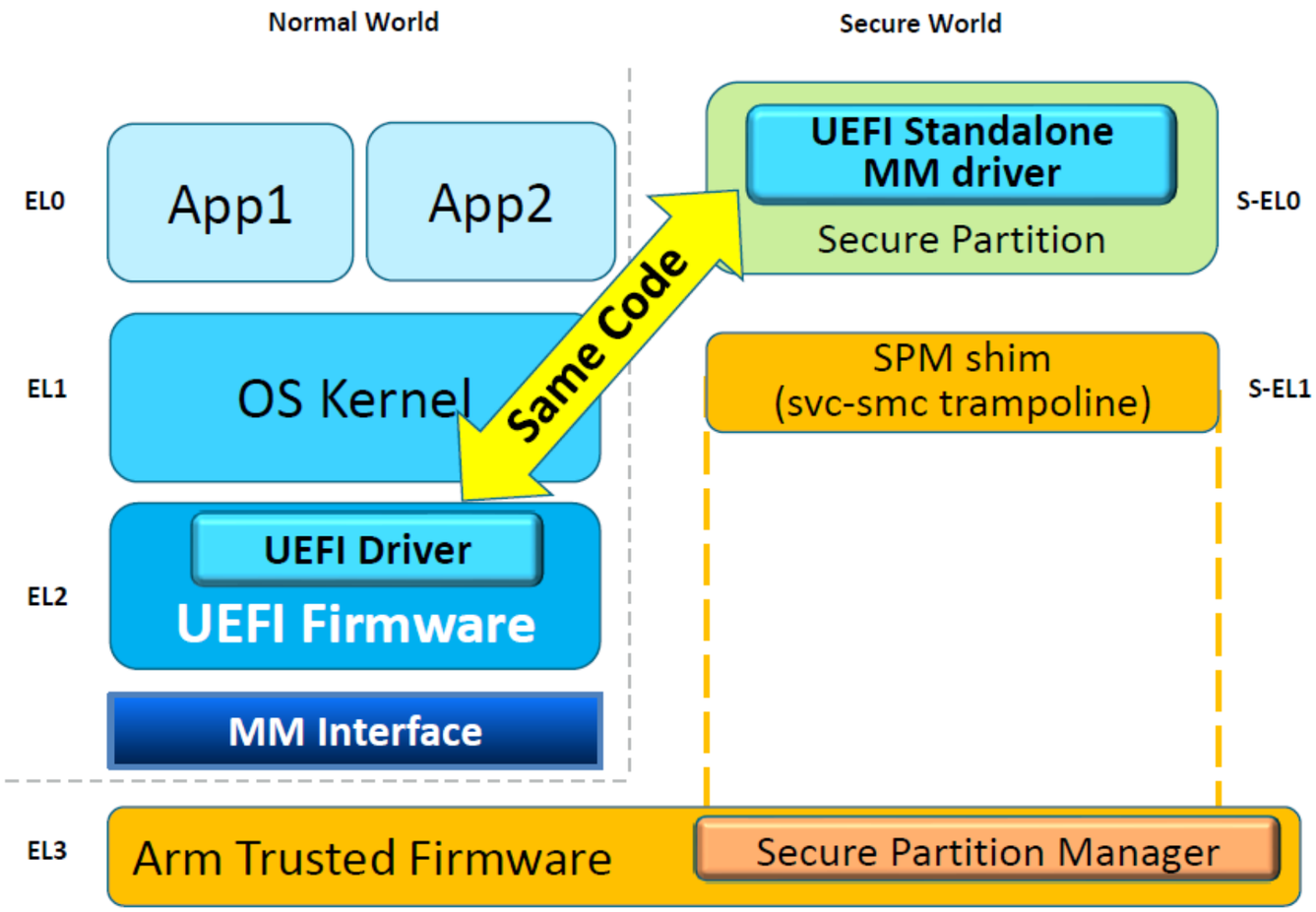


Who should own the flash BL3 runtime or UEFI

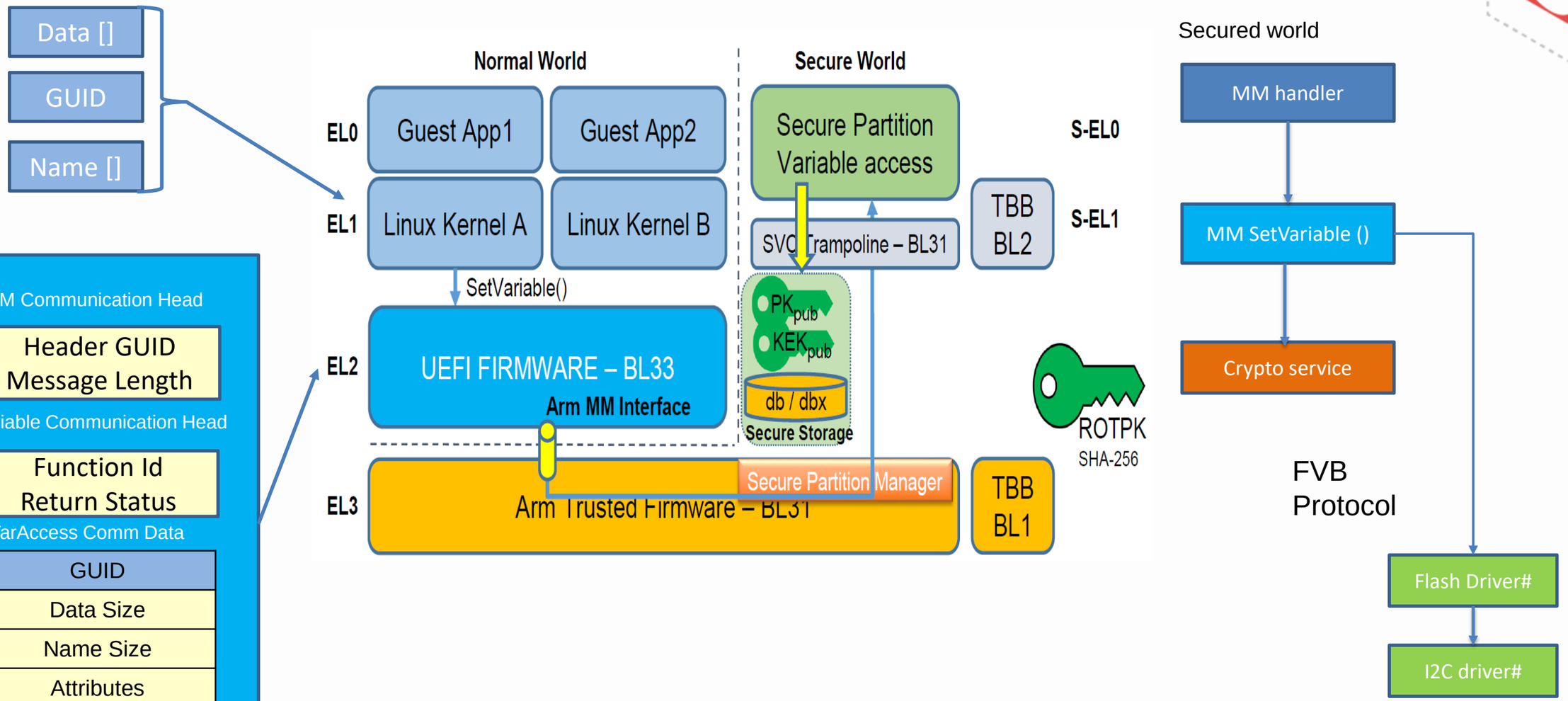
- BLx is also stored on flash
- Security ??

MM mode

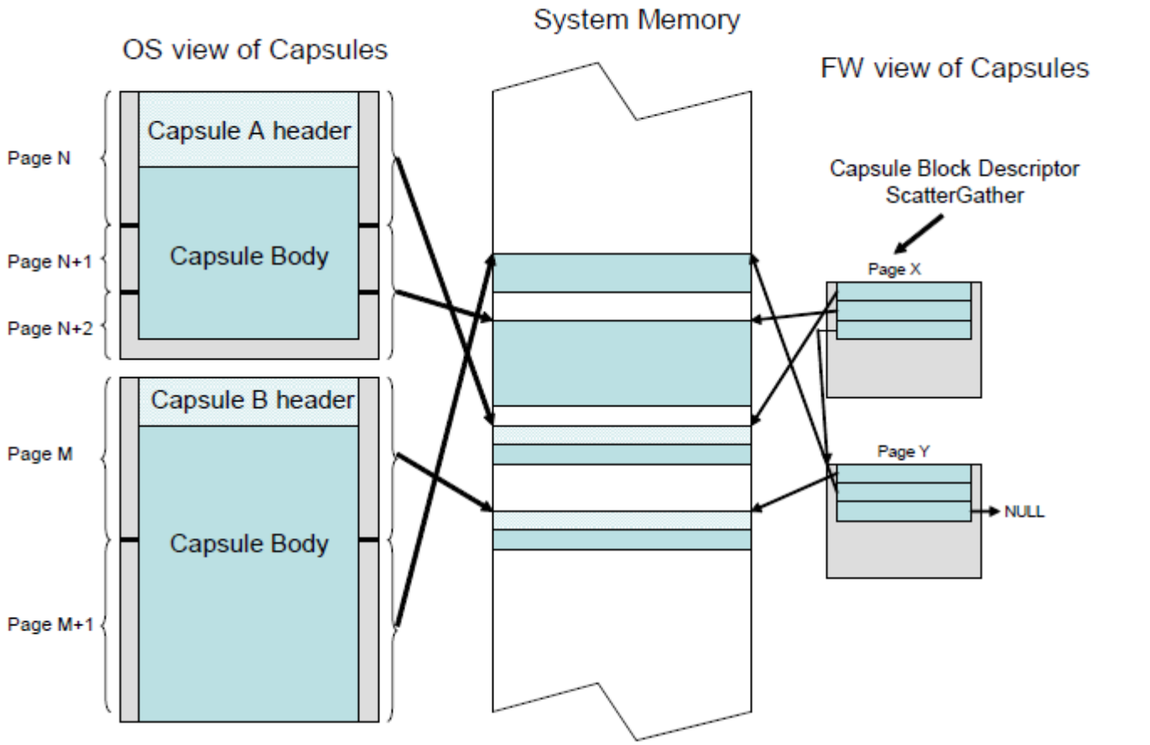
Can secure side of UEFI own flash driver ???

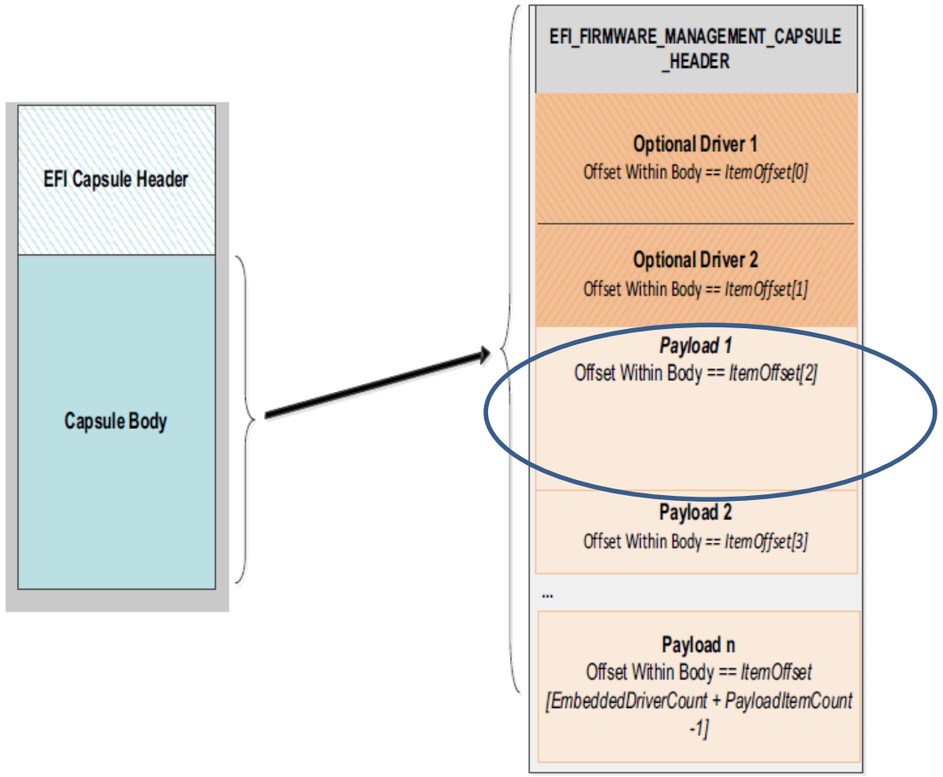


Arm : Set Variable

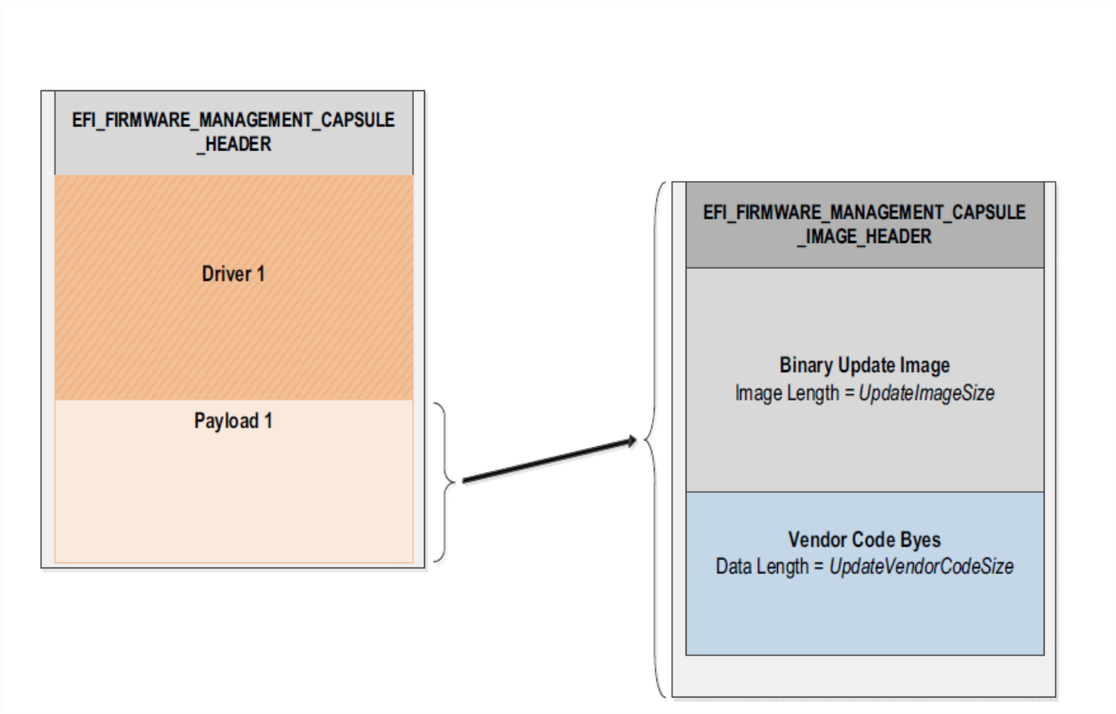


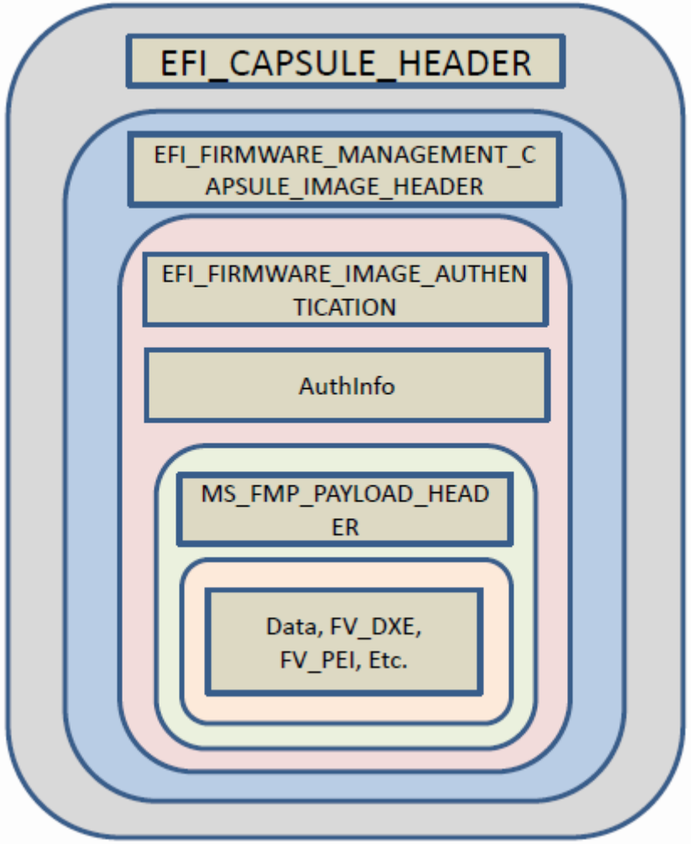
Capsule Structure



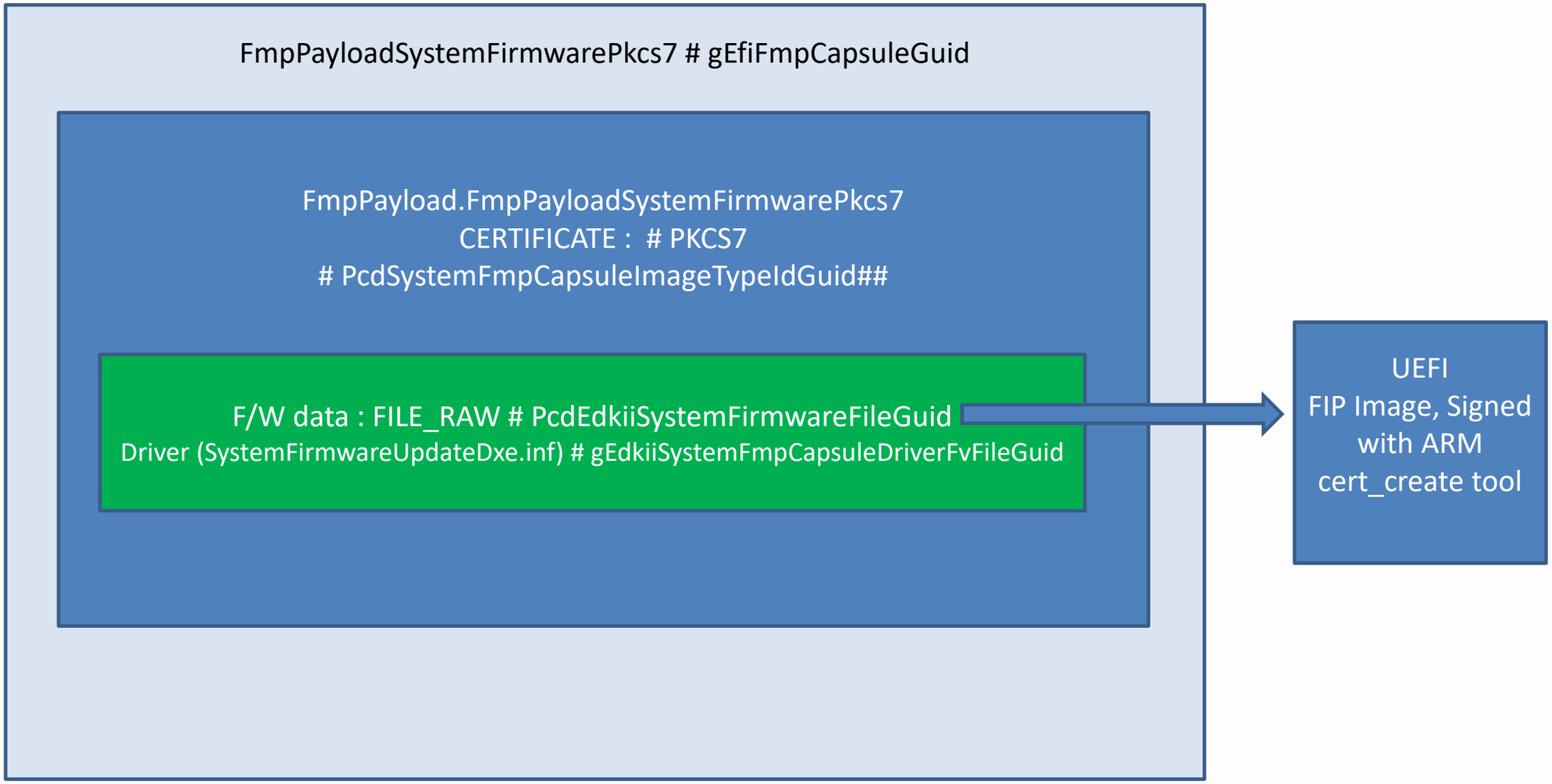


Capsule Structure

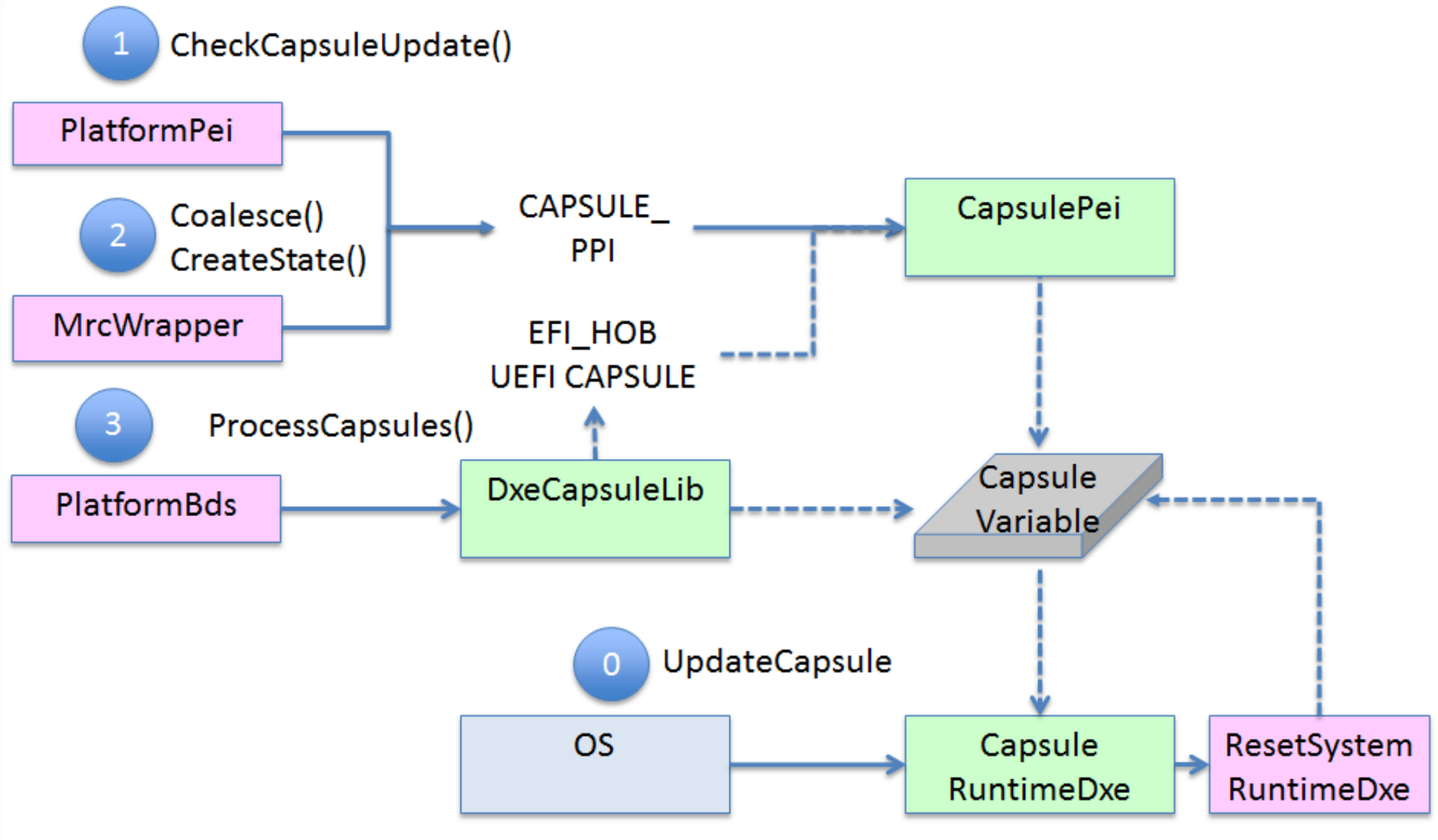




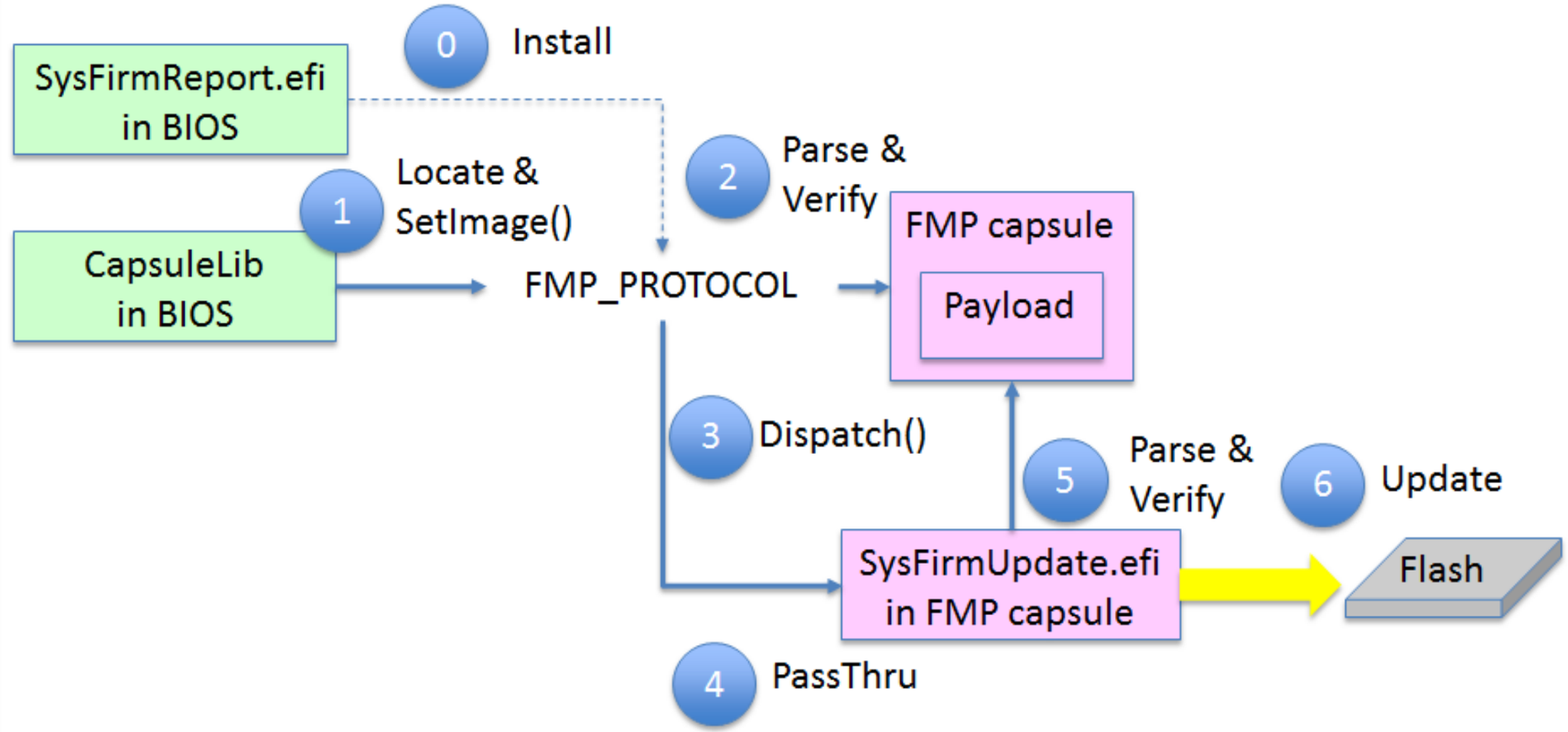
How to build capsule



Traditional Update flow

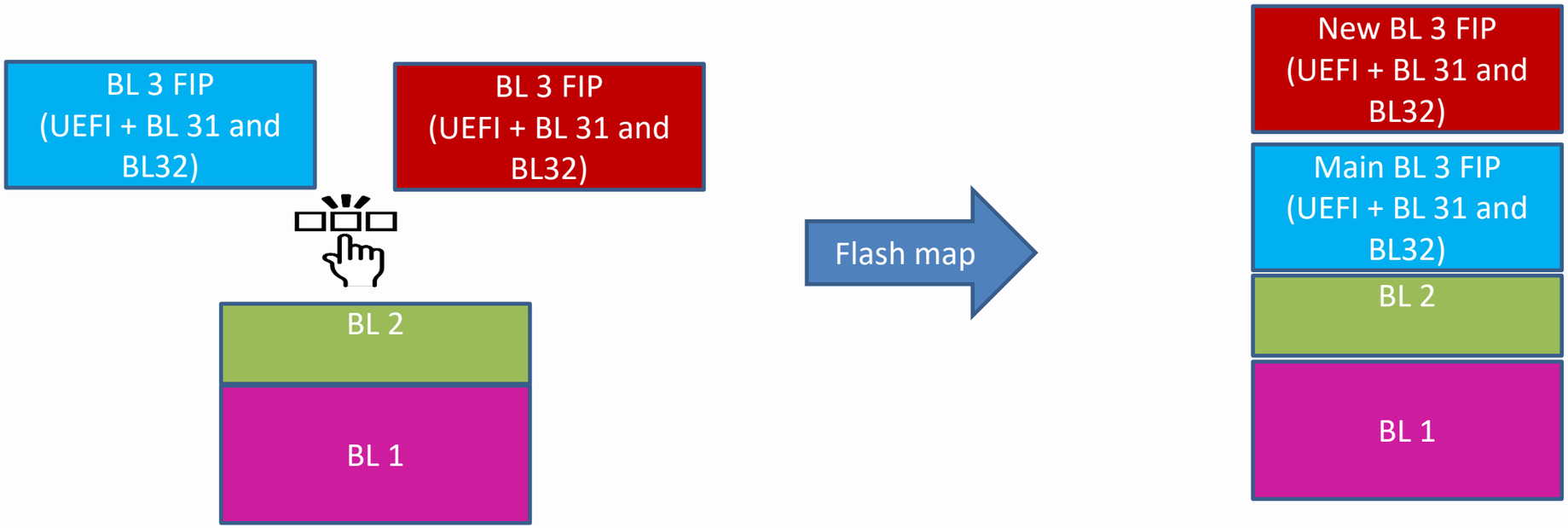


Traditional Update flow

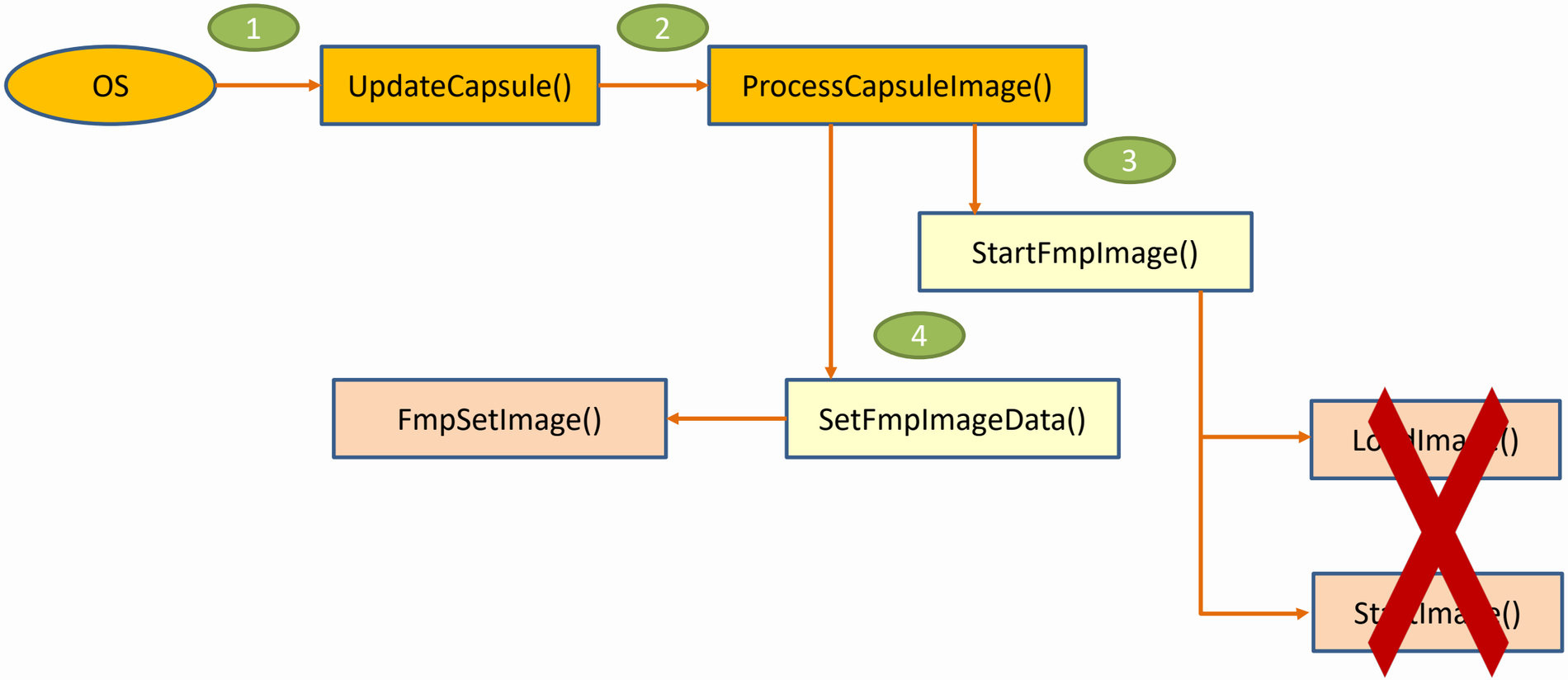


Few rules/OEM specific

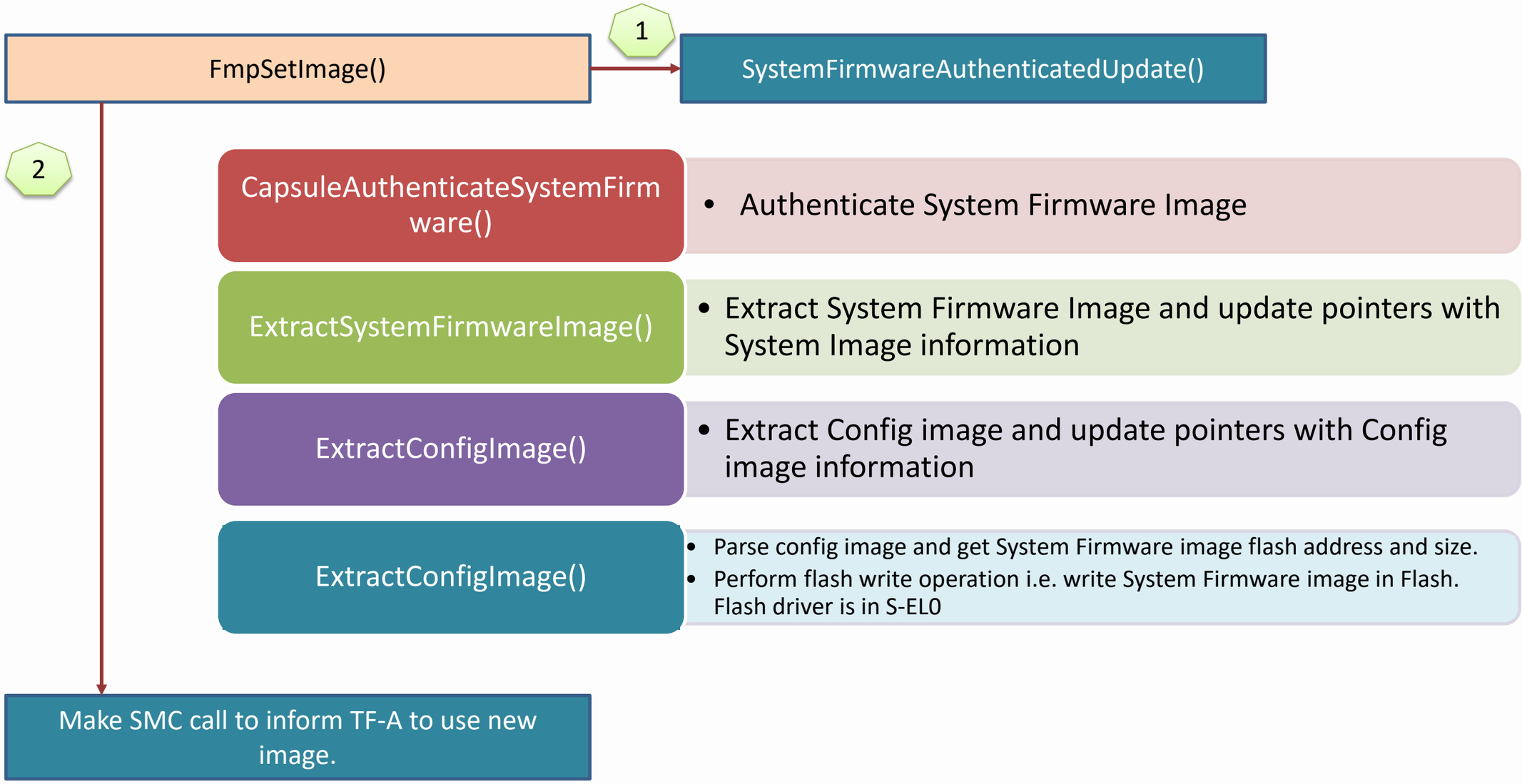
- Flash Storage should accommodate two copies of firmware
- One latest copy and another copy for fallback
- BL2 Image should choose between latest/recovery firmware
- Fip image will be updated (BL31, BL32 and BL33) combined (Consider as RAW FILE)



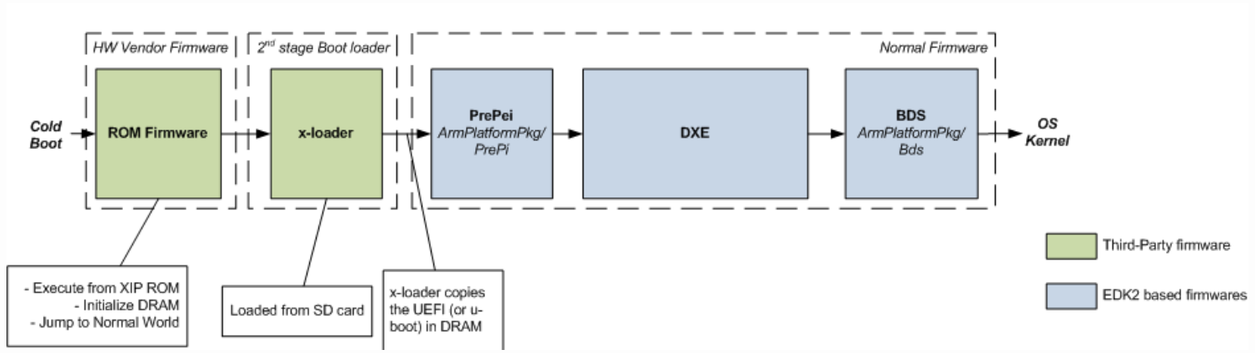
Updating capsule with MM



Updating capsule with MM



Advantage



- Security
- Can be used with thin PrePei way of working

References/Acknowledgment

- UEFI Specification 2.7
- ARM TF-A (https://github.com/ARM-software/arm-trusted-firmware/tree/master/docs)
- A_Tour_Beyond_BIOS_Capsule_Update_and_Recovery_in_EDK_II (https://github.com/tianocore-docs/Docs/raw/master/White_Papers/A_Tour_Beyond_BIOS_Capsule_Update_and_Recovery_in_EDK_II.pdf)
- Microsoft Walkthrough on Firmware Updates (http://www.uefi.org/sites/default/files/resources/Microsoft_Spring%202018%20UEFI_Plugfest_Template_Day3.pdf)
- EDK-II source code
- ARM TZ


QUESTIONS?

Thanks for attending the Fall 2018 UEFI Plugfest

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

presented by

SECURE CONNECTIONS FOR A SMARTER WORLD