ByteDance 字节跳动

Intel® Universal Scalable Firmware (USF) Strategy and Intel® Firmware Support Package (Intel® FSP)

Yufu(Kevin) Li, Firmware Director, Intel
Daocheng(Amos) Bu, Firmware Architect, Intel
Vincent Zimmer, Senior PE, Chief Firmware Architect, Intel

Agenda

- Intel ® Universal Scalable Firmware Strategy
- Intel ® Universal Scalable Firmware Practice
- Intel ® Firmware Support Package Overview
- Intel ® Firmware Support Package SMM

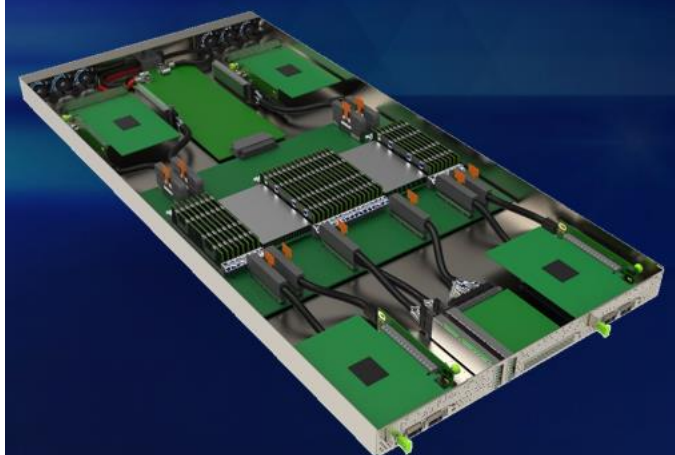
Agenda

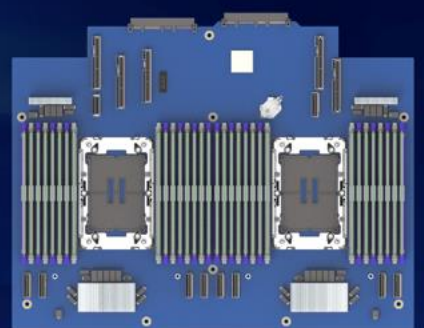
- Intel ® Universal Scalable Firmware Strategy
- Intel ® Universal Scalable Firmware Practice
- Intel ® Firmware Support Package Overview
- Intel ® Firmware Support Package SMM

Reusable Compute Block

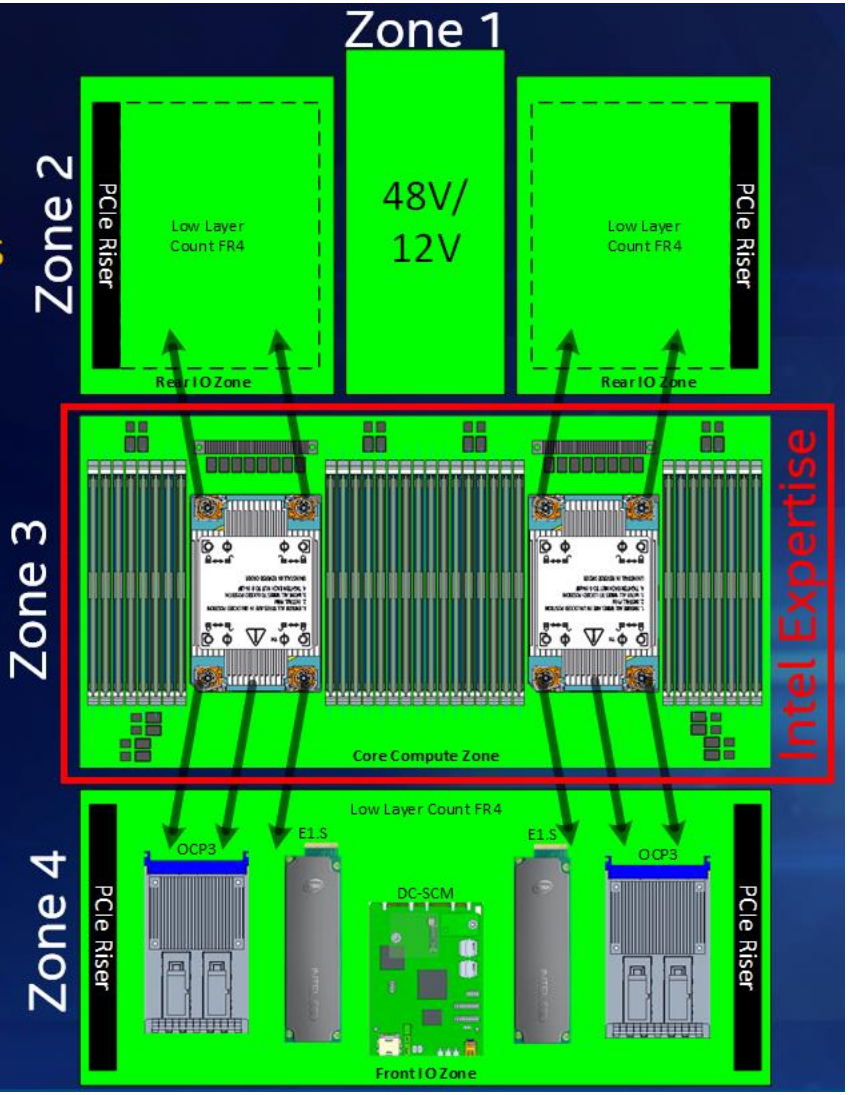
Intel vision is a server with four primary zones

- Zone 1: Power and cooling
- Zone 2: North IO
- Zone 3: Reusable Compute Block
- Zone 4: South IO

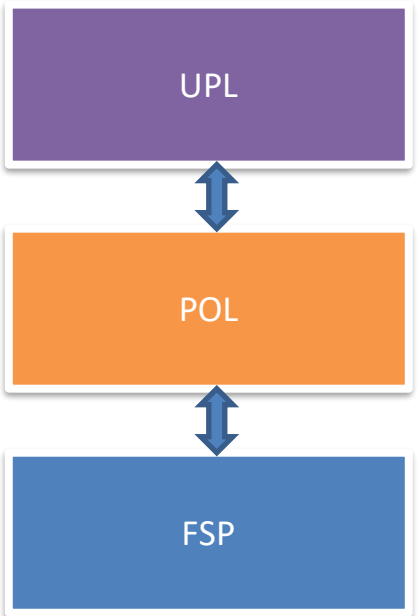


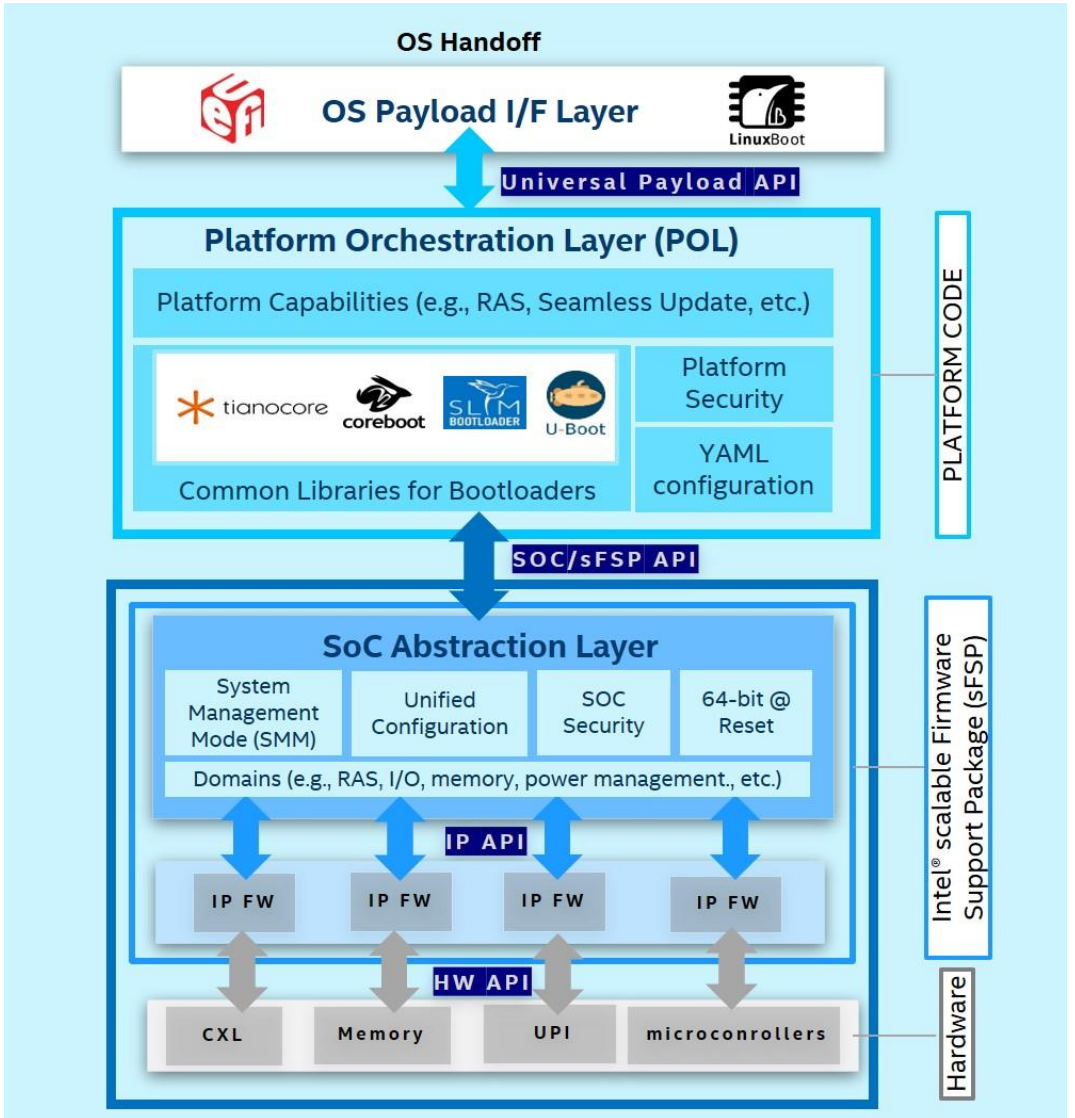


Zone 3
Implemented

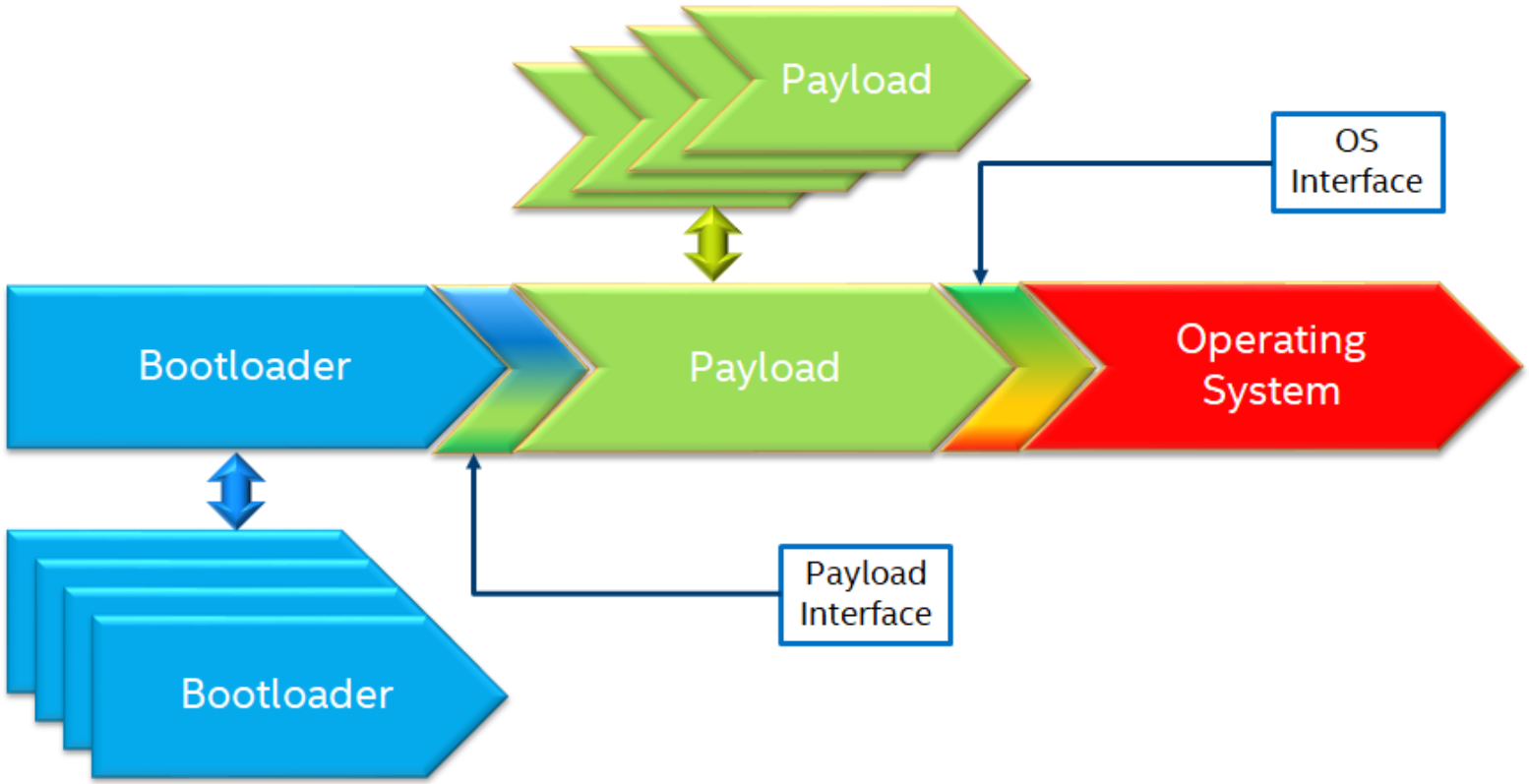


Universal Scalable Firmware (USF) Architecture





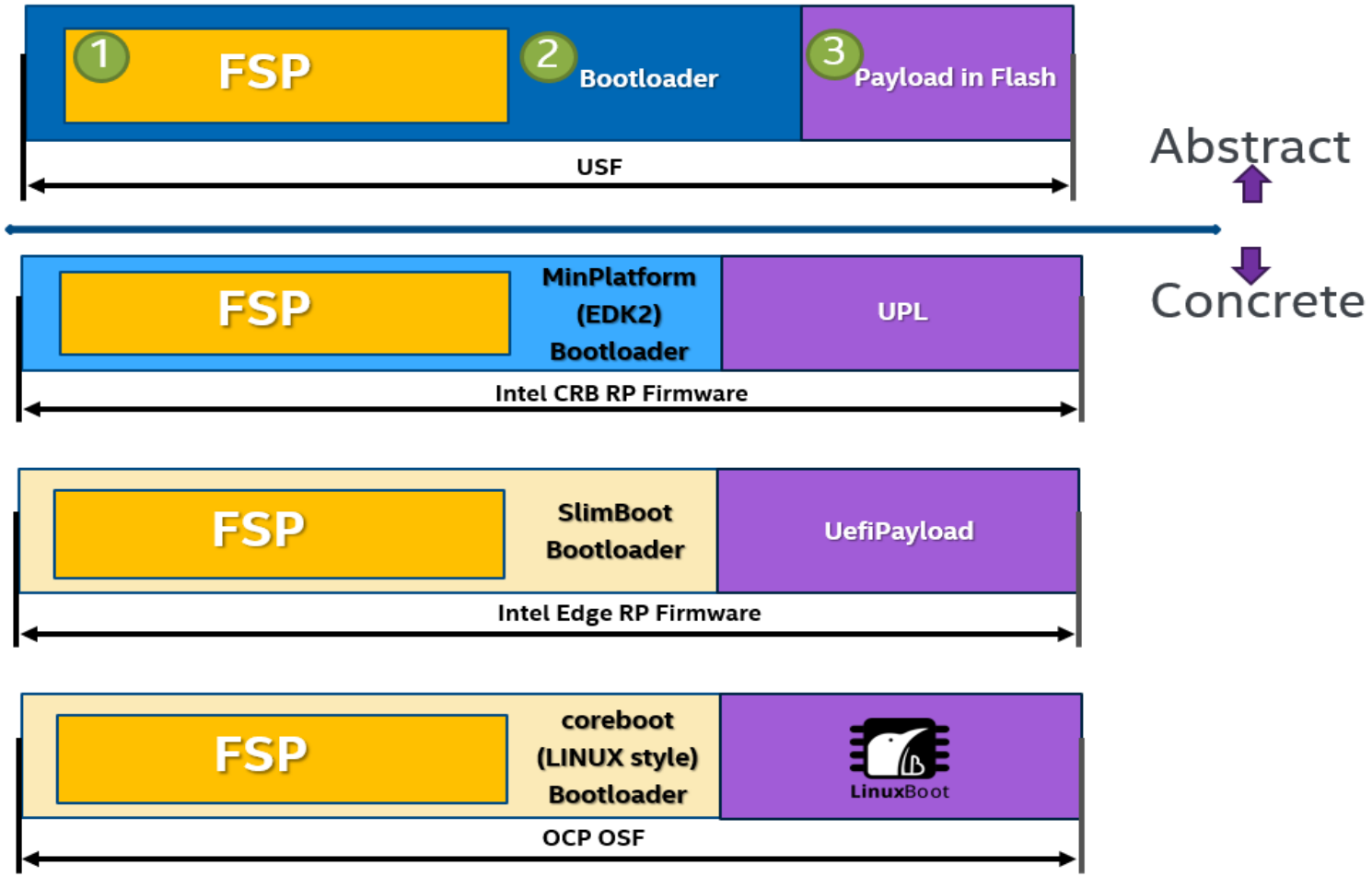
Universal Payload (UPL)



Agenda

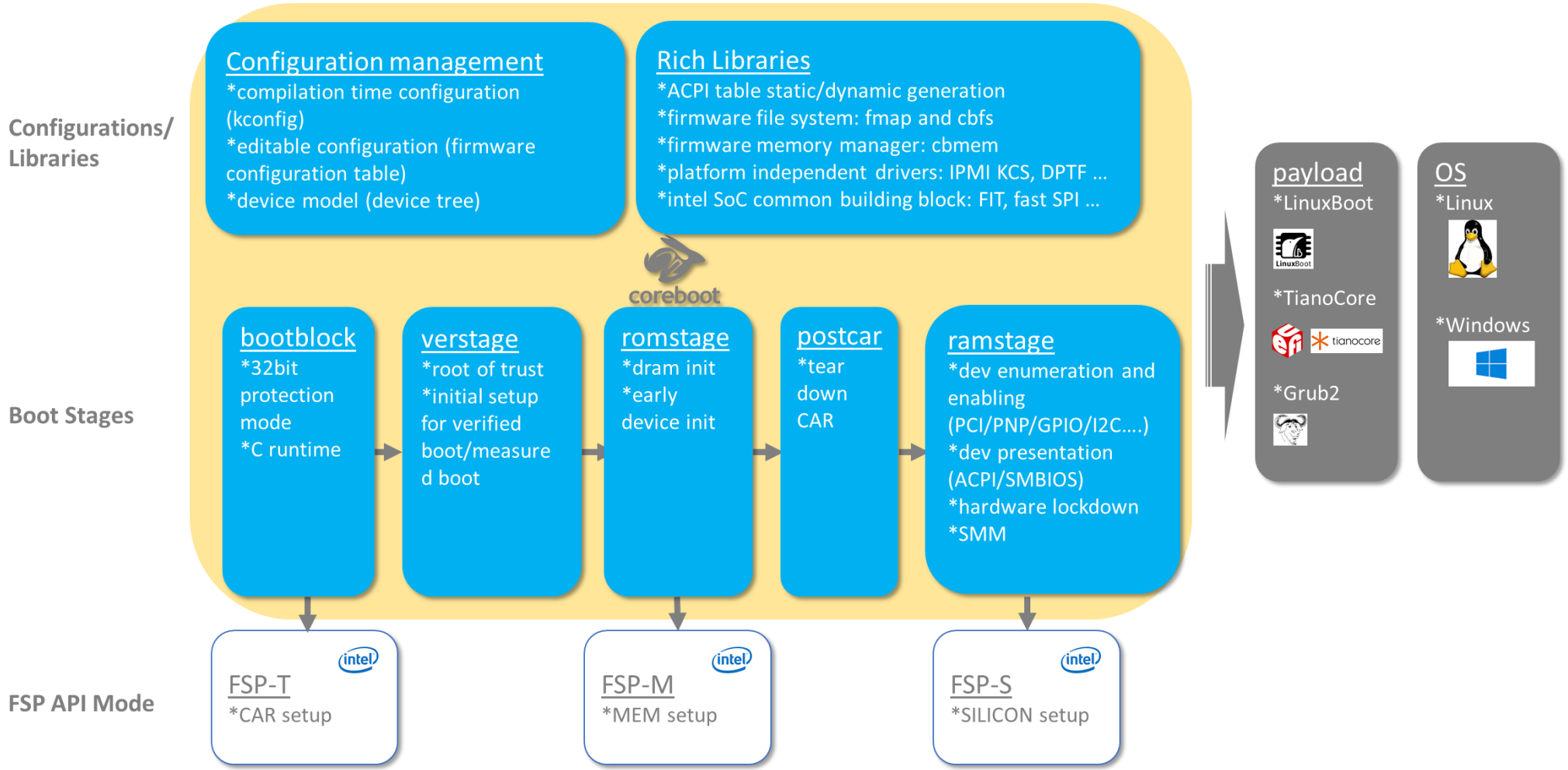
- Intel ® Universal Scalable Firmware Strategy
- Intel ® Universal Scalable Firmware Practice
- Intel ® Firmware Support Package Overview
- Intel ® Firmware Support Package SMM

Universal Scalable Firmware (USF) Concrete Practice



ByteDance字节跳动

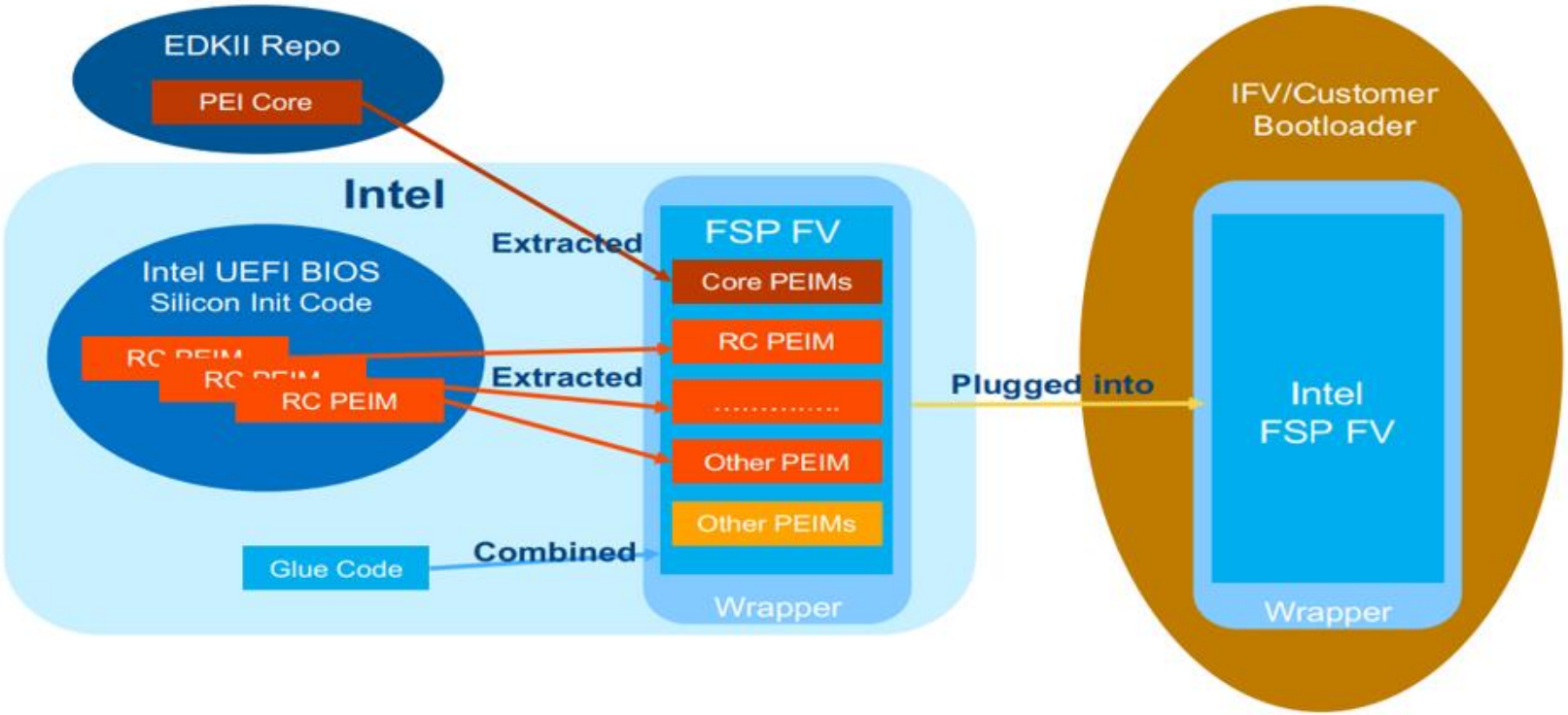
Universal Scalable Firmware (USF) ByteDance Practice for Intel® Xeon® 4th-generation Processors



Agenda

- Intel ® Universal Scalable Firmware Strategy
- Intel ® Universal Scalable Firmware Practice
- Intel ® Firmware Support Package Overview
- Intel ® Firmware Support Package SMM

Why Intel® Firmware Support Package (Intel® FSP)

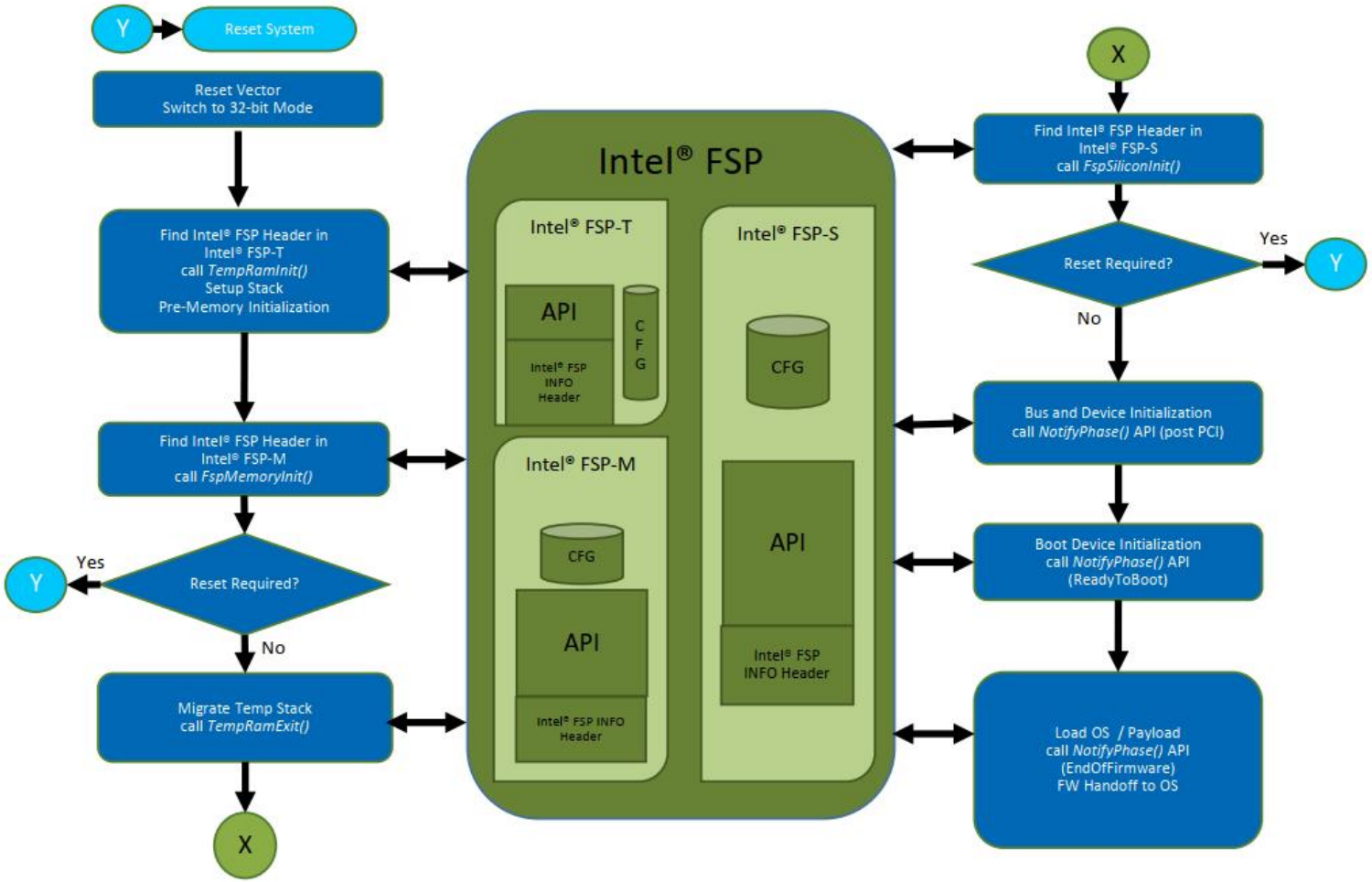


Intel® FSP Design Philosophy

System Firmware
Full solution, all the features, ready to use, with licensing and royalties from third parties

Intel® Firmware Support Package (Intel® FSP)
Only the engine – can be put into any vehicle, but the customer provides the vehicle

Intel® FSP Generic Boot Flow



Agenda

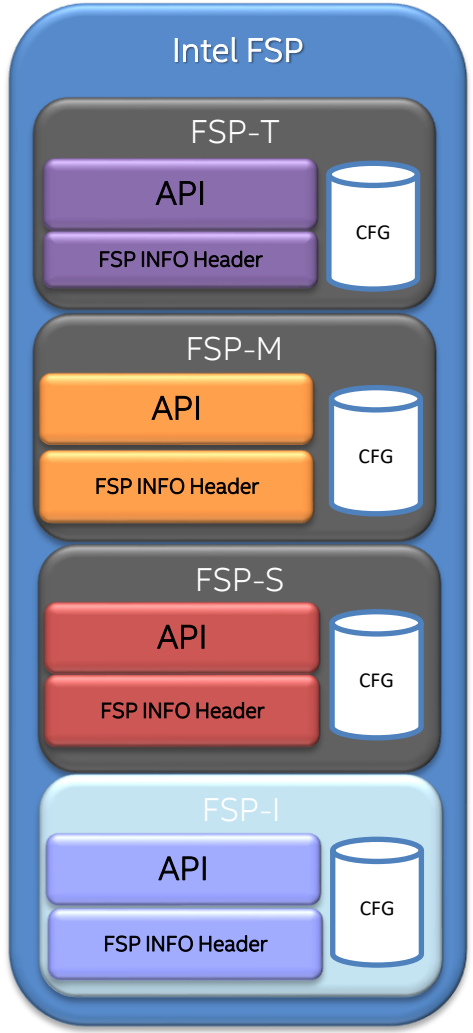
- Intel ® Universal Scalable Firmware Strategy
- Intel ® Universal Scalable Firmware Practice
- Intel ® Firmware Support Package Overview
- Intel ® Firmware Support Package SMM

Intel® FSP - SMM Background

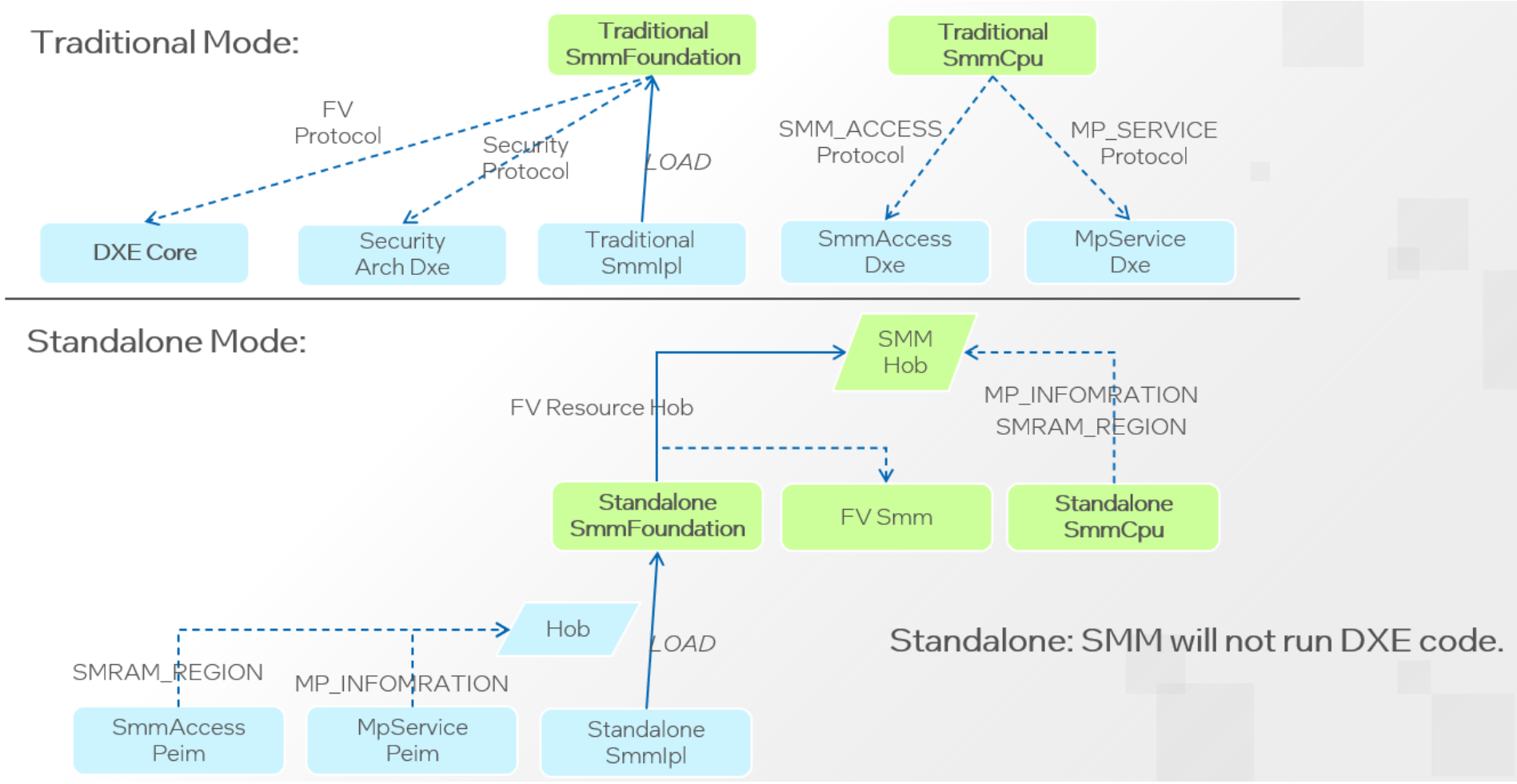
- Till FSP2.4, FSP does not support SMM related function and bootloaders own SMM foundation and features in SMM itself.
- However, for mainly SMM functions: server RAS/Security runtime features, it is too hard to support it without hardware/silicon IPs exposed for some bootloader (like coreboot/SlimBoot).
- In FSP2.4, we will have a unified solution for both EDKII and non-EDKII bootloader with FSP-SMM to support SMM foundation and features.

Intel® FSP - SMM API

- The Intel® FSP binary follows the UEFI Platform Initialization Firmware Volume Specification format.
  - Split into 4 separate FSP ingredients
- FSP-SMM: SMM initialization phase(FSP owns SMRAM
  - Primary purpose of this phase is to provide a collection of **silicon** SMI handlers that provide value-add services that a bootloader can use.
    - **FspSmmInit()** : Initialize SMM Foundation, dispatch all Standalone MM drivers, build SMM environment, install all MM handlers.

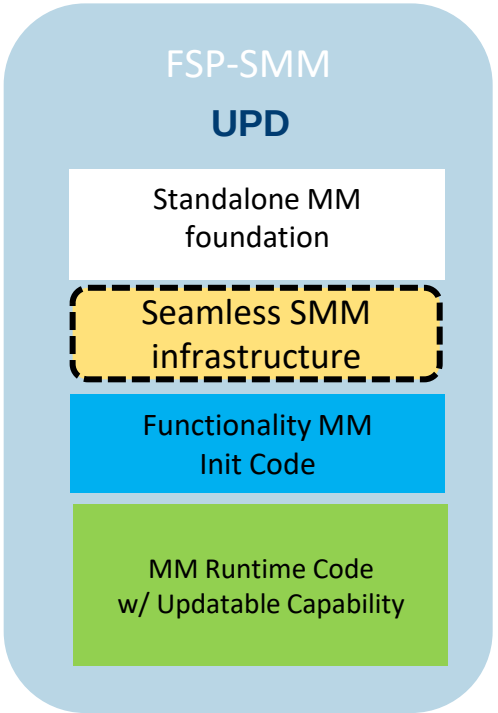


SMM Traditional Mode Vs. Standalone Mode



Intel® FSP - SMM Stack

- Intel® FSP-SMM infrastructure
- Standalone MM infrastructure
- Optional*: Seamless SMM infrastructure
  - SMM code injection
  - SMM Driver Update(SDU)
- RAS mm functions
  - Init code
  - MM runtime code
  - Optional* under SSDU infra: Updatable capability



ByteDance 字节跳动

Notices & Disclaimers

- Performance varies by use, configuration and other factors.
- Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.
- Your costs and results may vary.
- Intel technologies may require enabled hardware, software or service activation.
- Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.
- Code names are used by Intel to identify products, technologies, or services that are in development and not publicly available. These are not "commercial" names and not intended to function as trademarks.
-

ByteDance字节跳动

Thanks!