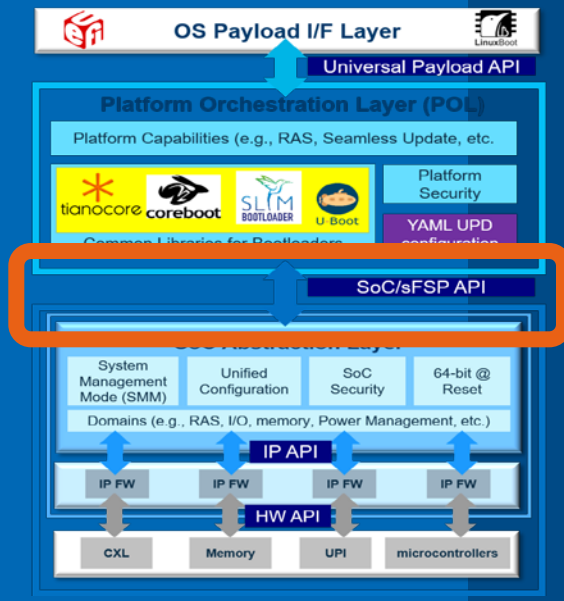
System Firmware Training

Universal Scalable Firmware (USF)
Scalable Intel® Firmware Support Package Overview



What is Scalable Intel® FSP?

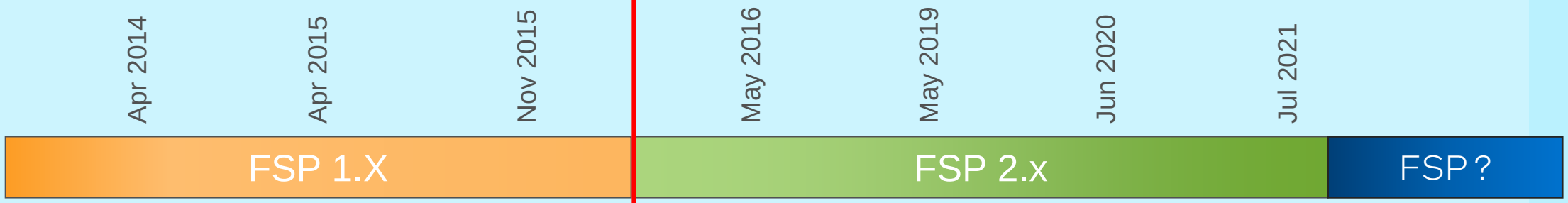
Platform Orchestration Layer POL uses Intel® Firmware Support Package (Intel® FSP)
Scalable FSP is an evolution of the Intel® FSP

http://www.intel.com/fsp

History timeline in the evolution of Intel® FSP

Intel® FSP provides key programming information for initializing Intel silicon and can be easily integrated into a boot loader of the developer's choice.

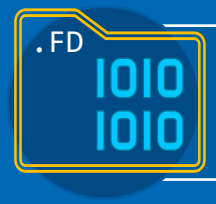
V1.0	Initial Release	V2.0	New design, Not compatible with 1.x,, 3 separate FV FSP-T, FSP-M, FSP-S in binary
V1.1	Split Silicon & Memory Init API, 2 boot flows	V2.1	Added Dispatch mode
V1.1a	Minor updates, FspInit Optional, Etc.	V2.2	Improve Initialization of Silicon Init API
		V2.3	Added FSP_NON_VOLATILE_STORAGE_HOB2
		FSP Next - FSP V3.0 ???	



intel.

What is Intel® Firmware Support Package?

Includes:



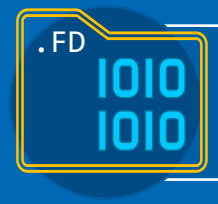
A binary firmware device (FD) file - contains multiple FSP Modules

An integration guide

intel.

What is Intel® Firmware Support Package?

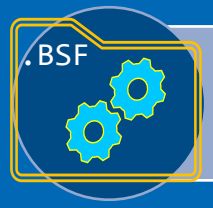
Includes:



A binary firmware device (FD) file - contains multiple FSP Modules

An integration guide

A rebasing tool



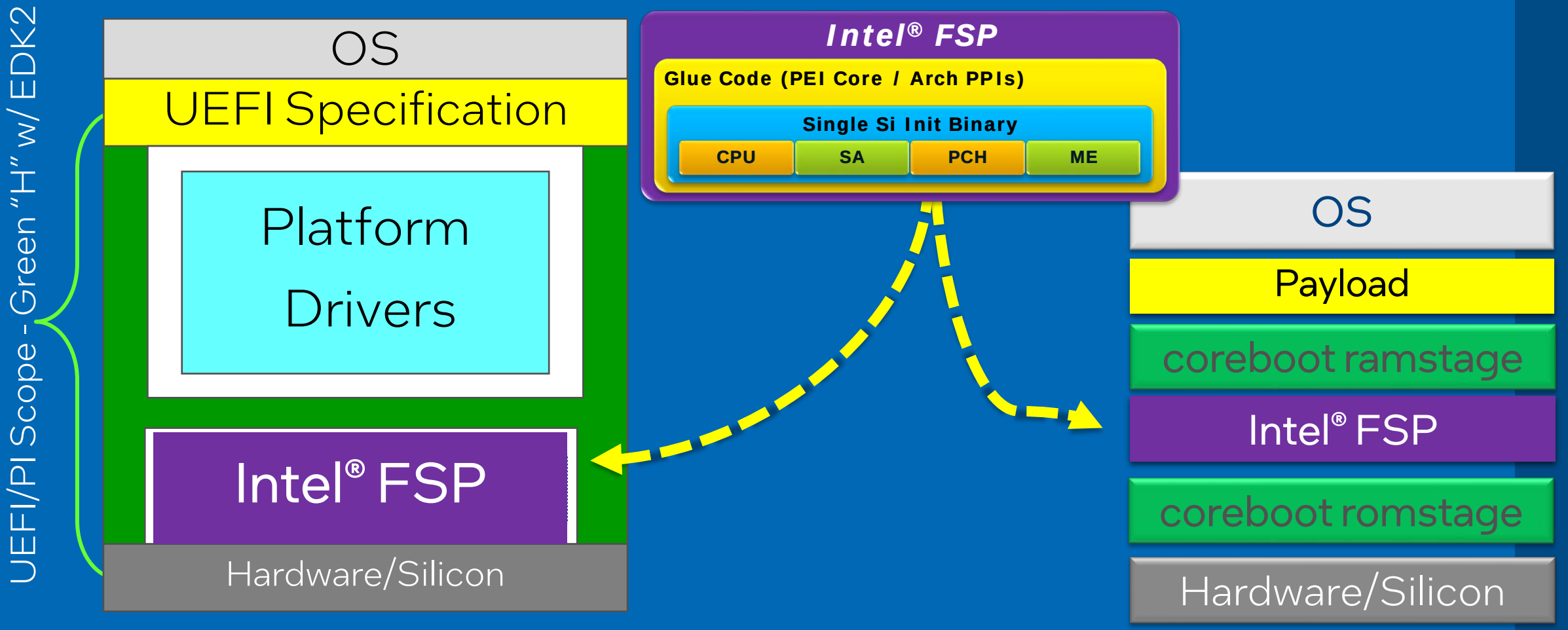
A Boot Setting File (BSF) or YAML file for Configuration of the Updatable Product Data (UPD)

intel

Intel® Firmware Support Package

- Provides silicon initialization code:
  - Initializes processor core, chipset as explained in BIOS Writers' Guide
  - Is relocatable in ROM
  - Can be configured for platform customization
- Boot loader agnostic and can be easily integrated with many options:
  - Open source boot loaders: UEFI –EDK II, Coreboot, U-boot, etc.
  - RTOS
  - Others

Intel® FSP "Produced" to "Consuming" Intel® Architecture Firmware



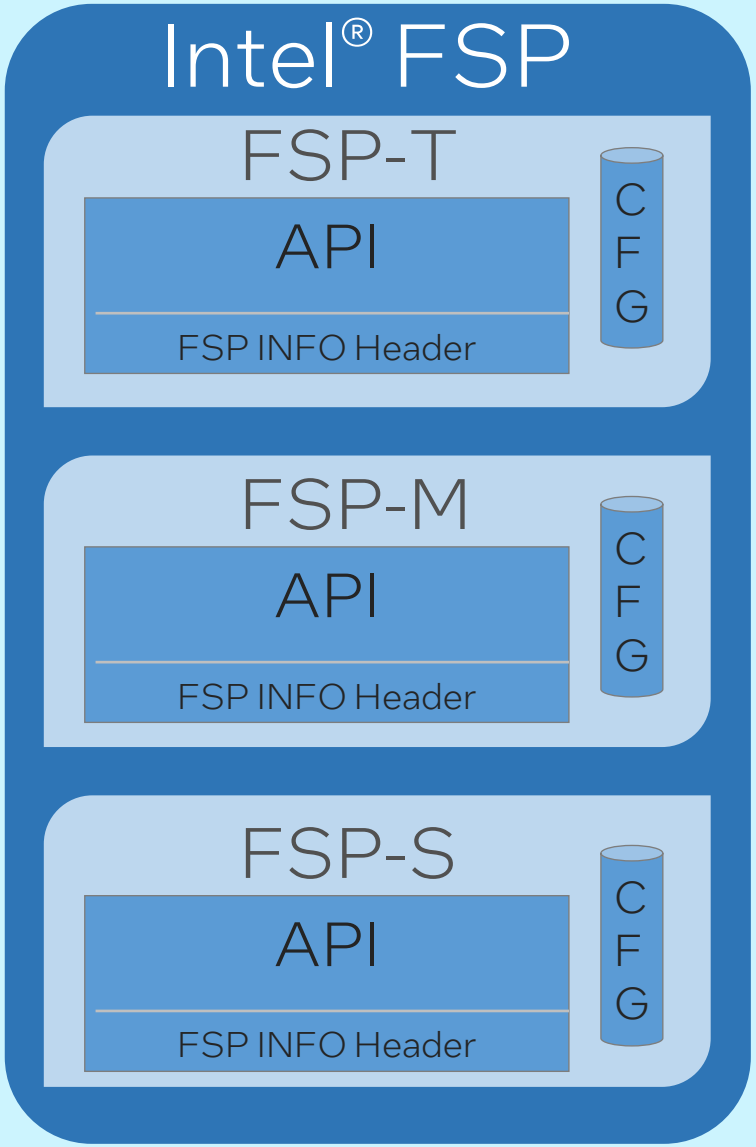
Intel FSP is independent of the bootloader solutions

Intel® FSP V2.3 Binary Component View

Firmware Volume Layout of the Intel FSP Binary

- FSP-T: Temporary RAM initialization phase
  - `TempRamInit()`
- FSP-M: Memory initialization phase
  - `FspMemoryInit()`
  - `TempRamExit()`
- FSP-S: Silicon initialization phase
  - `FspSiliconInit()`
  - `NotifyPhase()`
  - `FspMultiPhaseSiInit()`

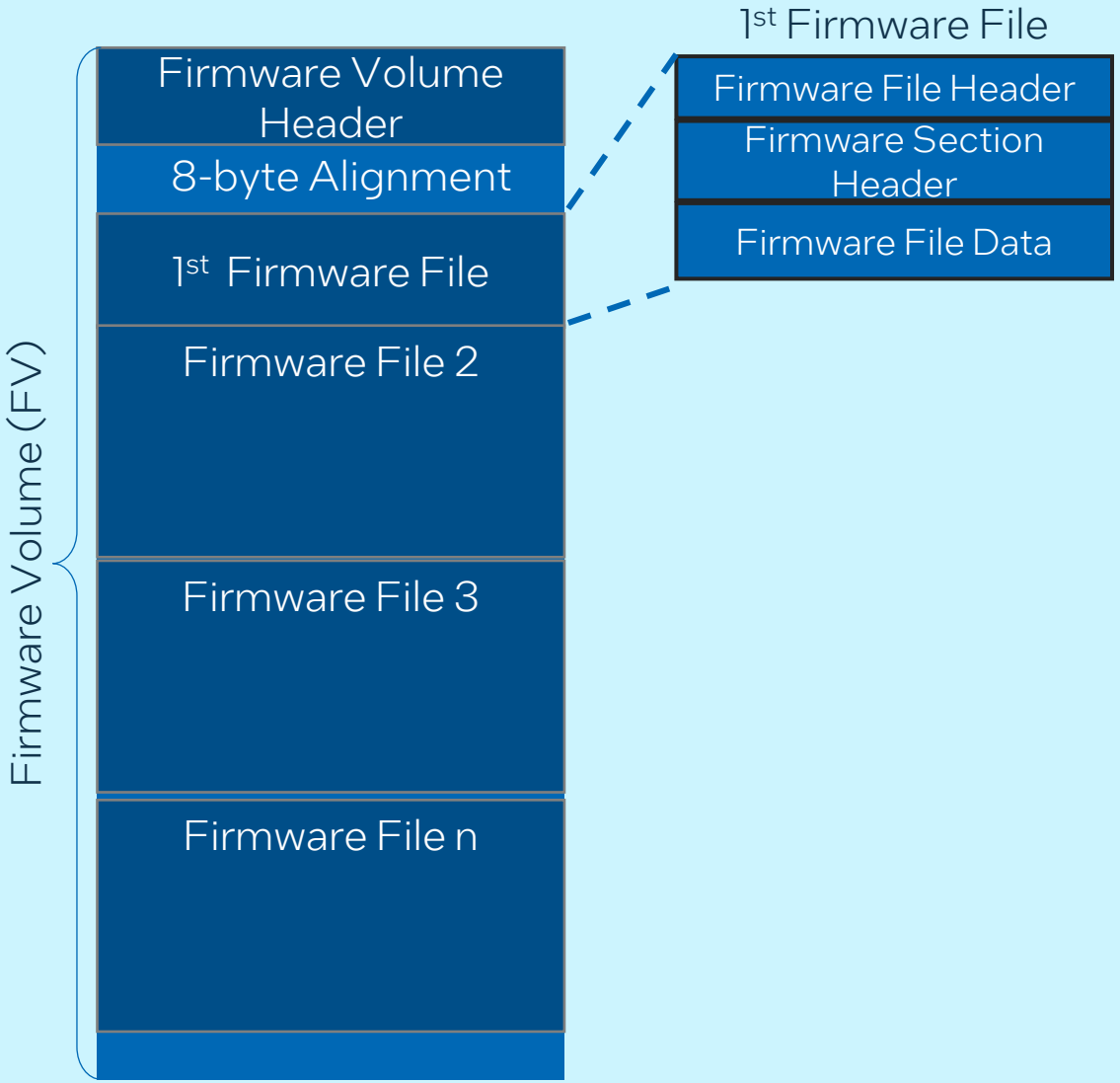
- Intel® FSP 2.Next or FSP 3.0 or ???
  - FSP-V – Validation
  - FSP-R – Runtime
  - 64 Bit @ Reset
  - SMM Loading
  - Etc.



Intel® FSP Spec 2.3 Figure 1

Intel® FSP Binary Structure FSP_INFO_HEADER

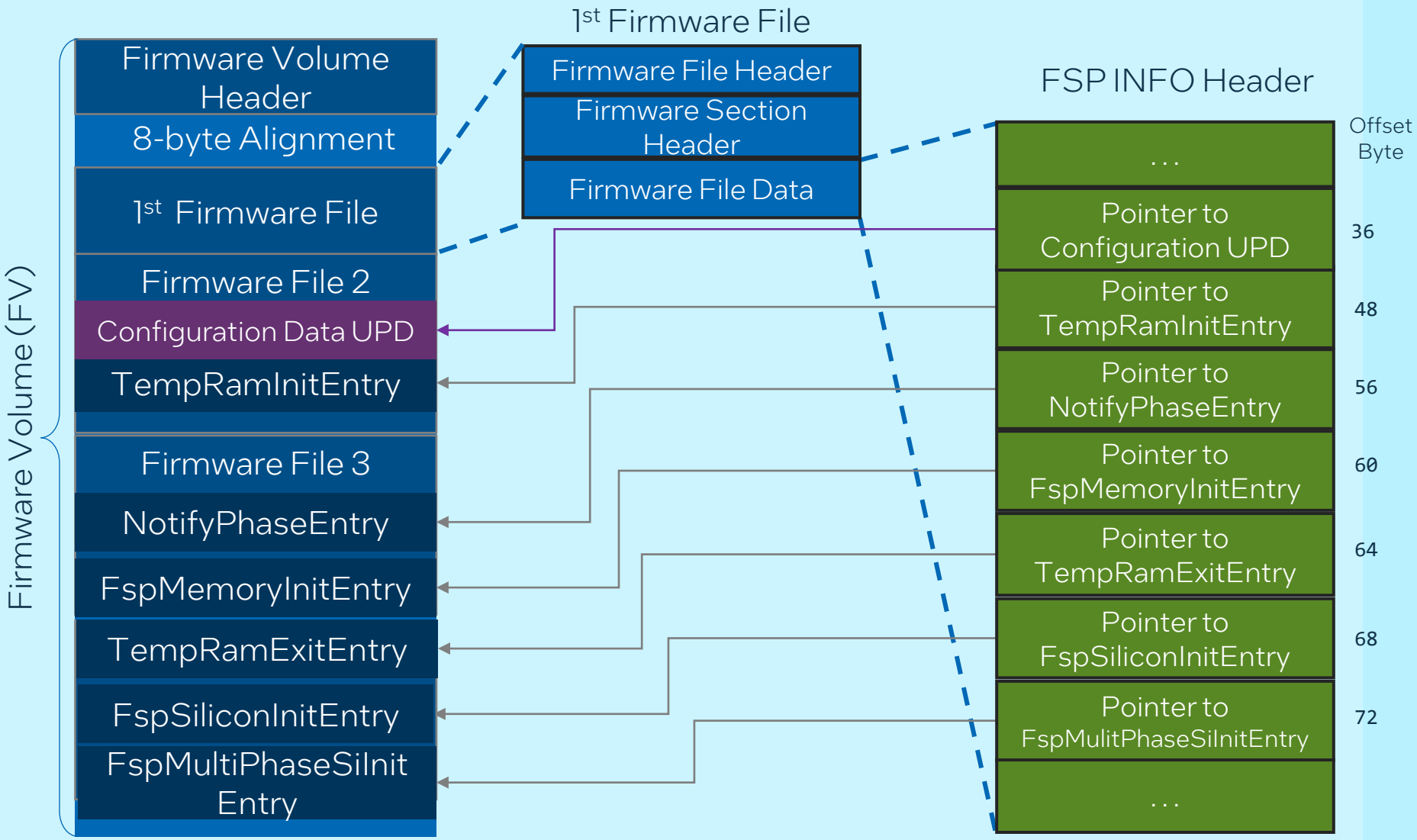
FSP INFO Header is the first Firmware File within each of the FSP Component's FV



Intel® FSP Binary Structure FSP_INFO_HEADER

FSP INFO Header is the first Firmware File within each of the FSP Component's FV

If a pointer in the FSP INFO Header is 0x00000000 then API not available in this component

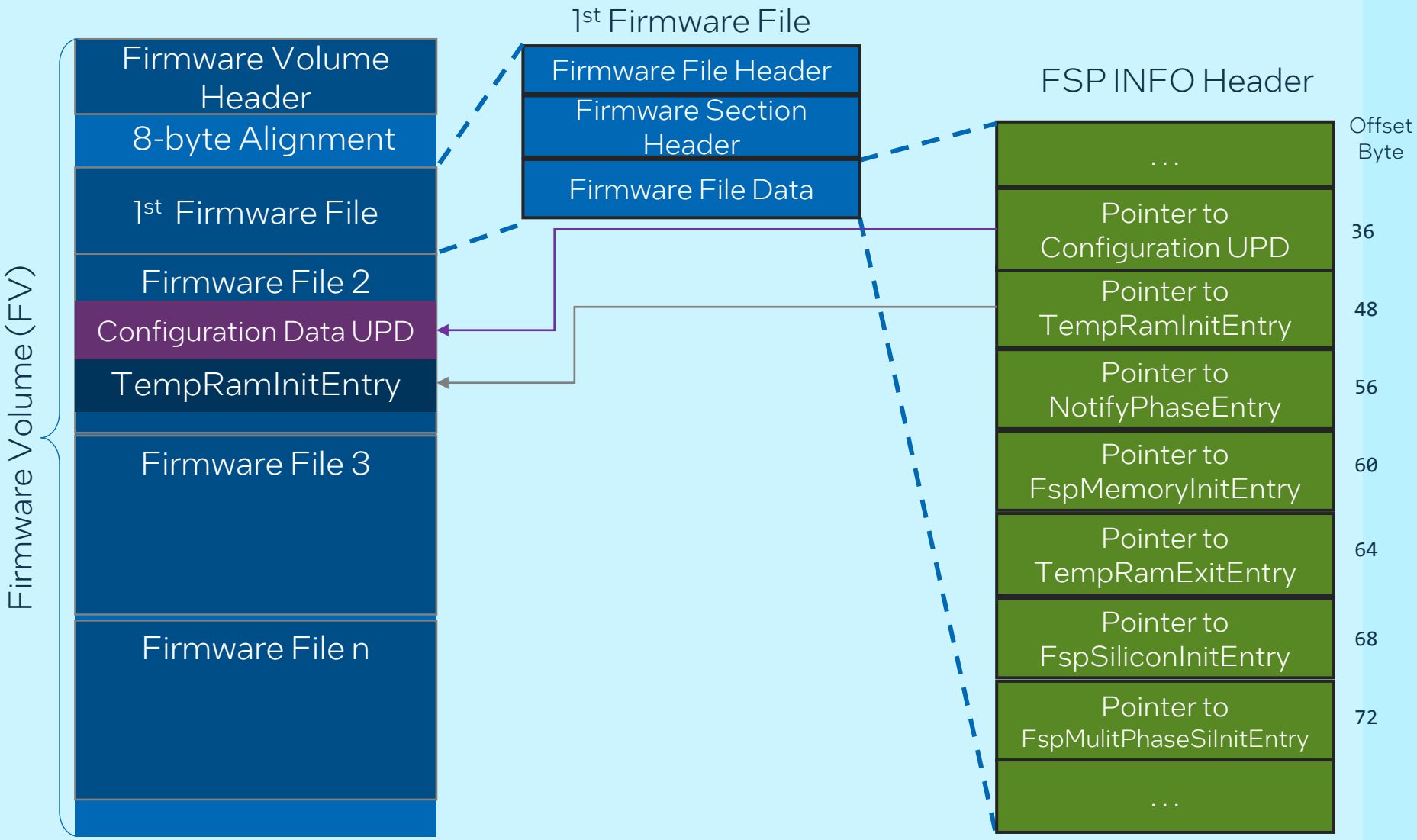


intel.

Intel® FSP Binary Structure `FSP_INFO_HEADER`

FSP INFO Header is the first Firmware File within each of the FSP Component's FV

If a pointer in the FSP INFO Header is 0x00000000 then API not available in this component

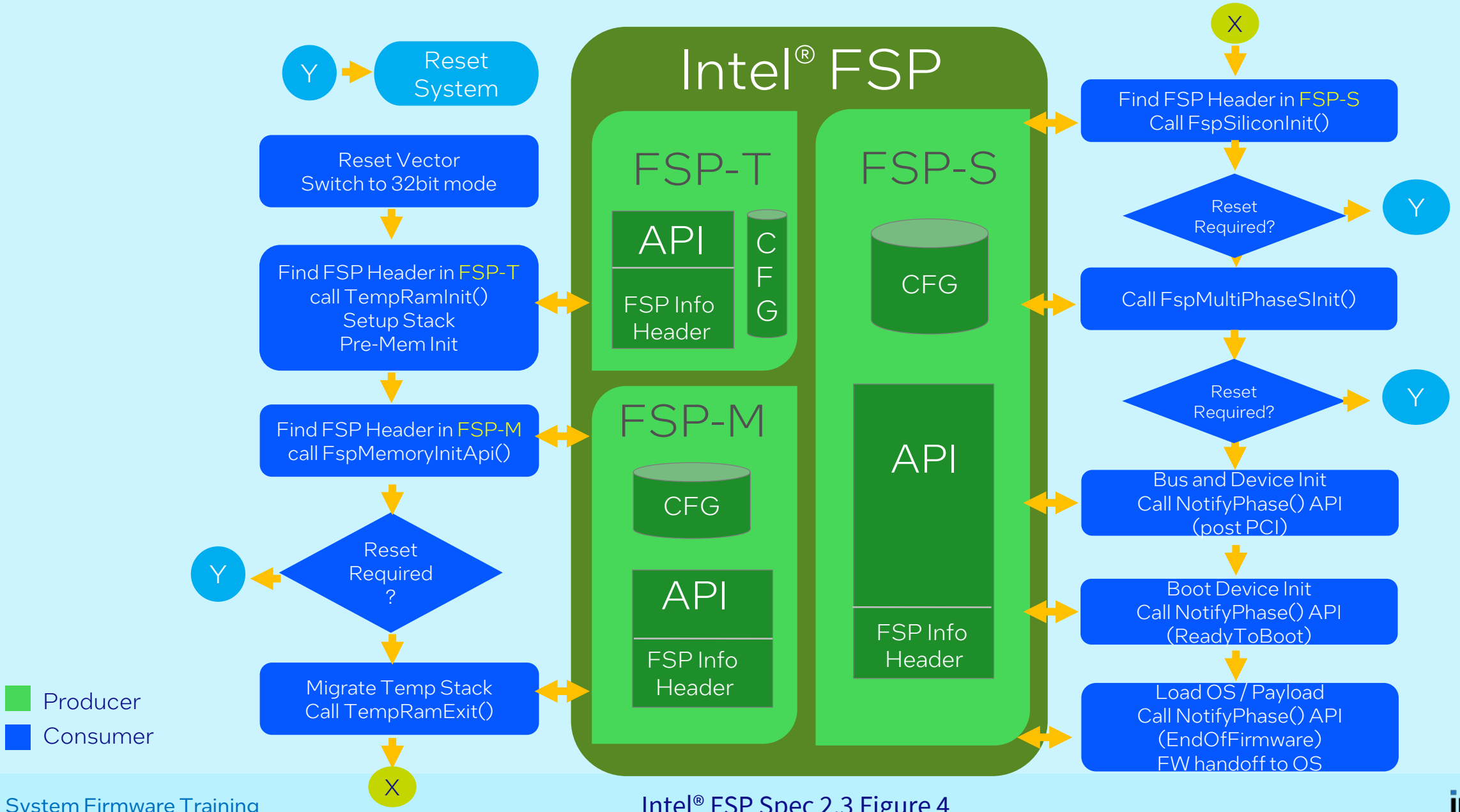


FSP-T FV only **`TempRamInitEntry`** is non-zero

intel.

Intel® FSP V2.3 Boot Flow

Using Intel® FSP w/ EDK II: PDF



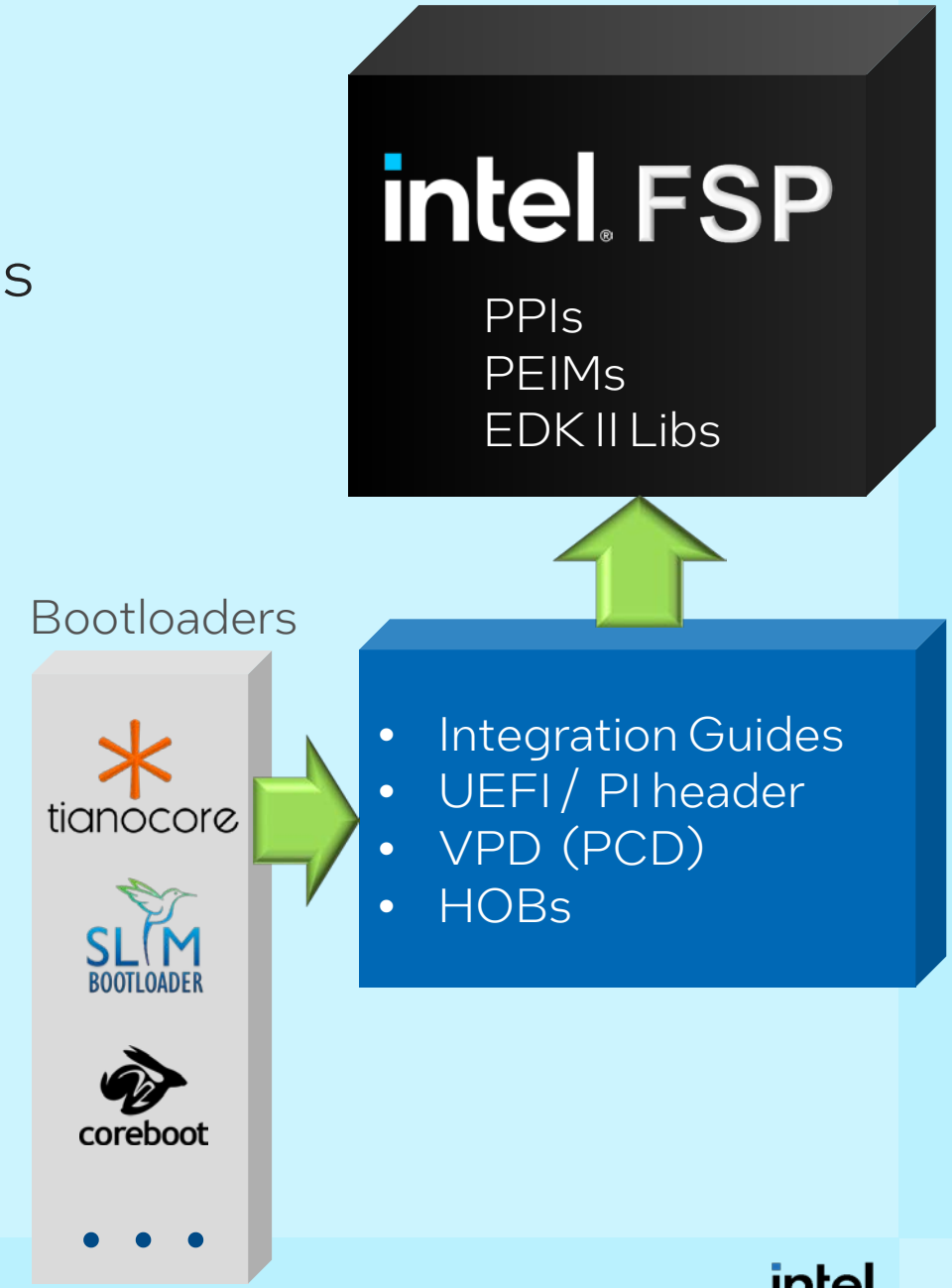
Intel® FSP Spec 2.3 Figure 4

intel.

Intel® FSP Producer

- Examples of binary instances on http://www.intel.com/fsp w/integration guides
  - This includes hardware initialization code that is EDK II based PEI Modules (PEIM's)
- Modules are encapsulated as a UEFI PI firmware volume w/ extra header
- Configure w/Vital Product Data (VPD)-style Platform Configuration Data (PCD) externalized from the modules
- Resultant output state reported via UEFI Platform Initialization (PI) Hand Off Block (HOB)

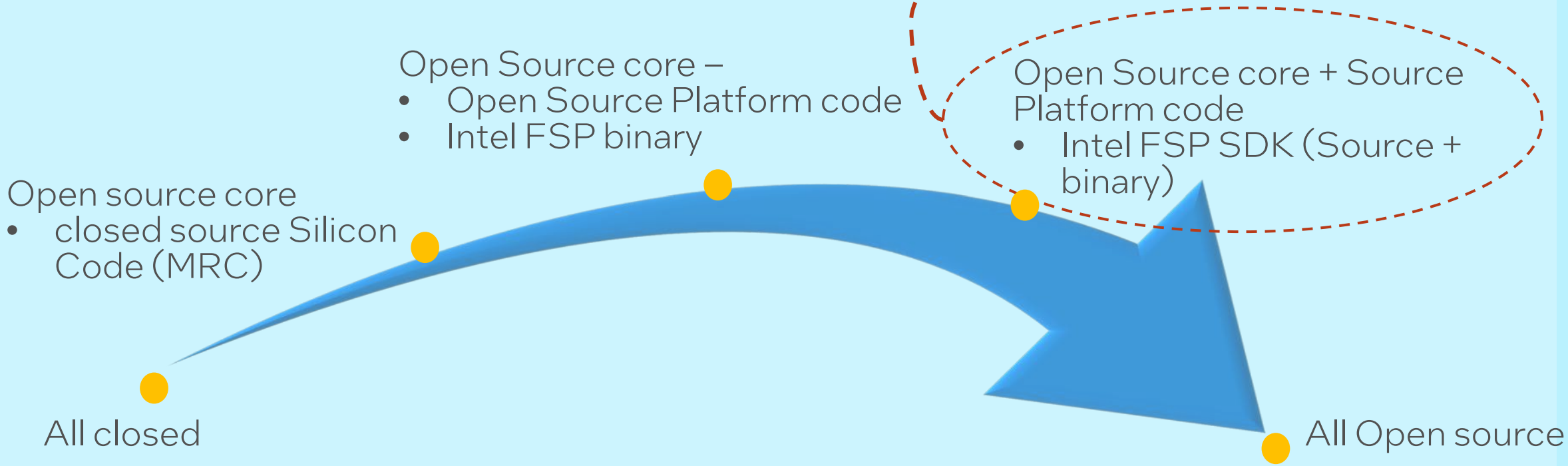
Intel® Firmware Support Package (Intel® FSP) External Architecture Specification (EAS) v2.3 Link v2.0
Resource:
https://software.intel.com/content/www/us/en/develop/articles/intel-firmware-support-package.html



Scalable Intel® FSP Path to Openness

https://github.com/UniversalScalableFirmware/fspsdk

View branches for QEMU POC examples
https://github.com/UniversalScalableFirmware/fspsdk/tree/sbl_qemu_fsp_x64_fspt64



Pre and Post Intel® FSP Function Invocation

32bit Flat	▪ Host Bootloader must be in 32bit flat mode
4GB Address	▪ Both the code and data selectors should have 4GB access range
Interrupts	▪ All Interrupts disabled
Return Status	▪ All Intel FSP API return an unsigned 32bit integer as status
Reserved Memory	▪ Intel® FSP will reserve a region of memory for its own use throughout the operation and needs to be reserved by the bootloader and OS.

intel.

Intel® FSP Return Data to the Bootloader

Intel FSP build a set of data structures before passing them back to the host bootloader

The data structures comply with the UEFI Hand-Off-Block (HOB) format

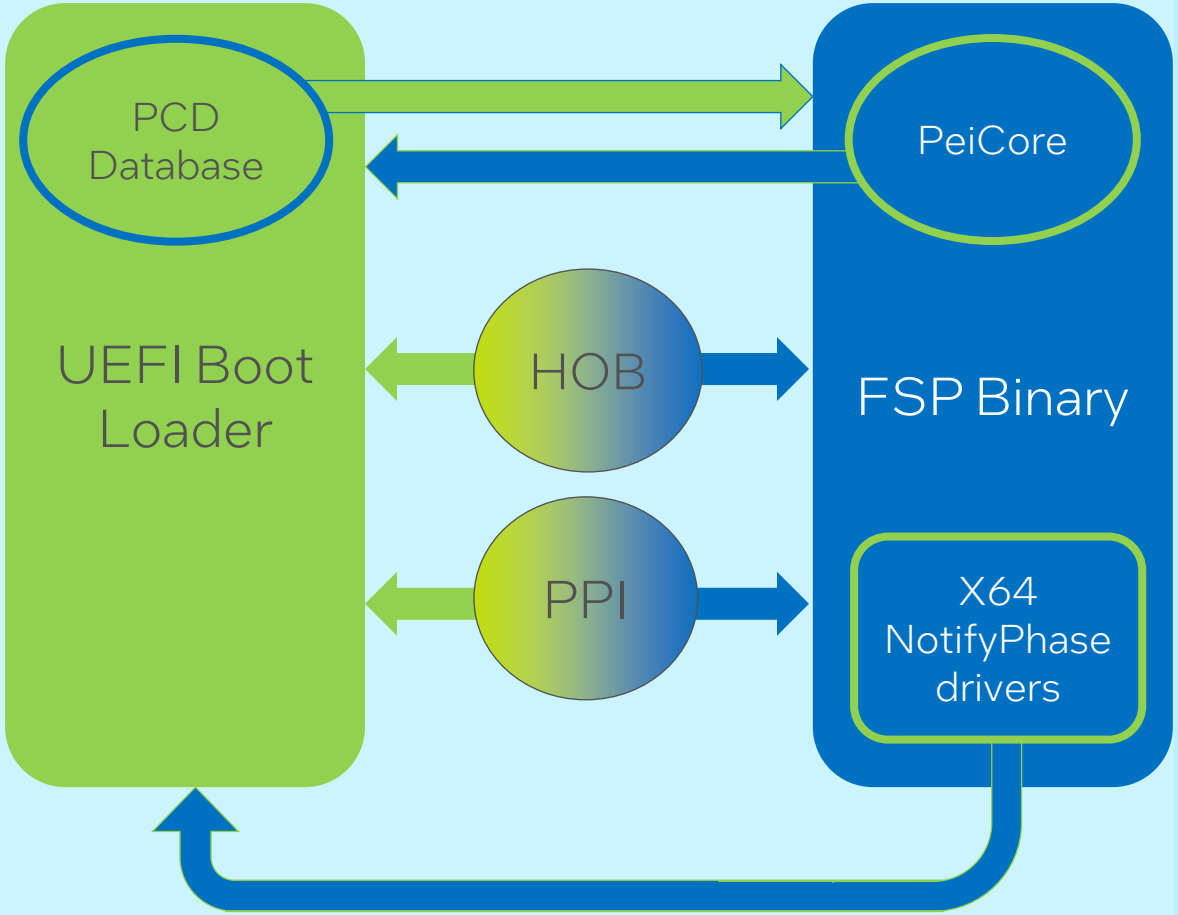
It is up to the host bootloader developers to decide how to consume the data in the HOB because some data may be irrelevant to some bootloaders

Example: Bootloader can use the resource descriptor HOB information to get the system memory mapping information.

intel.

Intel FSP Dispatch Mode Interface

- Optional boot flow intended to enable Intel FSP to integrate well in to UEFI bootloader implementations.
- Conforms to UEFI & PI Specifications
- The FSP-T, FSP-M, and FSP-S are containers that expose firmware volumes (FVs) directly to the bootloader.
- UPD Mechanism to pass Config data is not needed
- PCD Database Required



FSP Spec 2.3 Figure 6

intel.

Intel FSP Authentication

Intel FSP

- A **binary** to preform silicon initialization.
- Released by Intel.
- Can be integrated into OEM BIOS

Question?

- It the FSP binary in OEM BIOS from Intel?
- Is it the latest FSP binary with known bug fixes?

Intel FSP 2.x Measurement Attestation Spec v1.0

intel.

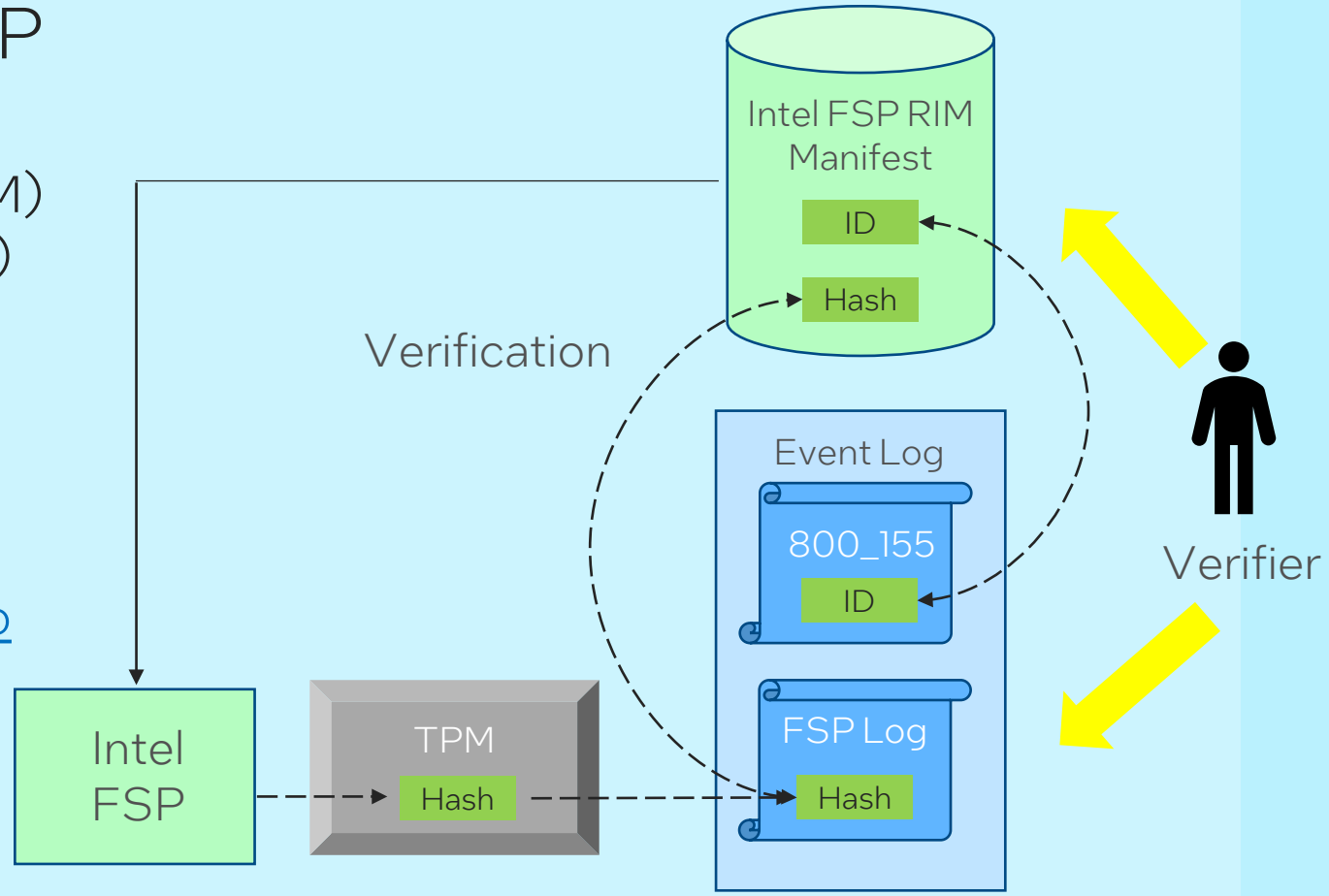
Intel® FSP 2.x Measurement and Attestation 1.0

Verify the provenance of the FSP binary

- Intel FSP Reference Integrity Manifest (RIM)
- FSP firmware integrity measurement (FIM)
  - Measure the FSP binary component during boot
- FSP Component Attestation

- Measure data to TPM [EDK II IntelFsp2WrapperPkg/Include/Library/FspMeasurementLib.h]

National Institute of Standards & Technology [NIST SP 800-155] : Firmware Integrity Measurement



Scalable Intel® FSP Summary

- Scalable FSP is an evolution of the Intel® FSP
- The Intel FSP is the reference code Bootloaders will interface with for initializing Intel silicon platforms or SOCs
- Intel FSP Next has proof of concepts available in the open source: https://github.com/UniversalScalableFirmware
- Intel FSP Authentication is accomplished through measurements and attestation verifying the provenance of the FSP binary

intel


intel