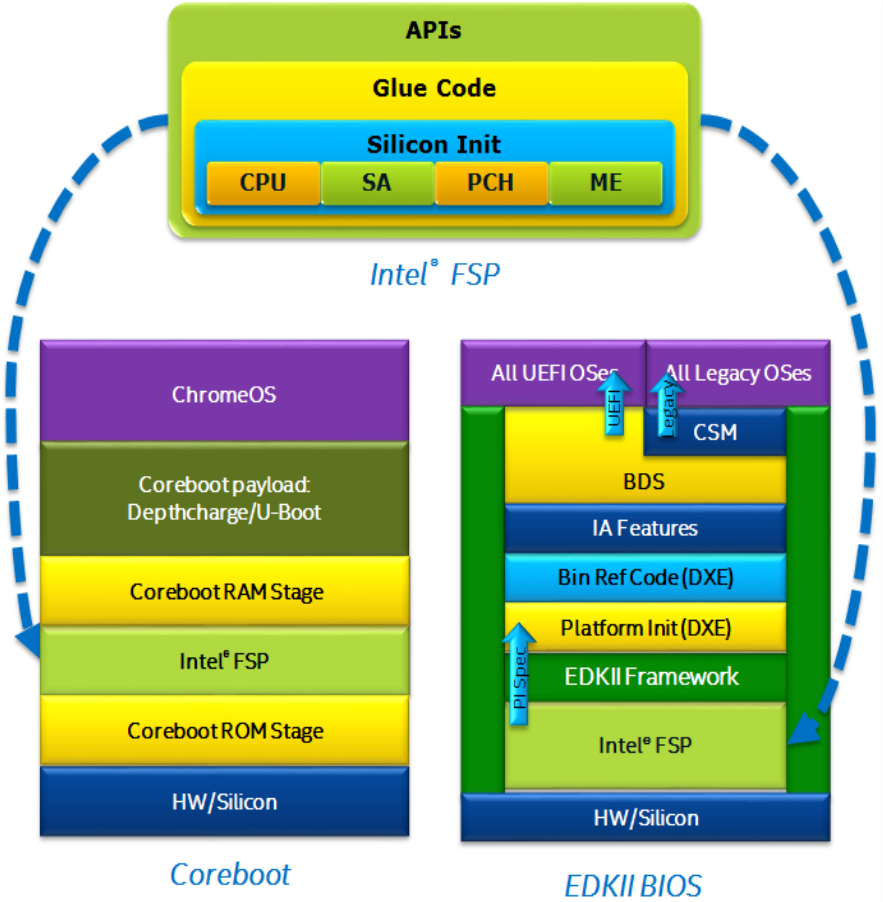
Intel® Firmware Support Package (Intel® FSP) v2.0 Overview

Giri Mudusuru Principal Engineer, Intel
Vincent Zimmer Sr. Principal Engineer, Intel

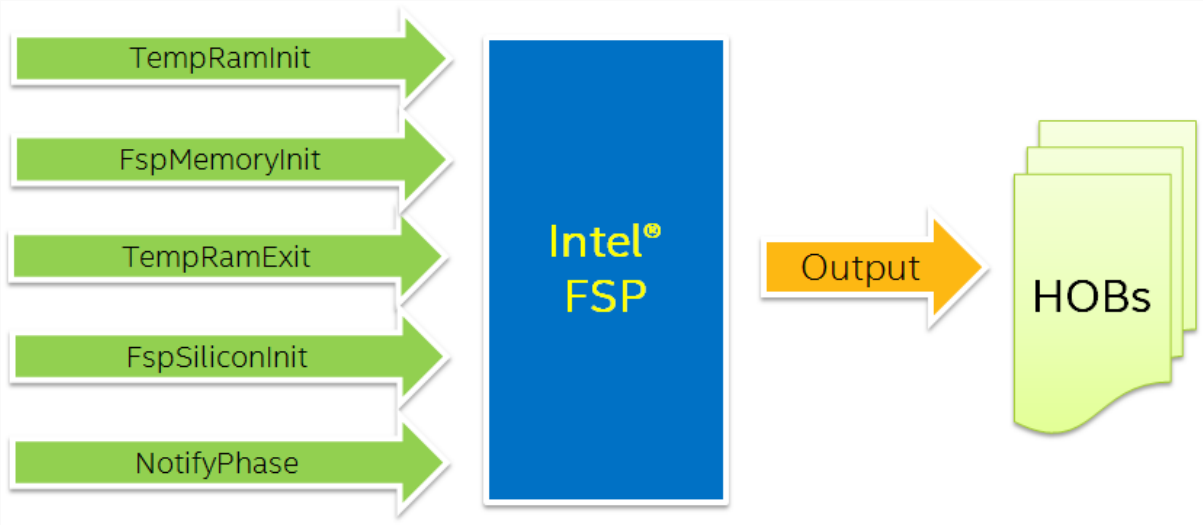
What is Intel FSP?

Intel FSP provides processor & chipset initialization in a format that can be incorporated into existing bootloader frameworks like Coreboot, EDK2 etc..

- Enable Open Source development
- Protect Intellectual Property (IP)
- Simplify bootloader integration
- Enable binary customization



Intel FSP External Interfaces



APIs:

TempRamInit(); FspMemoryInit(); TempRamExit(); FspSiliconInit(); NotifyPhase()

Input: UPD: Updateable Product Data - Configuration data

Why Intel FSP v2.0?

- Support booting from non-memory mapped storage
  - eMMC boot along with SPI boot
- Enable modularity (components) and simplify the Dual FSP usage (and other firmware security & update flows)
  - Minimize the size with Dual FSP usage & ROM/RAM stage
- Each component contains the related static configuration data
  - Data modularity and separation
- Enable Reset flexibility for bootloader
  - Support bootloader housekeeping (Notify EC etc.) before performing reset

Intel FSP - Layout v1.x & v2.0

Split into components (phases)

FSP-T (Temp Ram Init Phase)

TempRamInit () API

FSP-M (Memory Init Phase)

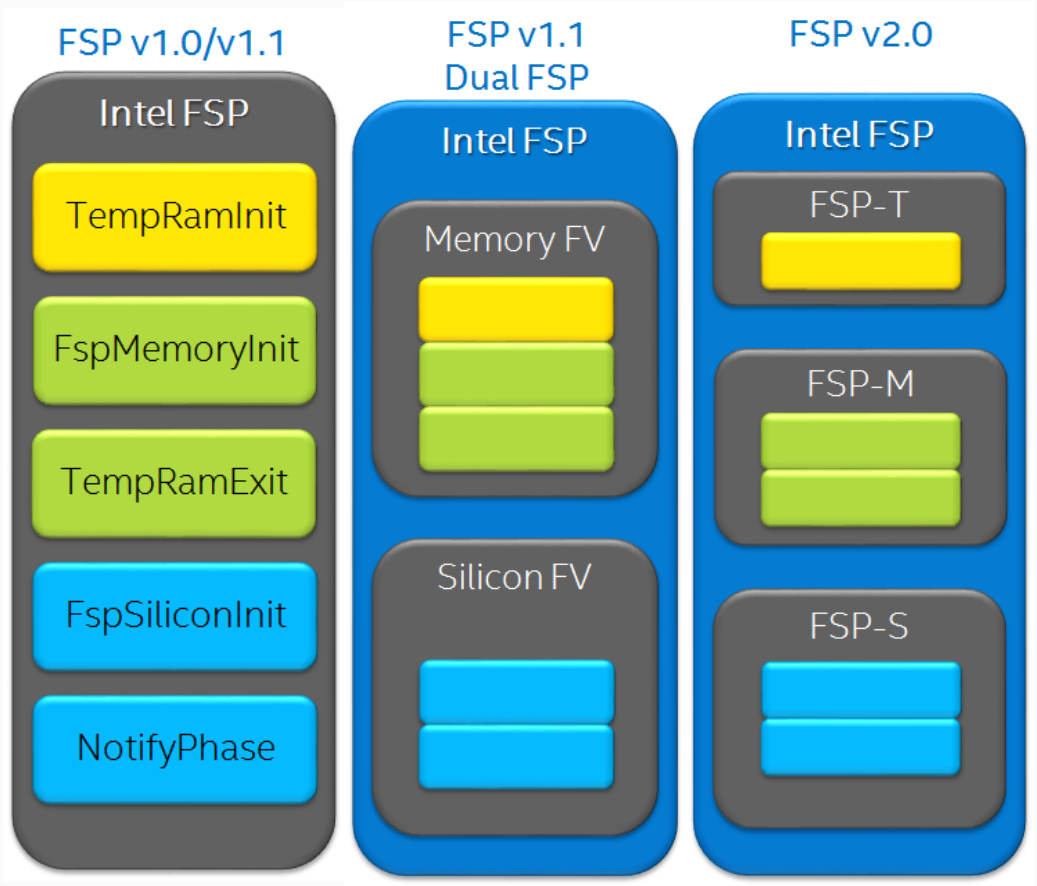
FspMemoryInit () API

TempRamExit () API

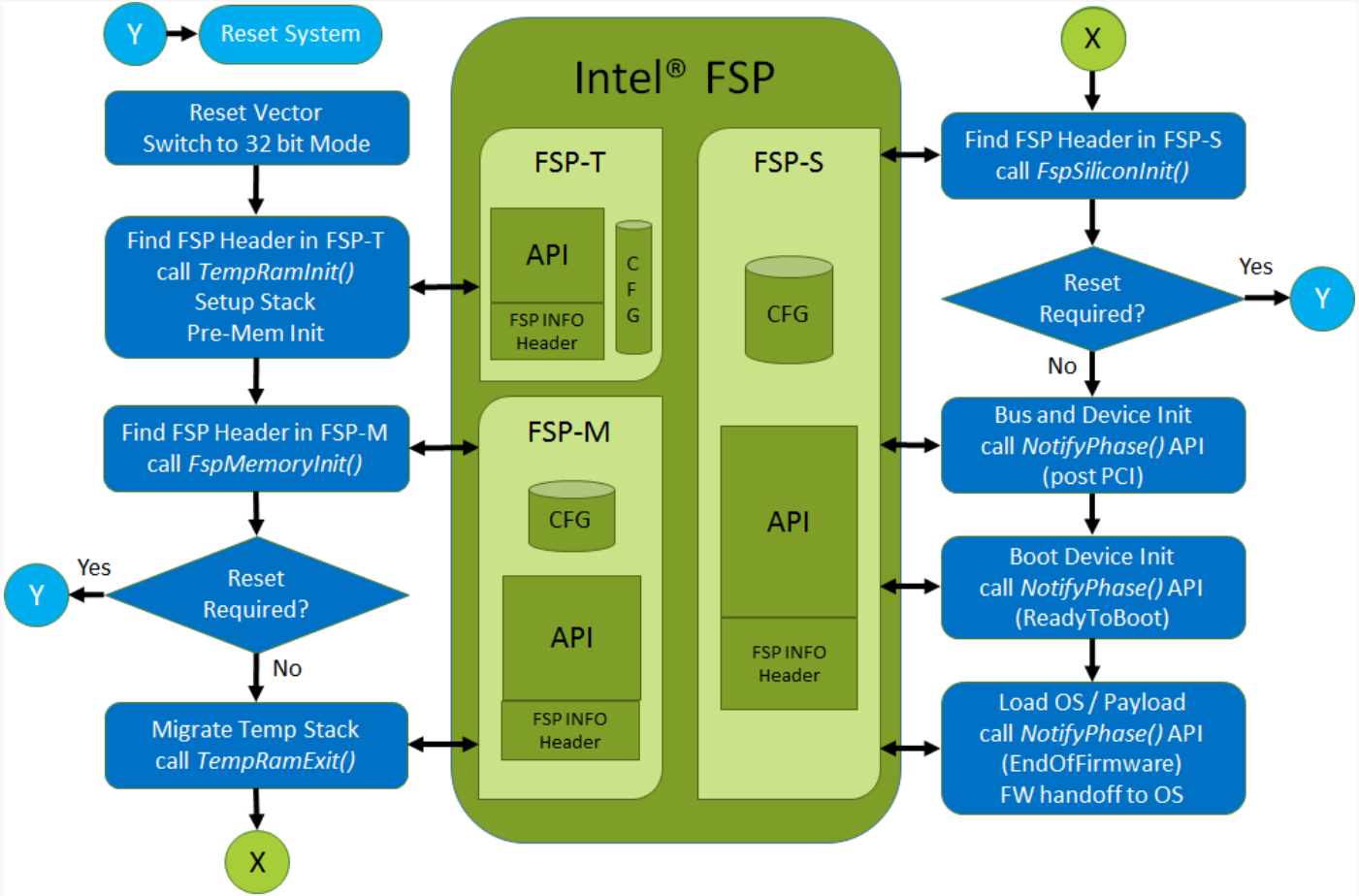
FSP-S (Silicon Init Phase)

FspSiliconInit () API

NotifyPhase () API



Intel FSP v2.0 Boot flow



FSP_INFO_HEADER changes from v1.1 to v2.0

Added ***SpecVersion*** field

- Indicates compliance with a revision of this specification in the BCD format.
  - Bits[3:0] - Minor Version & Bits[7:4] - Major Version
- For revision v2.0 the value will be 0x20

Updated the ***HeaderRevision*** from 2 to 3

Reduced ***ImageAttribute*** from DWORD to WORD

Added ***ComponentAttribute*** field as WORD with below attributes

- Bit [0] – Build Type: Debug(0) and Release(1)
- Bit [1] – Release Type: Test(0) and Official (1)
- Bits [15:12] - Component Type
  - 0001b – FSP-T: Component to initialize Temp RAM Init Phase
  - 0010b – FSP-M: Component to initialize Memory Init Phase
  - 0011b – FSP-S: Component to initialize the Silicon Init Phase
  - 1000b – FSP-O: Component for OEM specific content
  - Other values are Reserved

Removed ***FspInitEntryOffset*** field and marked it as reserved. It must be set to 0x00000000

Intel FSP - API changes from v1.1 to v2.0

```
typedef
EFI_STATUS
(EFIAPI *FSP_TEMP_RAM_INIT) (
  IN FSP_TEMP_RAM_INIT_PARAMS *TempRamInitParamPtr
);
typedef
EFI_STATUS
(EFIAPI *FSP_MEMORY_INIT) (
  IN OUT FSP_MEMORY_INIT_PARAMS *FspMemoryInitParamPtr
);
typedef
EFI_STATUS
(EFIAPI *FSP_TEMP_RAM_EXIT) (
  IN OUT  VOID  *TempRamExitParamPtr
);
typedef
EFI_STATUS
(EFIAPI *FSP_SILICON_INIT) (
  IN OUT  VOID  *UpdDataPtr
);
```

```
typedef
EFI_STATUS
(EFIAPI *FSP_TEMP_RAM_INIT) (
  IN  VOID     *FsptUpdDataPtr
);
typedef
EFI_STATUS
(EFIAPI *FSP_MEMORY_INIT) (
  IN  VOID     *FspmUpdDataPtr
  OUT VOID     **HobListPtr;
);
typedef
EFI_STATUS
(EFIAPI *FSP_TEMP_RAM_EXIT) (
  IN VOID      *TempRamExitParamPtr
);
typedef
EFI_STATUS
(EFIAPI *FSP_SILICON_INIT) (
  IN VOID      *FspsUpdDataPtr
);
```

Intel FSP v2.0 UPD structures

```
typedef struct {
  /** Offset 0x0000 **/
  UINT64                        Signature;
  /** Offset 0x0008 **/
  UINT8                         Revision;
  /** Offset 0x0009 **/
  UINT8                         Reserved[23];
} FSP_UPD_HEADER;


typedef struct {
  /** Revision v1 for FSP v2.0 **/
  UINT8                         Revision;
  UINT8                         BootMode;
  UINT8                         Reserved[2];
  VOID                          *NvsBufferPtr;
  VOID                          *StackBase;
  UINT32                        StackSize;
  UINT32                        BootLoaderTolumSize;
  UINT8                         Reserved1[12];
} FSPM_ARCH_UPD;
```

```
typedef struct {
  FSP_UPD_HEADER                UpdHeader;

  /** Platform specific parameters **/
...
} FSPT_UPD;

typedef struct {
  FSP_UPD_HEADER                UpdHeader;
  FSPM_ARCH_UPD                 FspmArchUpd;

/** Platform specific parameters **/
...
} FSPM_UPD;

typedef struct {
  FSP_UPD_HEADER                UpdHeader;

/** Platform specific parameters **/
...
} FSPS_UPD;
```

Intel FSP - SDK

SDK - Open Source

https://github.com/tianocore/edk2/

BaseTools, MdePkg, MdeModulePkg

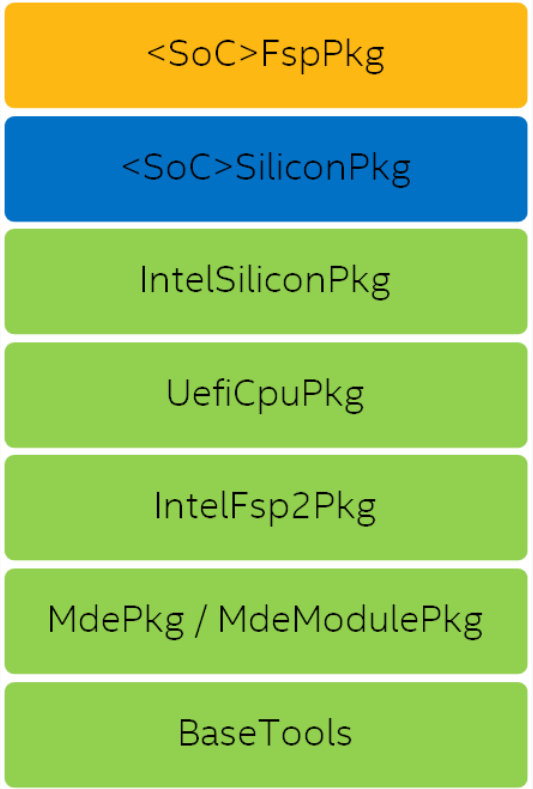
IntelFsp2Pkg, IntelSiliconPkg, UefiCpuPkg

Silicon specific

<Soc>SiliconPkg

Silicon specific FSP Glue code

<Soc>FspPkg



Intel FSP - Distribution

Fsp.bin - FSP Binary

FspUpd.h; FsptUpd.h; FspmUpd.h; FspsUpd.h - Configuration structures

Integration Guide

Fsp.bsf - Boot settings file for static configuration

Additional data structure files as needed

Sample code as needed

Intel FSP - versions and intercepts

Intel FSP v1.0

5th Generation Intel® Core™ Processors and chipsets (formerly Broadwell)
Intel® Atom™ processor C2000 product family (formerly Rangeley)
Intel® Atom™ processor E3800 product family (formerly Bay Trail)
Intel® Xeon® Processor D Product Family (formerly Broadwell-DE)

Intel FSP v1.1

6th Generation Intel® Core™ Processors and chipsets (formerly Skylake)
Intel® Pentium® and Celeron® Processor N3000 Product Families and Intel® Atom™ x5-E8000 Processor (formerly Braswell)

Intel FSP v2.0

Kabylake (follow on to Skylake)
Apollolake (follow on to Braswell)

Visit www.intel.com/fsp for additional details and links

Future direction

Share the FSP binary and associated files thru Git

- Eliminate the web based click thru license
- Simplify updating to latest versions when available

Continue to increase open source content inside the FSP binary

- UefiCpuPkg for CPU initialization
- IntelSiliconPkg for other silicon initialization

Enable generating FSP binary using public code

- Limit binaries for IP specific modules
- Reduce binary footprint

Intel FSP - GitHub URLs

IntelFspPkg (FSP v1.x)

https://github.com/tianocore/edk2/tree/master/IntelFspPkg

IntelFsp2Pkg (FSP v2.0)

https://github.com/tianocore/edk2/tree/master/IntelFsp2Pkg

SplitFspBin.py - Tool to split FSP components & rebase

https://github.com/tianocore/edk2/blob/master/IntelFsp2Pkg/Tools/SplitFspBin.py

Intel FSP - Related URLs #IntelFSP

FSP Home page - www.intel.com/fsp

FSP External Architecture Specification (EAS) v2.0
http://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/fsp-architecture-spec-v2.pdf

FSP External Architecture Specification (EAS) v1.1a
http://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/fsp-architecture-spec-v1-1a.pdf

Boot Settings File (BSF) Specification v1.0
https://firmware.intel.com/sites/default/files/BSF_1_0.pdf

Binary Configuration Tool (BCT) - Windows and Linux (32 & 64 bit) versions at www.intel.com/fsp

Backup

Intel FSP v1.0 & v1.1 Boot flows