IDF14

Firmware Flexibility using Intel® Firmware Support Package

Vincent Zimmer – Senior Principal Engineer, Intel Corporation

STTS001

intel

Agenda

- Overview of the Intel® Firmware Support Package (Intel® FSP) to encapsulate Intel® silicon initialization
- Scaling platform initialization with the Intel FSP and open source Intel® Architecture (IA) firmware ecosystems
- Details on building an open source IA platform with Intel FSP
- Full openness
- Summary and next steps

Agenda

- Overview of the Intel® Firmware Support Package (Intel® FSP) to encapsulate Intel® silicon initialization
- Scaling platform initialization with the Intel FSP and open source Intel® Architecture (IA) firmware ecosystems
- Details on building an open source IA platform with Intel FSP
- Full openness
- Summary and next steps

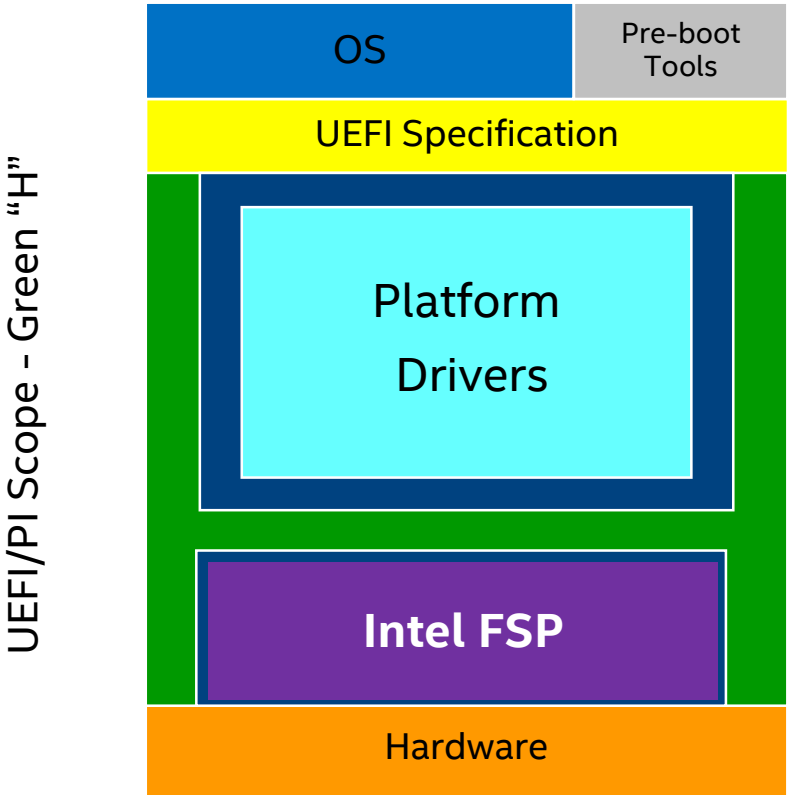
The Intel® Firmware Support Package (Intel® FSP)

Intel® Firmware Support Package (Intel® FSP) components

- CPU, memory controller, and chipset initialization functions as a binary package
- Provides silicon initialization ingredients
- Plugs into existing firmware frameworks
- Integration guide, includes API documentation

Intel FSP is currently available for the many Intel® hardware-producing divisions

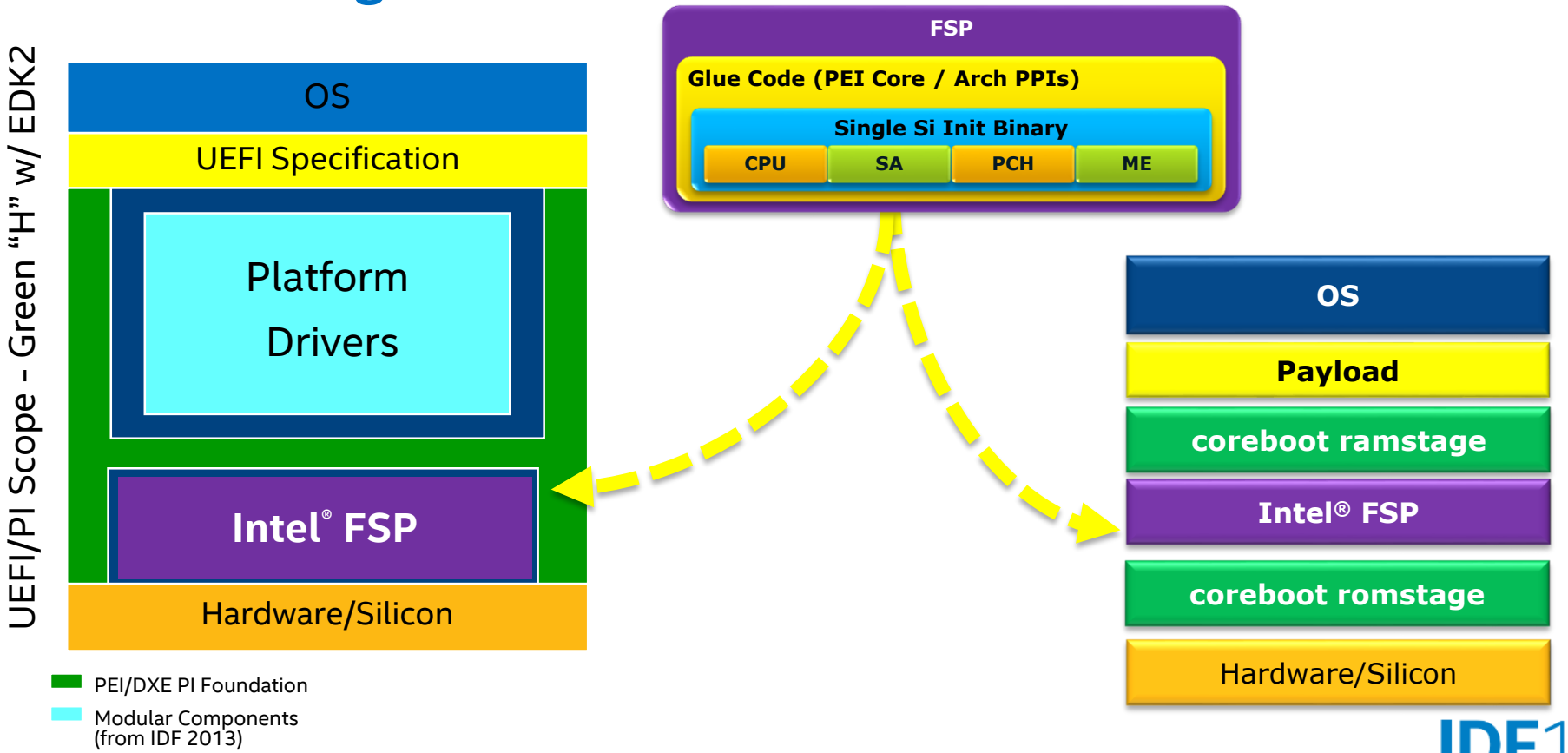
From IDF 2013 Applying Intel® Firmware Support Package to Open Source EDK II



EDK II provides the framework ("Green H")

Intel® Firmware Support Package (Intel® FSP) provides low level of silicon initialization

Applying “Produced” Intel® Firmware Support Package (FSP) to “Consuming” IA firmware



Intel® FSP Producer

- Examples of binary instances on http://www.intel.com/fsp with integration guides
- This includes hardware initialization code that is EFI Developer Kit II (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)
- Present 1.0 specification at FSP 1.0 External Architecture Specification (EAS)

The Source for the Intel® FSP Producer Code

- CPU and chipset-specific code for PEIM's inside of the Intel FSP can be open or closed, added to…
- PEI core and infrastructure code at https://svn.code.sf.net/p/edk2/code/trunk/edk2/MdePkg and https://svn.code.sf.net/p/edk2/code/trunk/edk2/MdeModulePkg
- And the code to create the Intel FSP interfaces can be found at https://svn.code.sf.net/p/edk2/code/trunk/edk2/IntelFspPkg/

Intel FSP can encapsulate IP protected initialization code PRODUCED by Intel business units

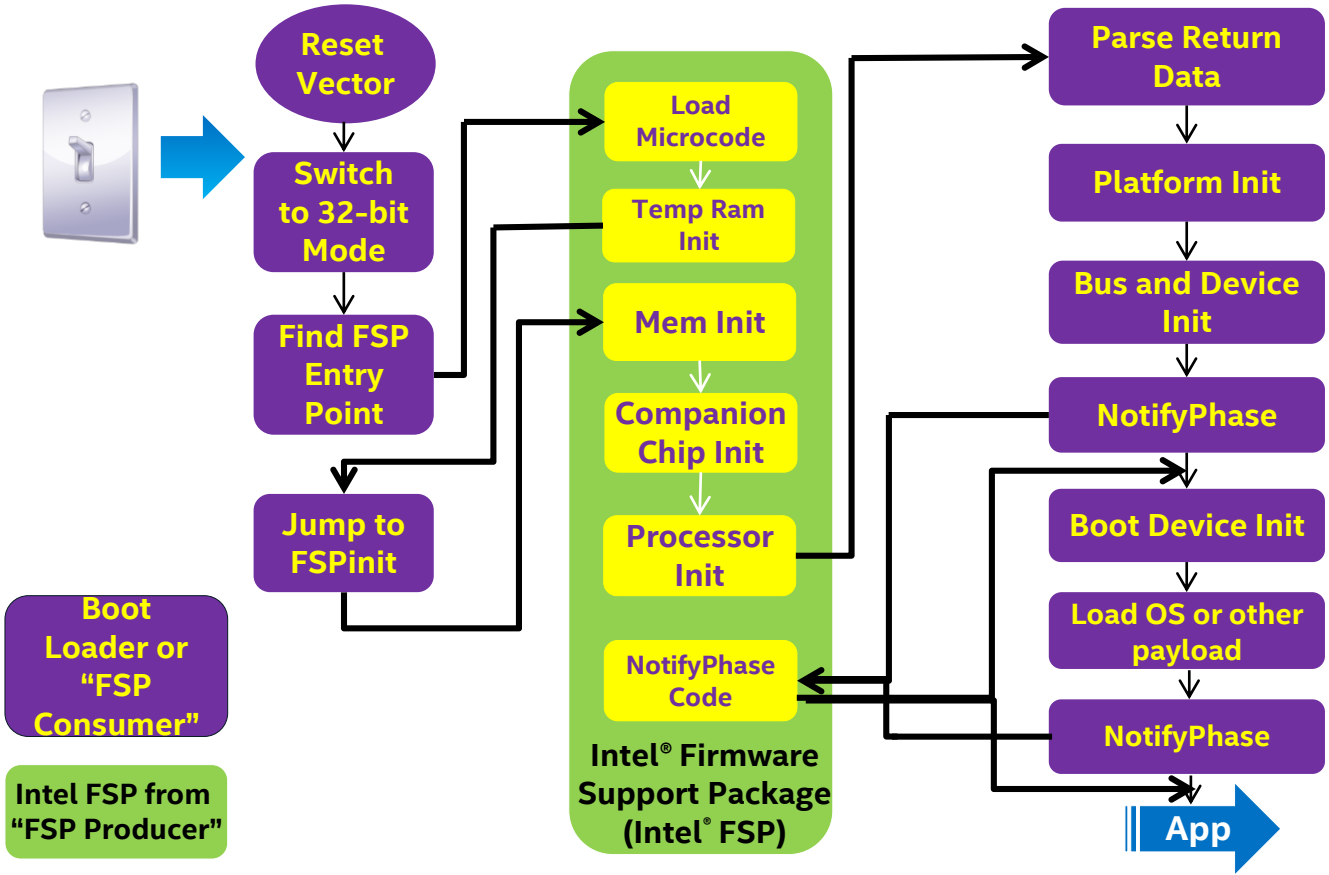
Agenda

- Overview of the Intel® Firmware Support Package (Intel® FSP) to encapsulate Intel® silicon initialization
- Scaling platform initialization with the Intel FSP and open source Intel® Architecture (IA) firmware ecosystems
- Details on building an open source IA platform with Intel FSP
- Full openness
- Summary and next steps

Intel® FSP Consumer

- Consumer Firmware can be bootloaders from board support packages, traditional BIOS, UEFI/PI based EDK II firmware, or other embedded software solutions
- Firmware to absorb, integrate, or ‘consume’ the Intel FSP binary
- Consistent consumer code in the open source Intel® Architecture firmware up streams
- Enables fully open work-flow of using Intel FSP and open source IA firmware code

Intel® FSP Boot Flow



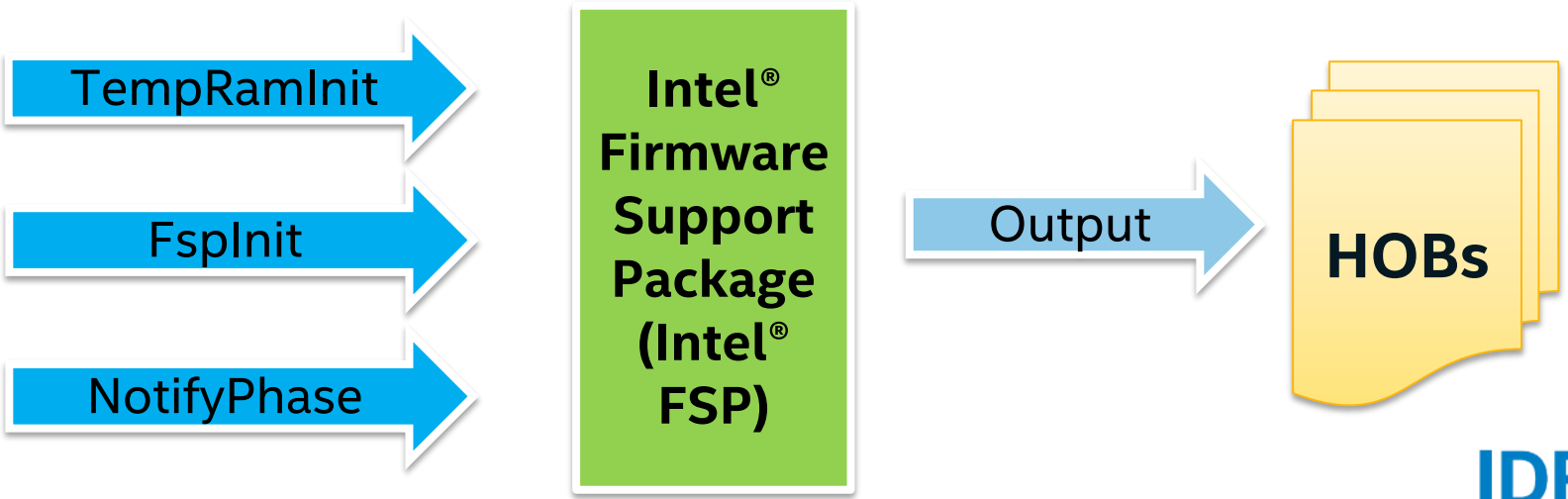
Intel® FSP External Interfaces

APIs published by the Intel FSP Producer and invoked by the Consumer

- **TempRamInit** - Enables cache for using as temporary memory and code caching
- **FspInit** - Performs the processor and companion chipset initialization
- **NotifyPhase** - Hooks for certain phase during the platform initialization

Intel FSP Producer/binary creates the UEFI PI Hand-off Blocks (Vol 3 of the UEFI PI spec)

- Contains basic platform information



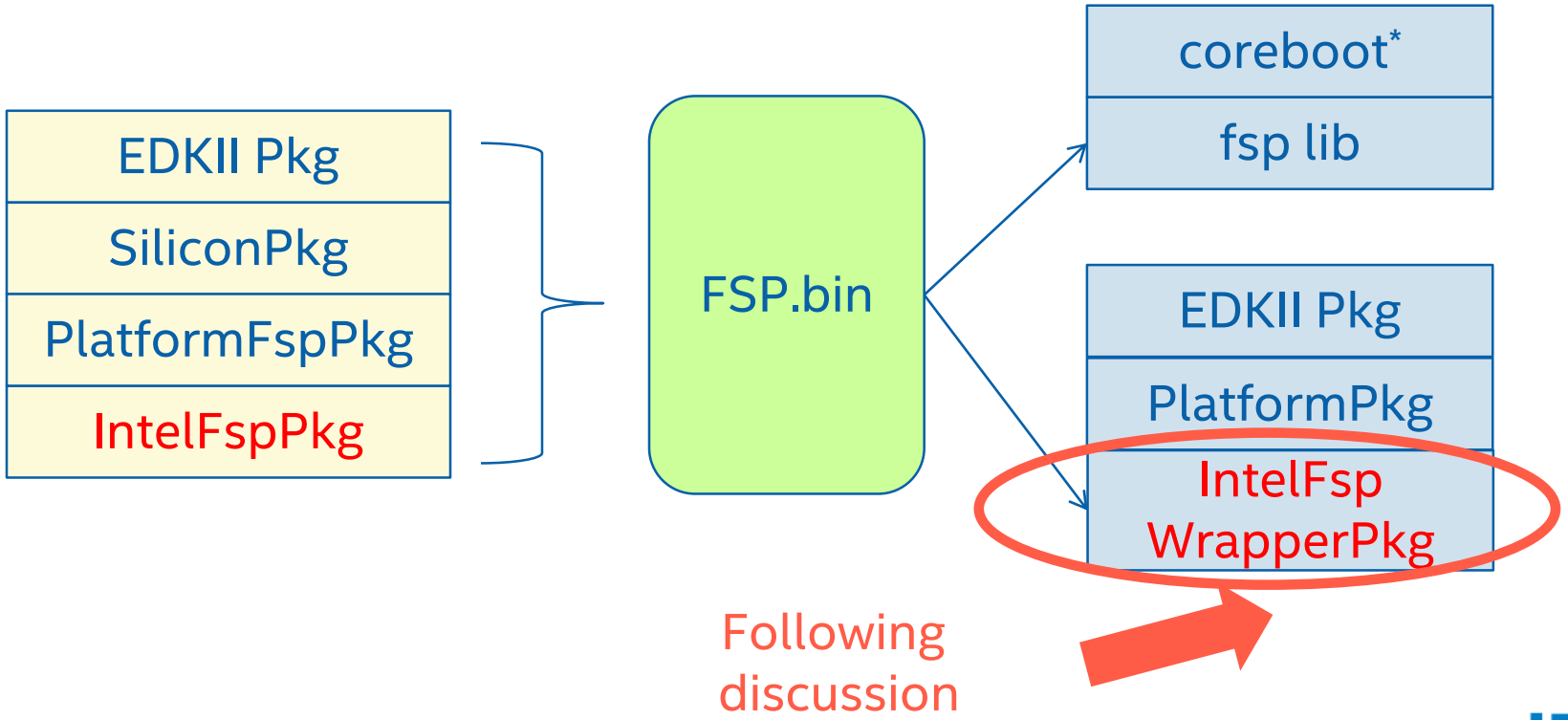
Agenda

- Overview of the Intel® Firmware Support Package (Intel® FSP) to encapsulate Intel silicon initialization
- Scaling platform initialization with the Intel FSP and open source Intel® Architecture (IA) firmware ecosystems
- Details on building an open source IA platform with Intel FSP
- Full openness
- Summary and next steps

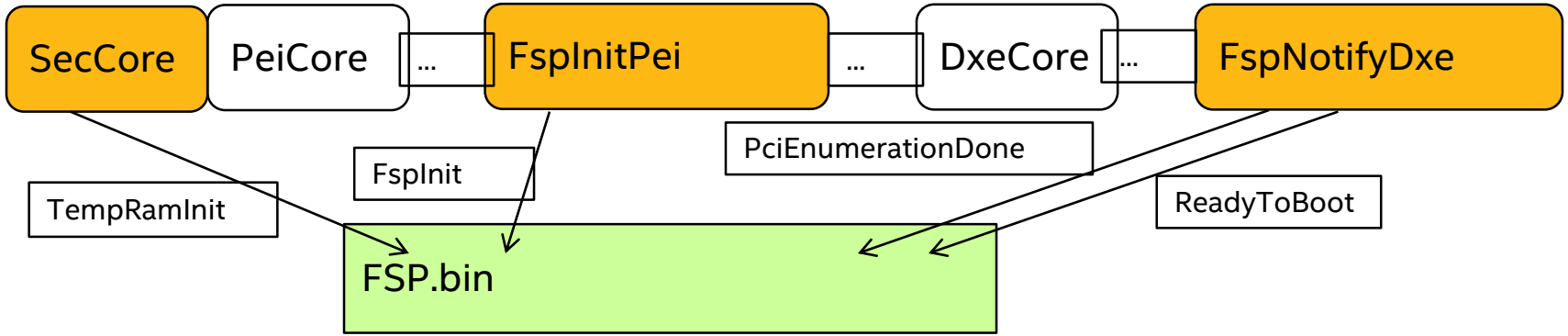
2 Consumers: EDK II firmware and coreboot*

Functionality	coreboot	UEFI / PI
The reset vector and pre cache-as-ram setup	bootblock	Security Phase (SEC)
Cache as Ram setup, early silicon initialization, memory setup. Covered largely by Intel® Firmware Support Package	romstage	Pre-EFI Initialization (PEI) Create HOBs
Normal device setup and mainboard configuration. Publish SMBIOS/ACPI Tables	ramstage	Early Driver Execution Environment (DXE)
Memory map hand-off	CBMEM	UEFI Memory Map
The OS or application bootloader	payload	DXE BDS and UEFI Drivers

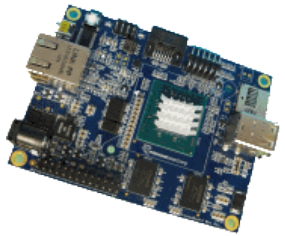
EDK II based Intel® FSP Consumer Details



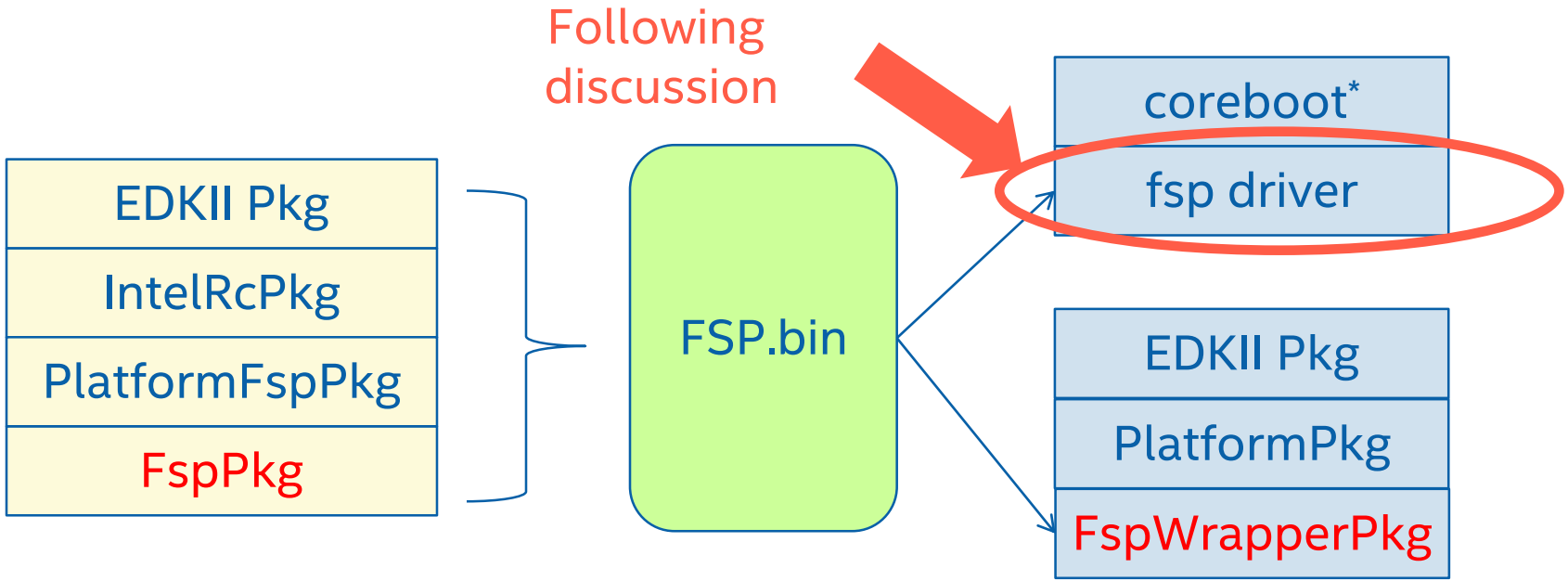
EDK II based Intel® FSP Consumer Flow



- Generic EDK II code, the *FSP Wrapper*
- https://svn.code.sf.net/p/edk2/code/trunk/edk2/IntelFspWrapperPkg/
- Allows for integration of Intel® Firmware Support Package binary into EDK II-based platform code
- Some sample platform code at http://uefidk.com



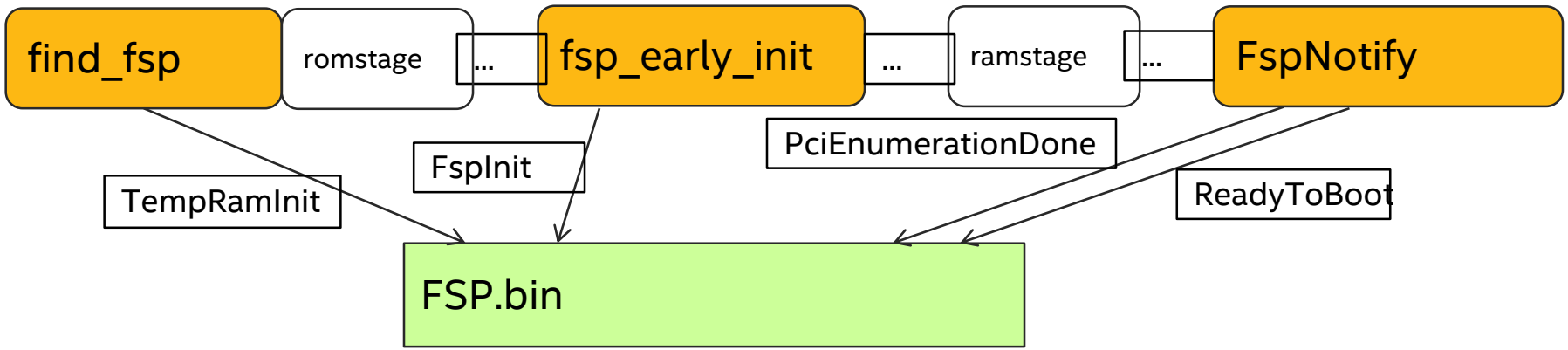
coreboot* based Intel® FSP Consumer Details



coreboot* Intel® FSP Consumer Code Details

coreboot* driver	Functionality
find_fsp	Function to find the FSP in memory
fsp_early_init	FSP memory and early device setup function. Called in romstage by the chipset driver
romstage_fsp_rt_buffer_callback	Callback from fsp_early_init for mainboard specifc RT buffer customizations (soldered down memory timings, etc.)
FspNotify	There are two notify calls in ramstage. AfterPciEnumeration during device finalize and ReadyToBoot during chip finalize.
save_mrc_data	Called in romstage after fsp_early_init to save the memory configuration to CBMEM
update_mrc_cache	Moves the mrc data from CBMEM to NVRAM in late ramstage

coreboot* based Intel® FSP Consumer Flow



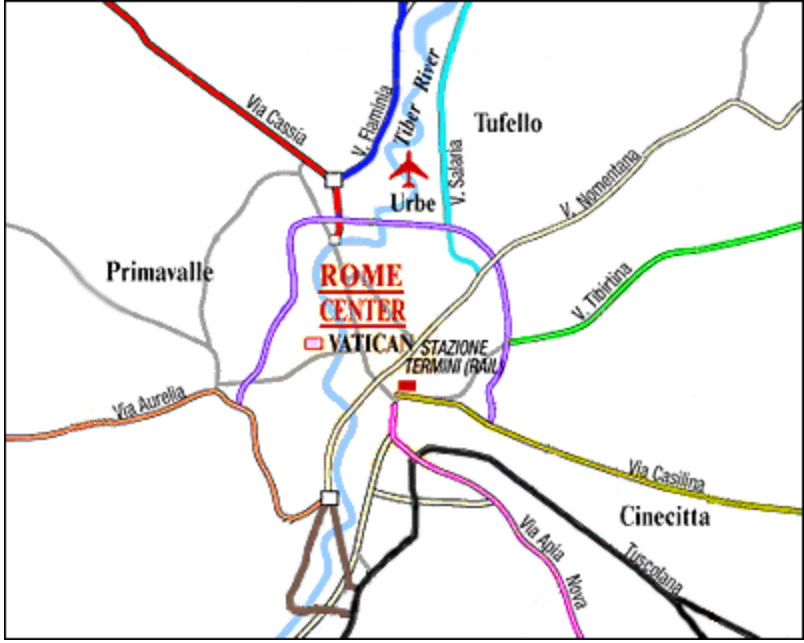
The EDK II and coreboot* open source ecosystems can CONSUME FSP's with the upstreamed FSP wrapper package & driver

Agenda

- Overview of the Intel® Firmware Support Package (Intel® FSP) to encapsulate Intel silicon initialization
- Scaling platform initialization with the Intel FSP and open source Intel® Architecture (IA) firmware ecosystems
- Details on building an open source IA platform with Intel FSP
- Full openness
- Summary and next steps

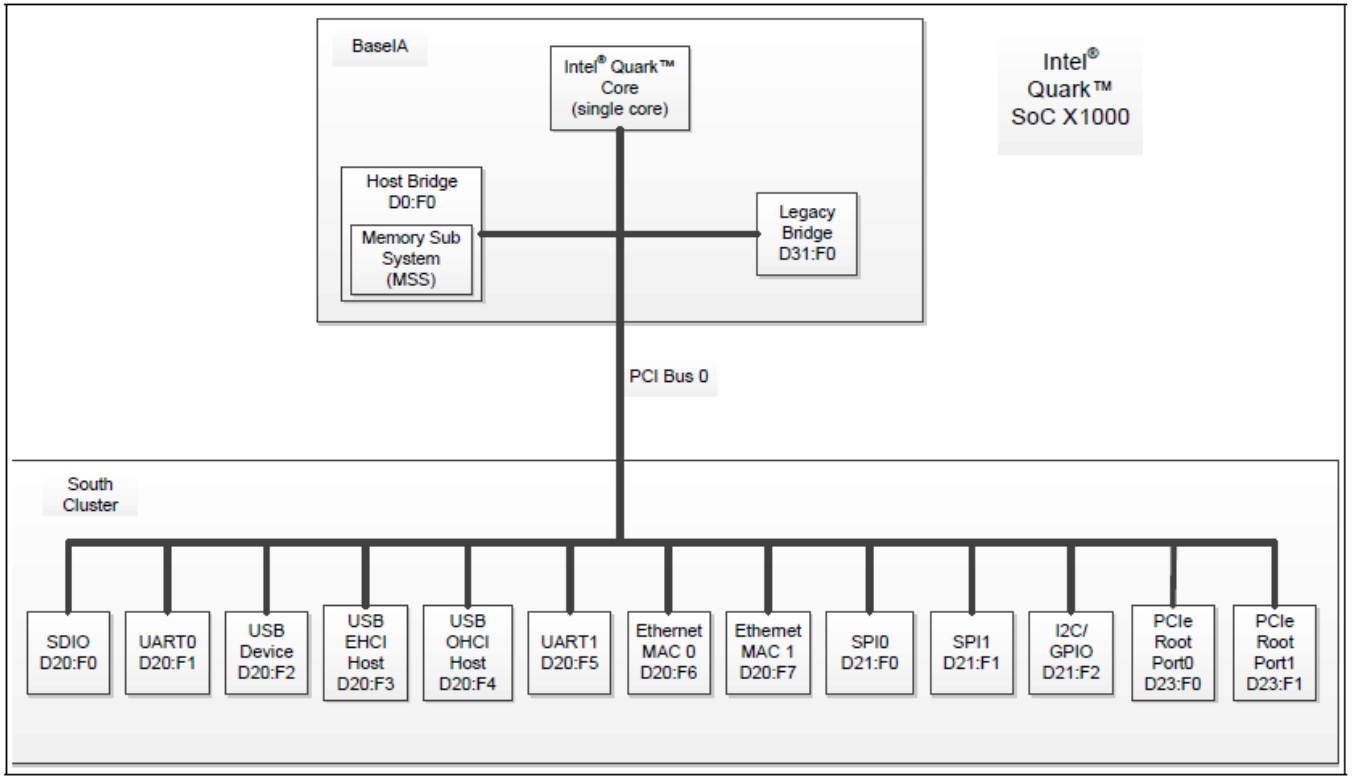
Many Paths for Enabling

- We’re moving into a world where it is easier to work with Intel® platforms
- Open platforms, open source
- Intel® Unified Binary Management System (Intel® UBMS)
- Development kits, Reference boards
- There is also a full open source EDK II option
  - See full platform sources for Intel® Quark™ SoC, including a feature rich UEFI build



Intel® Quark™ SoC – Hardware Overview

- 32 bit Intel® Pentium® ISA-class processor
- PCI
- USB
- I2C
- Single core



UEFI for Intel® Quark™ SoC

- First fully open source Intel-based platform
- Builds on Intel® UDK2010 packages like MdePkg, MdeModulePkg w/ a 32-bit build, adding
  - IA32FamilyCpuBasePkg
  - QuarkPlatformPkg
  - QuarkSocPkg
- Standard build is 1 Mbyte image w/full features
  - Capsule update, SMM, S3, PCI, recovery, full UEFI OS support, FAT OS support, UEFI variables

UEFI for Intel® Quark™ SoC

- A modular firmware architecture like UEFI PI and code-base like EDK II allows for scaling the technology
- Fixed function UEFI OS load experiences can scale in size
- Introducing “TinyQuark” open source example
  - 64 kbyte to boot UEFI-aware Yocto* image from SPI NOR flash

Module	Size (K)	%
Generic	34	50%
Silicon	10	14%
Platform	24	36%

```
FV Space Information
EDKII_BOOT_STAGE1_IMAGE1 [99%Full] 65536 total, 65216 used, 320 free
```

Many paths for enabling, including full openness

Agenda

- Overview of the Intel® Firmware Support Package (Intel® FSP) to encapsulate Intel silicon initialization
- Scaling platform initialization with the Intel FSP and open source Intel® Architecture (IA) firmware ecosystems
- Details on building an open source IA platform with Intel FSP
- Full openness
- Summary and next steps

Summary

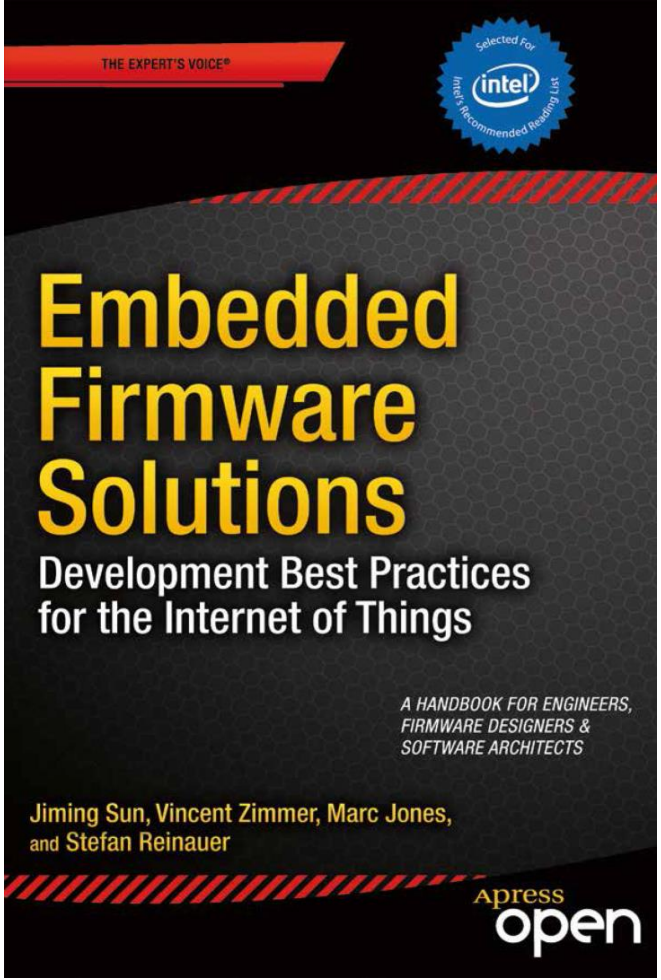
- Intel® Firmware Support Package (Intel® FSP) can encapsulate IP protected initialization code PRODUCED by Intel business units
- The EDK II and coreboot* open source Intel® Architecture (IA) firmware ecosystems can CONSUME FSP's with the up streamed FSP wrapper package and driver code
- Beyond mixing binary FSP and source, a full open source EDK II experience is possible, as noted by the Intel Quark Firmware

Next Steps

- Start to examine the Intel® Firmware Support Package (Intel® FSP) collection at intel.com/fsp, support code at tianocore.org, and sample projects at uefidk.com
- Provide Intel feedback as Intel FSP 1.0 EAS evolves going forward for new platform topologies FSP 1.0 External Architecture Specification (EAS) and whitepaper at FSP on EDKII Whitepaper
- Build more platforms with open source platform packages on www.tianocore.org and www.coreboot.org
- Evaluate the first fully-featured platforms on uefidk.com, like Intel® Quark™ SoC https://communities.intel.com/docs/DOC-22226 and Tiny Quark https://uefidk.com/content/get-started-intel-galileo-development-board and whitepaper at TinyQuark Whitepaper

Additional Sources of Information

- A PDF of this presentation is available from our Technical Session Catalog: www.intel.com/idfsessionsSF. This URL is also printed on the top of Session Agenda Pages in the Pocket Guide.
- More web based info:
  www.tianocore.org
  www.intel.com/fsp
  www.uefidk.com
  www.coreboot.org
- More on topics discussed in this presentation:
  see upcoming book
  Embedded Firmware Solutions
  http://www.apress.com/9781484200711



Participate for Chance to Win!!

Innovation and fun go hand in hand!

- Get your RFID/USB wristband and details at the Software & Services Pavilion in the Technology Showcase, or at our mobile carts outside Moscone West.
- Once you register, you're connected to:
  - Software and services content
  - Tracking earned coins for the "Surf the Code" game and other prizes
  - Your own 3D avatar with 10 coins… Play the game, share with friends
- Visit the Software & Services Pavilion to earn more coins
  - Talk with Intel experts about your development needs and plans
  - Tinker on your own time with self-run labs, source code, tools
  - Swipe your wristband on the Galileo Scan Stations to get coins
- Play to Win in the Software & Services Pavilion
  - Get 5 coins to play "Surf the Code"… Gift cards for three highest scores!
  - Get 10 coins to get your 3D avatar… And enter daily drawing for tablets and 2-in-1s
  - Get 15 coins for your King Code t-shirt, and increase total game score potential

Don't let the fun stop!
Daily lunch at food trucks

IDF14

Other Technical Sessions

from Software Services Group & System Tools and Technology Tracks

	Session ID	Title	Day	Time	Room
✓	SFTS005	Oracle* Exalytics in the Speed of Thought: Extreme Scaling on Intel® Xeon® Processor E7	Tues	4:00	2007
✓	SFTS006	Creating Immersive Augmented Reality Experiences on Android* Mobile Platforms Based on Intel® Architecture	Tues	5:15	2007
✓	STTS001	Firmware Flexibility Using the Intel® Firmware Support Package	Thurs	9:30	2008
	STTS002	Simplifying Firmware Development with Intel® Unified Binary Management Suite	Thurs	10:45	2008
	STTS003	Complex Systems Become Simple: Internet of Things with Wind River Simics*	Thurs	1:00	2008
	BIGS004	Accelerating Hadoop* Performance on Intel® Architecture Based Platforms	Thurs	1:00	2004
	IOTS007	Intel® Firmware Support Package for Internet of Things	Thurs	2:15	2001
	STTS004	Software Based System Power and Thermal Optimization Technology	Thurs	2:15	2008

✓ = DONE

Completing an online session evaluation by 10:00 a.m. tomorrow automatically enters you in a drawing to win.

Day 1 Prize

Win an Intel® Galileo Gen 2 Development Board

Day 2 Prize

Win an Intel® Gigabyte* BRIX Pro-Ultra Compact PC

Day 3 Prize

Win a Microsoft® Surface Pro 3

Winners will be announced by email

Copies of the complete sweepstakes rules are available at the Info Desk on Level 2.

Q&A

Legal Disclaimer

Risk Factors

The above statements and any others in this document that refer to plans and expectations for the second quarter, the year and the future are forward-looking statements that involve a number of risks and uncertainties. Words such as “anticipates,” “expects,” “intends,” “plans,” “believes,” “seeks,” “estimates,” “may,” “will,” “should” and their variations identify forward-looking statements. Statements that refer to or are based on projections, uncertain events or assumptions also identify forward-looking statements. Many factors could affect Intel’s actual results, and variances from Intel’s current expectations regarding such factors could cause actual results to differ materially from those expressed in these forward-looking statements. Intel presently considers the following to be important factors that could cause actual results to differ materially from the company’s expectations. Demand for Intel's products is highly variable and, in recent years, Intel has experienced declining orders in the traditional PC market segment. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions; consumer confidence or income levels; customer acceptance of Intel’s and competitors’ products; competitive and pricing pressures, including actions taken by competitors; supply constraints and other disruptions affecting customers; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Intel operates in highly competitive industries and its operations have high costs that are either fixed or difficult to reduce in the short term. Intel's gross margin percentage could vary significantly from expectations based on capacity utilization; variations in inventory valuation, including variations related to the timing of qualifying products for sale; changes in revenue levels; segment product mix; the timing and execution of the manufacturing ramp and associated costs; excess or obsolete inventory; changes in unit costs; defects or disruptions in the supply of materials or resources; and product manufacturing quality/yields. Variations in gross margin may also be caused by the timing of Intel product introductions and related expenses, including marketing expenses, and Intel's ability to respond quickly to technological developments and to introduce new products or incorporate new features into existing products, which may result in restructuring and asset impairment charges. Intel's results could be affected by adverse economic, social, political and physical/infrastructure conditions in countries where Intel, its customers or its suppliers operate, including military conflict and other security risks, natural disasters, infrastructure disruptions, health concerns and fluctuations in currency exchange rates. Intel’s results could be affected by the timing of closing of acquisitions, divestitures and other significant transactions. Intel's results could be affected by adverse effects associated with product defects and errata (deviations from published specifications), and by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust, disclosure and other issues, such as the litigation and regulatory matters described in Intel's SEC filings. An unfavorable ruling could include monetary damages or an injunction prohibiting Intel from manufacturing or selling one or more products, precluding particular business practices, impacting Intel’s ability to design its products, or requiring other remedies such as compulsory licensing of intellectual property. A detailed discussion of these and other factors that could affect Intel’s results is included in Intel’s SEC filings, including the company’s most recent reports on Form 10-Q, Form 10-K and earnings release.

Rev. 4/15/14