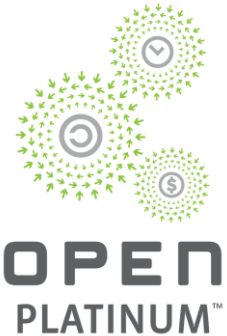
OPEN POSSIBILITIES.

FSP and MinPlatform for Sapphire Rapids Intel® Xeon® Scalable Processors

NOVEMBER 9-10, 2021

FSP and MinPlatform for Sapphire Rapids Intel® Xeon® Scalable Processors

Nate DeSimone, Firmware Engineer, Intel
Isaac Oram, Principal Engineer, Intel



OPEN POSSIBILITIES.

Agenda

OPEN SYSTEM FIRMWARE

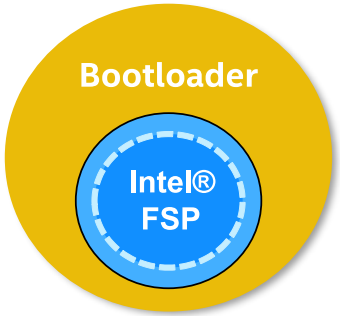
- FSP & MinPlatform Overview
- Recent Development Progress
- Plans for Sapphire Rapids
- Project Opportunities
- Call to Action

OPEN POSSIBILITIES.

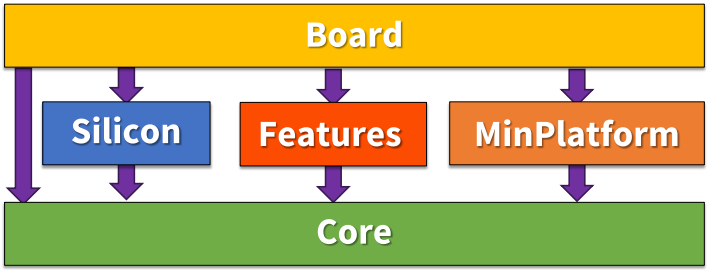
FSP & MinPlatform Overview

OPEN SYSTEM FIRMWARE

- Intel® FSP is a silicon initialization binary
  - Easily integrable into diverse OSF solutions.



- MinPlatform is a sub-project of TianoCore with 2 primary goals:
  1. Improve the architecture, modularity, and consistency of UEFI Firmware
  2. Run open source EDK II on real systems



OSF on Intel Xeon

OPEN SYSTEM FIRMWARE

- Intel provides industry leading support for diverse OSes (RHEL, Debian, Windows, VMware…) on Xeon.
  - Now… that extends to OSF: tianocore, LinuxBoot, coreboot, SLIM BOOTLOADER, U-Boot
- Intel makes diverse OSF possible with:
  1. Publicly redistributable FSP binaries
  2. MinPlatform as an example OSF that can be referenced/modified

Targeting a best-in-class OSF experience!

Better Together

OPEN SYSTEM FIRMWARE

- FSP + MinPlatform creates an OSF solution that meets the OCP Accepted Checklist requirements.

- FSP & MinPlatform derive from the same codebase and fit together exactly.

FSP + MinPlatform = Fastest TTM for OSF on Xeon

coreboot vs. MinPlatform APIs

OPEN SYSTEM FIRMWARE

- MinPlatform board APIs offer a similar experience to the coreboot mainboard APIs:

coreboot	MinPlatform
`bootblock_mainboard_init()`	`BoardInitBeforeMemoryInit()`
`mainboard_init()`	`BoardInitBeforeSiliconInit()`
`mainboard_memory_init_params()`	`SiliconPolicyUpdatePreMem()`
`mainboard_silicon_init_params()`	`SiliconPolicyUpdatePostMem()`

Recent Progress

OPEN SYSTEM FIRMWARE

- Ice Lake and Cooper Lake MinPlatform is now open-source

- Includes publicly redistributable FSP binaries

tianocore / **edk2-platforms** Public

master **edk2-platforms** / Platform / Intel / **WhitleyOpenBoardPkg** /

CooperCityRvp	24 days ago
Include	last month
Library	8 days ago
Platform	2 months ago
Uba	29 days ago
WilsonCityRvp	24 days ago
..	

https://github.com/tianocore/edk2-platforms/tree/master/Platform/Intel/WhitleyOpenBoardPkg

Recent Progress (Cont.)

OPEN SYSTEM FIRMWARE

- Since OCP Tech Week 2020, 5 new boards have been liberated!

Machine Name	Chipset	Build Target Name
Intel Wilson City RVP	IceLake-SP	WilsonCityRvp
Intel Cooper City RVP	Cooper Lake	CooperCityRvp
Facebook Tioga Pass	Purley-R	BoardTiogaPass
Intel TGL-U DDR4 RVP	Tiger Lake	TigerlakeURvp
Acer Aspire VN7-572G	Sky Lake	AspireVn7Dash572G

Recent Progress (Cont.)

OPEN SYSTEM FIRMWARE

- Native support for LinuxBoot is now upstream
- 64-bit handoff via the kernel's EFI stub boot protocol

tianocore / **edk2-platforms** Public

master **edk2-platforms** / Platform / Intel / PurleyOpenBoardPkg / Features / **LinuxBoot** /

LinuxBinaries	2 months ago
LinuxBoot.c	2 months ago
LinuxBoot.h	2 months ago
LinuxBoot.inf	2 months ago
LinuxBootNull.c	2 months ago
LinuxBootNull.inf	2 months ago
Readme.md	2 months ago

https://github.com/tianocore/edk2-platforms/tree/master/Platform/Intel/PurleyOpenBoardPkg/Features/LinuxBoot

Planned LinuxBoot Improvements

OPEN SYSTEM FIRMWARE

- Move from PurleyOpenBoardPkg to a unified LinuxBootFeaturePkg.
- Support kernel 5.7+ arch-agnostic EFI initrd load.
  https://lore.kernel.org/linux-efi/20200207202637.GA3464906@rani.riverdale.lan/T/#m4a25eb33112fab7a22faa0fd65d4d663209af32f
- LinuxBoot customized/optimized BdsDxe.
- Open Question to Community: What should we do about the kernel command line? We currently have:

```
char CmdLine[] = " ";
```

Plans for 4th Gen Xeon® Scalable

OPEN SYSTEM FIRMWARE

- Improved support for FSP API mode
- More open-source advanced features for MinPlatform available out-of-box
- Gradual progress on evolving traditional UEFI BIOS towards the lightweight and open MinPlatform design

Project Opportunities

OPEN SYSTEM FIRMWARE

- Unified LinuxBoot Advanced Feature
- Phase Agnostic Serial Logging (PEI/DXE/SMM)
- Binary silicon init policy abstraction
- Universal Payload use

Call to Action

OPEN SYSTEM FIRMWARE

1. Use FSP + MinPlatform to build OSF for your upcoming OCP design.
   - We are happy to help merge new board ports upstream to TianoCore!
   - Its open source – contributions from other silicon vendors are welcome!
2. Collaborate with us on Project Opportunities!
   - LinuxBoot Advanced Feature, Phase Agnostic Logging, Universal Payload, etc.
3. Join the TianoCore Development Mailing list.
   - https://edk2.groups.io/g/devel
4. Check out the MinPlatform training material.
   - https://github.com/tianocore-training/Presentation_FW/blob/main/FW/Presentations/_D_05_EDK_II_Open_Source_MinPlatform_pres.pdf
   - https://github.com/tianocore-training/Presentation_FW/blob/main/FW/Presentations/_U4_07_EDK_II_OpenBoard_MinPlatform_Porting_pres.pdf

Thank you!