EDK-II & CorebootPayloadPkg

Lee Leahy, Vincent Zimmer - Intel Corp

History of PC Booting

PC BIOS Int-x’s API in early 1980’s

EFI 1.02 in 1998

Framework specs + Tiano in early 2000’s

UEFI 2.0 in 2005

UEFI 2.6, PI1.4, ACPI 6.1 & EDKII / UDK

Standards

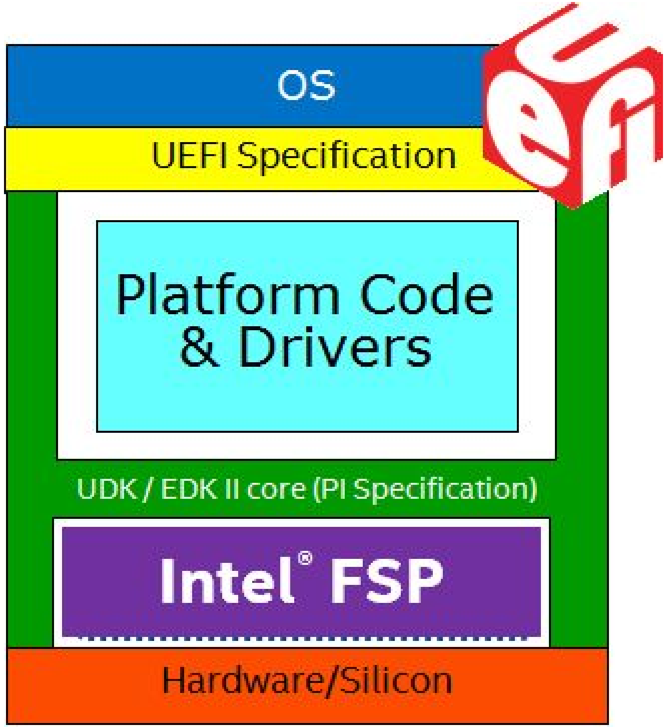
- UEFI
  - OS interface
- PI
  - Building blocks underneath UEFI
- ACPI
  - OS runtime tables
- DMTF
  - Manageability, like SMBIOS
- TCG
  - TPM h/w definition, platform specs on firmware TPM usage

EDK II

- Lib
  - MdePkg - baselibs, like the SDK for UEFI PI firmware
- Packages
  - Unit of distribution for code and binary
- PCD
  - Platform Configuration Database.
  - Fixed at build (like ifdef), or dynamic settings
- Cross platform build
  - Build on Linux, OS X, Windows w/ GCC, CLang, Intel ICC, MS Compiler
- Community moved to Github

Workflow

- Platform → BDS
- Open source core on tianocore.org
- FSP binary from intel.com/fsp
- Platform code from open or closed Repository
- SEC (temp ram) -> PEI (establish perm memory/DRAM) -> DXE (PCI, SMBIOS, ACPI, SMM) -> BDS
  - UEFI API's now ready. Run 3rd party code



FSP

- 1.0 → 1.1 → 2.0
- Platform Independent
- Memory Initialization
- Critical SOC Initialization
- Building Quark FSP

CorebootPayloadPkg Features

- Generic Hardware Support
    - Disks
    - Graphics
    - Serial Output
    - USB
        - Hub
        - Keyboard
- BDS
- EDK-II Shell

How to Build CorebootPayloadPkg

EDK II Build environment

Building CorebootPayloadPkg on LInux:

- IA32:

  ```
  build  -p CorebootPayloadPkg/CorebootPayloadPkgIa32.dsc  \
  -a IA32  -t GCC48  -b RELEASE
  ```

- X64:

  ```
  build  -p CorebootPayloadPkg/CorebootPayloadPkgIa32X64.dsc  \
  -a IA32  -a X64  -t GCC48  -b RELEASE
  ```

Integrating CorebootPayloadPkg with Coreboot

- CONFIG_PAYLOAD_ELF=y
- CONFIG_PAYLOAD_FILE="path to UEFIPAYLOAD.fd"

https://review.coreboot.org/#/c/15057/

Inputs From Coreboot

- Initializes PCI devices
- Serial Port Description
- Memory Map
- ACPI Tables

Challenges

- Flash
- SMM
- UEFI Secure Boot

User Feedback

- Future
- Opens
- Questions
- Complaints

References

- EDK II
    - Source Tree - https://github.com/tianocore/edk2
    - Development Process
    - Documentation
    - White Papers
- FSP Specifications
- Coreboot - MinnowMax
- CorebootPayloadPkg - Quark
- Acquiring, Building, and Configuring the Payload Compatible with the Coreboot Reference Bootloader Developed by Intel - Older EDK II sources