Unified Extensible Firmware Intreface (UEFI)

Mohsen Pahlevanzadeh
<mohsen@tehlug.org>

Table Of Contents

- What's UEFI?
- History of UEFI
- technical advantages over a traditional BIOS system
- Contents
- Some of Capabilities
- Windows 8 ,Monopoly and solutions

What's UEFI?

The Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. UEFI is meant as a replacement for the Basic Input/Output System (BIOS) firmware interface, present in all IBM PC-compatible personal computers. In practice, most UEFI images have legacy support for BIOS services. It can be used to allow remote diagnostics and repair of computers, even without another operating system.

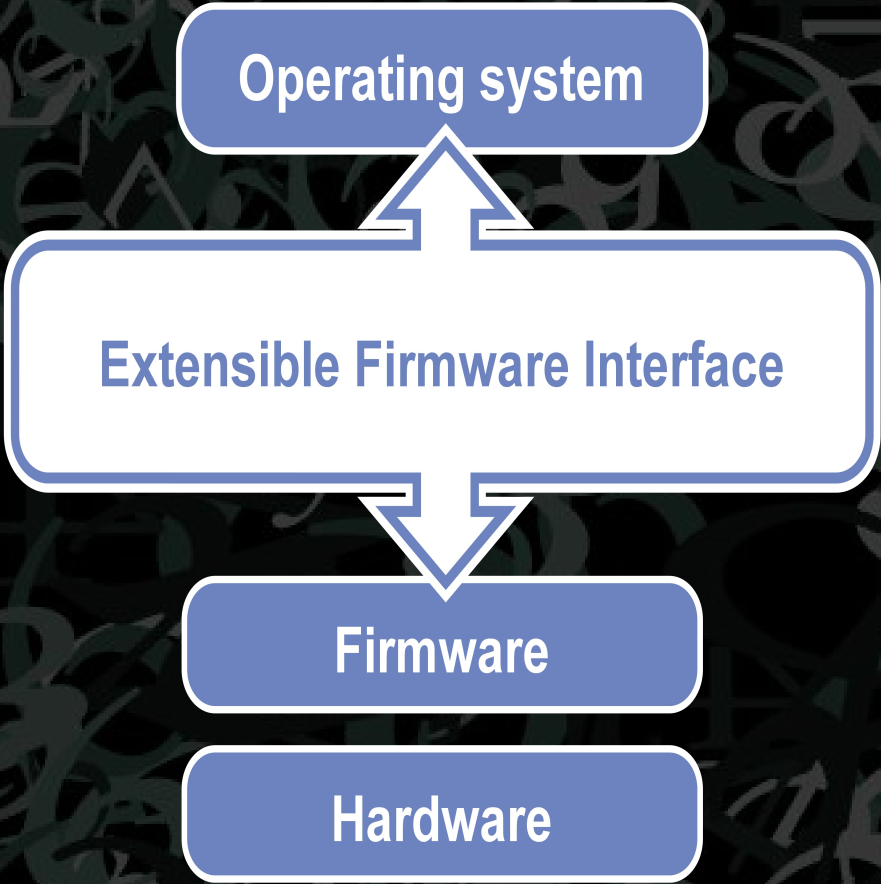


Table Of Contents

- What's UEFI?
- History of UEFI
- technical advantages over a traditional BIOS system
- Contents
- Some of Capabilities
- Windows 8 ,Monopoly and solutions

History of UEFI

- The original motivation for EFI came during early development of the first Intel–HP Itanium systems in the mid-1990s.
- BIOS limitations (such as 16-bit processor mode, 1 MB addressable space and PC AT hardware) were unacceptable for the larger server platforms Itanium was targeting. The effort to address these concerns was initially called *Intel Boot Initiative*, which began in 1998 and was later renamed EFI.
- In July 2005 Intel ceased development of the EFI spec at version 1.10, and contributed it to the Unified EFI Forum, which has evolved the specification as the Unified Extensible Firmware Interface (UEFI). The original EFI spec remains owned by Intel, which exclusively provides licenses for EFI-based products, but the UEFI specification is owned by the Forum.
- Version 2.1 of the UEFI (Unified Extensible Firmware Interface) specification was released on 7 January 2007. It added cryptography, network authentication and the User Interface Architecture (Human Interface Infrastructure in UEFI). The current UEFI specification, version 2.3.1, was approved in April 2011.

Table Of Contents

- What's UEFI?
- History of UEFI
- technical advantages over a traditional BIOS system
- Contents
- Some of Capabilities
- Windows 8 ,Monopoly and solutions

technical advantages over a traditional BIOS system.

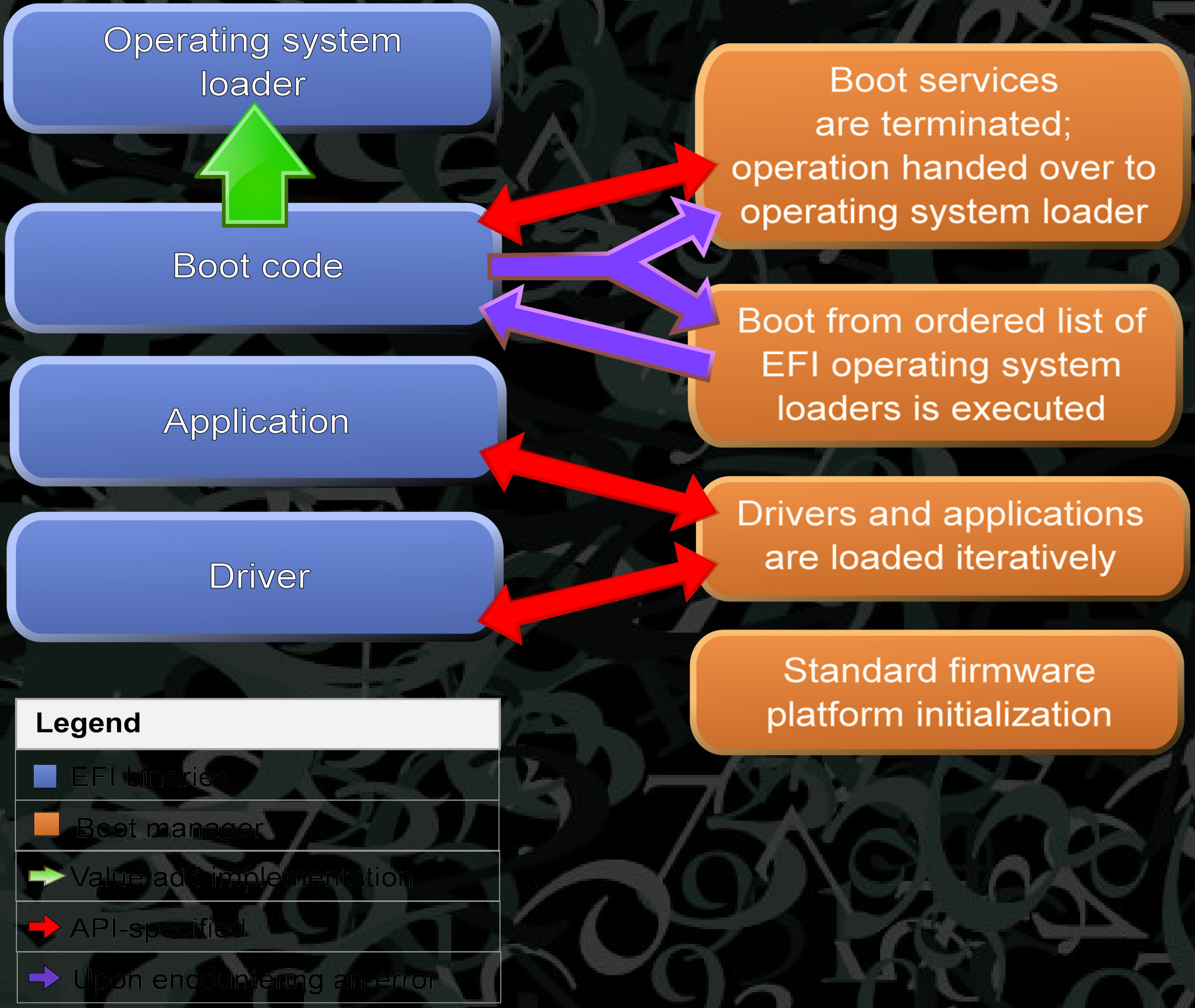
- Ability to boot from large disks (over 2 TiB) with a GUID Partition Table, GPT.
- CPU-independent architecture.
- CPU-independent drivers.
- Flexible pre-OS environment, including network capability.
- Modular design.

Table Of Contents

- What's UEFI?
- History of UEFI
- technical advantages over a traditional BIOS system
- Contents
- Some of Capabilities
- Windows 8 ,Monopoly and solutions

Contents

The interface defined by the EFI specification includes data tables that contain platform information, and boot and runtime services that are available to the OS loader and OS.



Operating system loader

Boot code

Application

Driver

Boot services are terminated; operation handed over to operating system loader

Boot from ordered list of EFI operating system loaders is executed

Drivers and applications are loaded iteratively

Standard firmware platform initialization

Legend

🟦 EFI binaries

🟧 Boot manager

➡ Value add implementation

➡ API-specified

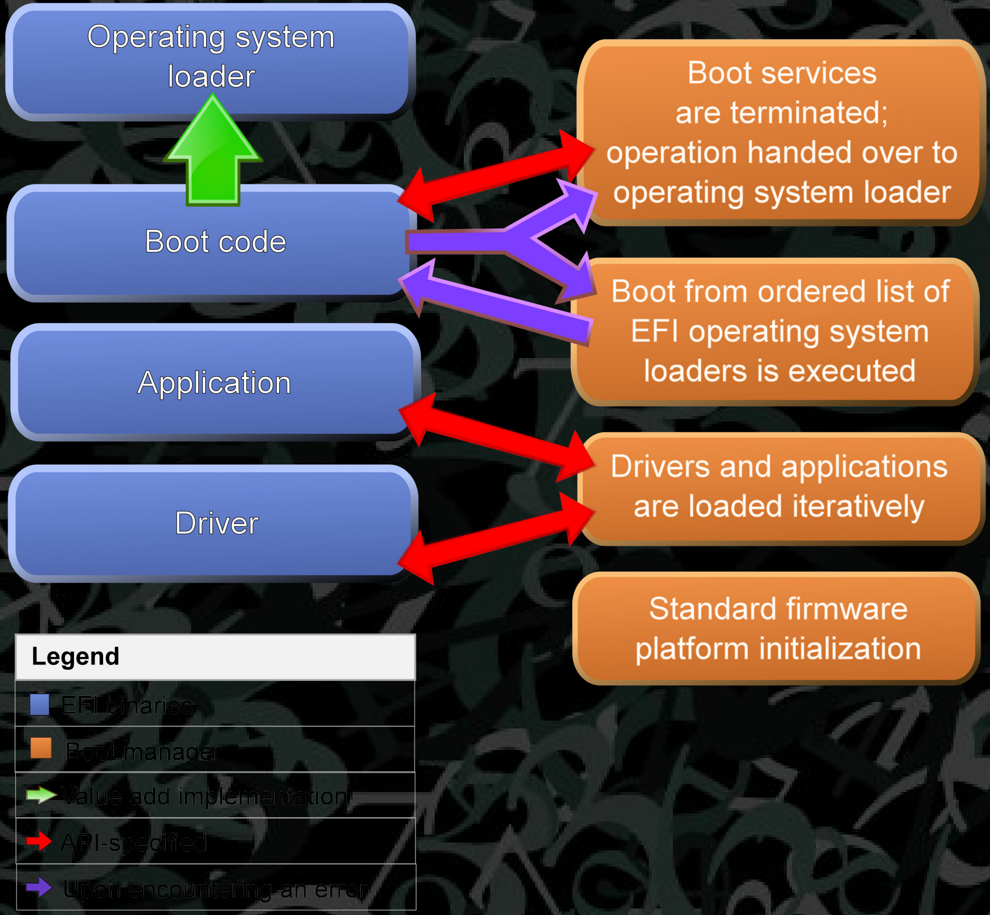
➡ Upon encountering an error

Table Of Contents

- What's UEFI?
- History of UEFI
- technical advantages over a traditional BIOS system
- Contents
- Some of Capabilities
- Windows 8 ,Monopoly and solutions

Some of Capabilities

- Processor compatibility
- Disk device compatibility
- Services
- Variable services
- Time services
- Protocols
- Device drivers
- Graphics features
- Booting
- Secure boot
- The EFI shell
- Extensions



Operating system loader

Boot code

Application

Driver

Boot services are terminated; operation handed over to operating system loader

Boot from ordered list of EFI operating system loaders is executed

Drivers and applications are loaded iteratively

Standard firmware platform initialization

Legend

- 🟦 EFI binaries
- 🟧 Boot manager
- → Value add implementation
- → API-specified
- → Upon encountering an error

Table Of Contents

- What's UEFI?
- History of UEFI
- technical advantages over a traditional BIOS system
- Contents
- Some of Capabilities
- Windows 8 ,Monopoly and solutions

Windows 8 ,Monopoly and solutions

- RedHat disclosed MS private key of win 8
- Ubuntu presented “shim” to load GRUB on UEFI systems, which will be used to boot an unsigned kernel.
- Fedora will also use “efilinux” as a shim, but will also sign the kernel and GRUB with the key, and will also maintain its own signing key.
- In October 2012, the Linux Foundation announced that it would be developing its own minimal UEFI bootloader signed with a Microsoft key that will serve as a shim to launch the main bootloader. However, to maintain security and prevent the bootloader from being used to silently load malware, it will require user input in order to boot.

Answer/Question