UEFI

Unified Extensible Firmware Interface

Hans Lunsing
(hans.lunsing@xs4all.nl)

14 april 2015

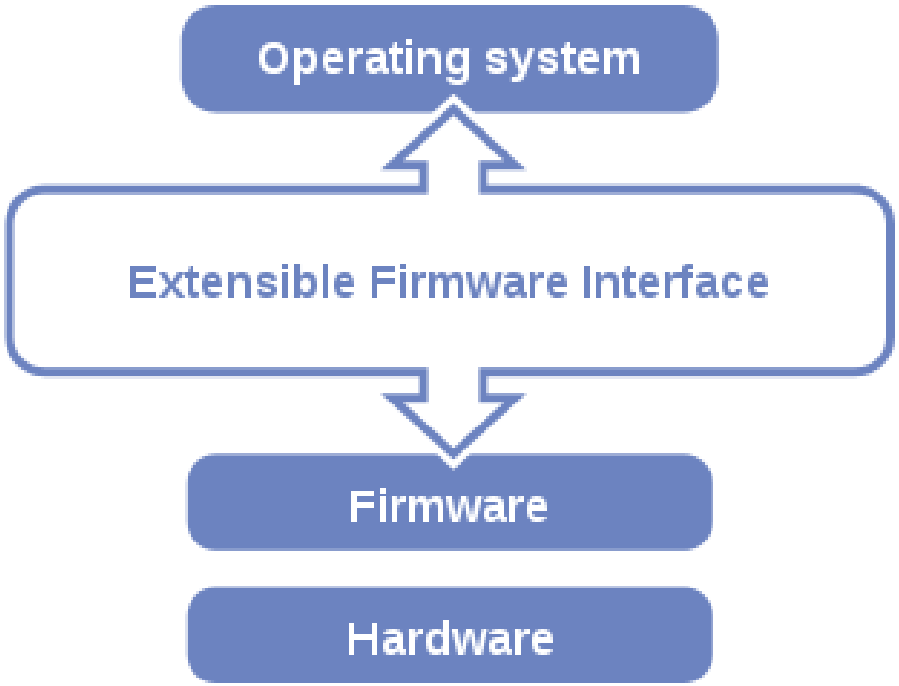
Wat is UEFI?

- Unified Extensible Firmware Interface:
  software interface tussen firmware en besturingssysteem
- Verzorgt ook het opstartproces
  en draagt dan de besturing over aan een besturingssysteem
- Kan eigen programma's draaien
  zoals een boot manager, een shell en een tekst editor
- Opvolger van het BIOS
  dat niet meer met moderne besturingssystemen kan communiceren
- Kan zich voordoen als een BIOS
  dank zij de CSM (Compatibility Support Module)
- Sinds komst Windows 8 in 2012 standaard
  daarvoor al toegepast sinds 2008 in BIOS vermomming

Wat is firmware?

- Software geïnstalleerd in niet-vluchtig geheugen
  PROM of EEPROM (Electrically Erasable Programmable Read-Only Memory)
- Initialiseert de hardware
  processor, geheugen, schijven etc. via de POST (Power-On Self Test)
- Geeft dan besturing over aan UEFI / OS lader
  die de firmware interfaces gebruikt voor initialisatie van OS

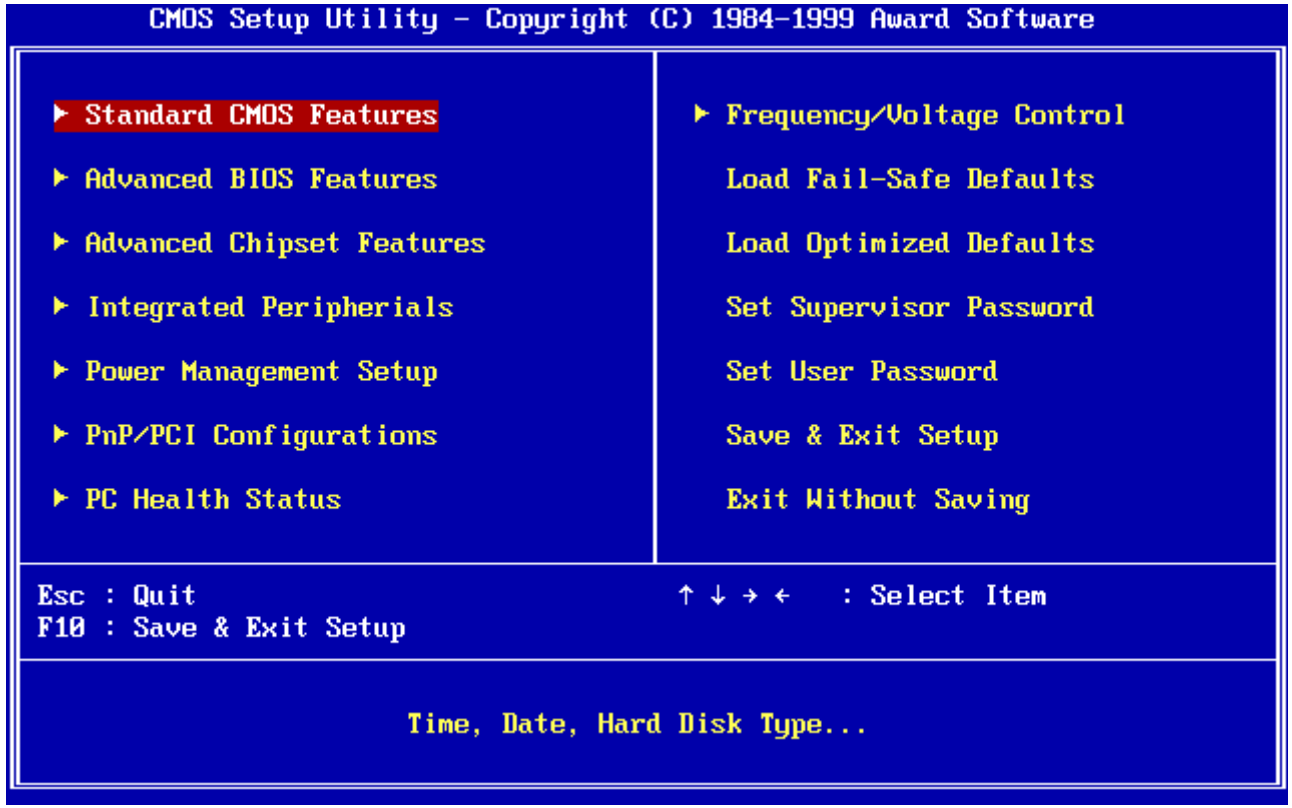
Positie van UEFI



Over het BIOS

- Basic Input/Output System
  dateert van 1981 in de IBM PC
- Start OS via MBR op schijf
  MBR is het Master Boot Record met de opstartcode
- Geeft OS toegang tot hardware via interrupts
  in 16-bit real mode, in 32+-bit OS'en in protected mode niet meer gebruikt, afgezien van ACPI etc.
- Toegang tot instellingen via toetsindruk bij start
  Esc, Del of een functietoets, leverancierafhankelijk

Award BIOS 1999



BIOS en schijfindeling

- MSDOS / MBR partitietabel
- Eerste record van 512B is het MBR
  bevat opstartcode van de bootloader en de partitietabel
- Maximum aantal partities is 4
  Meer passen er niet in de tabel. Dit zijn de primaire partities.
- Eén van de 4 partities kan *extended* zijn
  en tot maximaal 64 logische partities bevatten
- Maximum aantal bruikbare partities is dus 67

Nadelen van het BIOS

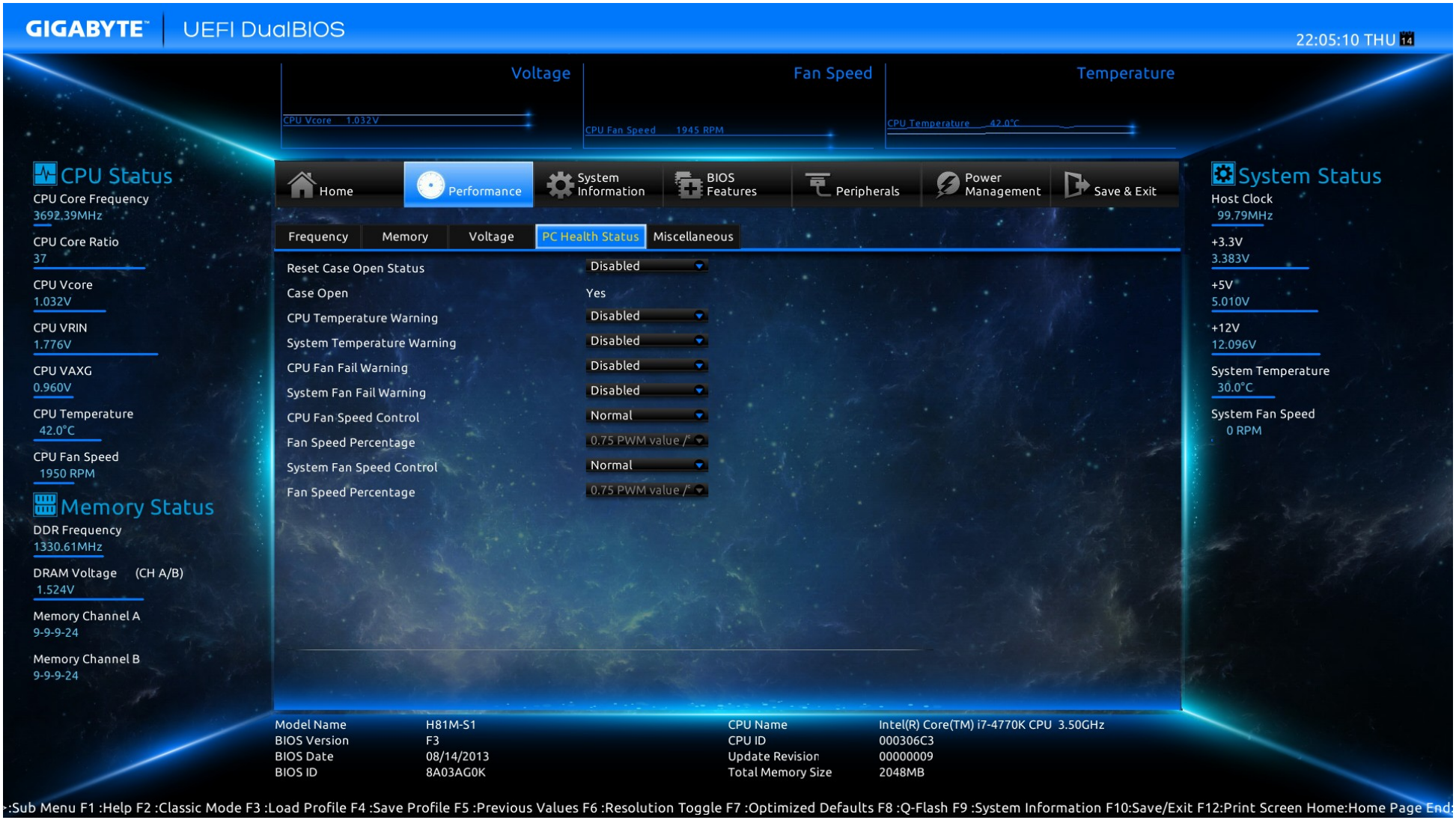
- 16-bit real mode
  Daarom hebben moderne OS'en eigen drivers voor toegang hardware
- Daarom ook maar 1 MB adresseerbaar geheugen
- Maximale grootte opstartschijf is 2,2 TB
- Per schijf maar 1 bootloader (in MBR)
- Ondersteunt alleen PC's
  dus geen tablets of smartphones
- Niet te beveiligen tegen malware, zoals rootkits
- Geen grafische interface mogelijk
- Is lappendeken door ad-hoc ontwikkeling
- Overal verspreide documentatie

En nu UEFI

- Dateert van 1998, als Intel Boot Initiative, later EFI
- In 2005 overgedragen aan UEFI Forum
  waarvan veel ICT bedrijven en organisaties lid zijn (Unified!)
- UEFI Forum zorgt voor verdere ontwikkeling
- Heeft een eigen Boot Manager
  die helaas niet door elke leverancier bereikbaar wordt gemaakt
- Start OS'en met bootloaders in speciale partitie
  de EFI System Partition (ESP)
- Biedt OS interface voor hardware en netwerk

  zodat OS kan volstaan met standaard drivers
- Toegang tot UEFI op verschillende manieren
  toetsindruk bij start, aparte knop (laptops!), vanuit Windows 8 bootmenu

GIGABYTE UEFI DualBIOS



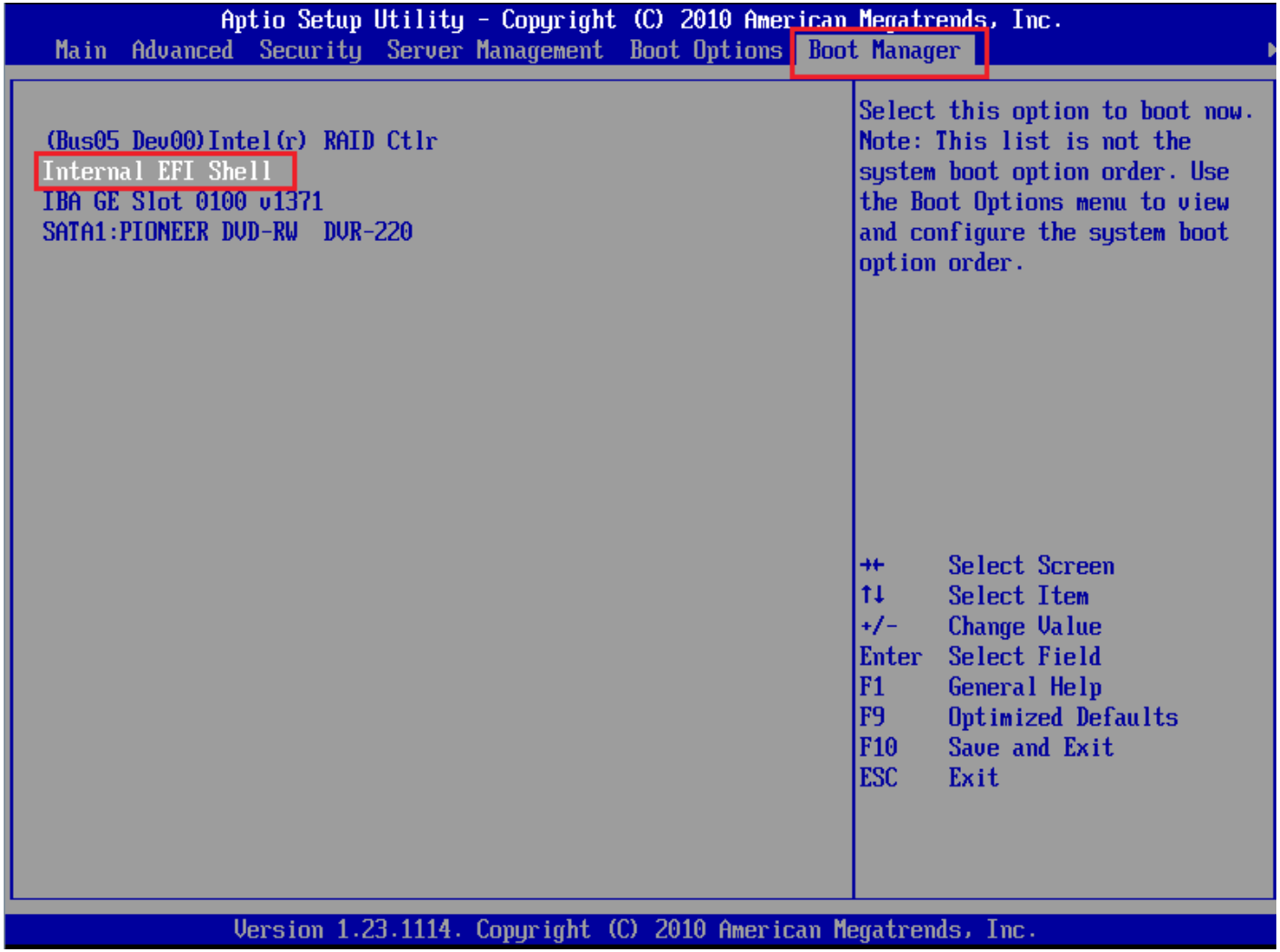
Voordelen van UEFI

- Ondersteunt 64-bit processor modus
- 17,2 miljard GB adresseerbaar geheugen
- Maximale grootte van opstartschijf is 9,4 miljard TB
  dat is meer dan wat er nu op aarde aan opslagruimte is
- Meerdere bootloaders per schijf mogelijk (in ESP)
- Platform onafhankelijk
  dus ook voor Apple Mac's, tablets en smartphones
- Bescherming tegen malware met Secure Boot
- Grafische interface mogelijk
- Ontwikkeling gestuurd door UEFI Forum
- UEFI Forum verzorgt ook goede documentatie

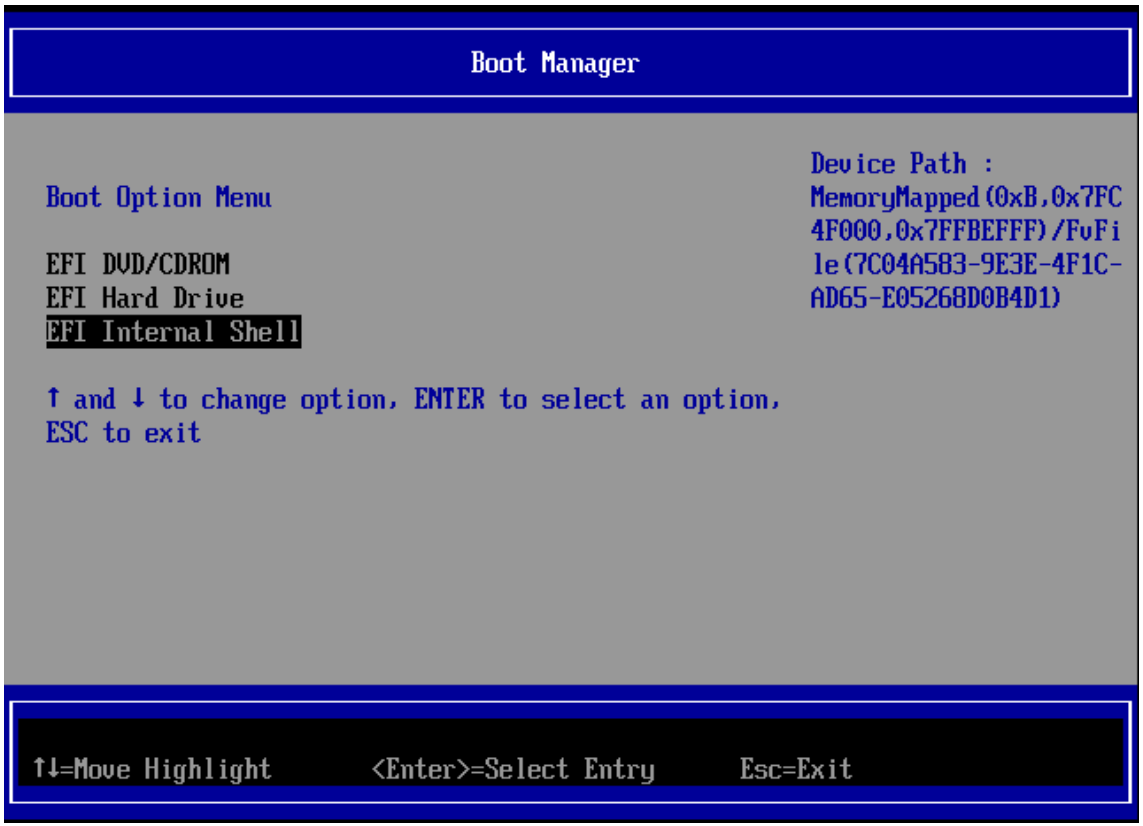
Elementen van UEFI

- De EFI Systeem Partitie (ESP)
  met bestanden voor het starten van OS'en
- De EFI Shell
  command line interface voor booten, instellingen, informatie, etc.
- De GUID Partitie Tabel (GPT)
  die maximaal 128 partities kan herbergen
  UEFI kan ook nog overweg met oude MSDOS partitie tabel (CSM?)
- De Compatibility Support Module (CSM)
  die UEFI kan laten werken als een BIOS
- Secure Boot
  een protocol voor bescherming tegen malware en rootkits
- UEFI variabelen die aspecten van UEFI bepalen
  met speciale software door gebruiker zelfs vanuit OS aan te passen

UEFI Boot Manager van AMI



UEFI Boot Manager van VirtualBox



EFI Systeem Partitie

- In plaats van het MBR
- Bij voorkeur de eerste niet verborgen partitie
- VFAT bestandssysteem
  FAT32, maar FAT16 of FAT12 op verwisselbare media
- Grootte minimaal 100 MB
  met sectoren van 512 B, maar 260 MB met sectoren van 4096 B
- Type GUID is C12A7328-F81F-11D2-BA4B-00A0C93EC93B
- Type ID in MSDOS partitietabel is 0xEF
- Bevat bestanden nodig voor opstart systeem

Bestanden op ESP

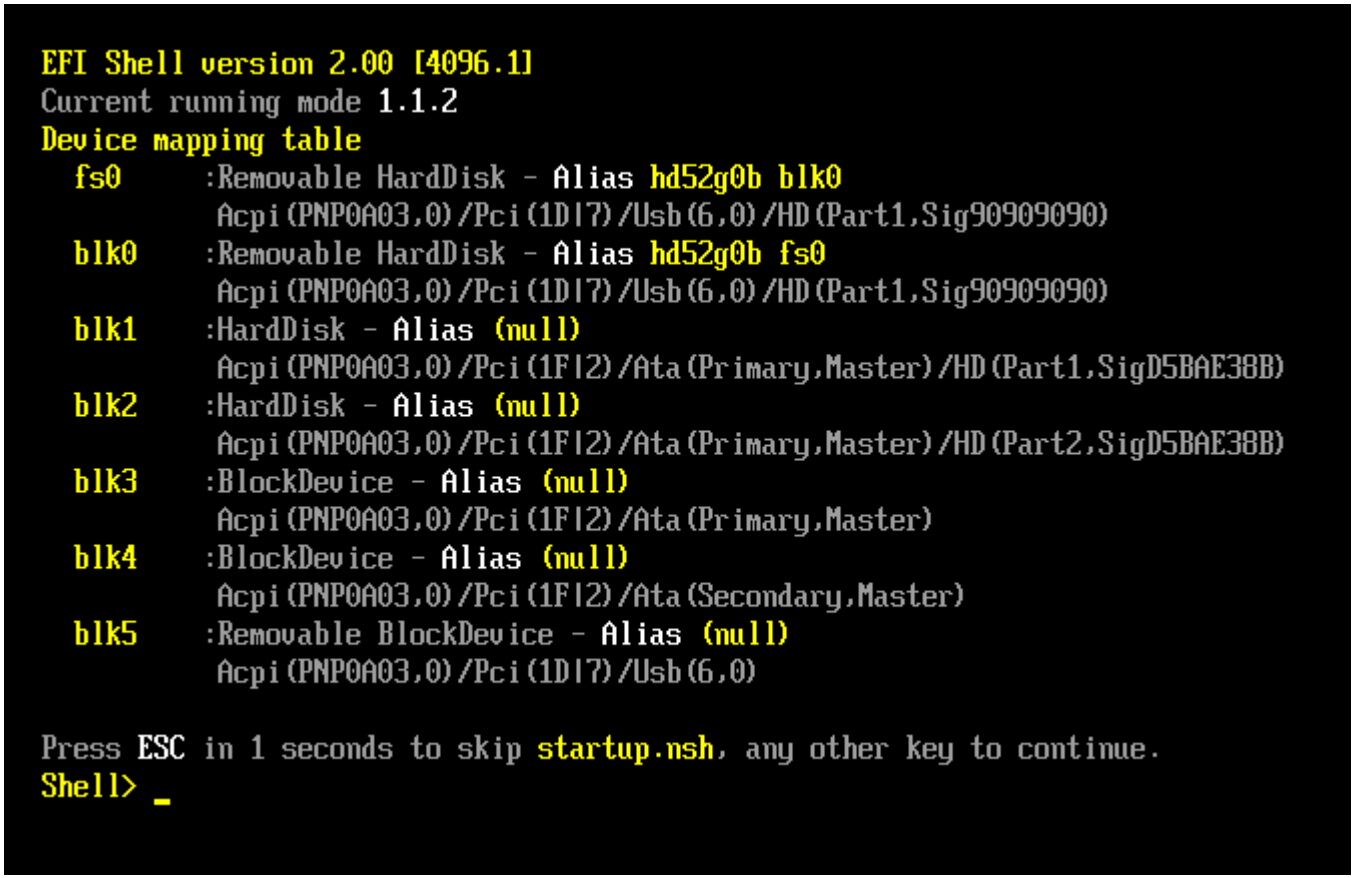
- Bootloaders voor geïnstalleerde OS'en
  in leverancier specifieke submappen in map \EFI
- Default bootloader
  genaamd BOOTX64.EFI in map \EFI\BOOT
- Drivers voor bij booten gebruikte apparaten
- Systeemtools die voor start OS worden gedraaid
- Gegevensbestanden
  zoals configuratiebestanden en foutenlogs

EFI Shell

- Command line interface voor UEFI programma's
- Te bereiken via
  - Optie in firmware instellingen, of
  - UEFI Boot Manager (VirtualBox!), of
  - Speciale toets bij opstart, of
  - Helemaal niet!
- Ingebouwde tools voor
  - opvragen van informatie over systeem of firmware
  - aanpassen configuratie boot manager
  - partitionering van schijven
  - laden van efi drivers
  - bewerken van tekstbestanden, etc.
- Uitvoeren externe UEFI programma's

  in het bijzonder bootloaders van besturingssystemen of boot managers

EFI Shell van VirtualBox



GUID Partition Table (GPT)

- GUID = Globally Unique Identifier
  pseudo willekeurige code van 16 bytes
- Elke schijf heeft 1 GUID: identificatie
- Elke partitie heeft 2 GUID's: type en identificatie
- Protective MBR in eerste sector
  Protective: partitietabel toont 1 grote partitie met voor oudere software onbekend type 0xEE
- Ondersteunt BIOS boot
  met bootloader in PMBR en 2e-fase opstartcode in BIOS Boot Partition
- Partitietabel in 33 sectoren na PMBR
  voor maximaal 128 partities
- Backup van partitietabel aan het eind van de schijf

Voordelen van de GPT

- Veel meer partities (128) mogelijk
  zonder onderscheid naar primair, extended en logisch
- Maximum grootte van schijf 9,4 miljard TB
  bij sectoren van 512 B. Na transitie naar 4096 B zelfs 75,2 miljard TB
- Unieke identificatie van schijven en partities
  met GUID's
- Bedrijfszekerder dank zij backup van partitietabel
- Verifiëert integriteit met CRC32 check

Compatibility Support Module (CSM)

- Hiermee gedraagt UEFI zich als BIOS
  met opstarten via het MBR
- Nodig voor OS'en die UEFI nog niet ondersteunden
- Was aanvankelijk vaak standaard ingeschakeld
  van begin toepassing UEFI in 2006 tot in 2012 (komst Windows 8)
- Zal in de toekomst verdwijnen
- Vaak voor specifieke schijven in- of uit te schakelen

Secure Boot

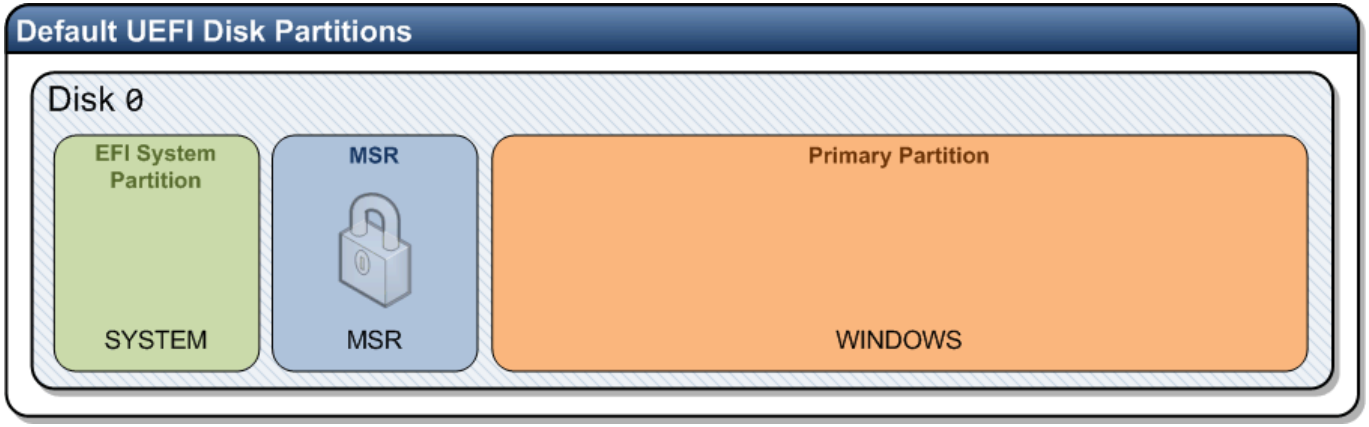
- Protocol voor ondersteuning en afdwingen van cryptografische verificatie van OS laders en drivers
- Zo kan rootkits e.a. malware de pas worden afgesneden
- Maakt sinds november 2010 deel uit van de UEFI-specificatie.
- Voor certificatie van PC's voor Windows 8 en hoger is UEFI met Secure Boot nodig
- Wordt in principe ook de Linux ondersteund
  zij het dat er nog wel eens problemen optreden
- Komt een volgende keer aan de orde....

OS'en met ondersteuning UEFI

- Windows op PC's vanaf Vista SP1, alleen 64-bit
  Alleen UEFI met GPT.
  Vóór Windows 8 toch meestal UEFI met CSM of BIOS.
- Apple vanaf OS X 10.4 (Tiger)
  Alleen op Intel PC's. Eigen implementatie.
- Linux vanaf begin 2000 met boot manager elilo
  vanaf 2008 ook met boot manager Grub
  en vanaf versie 3.3 (maart 2012) ook rechtstreeks te booten.

Windows 8(en nieuwer) en UEFI

- Typische schijfindeling



- Ondersteunt geen UEFI boot van MBR schijf
- Hoe geboot?
  Systeembeheer → Systeeminformatie → BIOS mode: UEFI of legacy
- Drive letter voor ESP: mountvol <driveletter>: /s
  Alleen als Administrator. Ook in Windows 7.
- Toegang tot UEFI instellingen:
  Net zoals bij BIOS: toets bij opstarten. Vanuit Windows 8 vaak ook: Shift toets ingedrukt houden bij klikken op Opnieuw opstarten

Linux en UEFI

- Maakt ESP als 1e partitie als hij er nog geen ESP is
- ESP wordt gekoppeld aan `/boot/efi`
  voor ieder zichtbaar, maar kan alleen door root worden aangepast
- Runtime informatie van kernel in `/sys/firmware/efi`
  EFI variabelen in `/sys/firmware/efi/vars` en ook dank zij module 'efivarfs'
  in `/sys/firmware/efi/efivars`. Deze laatste geraadpleegd door Grub installer.
- Programma '`efibootmgr`' voor bekijken en aanpassen instellingen UEFI Boot Manager
  Hierbij wordt module 'efivarfs' gebruikt.
- Grub + Linux ondersteunen BIOS boot van GPT schijf
  Voor de 2e-fase opstartcode van Grub is dan een BIOS Boot Partition nodig.

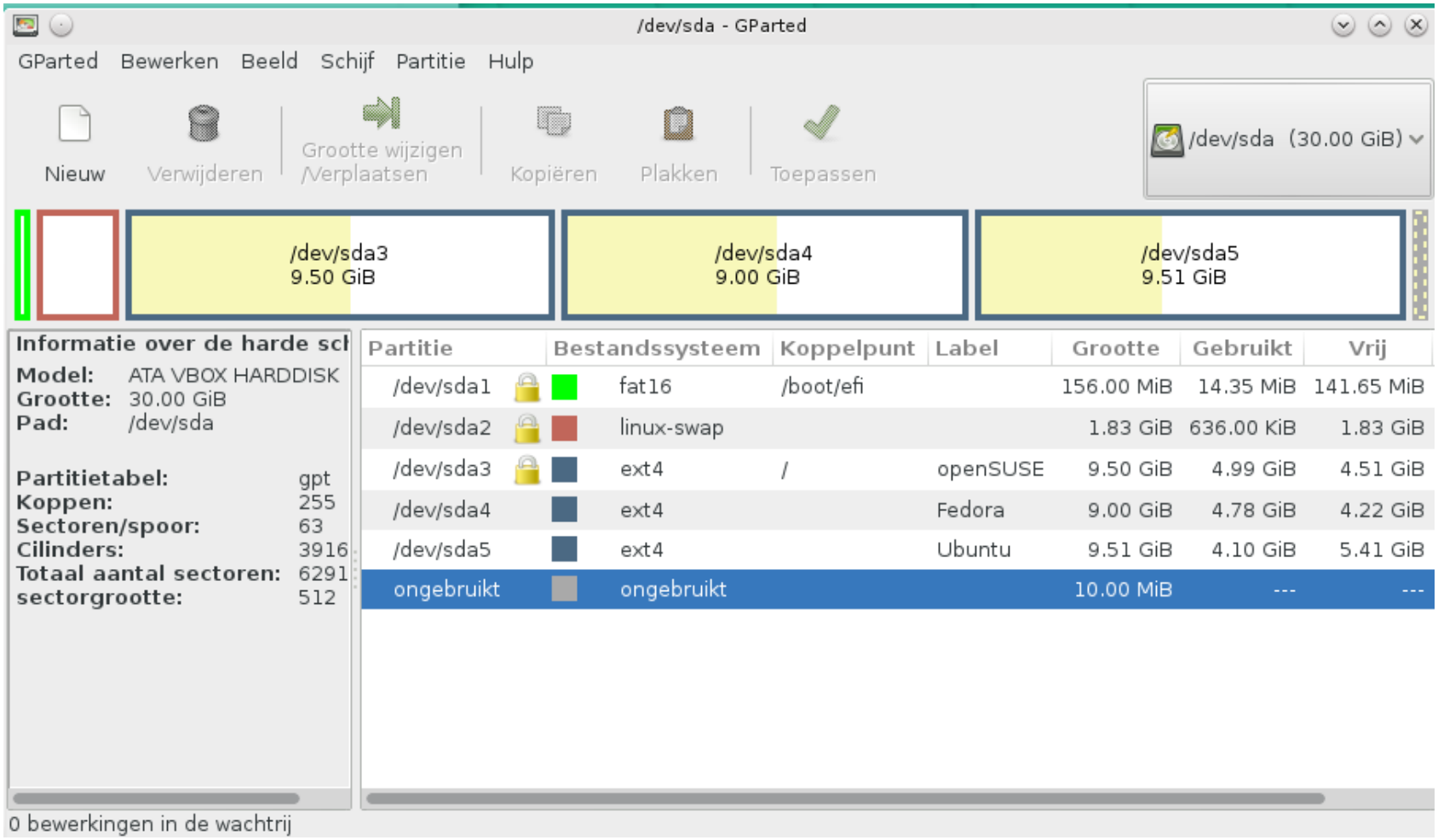
BIOS Boot Partition

- Is nodig voor BIOS boot van GPT schijf
- Bevat 2e-fase opstartcode van bootloader
  en heeft geen bestandssysteem
- Kan vrij klein zijn: minimaal ca 31KB, liever 1MB
- Type GUID is 21686148-6449-6E6F-744E-656564454649
  in vertaling als ASCII codes “!haH-dI-no-tN-eedEFI, en met omgekeerde volgorde eerste 3 delen (little endian): “Hah!-Id-on-tNeedEFI”

Linux progs voor bewerken GPT

- 'Parted' en zijn grafische evenknie 'gparted' kunnen goed met GPT schijven overweg
- Command-line progs 'fdisk', 'cfdisk' en 'sfdisk' soms wel, soms niet: hangt af van distributie
- Alternatieven 'gdisk', 'cgdisk' en 'sgdisk' specifiek voor GPT schijven
  Zelfs conversie van MBR naar GPT mogelijk, zij het met verlies data.

gparted


/dev/sda - GParted
GParted Bewerken Beeld Schijf Partitie Hulp
Nieuw
Verwijderen
Grootte wijzigen /Verplaatsen
Kopiëren
Plakken
Toepassen
/dev/sda (30.00 GiB)
/dev/sda3 9.50 GiB
/dev/sda4 9.00 GiB
/dev/sda5 9.51 GiB
Informatie over de harde sch
Model: ATA VBOX HARDDISK
Grootte: 30.00 GiB
Pad: /dev/sda
Partitietabel: gpt
Koppen: 255
Sectoren/spoor: 63
Cilinders: 3916
Totaal aantal sectoren: 6291
sectorgrootte: 512
Partitie Bestandssysteem Koppelpunt Label Grootte Gebruikt Vrij
/dev/sda1 fat16 /boot/efi 156.00 MiB 14.35 MiB 141.65 MiB
/dev/sda2 linux-swap 1.83 GiB 636.00 KiB 1.83 GiB
/dev/sda3 ext4 / openSUSE 9.50 GiB 4.99 GiB 4.51 GiB
/dev/sda4 ext4 Fedora 9.00 GiB 4.78 GiB 4.22 GiB
/dev/sda5 ext4 Ubuntu 9.51 GiB 4.10 GiB 5.41 GiB
ongebruikt ongebruikt 10.00 MiB --- ---
0 bewerkingen in de wachtrij

VirtualBox

- Biedt virtuele PC voor installatie OS'en
- Ondersteunt UEFI zonder Secure Boot
  Experimenteel. Alleen Linux en OS X als gastsystemen.
- Heeft eigen Boot Manager en Boot Maintenance Manager
  Via Boot Manager toegang tot de EFI Shell
- Aardige manier om vertrouwd te raken met UEFI
  ook al heb je zelf geen UEFI computer

Boot Managers voor UEFI

- rEFInd

  URL: www.rodsbooks.com/refind. Grafisch of tekstmodus.
  Automatische standaardconfiguratie, maar geheel aanpasbaar.
  Heeft drivers voor Linux bestandsystemen.

Boot Managers voor UEFI

- gummiboot
  URL: freedesktop.org/wiki/Software/gummiboot. Alleen tekstmodus.

Meer informatie

- http://www.uefi.org/
  Officiële website van het UEFI Forum
- http://www.rodsbooks.com/linux-uefi/
  Introductie in UEFI voor Linux gebruikers
- http://www.rodsbooks.com/efi-bootloaders/
  Over EFI boot methoden, EFI bootloaders en Secure Boot
- https://www.happyassassin.net/2014/01/25/uefi-boot-how-does-that-actually-work-then/
  Hoe werkt UEFI boot?
- http://en.wikipedia.org/wiki/UEFI
  Encyclopedische informatie over UEFI

UEFI

Unified Extensible Firmware Interface

Dank voor uw aandacht!