Firmware

(U)EFI vs BIOS

Inhoud #1

- Hoe
- Wie / Wat / Waar / Waarom / Wanneer
- Legacy – BIOS
  - Concepten
  - Voordelen / nadelen

- (U)EFI
  - Concepten
  - Versies
  - Boot proces
  - CSM

Inhoud #2

- (PKI)
- Secure boot
  - (On)mogelijkheden
- Measured boot
- Tools
  - Ingebouwd
  - 3rd party
- Meer weten

UEFI – Hoe (komt iemand ertoe UEFI uit te pluizen)

- HP Pavilion X2 Windows 8.1 x64 hybride tablet
  - UEFI boot, secure boot uit
  - Boot opties toegankelijk
  - Poging #1: boot live linux usb boot
  - Fail #1..42: Boot medium niet geschikt
  - Poging #2: ...documentatie lezen...
  - *Aha* moment: CPU is AMD64 maar de UEFI is IA32
  - Poging #2: prepareer 32bit UEFI bootloader
  - Succes!
  - Maar wat was er eigenlijk aan de hand...?!?

UEFI – Hoe #2

- Geklungel met USB booten toonde aan dat kennis UEFI beperkt was.
- (symptoom: bij boot / installatie problemen is eerste actie de bootmethode naar ‘legacy’ (a.k.a. BIOS/MBR) probeen om te zetten)
- Opzet #1: Workshop: boot via UEFI en maak een kloon
  - Voordeel: aandacht
  - Nadeel: Risico van ‘volg de stapjes’
- Opzet #2: Theorie eerst
  - Voordeel: Big picture
  - Nadeel: Niet concreet / relevant / ...
  - Nadeel: Workshop niet heel nuttig
- Beslissing: Opzet #2

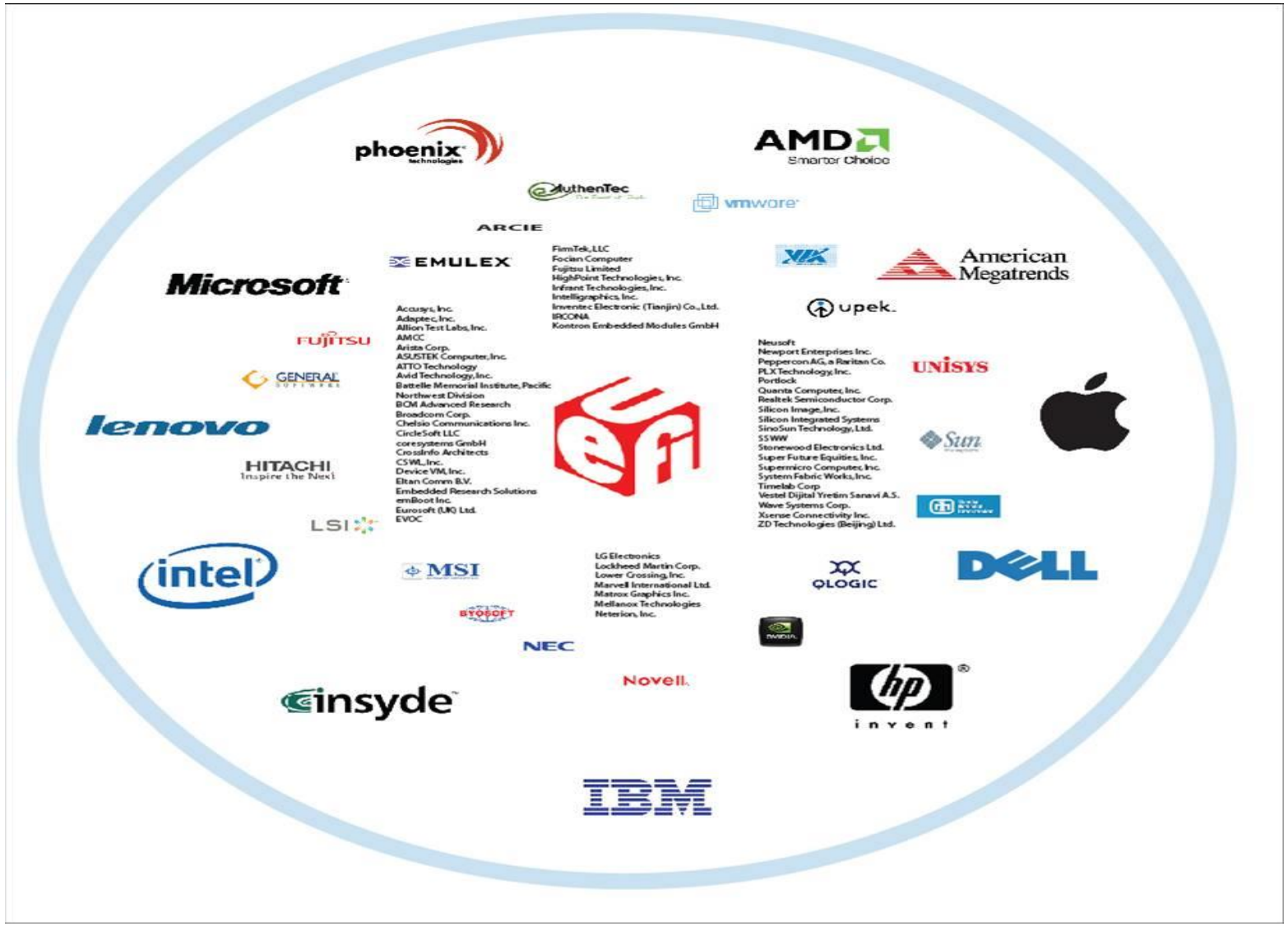
UEFI vogelvlucht

miep miep

UEFI – Wat (is het) #1

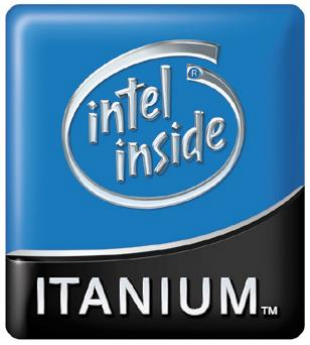
- Unified Extensible Firmware Interface
- Raakvlakken / verweven met:
  - Platform Initialization - P.I.
  - Secure Boot*
  - ACPI
- Firmware i.s.m. software
  - Computer veranderen van blok ijzer naar dure calculator
  - ‘Bootstrap’: breng computer in staat waarin booten OS mogelijk is
  - Hulp programma’s tbv beheer en recovery
- Interface specificatie, geen implementatie ontwerp
  - Het ‘wat’ ligt vast, het ‘hoe’ is aan de OEM / IHV
- In beheer bij UEFI forum

UEFI – Wat (is het) #2



UEFI – Waar (zit het in) #1

- Desktops / servers
  - Inmiddels ook ARM (AARCH32/64)
- Mobile
  - Windows Mobile 8/10
  - (Android: android x86)
- Niet:
  - o.a. Apple Iphone / Android (ARM)
  - Oudere PC hardware (soms buggy ondersteuning)



UEFI – Waar (zit het in) #2

- Maar ook (steeds meer):

- Want (o.a.):

JUNOS®

insyde H2O® BIOS

UEFI – Wie (heeft ermee te maken)

- OEM’s
- IHV’s / IFV’s
  - Hardware addons (PCI, USB, TB, ...)
- ISV’s / OSV’s
  - Anti-malware, recovery, diagnostics, DRM, ...
- Eind gebruikers
  - (on)mogelijkheden controle / beheer hardware
- Onderzoekers digitaal
  - Niet-destructief onderzoek aan niet-verwijderbare media
  - Ook: disk encryptie gekoppeld aan hardware (TPM, ...)

UEFI – Waarom (moet dit er zo nodig komen)

- BIOS is er sinds 1983 (oorsprong in CP/M)
  - ‘organisch gegroeid’
    - aka bij elkaar gehacked t.b.v. nieuwe hardware
  - (4 partities, 2.2TB bootdisk limiet, integriteit controle afwezig)
- x86 georienteerd
- s/w ontwikkelen lastig
  - (16 bit real mode, 1MB addresseerbaar geheugen, assembler)
- UEFI heft beperkingen op:
  - Niet langer disk (MBR) gebaseerd
  - Multi-arch, multiboot eenvoudiger
- UEFI voert beperkingen in:
  - Secure Boot, measured boot, software / hardware white- / blacklist

UEFI – Wanneer (staat dit allemaal te gebeuren)

- 1995: 1e versie tbv Itanium arch (IA64, EFI: Intel / HP)
- 2005: UEFI forum opgericht, specs overgedragen
- 2009: ARM (AArch32)
- 2011: MS focus op secure / measured boot (Win8)
- 2013: ARM (AArch64)
- 2016: UEFI versie 2.6 final
- 2005 → ...
  - Universele H/W standaarden beheren binnen één organisatie
  - UEFI / PI / GPT / TPM / ACPI / PXE / ?SMM? / ... ?

BIOS refresher

met een snufje MBR

Boot proces BIOS

CPU in Real Mode

BIOS boot code

POST

Load Option ROMs

MBR

Boot loader

Kernel Init (early)

BIOS services

CPU in Protected Mode

Kernel Init (OS)

User Mode

Kernel services

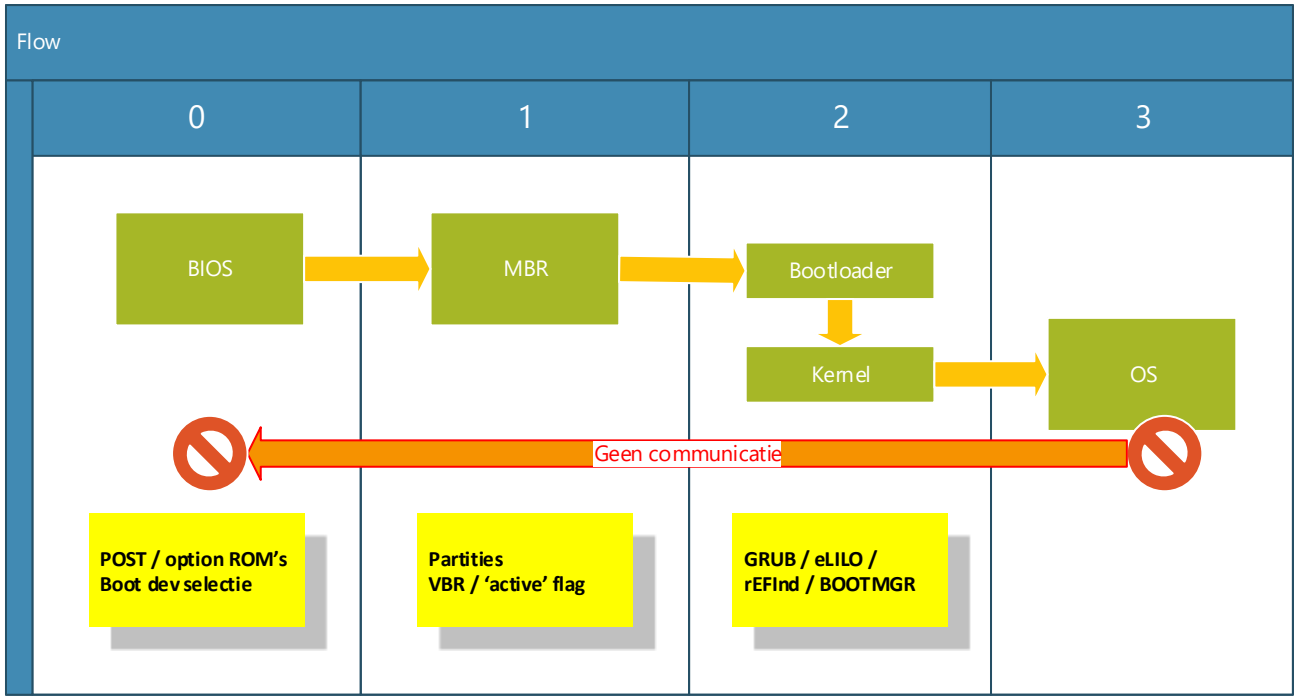
hardware

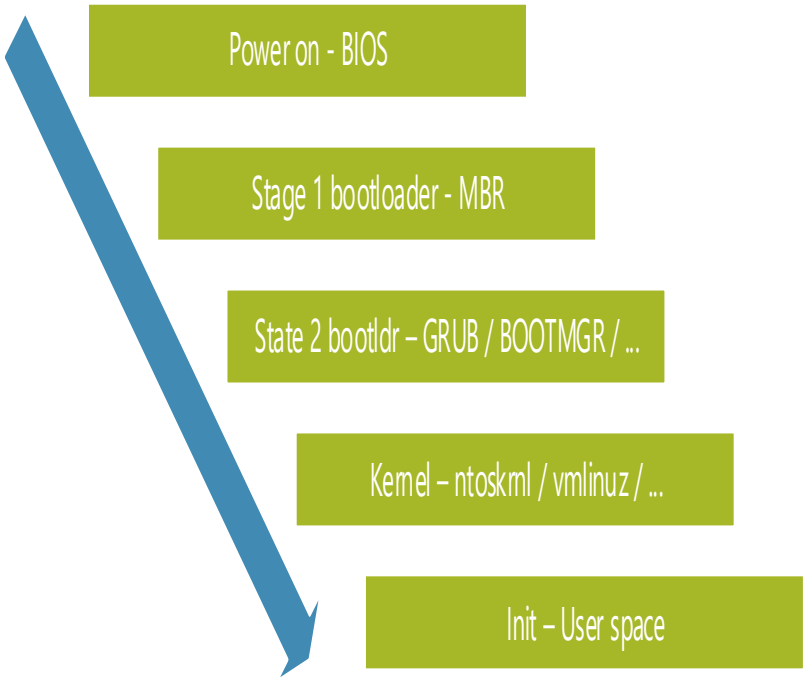
SMI

System Mamagement

CPU in SMM

F5 – BIOS i.s.m. MBR





F5 - BIOS i.s.m. MBR (bootloader)

- Bootstrap: CPU execs instructies in ROM / NVRAM (BIOS)
  - Reset vector (0xFFFFFFF0) wijst naar BIOS
  - JUMP naar initiële setup (POST)
    - Option ROMS's t.b.v. RAID / SAN / FDE...
  - Boot device sequence (check MBR boot sig 0xAA55)
  - JUMP naar boot code in MBR
  - ** Firmware is klaar en onzichtbaar **
  - Laden boot code, partitie tabel, VBR voor 'boot' flag

F5 - BIOS i.s.m. MBR (bootloader) # 2

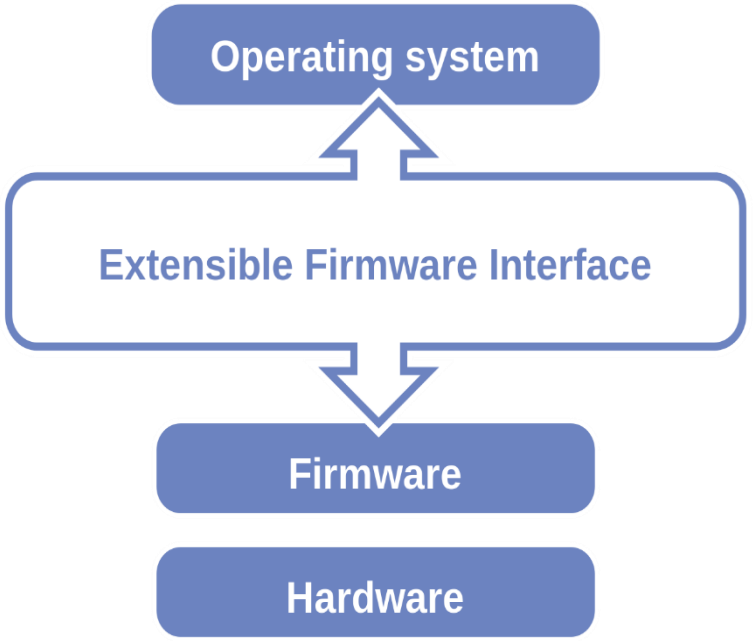
- bootloader:
  - 1st stage: van BIOS JMP in MBR bootloader
    - Max 446 bytes: <SOH><BOOTCODE><PART TABLE><DISK SIG>
  - 2nd stage bootloader:
    - GRUB, BOOTMGR, NTLDR, ...
  - Toevoegingen:
    - PXE boot (BOOTP) (inmiddels onderdeel van UEFI standaard)
- Eenrichtings verkeer
- Geen validatie / authenticatie / authorisatie (devices)
- Geen hulp uitgebreider dan POST resultaat

UEFI

En raakvlakken

UEFI (?)

- Unified Extensible Firmware Interface
- Opvolger van BIOS
- Eerste versies door Intel / HP (EFI)
- Overgedragen aan UEFI forum
  - http://uefi.org
  - AMD / Intel / Microsoft / Apple
  - Ook: Red Hat / Canonical / Google / ...



UEFI ← → BIOS

- Overeenkomsten:
  - Firmware
  - Initialisatie / bootstrap
- Verschillen
  - Boot methodes / boot medium detectie
  - Gebruik: BIOS afnemend, UEFI toenemend
  - Beschikbare hulpmiddelen (b.v. shell)
  - Beveiling
  - Toegang
  - GEEN specs (BIOS) vs 2706 pagina’s (UEFI 2.6)

UEFI terminologie

- UEFI: Unified Extensible Firmware Interface
- PI: Platform Initialization
- CSM: Compatibility Support Module
- ESP: EFI System Partition
- GPT: Guid Partitition Table
- NVRAM: Non-Volitile Random Access Memory
- Applications / Drivers / Services: Bluetooth, biometrics, python!

UEFI terminologie #2

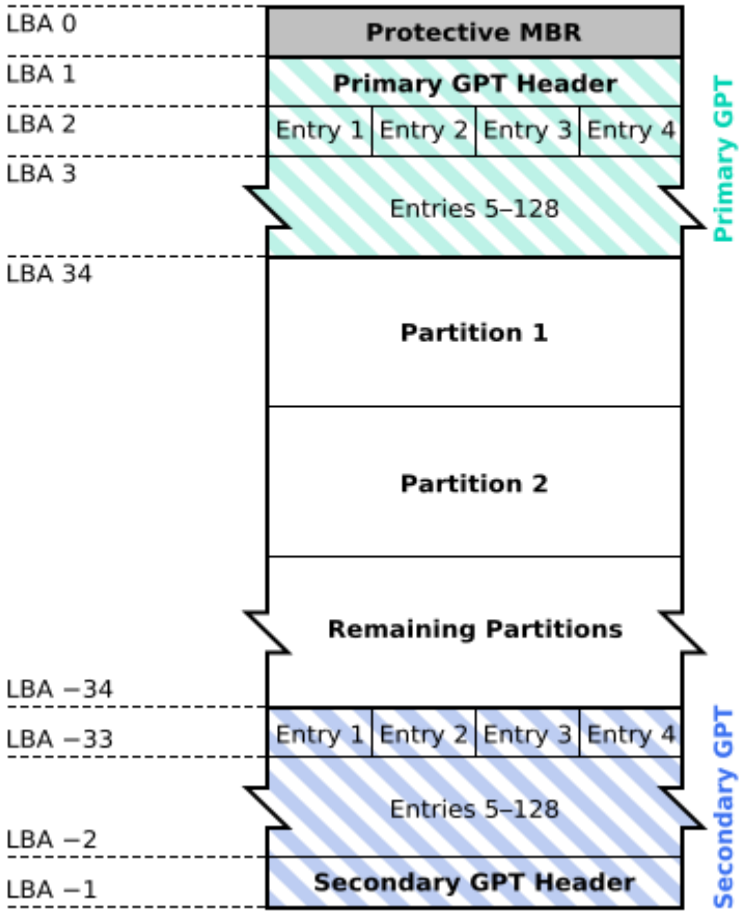
- PEI – Pre EFI Initialization
- DXE – Driver eXecution Environment
- BDS – Boot Device Select
- Secure Boot: Alleen ‘signed’ binaries / HW
- Measured Boot: Controleer binaries / aantonen integriteit

UEFI vereisten

- (Firmware ROM)
- GPT
- ESP
- EFI Image

Vereisten GPT

- GUID Partition Table
- vs MBR:
  - 32bit sector addressen: 2^32*512 bytes == 2TiB
  - Max 4 primaire parties
    - Wie roept ‘extended partities’?
- 64bit LBA: 2^64*512 == 8ZiB
  - Sector hoeft niet 512 bytes te zijn.
- GPT header bevat pointer naar partitie tabel
- Tabel heeft minimaal 16384 bytes beschikbaar



Vereisten ESP

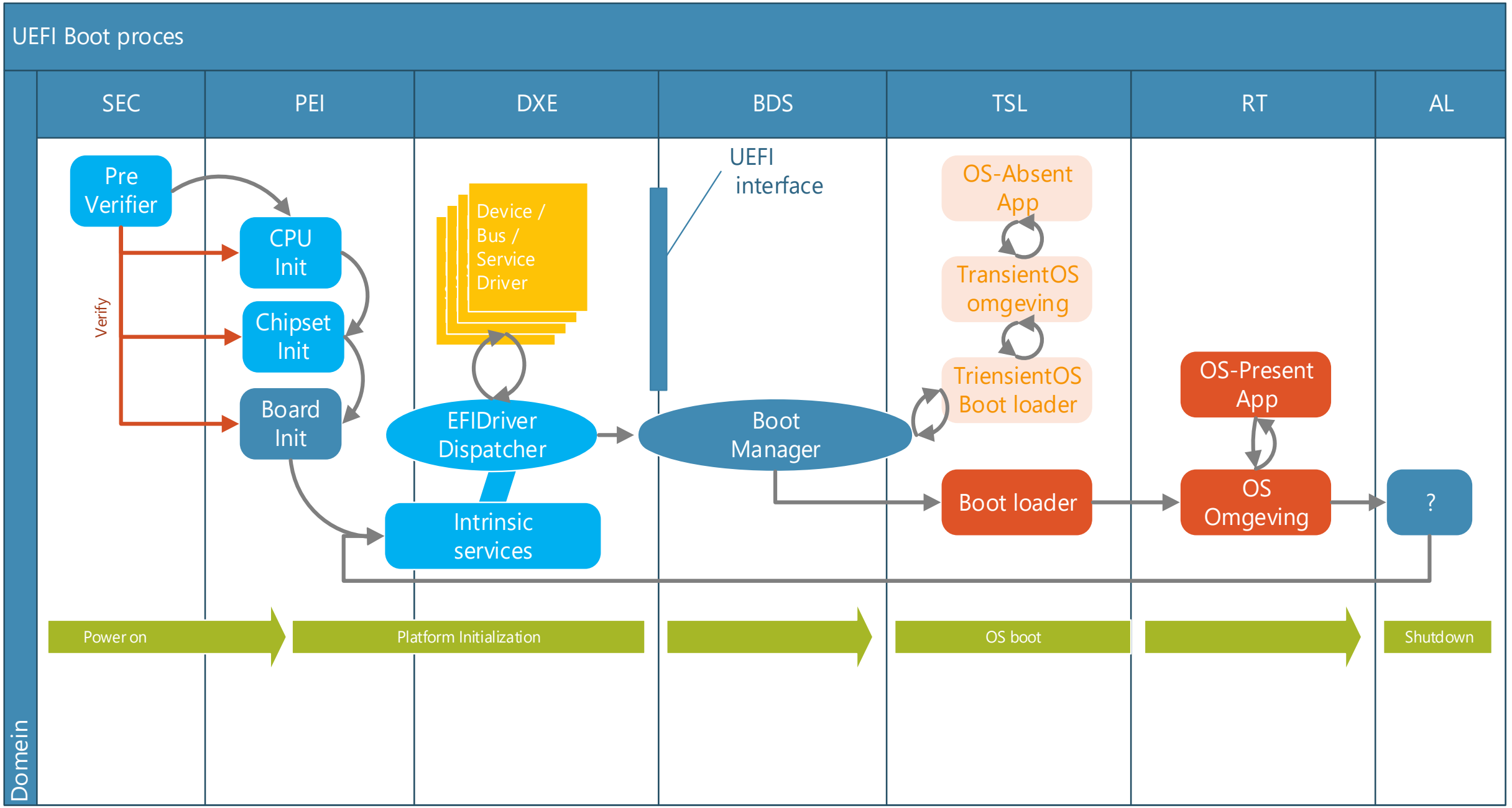
- EFI System Partition
- Geformaliseerde FAT32 spec (onafhankelijk van FAT spec
  - (...welke schijnbaar überhaupt niet bestaat...))
- GPT ID: {C12A7328-F81F-11D2-BA4B-00A0C93EC93B}
- MBR ID: 0xEF
- 1e sector bevat compatibiliteit code (legacy boot sector)

Vereisten EFI image

- PE format
  - (PE/COFF)
  - Portable Executable, Windows standaard sinds NT 3.1
- OS Loader
  - GRUB, rEFInd, Bootmanager, systemd-boot (Gummiboot)
- Maar ook
  - Shell, diagnostics, authenticatie app, linux kernel
    - CONFIG_EFI_STUB && CONFIG_CMDLINE_BOOL && CONFIG_CMDLINE
    - (http://www.rodsbooks.com/efi-bootloaders/efistub.html)

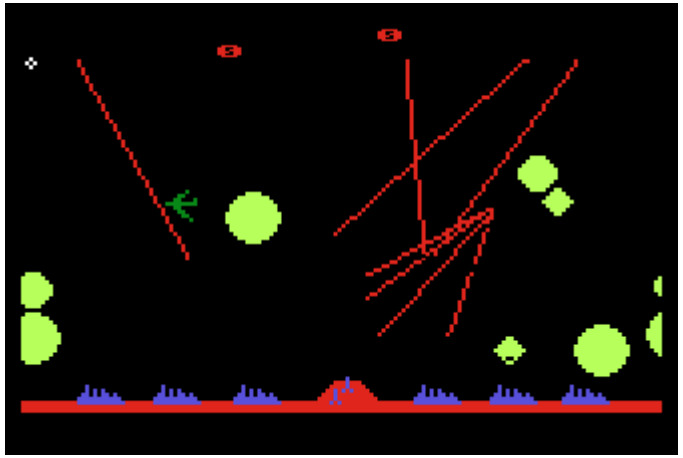
UEFI proces

ach so


UEFI Boot proces
SEC
PEI
DXE
BDS
TSL
RT
AL
Pre Verifier
Verify
CPU Init
Chipset Init
Board Init
Device / Bus / Service Driver
EFIDriver Dispatcher
Intrinsic services
UEFI interface
Boot Manager
OS-Absent App
TransientOS omgeving
TriensientOS Boot loader
Boot loader
OS-Present App
OS Omgeving
?
Power on
Platform Initialization
OS boot
Shutdown
Domein

UEFI boot – SEC

- Verantwoordelijkheden:
  - CPU caches flushed / initialized
  - Toepassen microcode patches
  - Init data store in CPU cache
  - Root of trust
  - Handover naar PEI



UEFI boot – PEI

- Verantwoordlijkheden:
  - Laden data van ROM
  - Init CRTM (Root of Trust Measurement, t.b.v. measured boot)
  - Laden platform afhankelijke modules
  - Init CPU’s / moederbord / on-board interfaces / RAM
  - Handover naar DXE
  - ACPI S3 resume (S3: suspend to RAM, a.k.a. standby)
- Grondslag
  - Minimale wat nodig is om volgende stap te zetten (DXE)
  - Gebruikt (initieel) alleen on-cpu resources zoals caches
  - Mogelijkheden architectuur afhankelijk

UEFI boot – DXE

- Verantwoordelijkheden:
  - Uitvoeren drivers
    - Afhankelijk van wat de PEI fase heeft klaargezet
    - CPU / chipset,
    - Software interface naar console, boot devices
  - I/O bus
  - Laden option-ROM / drivers van HBA kaarten
  - Boot services – opgeruimd in TSL fase
  - Runtime services – blijven beschikbaar in RT fase

UEFI boot – BDS

- Uitgevoerd nadat alle drivers in DXE actief zijn
- Verantwoordelijkheden:
  - Boot policy
  - Uitvoeren boot selectie

UEFI boot – BDS EFI image selectie

- Default vastgelegd
- Niet aanwezig dan auto boot ESP:
  - Zoek een ESP partitie
  - Binnen ESP zoek naar:
    - /BOOT/BOOT<MACHINE TYPE>.EFI
    - ‘BOOT/BOOTX64.EFI’ voor x86 boot of
    - ‘bootaa64.efi’ voor ARM64

UEFI boot – TSL

- Transient System Load
- Platform is gereed voor laden OS
- Opties
  - OS laden (de OS loader is een EFI applicatie)
  - Shell
  - …

UEFI boot – RT

- OS is geladen, boot services niet meer beschikbaar
  - ExitBootServices() aangeroepen
- Mogelijkheden:
  - Remote Attestation
    - Rapportage systeem state naar verificatie server (RTM waardes)
    - DRM: is het platform te vertrouwen
  - Toegang UEFI parameters
    - GetVariable() / SetVariable() / …
    - b.v. t.b.v. boot image selectie
    - update firmware componenten
- Systeem is klaar voor serieus gebruik

UEFI boot – RT User mode getting things done…

Options

DigitalVolcano
Fake Progress Bar

Version 1.1 - Freeware

©2006 DV. Thanks to GH for original idea.

Change Messages:

Title:
Tearing System Apart...

Status:	Delay:
Reading Files...	50
Linking Data...	23
Updating...	34
Reticulating Splines...	10
	12

Button Text:
Cancel

Appearance:

- [x] Dual progress bars
- [ ] Disable Screen Saver

Icon: Arrow

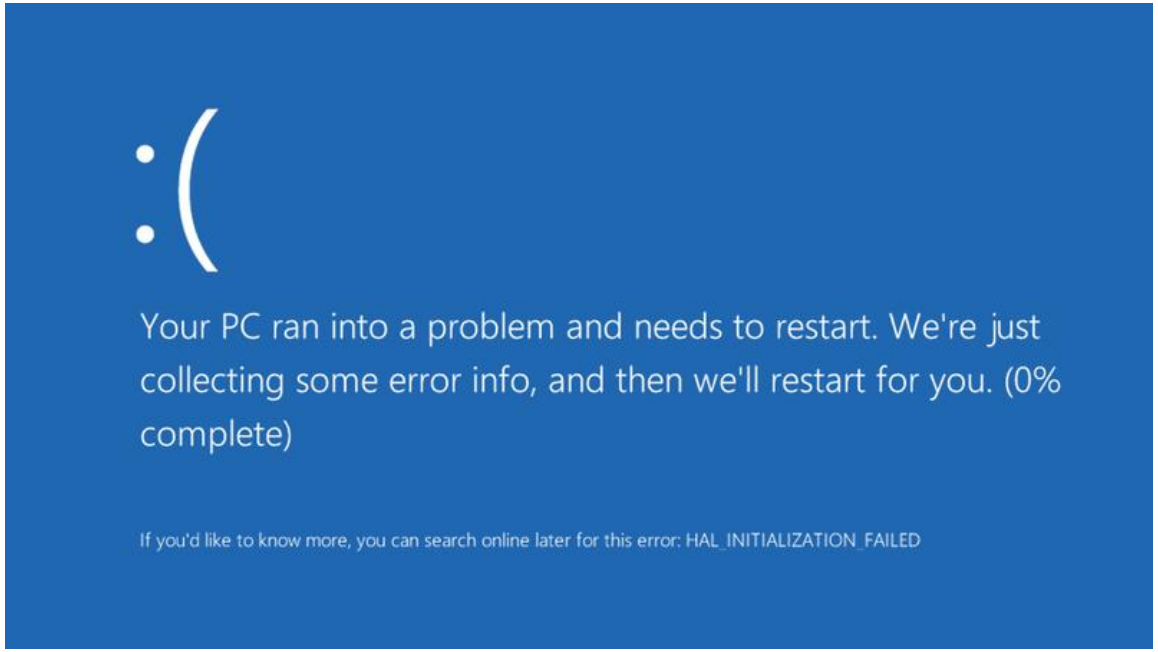
Custom Icon (32x32)

More Free Stuff - Visit Website

Apply OK

UEFI boot – AL

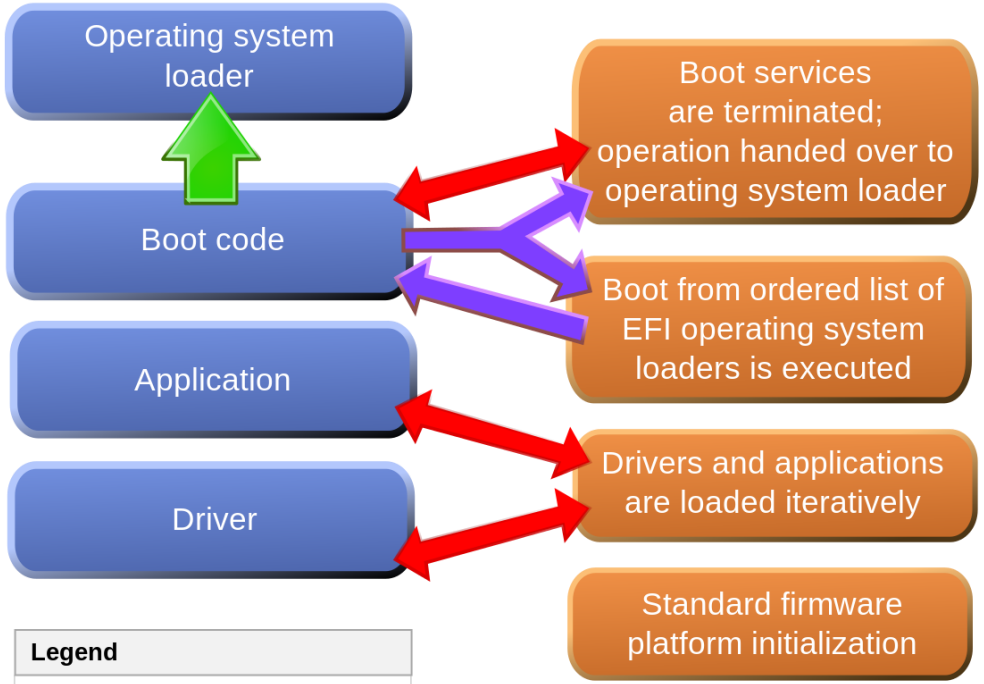
- AfterLife
- ACPI S3 / S4 / S5 state
- Crash handler
- Cleanup



UEFI boot - CSM

- Compatibility Support Module
- i.s.m. GPT protective MBR
- Mogelijk om ondanks UEFI systeem toch MBR stijl te booten
- BIOS is uit consensus gegroeid, CSM wildgroei nog meer
  1. voeg wat functionaliteit toe
  2. geef fancy naam, push in de markt
  3. ???
  4. profit
- Geen Secure Boot met actieve CSM!

UEFI - componenten



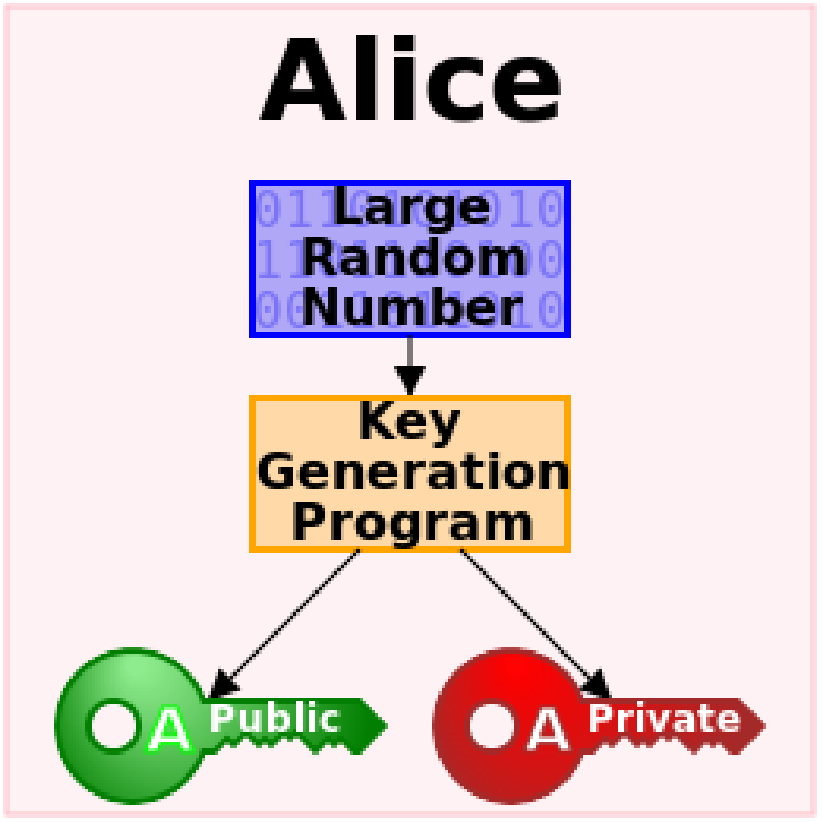
UEFI – classificaties

- Klasse 0
  - Geen UEFI
- Klasse 1
  - UEFI exclusief draaiend in CSM (UEFI onzichtbaar)
  - Vaak buggy UEFI implementatie
- Klasse 2
  - CSM aanwezig, maar optioneel
- Klasse 3
  - Geen CSM aanwezig
  - Incompatibel met Windows Vista / 7 / Server 2008 (INT 0x10 support)

Secure Boot

(en consorten)

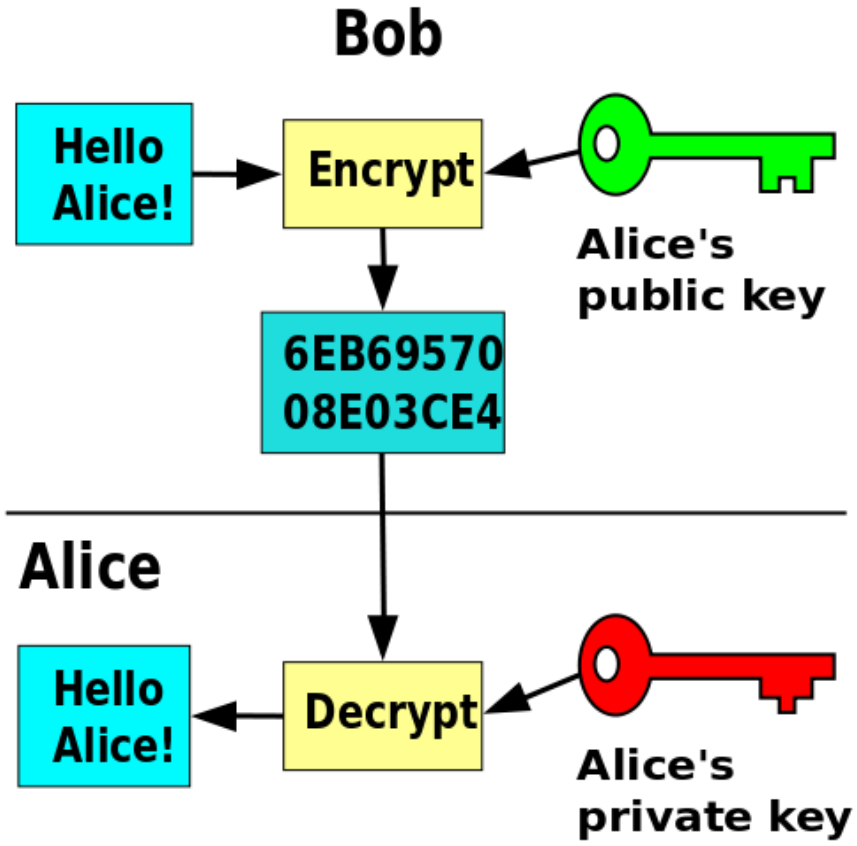
Secure Boot PKI vogelvlucht - sleutels



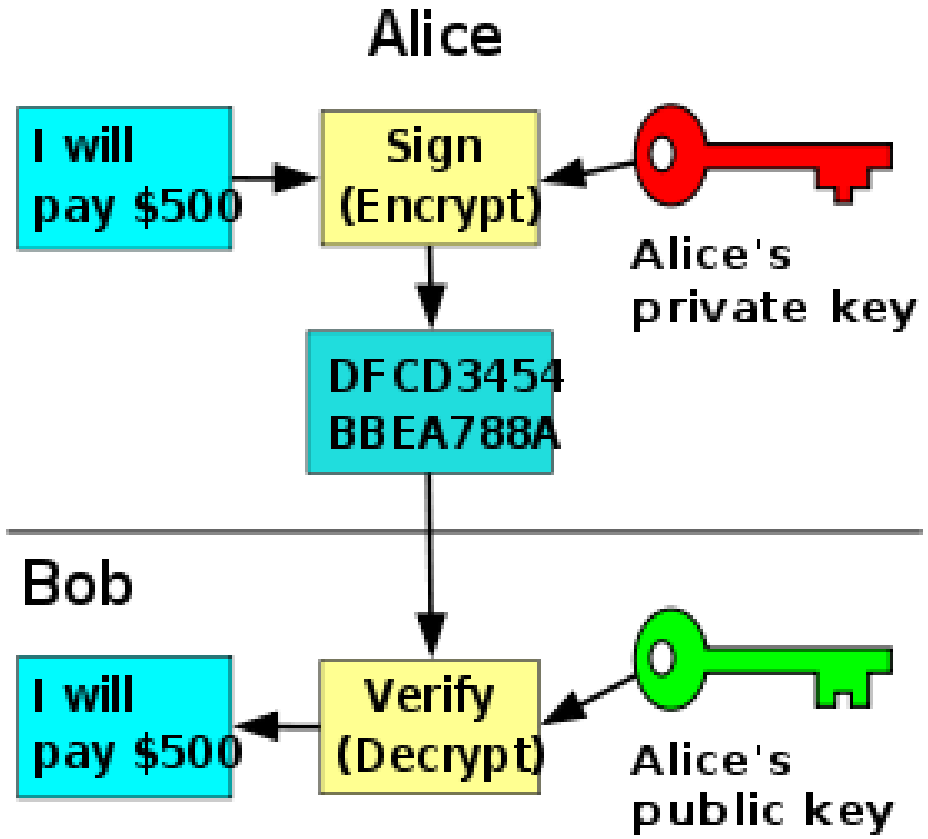
-----BEGIN RSA PRIVATE KEY-----
MIIBywIBAAJhALZz1EZ2VfqViPhypZLjyNYUPahiwTZd8N7D5ozXwkNMeuTVEu0T
lMDLe+3jlGAA8csgQiXK6aQ76jPpiK+48hwL1ZI767ziPKHwuPQ7lv3HJjbZq13X
RvCq6zY+zLDu/QIDAQABAmAQljsoJL3wSAPpwlJ3Jiot/C0Wz9OM48FwHxMonrzU
bXGGuDA+SVdup5EesV/d0ngBX/PRtJo1CI1GKhC0ep4kWEpyF776unxKtZZJC94g
v3hB83WOIw85t3L5O2gWQ+kCMQDwjpOKlYxHaHWRn2VrEXDen3sHdvIHdck+4W4g
cPj8W50hZvvMtgljjpL8Za1POmMCMQDCKlZHqWFqzP9NVBGgzjwbX9vxihBgBwD0
z3xib9HMPmBgIzeegmcOTmo+Nugjvx8CMQDbCVe6xnUWyDzVPghAt37IlvqVT28N
7+gww19dVsDAOEMZGQaJ3eiQq8+W1pY6H/UCMQCPw6NAykRsPL8n9YBb7XgJ2M9U
p6J6R5VIrrxtclgH/4OCi3DqN6mwqRT3XdZCaYcCMG/idYy7O5WYYkT8dR/E/Xf5
pWnUkLGbPe+PccACpjeWHoFq//xdhaaLyLKM/pxVCw==
-----END RSA PRIVATE KEY-----

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAYQC2c9RGdlX6lYj4cqWS48jWFD2oYsE2XfDew
+aM18JDTHrk1RLtE5TAy3vt45RgAPHLIEIlyumkO+oz6YivuPIcC9WSO+u84jyh8Lj0O5b
9xyY22atd10bwqus2Psyw7v0=

Secure Boot PKI vogelvlucht - encrypt

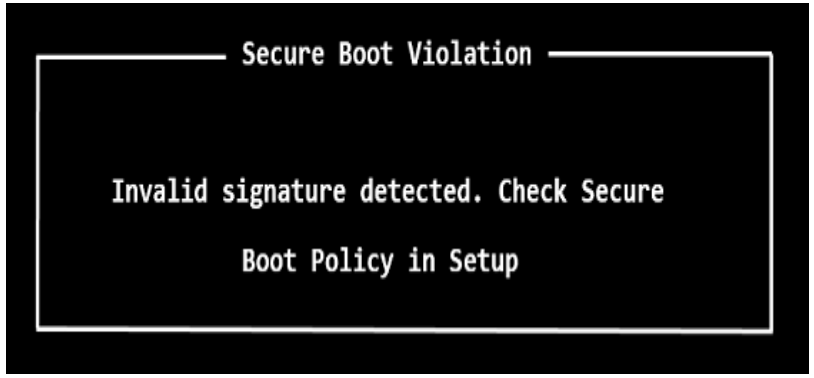


Secure Boot PKI vogelvlucht – sign



Secure Boot (concepten)

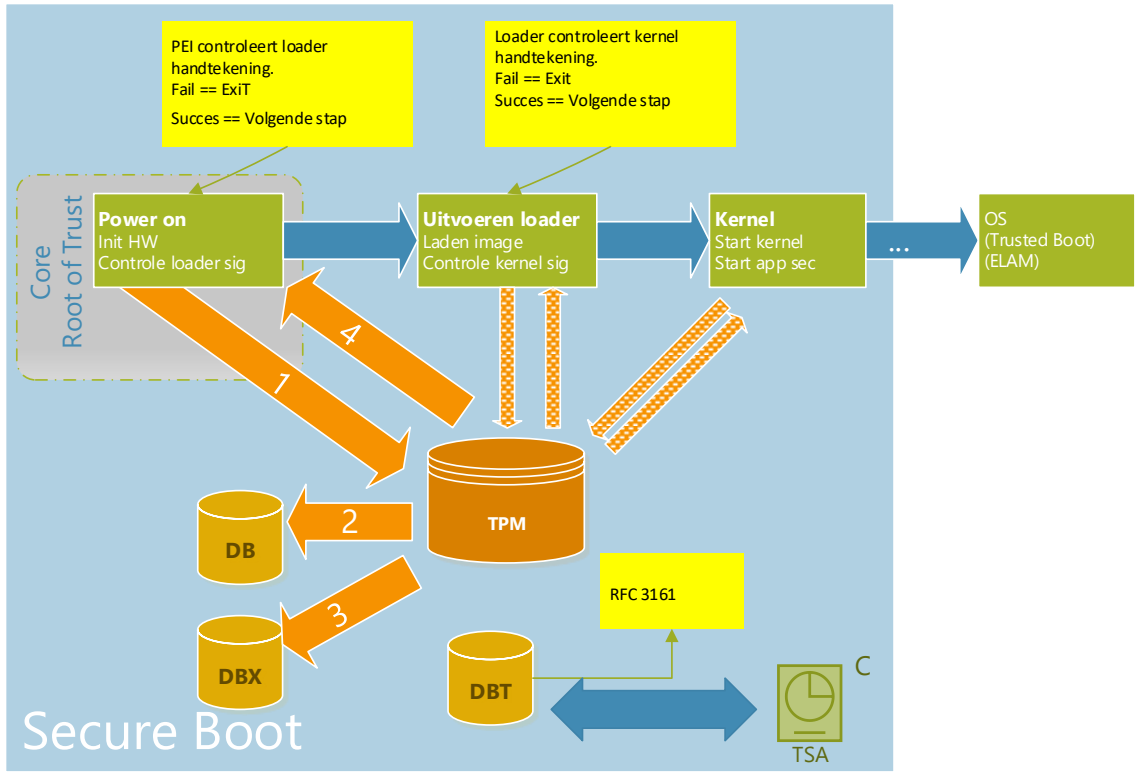
- UEFI spec 2.3.1c
- PKI gebaseerd
- TPM: Trusted Platform Module
- PCR: Platform Configuration Register
  - (TPM v1.2)
- RoT: Root of Trust
  - Fabrikant bepaald…



Secure Boot (concepten)

- PK – Platform Key
  - Private key: fabrikant
  - Public key: PK
  - Updates: getekend door oorsponkelijke sleutel
  - Beschermt KEK db
- KEK – Key Exchange Keys
  - Certs van (meestal) OSV’s
  - Mogen db / dbx / dbt aanpassen
- db – Whitelist database
- dbx – Blacklist database (eXclude)

Secure Boot (proces)



- Status KNOWN / UNKNOWN / BAD
- Policy bepaald

  Strict policy:

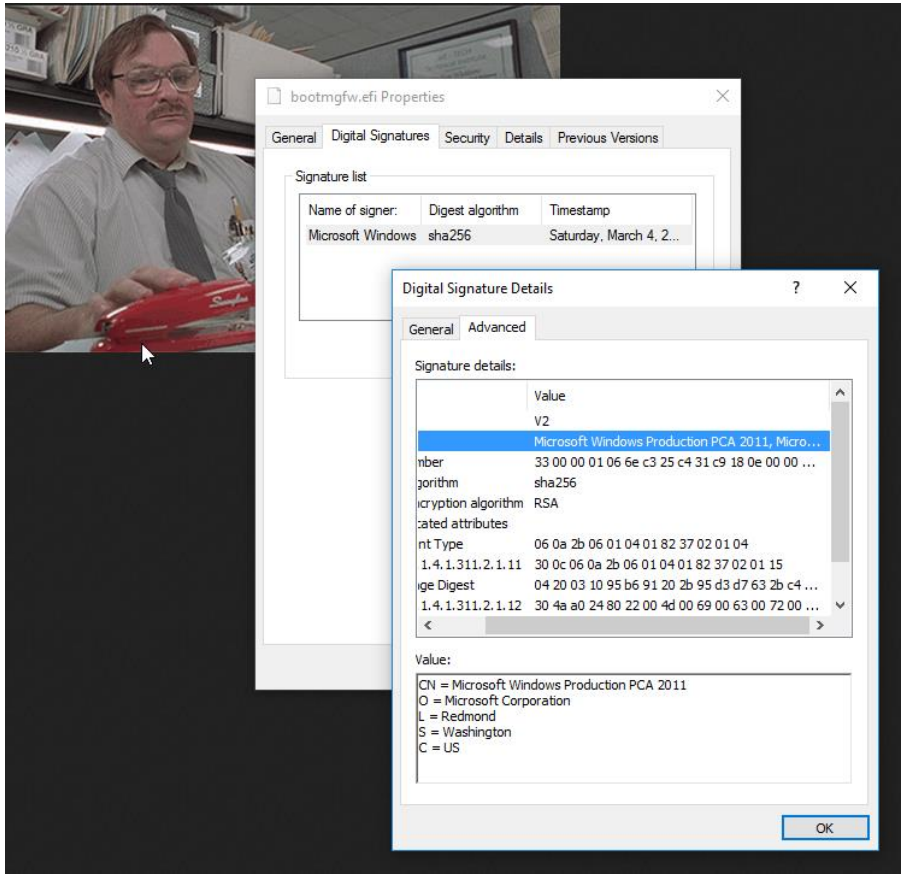
  Handover alleen indien:

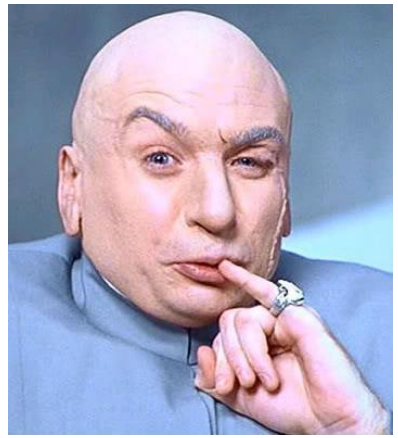
  <hash> IN DB == TRUE &&

  <hash> NOT IN DBX == TRUE

Secure Boot

- Windows bootloader
  - %WINDIR%\Boot\EFI\bootmgfw.efi





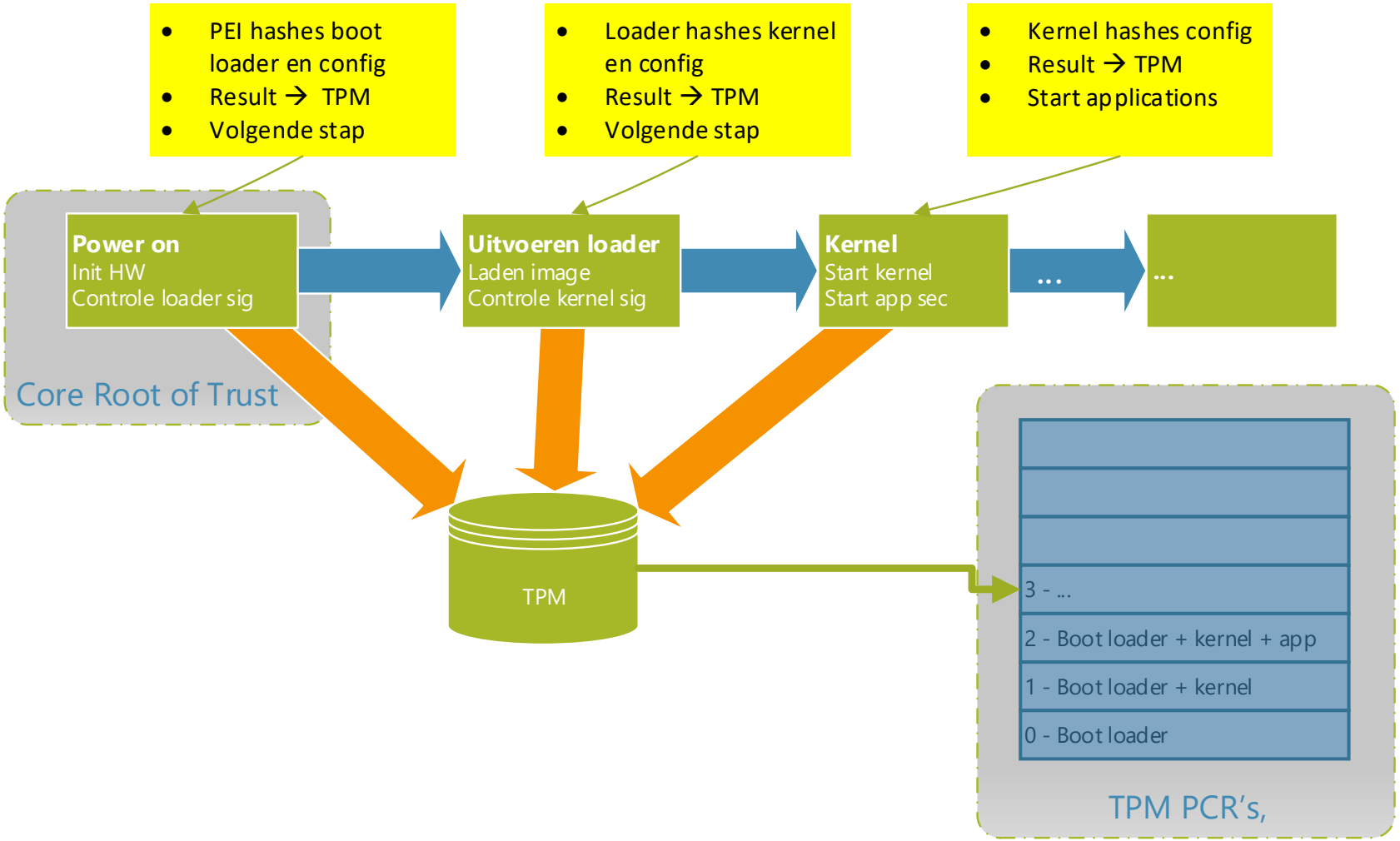
Measured Boot

...with frikin lasers...

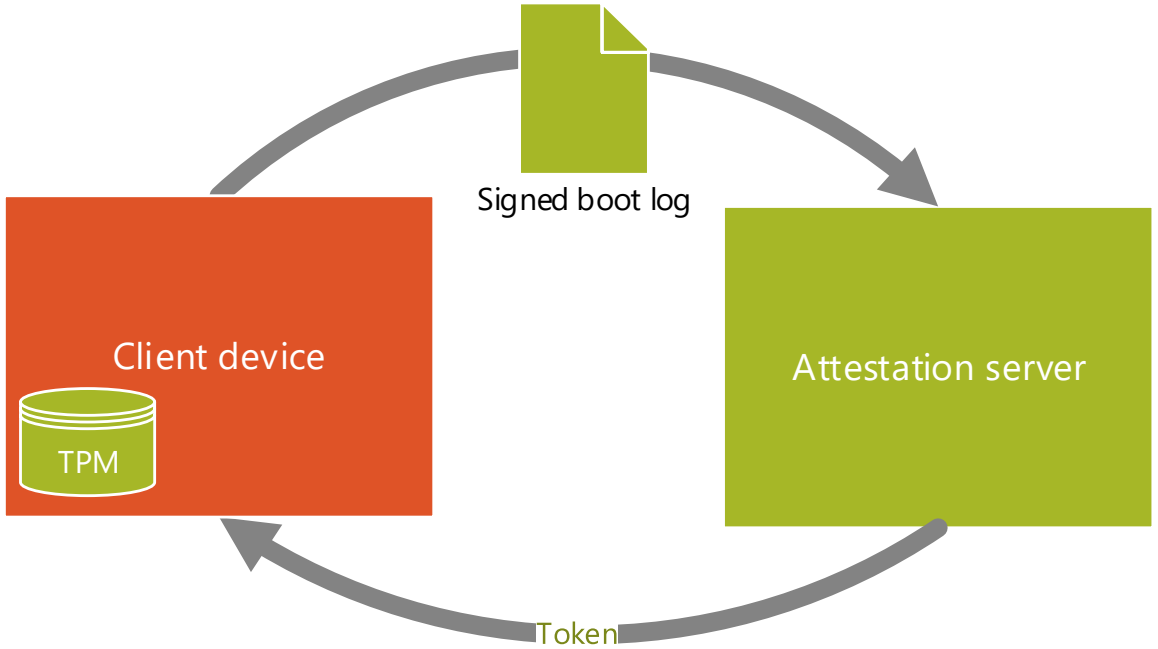
Measured Boot

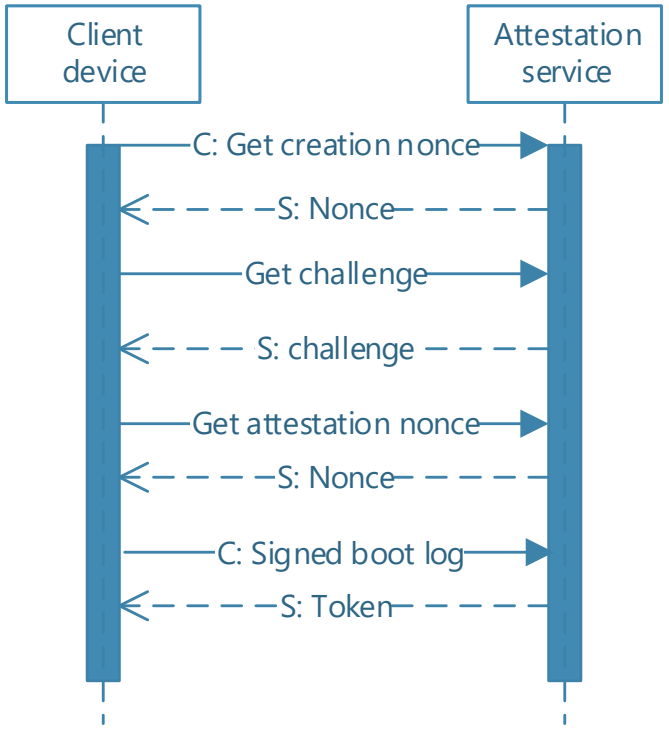
- Ook t.b.v. systeem integriteit
- TPM 1.2 (PCR geïntroduceerd)
- Maar andere route
  - Voorgaande module berekend (meet) hash volgende module
  - Hash wordt opgeslagen in PCR (maar geen controle op juistheid)
  - Systeem kan bevraagd worden (remote attestation)
  - Hash niet zoals verwacht → compromised
- TLDR: Bewijs welke componenten geladen zijn

Measured Boot



Measured Boot (attestation)



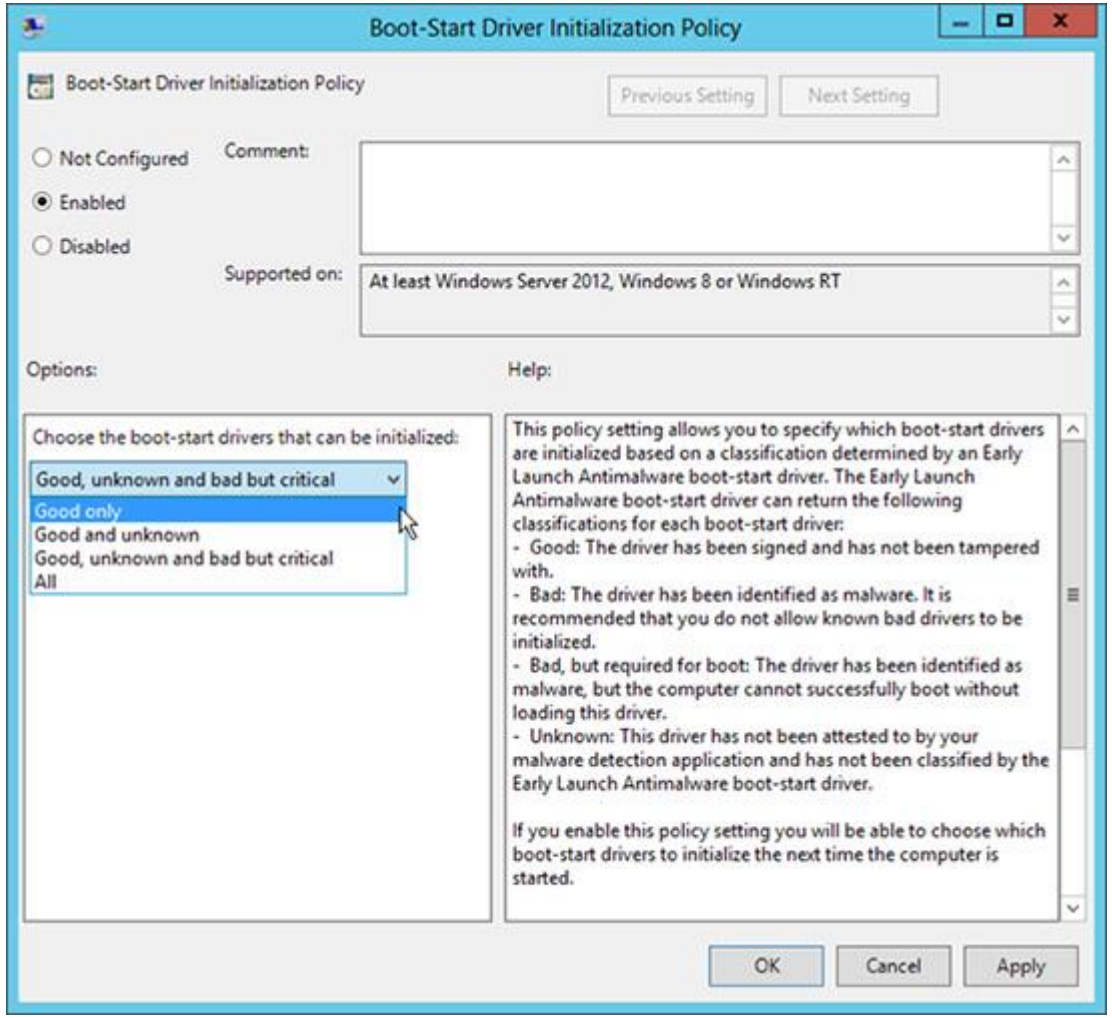


Measured Boot toepassingen

- Mobiel bankieren / betaalde online diensten
- Enterprise omgeving / hardware lease
  - Toestel succesvol gevalideerd → snelle login
  - Toestel onsuccesvol gevalideerd → fail
  - Toestel ongevalideerd → uitgebreide (b.v. MFA) login
  - (DEFCON 20 - Dan Griffin)
  - (DRM, ELAM, rootkit)
  - AD login alleen na gevalideerde boot
- (langzaam maar zeker steeds meer:
  - Iets met kikkers en kokend water)

Measured Boot ELAM

- Early Launch Anti Malware
- Specifiek type EFI driver
- Ingeladen voor alle andere drivers
- Waarschuwt als state != expected
- Handover naar regulier AM driver



Measured Boot was da den

- PCPTOOL
  - pcptool GetLog <out file>
  - pcptool DecodeLog <bootlog> > <out file>

```
<TCGLog>
 <WBCLBlob size="34205">
  00000000070000069d483c7142925d5eebc31c1508f884e70a14c3321000000426f6f74204775617264204465627567204d656173…
</WBCLBlob>
 <WBCL size="34205">
  <EV_CRTM_Contents PCR="00" Digest="69d483c7142925d5eebc31c1508f884e70a14c33" Size="33">
   426f6f74204775617264204465627567204d65617375726564203 2d4352544d00
   <!-- Boot.Guard.Debug.Measured.S.CRTM. -->
  </EV_CRTM_Contents>
  <EV_CRTM_Version PCR="00" EventDigest="c42fedad268200cb1d15f97841c344e79dae3320" Size="16">
   1efb6b540c1d5540a4ad4ef4bf17b83a
   <!-- ..kT..U...N..... -->
  </EV_CRTM_Version>
  <EV_Post_Code PCR="00" Digest="fa5252259db274ecea3e6e6e63060004d6b85602" Size="16">
   000082ff0000000050c1cb7700000000
   <!-- ........P..w.... -->
  </EV_Post_Code>
```

UEFI tools #1

- rEFInd
  - http://www.rodsbooks.com/refind/
- TianoCore EDK II (UDK)
  - https://www.tianocore.org/
- Windows:
  - BCDEDIT: https://technet.microsoft.com
  - PCPTool
  - Measured Boot Tool: http://mbt.codeplex.com/
- Linux:
  - efivar, efibootmgr: https://wiki.archlinux.org/

UEFI (tools) #2

- Libs
  - Gnu-efi (sourceforge)
  - EDK-II (tianocore.org)
- Hello World (rodsbooks.com)
- Eigen certificaten (Canonical)
- Eigen certificaten (Microsoft)

UEFI (meer weten?) #1

- DEFCON 20 – Dan Griffin
- 30c3 – Thwarting the Evil Maid Attacks
- 31c3 – Thunderstrike: EFI bootkits for Apple MacBooks
- 32c3 – Thunderstrike 2
- 32c3 – Beyond Anti Evil Maid
- 32c3 – Reversing UEFI by execution
- 33c3 – Bootstraping a slightly more secure laptop
- 30c3 – An introduction to Firmware Analysis
- 30c3 – Hardening hardware and choosing a goodBIOS

UEFI (meer weten?) #2

- Elke jaar nieuwe mogelijkheden
  - CCC, DEFCON, Blackhat, Kiwicon, …
- Want:
  - Complexe spec → complexe software → bugs (en loopholes in spec)
  - Copy paste gedrag IFV’s
    - Fork EDK → customize → gooi over schutting → Vulns?
      - NIMBY - LGSTO!
    - Case study: Apple EFI

UEFI – tot slot

- Voorgaande niet direct toepasbaar
  - Duiding / richting geven bij problemen
- Vervolg
  - EFI app tbv klonen
    - EFI stub linux kernel
    - Syslinux o.i.d. toolset
- Obstakels
  - Certs
  - Systeembeperkingen
    - Alleen FAT gegarandeerd
    - NTFS / EXT[2|3|4] / HFS+ / …