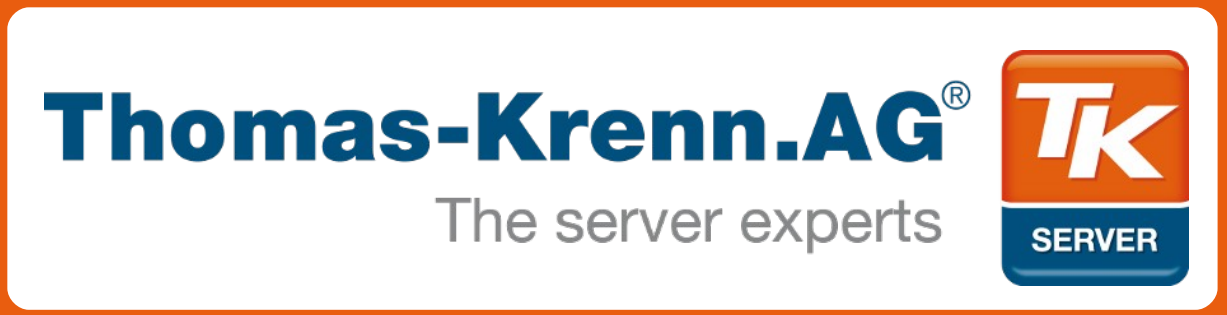

Thomas-Krenn.AG®
The server experts
TK
SERVER

Thomas-Krenn.AG®
The server experts

UEFI
Das neue BIOS kommt

TK Roadshow 2012

Agenda

1) Einführung

2) Vorteile u. Historie

3) GPT

4) Boot Prozess

5) UEFI Services

6) Aktuell: Secure Boot

7) Fazit

2) UEFI Einführung

Thomas-Krenn.AG®
The server experts

Modular aufgebaut

OS<->FW Spezifikation

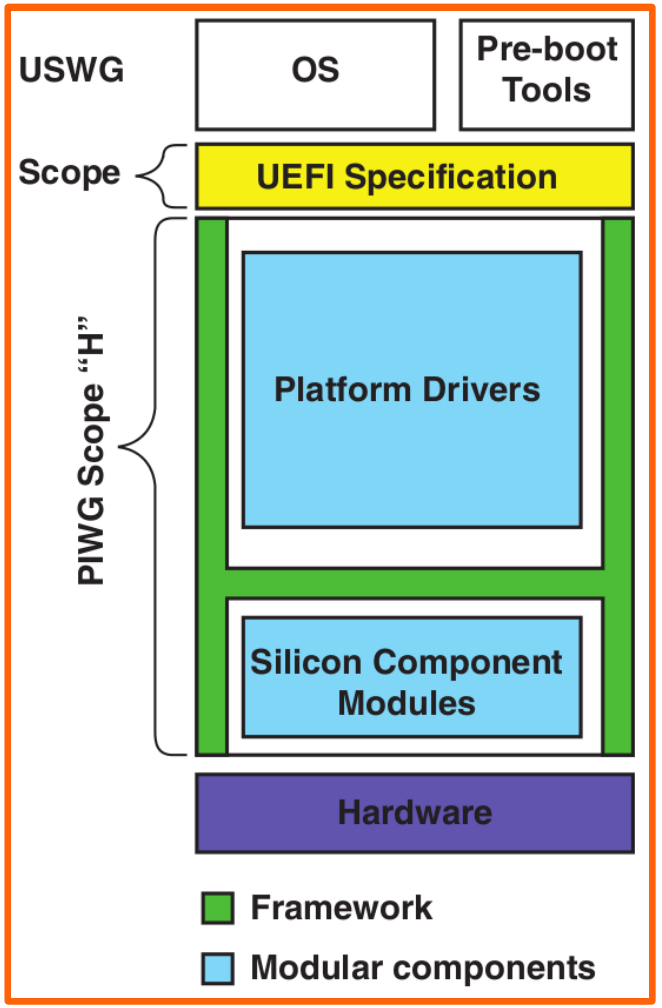
Unified Extensible Firmware Interface

Einfach erweiterbar

Plattform unabhängig

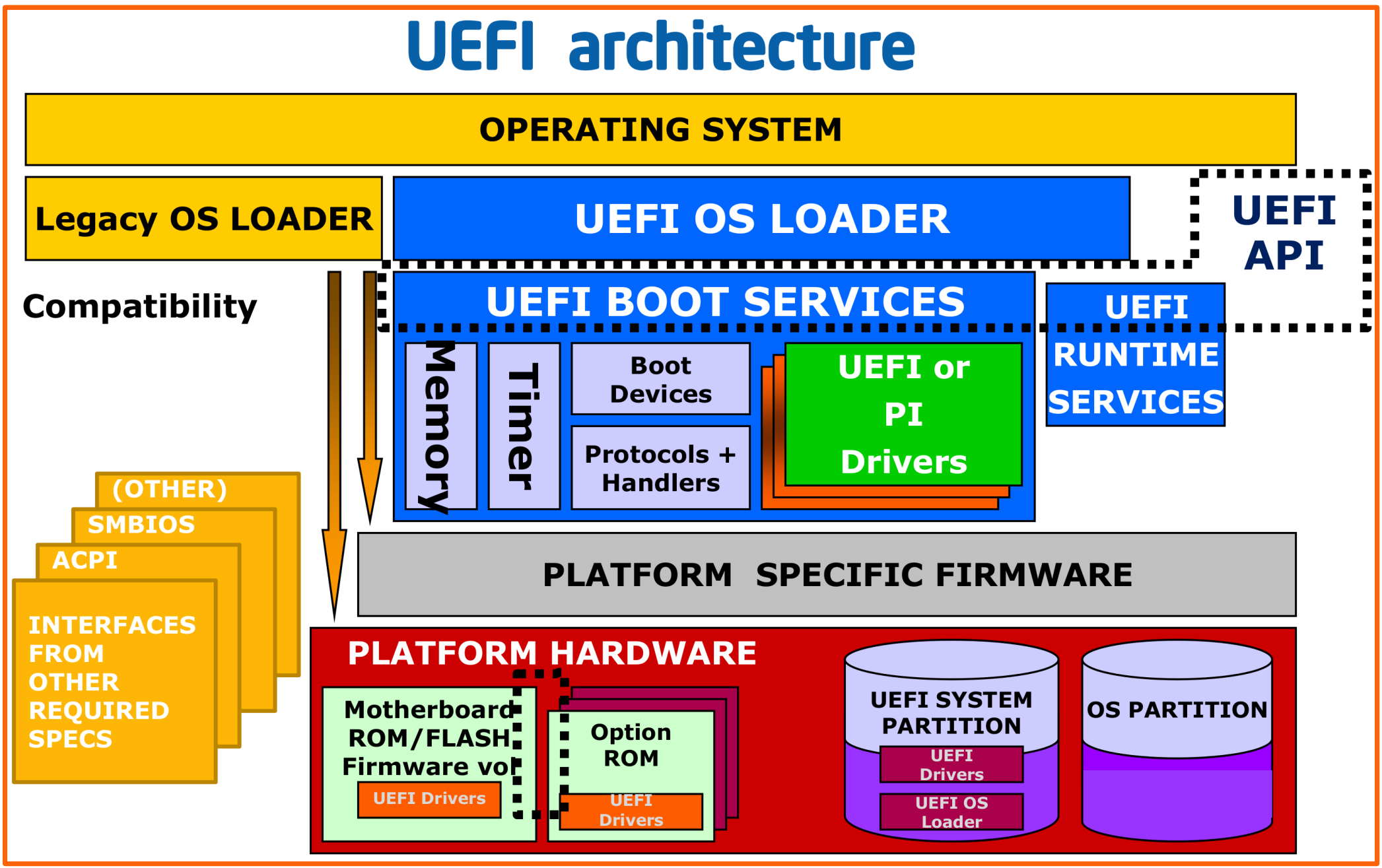
2) UEFI Vorteile

- Boot Partition – GPT
- 32/64 bit Modus
- Runtime Services
- Driver Model
- Boot Manager
  - Konsolidiertes Interface
  - Boot Options
- Pre-OS Applikationen
- GOP anstatt VGA für pre-boot GUIs



UEFI Today: Bootstrapping the Continuum, S. 17

UEFI architecture



2) UEFI Historie

- EFI Spezifikation
- Intel Itanium

2000

- EDK
- Tianocore.org

2005

- Unified EFI Forum
- UEFI 2.0
- Working Groups
- PI 1.0

2006

- UEFI 2.3.1
- UDK2010.SR1.UP1
- PI 1.2
- Secure Boot

2012

GPT

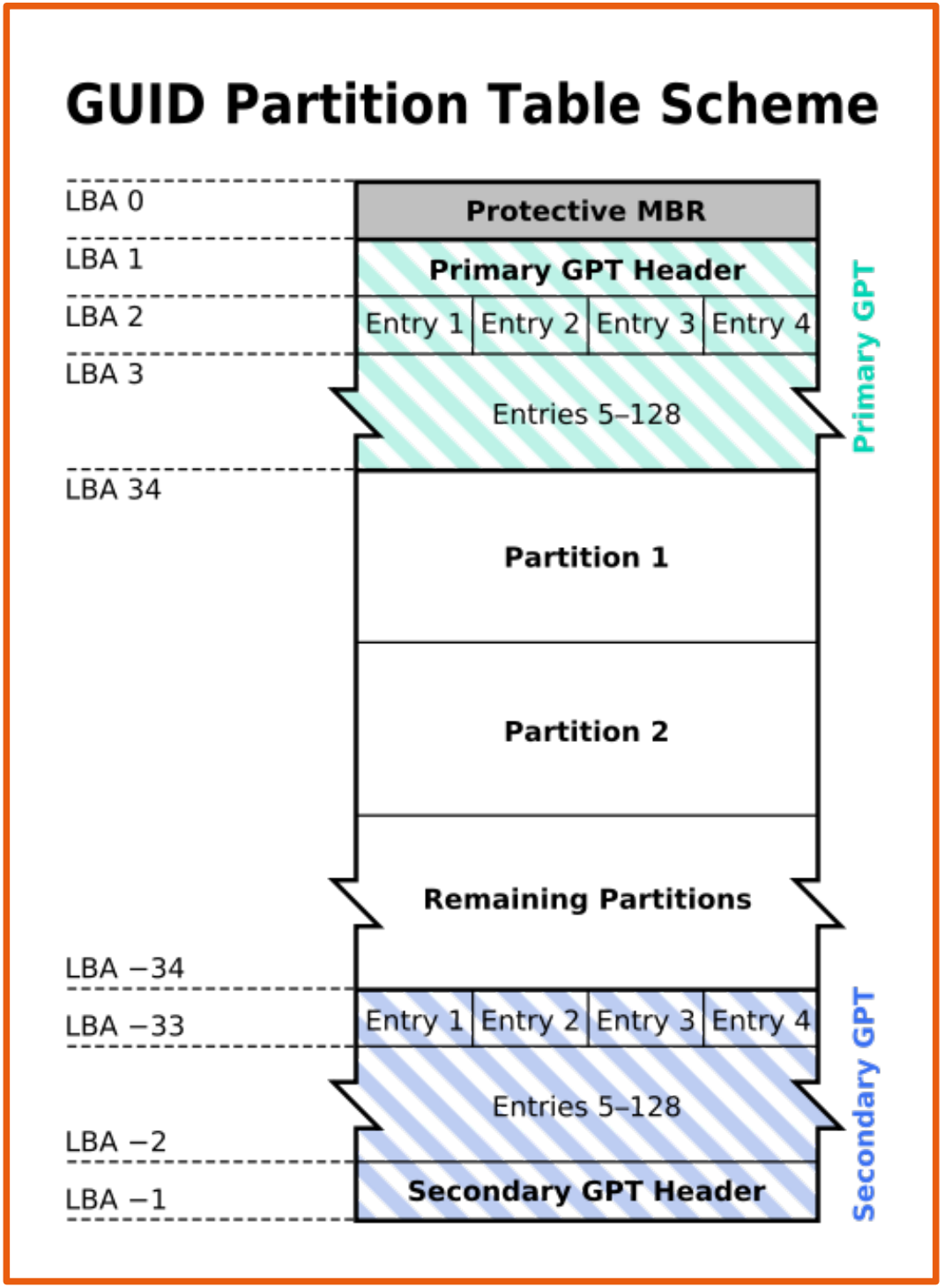
UEFI Spez. Kap. 5

3) GPT

- Entwickelt im Rahmen der UEFI-Spez.

GUID Partition Table

- 64bit LBAs
- Mehrere Partitionen (128)
- Primary u. Backup Table
- Checksummen (CRC32)
- Verwendet GUIDs



Wikipedia-Artikel: GPT

3) GPT

- Protective MBR

```
:~$ sudo fdisk -l /dev/sdc
WARNING: GPT (GUID Partition Table) detected on '/dev/sdc'! The util fdisk
doesn't support GPT. Use GNU Parted.
```

- Disk GUID (identify disk)

```
:~$ sudo gdisk /dev/sdc
Command (? for help): p
Disk /dev/sdc: 156301488 sectors, 74.5 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): F8FAC3BE-EB16-49DD-A4B4-E3C1472E2D9B
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 156301454
Partitions will be aligned on 1-sector boundaries
Total free space is 16 sectors (8.0 KiB)
```

- Partition Type GUID (OS Type in MBR)

```
Partition GUID code: A19D880F-05FC-4D3B-A006-743F0F84911E (Linux RAID)
```

3) GPT und OS

- Windows 7, Vista, Server 2008
  - Boot von GPT nur für 64bit mit UEFI[1]
- Windows 7/8, Server 2008/2012
  - Boot unter UEFI nur von GPT
  - Erstellt EFI System Partition
- Linux
  - Bootet auch unter BIOS von GPT → zumeist BIOS Boot Partition und z.B. Grub2
  - Ubuntu!

1 Windows and GPT FAQ
2 Installing Windows on UEFI Systems

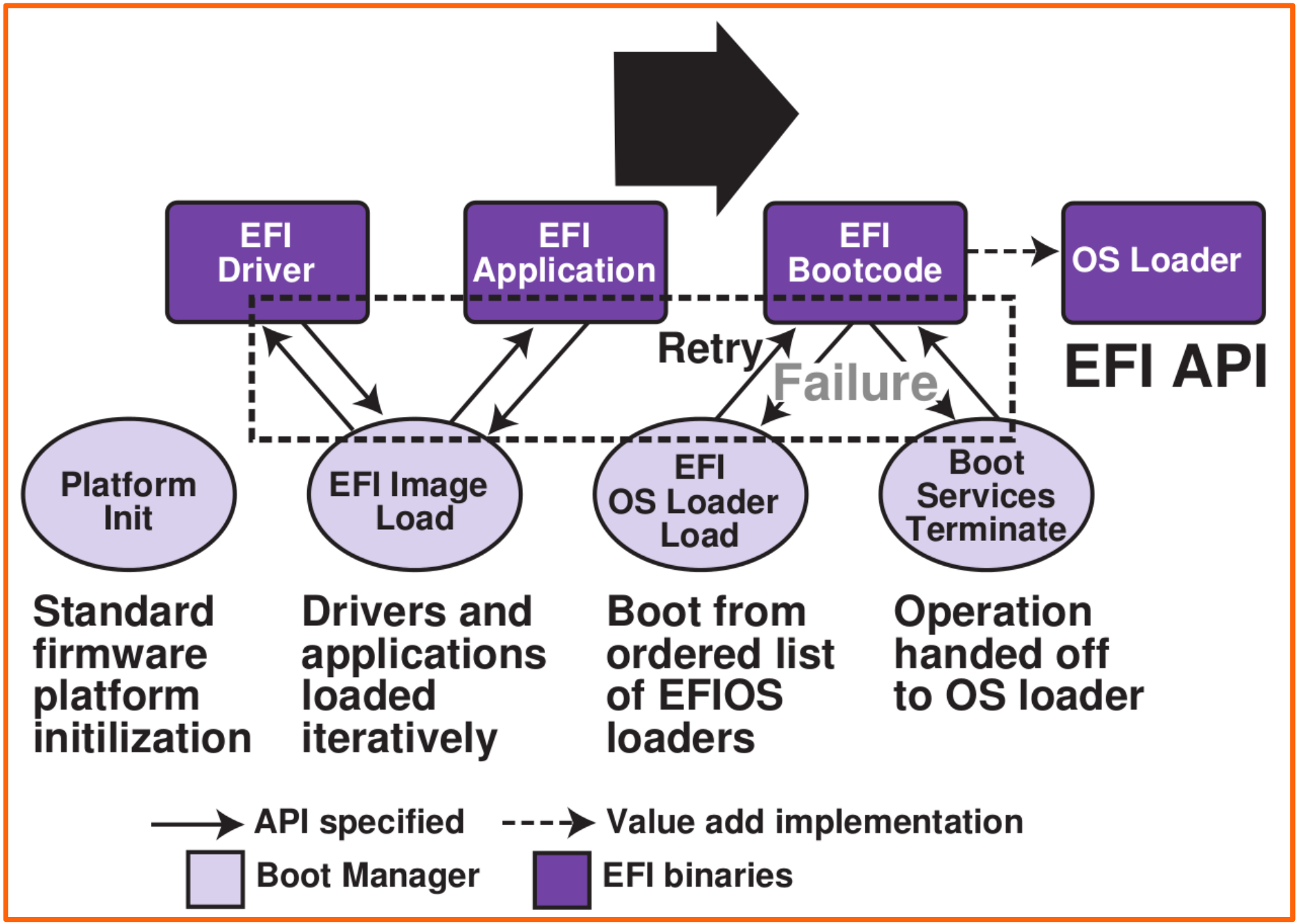
UEFI Boot u. Services

UEFI Spez. Kap. 2,6 u. 7

4) UEFI-Boot-Prozess

- EFI Boot Manager
  - Single Plattform Menu
  - Befindet sich als System Menu in der Firmware
  - Verwaltet vorhandene Boot Loader Programme

```
:~$ sudo efibootmgr
BootCurrent: 0000
Timeout: 1 seconds
BootOrder: 0000,000A,0009,0003,0007,0006
Boot0000* ubuntu
Boot0003* Network Card
Boot0006* UEFI: Built-in EFI Shell
Boot0007* USB
Boot0009* Hard Drive
Boot000A* UEFI: ATP Nano Vision 1100
```



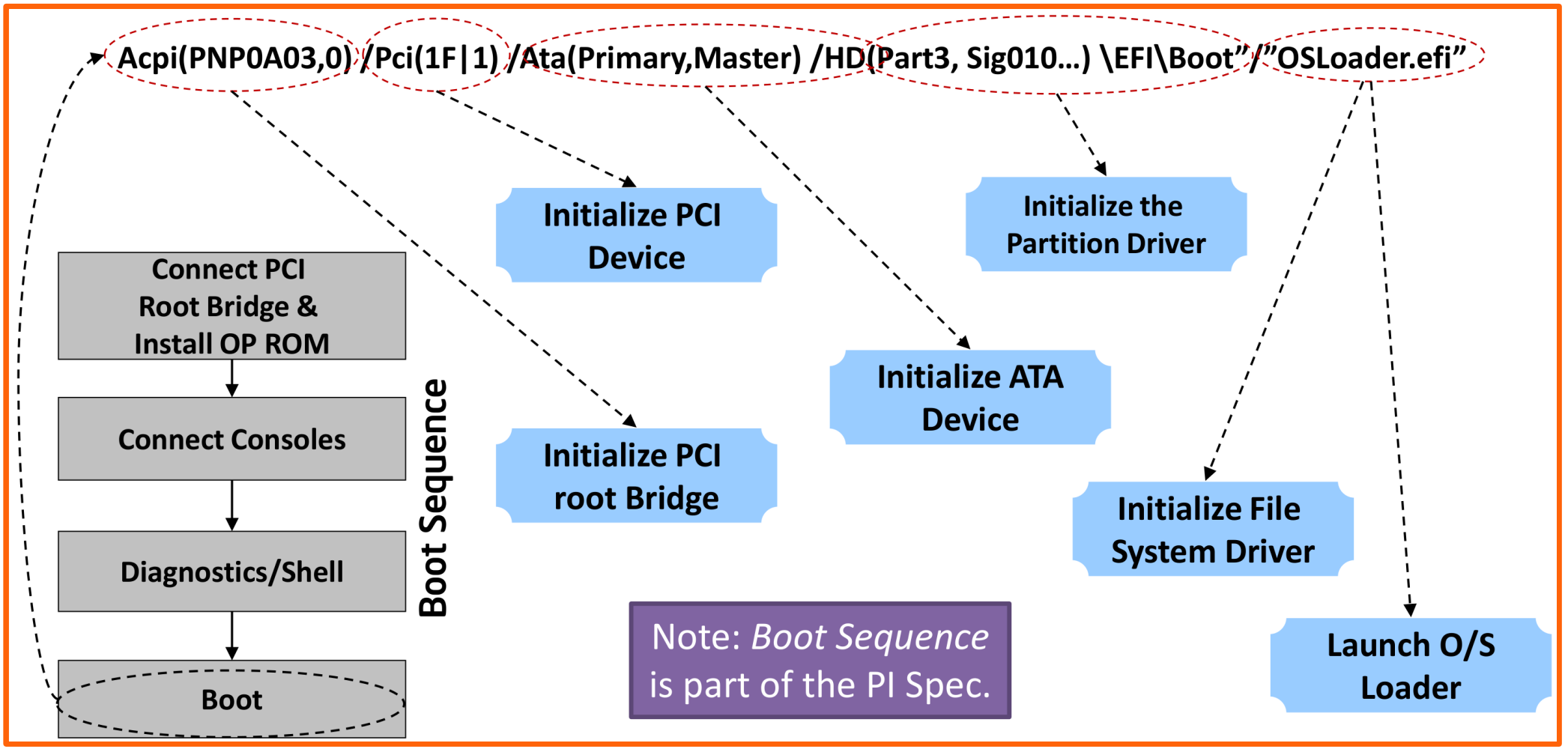
UEFI Spezifikation 2.3.1, Seite 17

4) UEFI-Boot-Prozess

- Für non-removeable Block-Device wird ESP benötigt

```
:~$ sudo gdisk /dev/sdc
[...]
Partition number (1-4): 1
Partition GUID code: C12A7328-F81F-11D2-BA4B-00A0C93EC93B
(EFI System)
[...]
:~$ mount -l
[...]
/dev/sdc1 on /boot/efi type vfat (rw)
[...]
:~$ ls /boot/efi/EFI/ubuntu/
grubx64.efi
```

- Ein Installationsmedium für Legacy und UEFI
- Applikationen/Driver sind auch ladbare Images

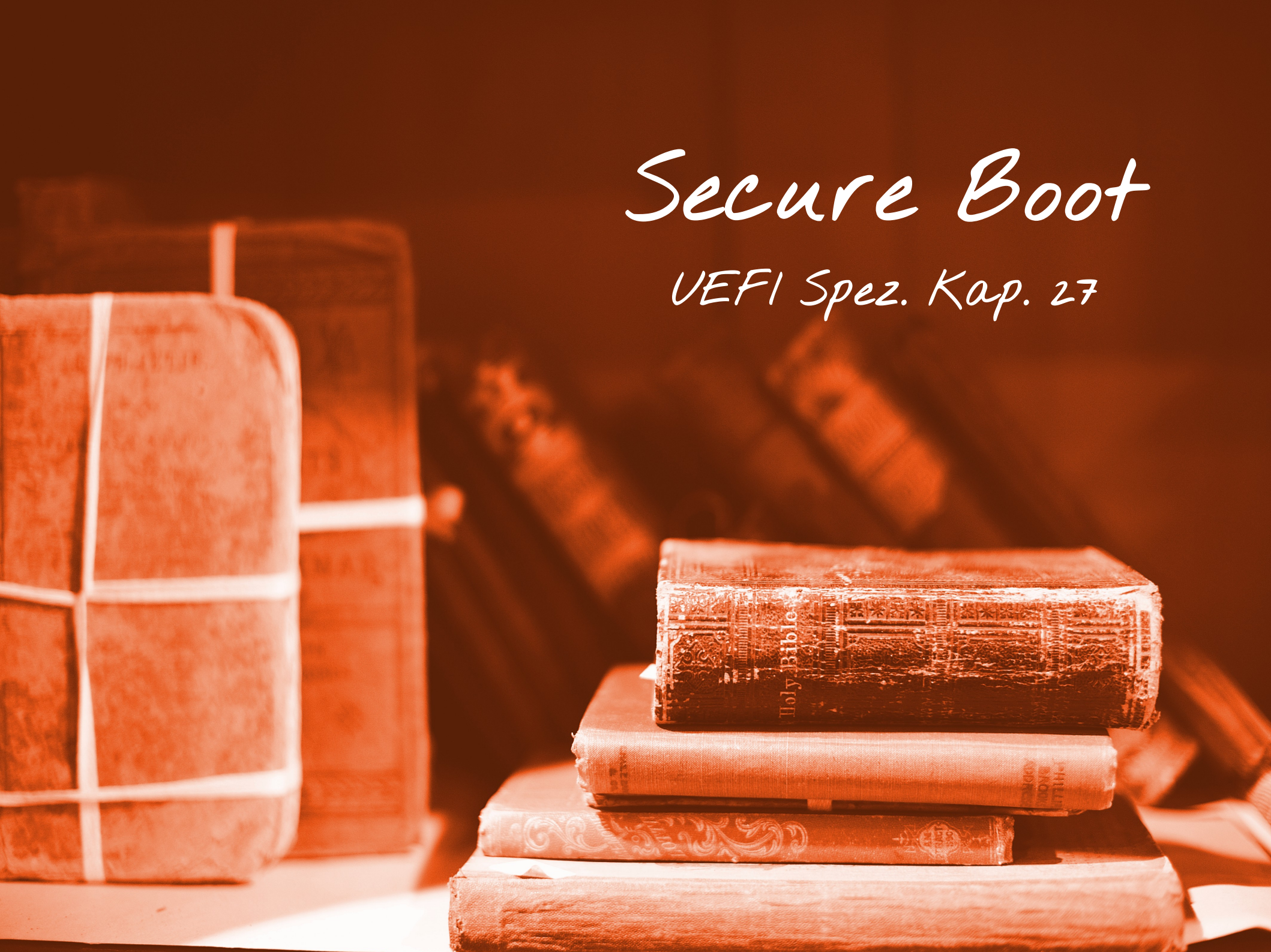

Acpi(PNP0A03,0)/Pci(1F|1)/Ata(Primary,Master)/HD(Part3, Sig010…)\EFI\Boot”/”OSLoader.efi”
Connect PCI Root Bridge & Install OP ROM
Connect Consoles
Diagnostics/Shell
Boot
Boot Sequence
Initialize PCI Device
Initialize PCI root Bridge
Initialize the Partition Driver
Initialize ATA Device
Initialize File System Driver
Launch O/S Loader
Note: Boot Sequence is part of the PI Spec.

5) UEFI-Services

- Manche „UEFI-Tabellen“ auch aus OS heraus zugänglich
  - UEFI Runtime Services (UEFI Spez. Kap. 7)
    - System Reset
    - Boot Manager Variablen bearbeiten
    - Timer Wakeup
- UEFI Boot Services nur bis zum Zeitpunkt des OS Loaders
  - Device Access
  - Memory Management

Secure Boot

UEFI Spez. Kap. 27



6) Secure Boot

- Firmware-Teile werden nur mit gültiger Signatur ausgeführt
- Wer bestimmt die gültigen Signaturen?
  - Platform Key (PK)
    - Platform Owner ↔ Platform Firmware
  - Key Exchange Key (KEK)
    - Operating System ↔ Platform Firmware
  - Signature Databases
    - Authorized (DB)
    - Forbidden (DBX)

6) Secure Boot

- Private Key PK/KEK
  - Updates für Signature Database
- Laden von Images
  - Digital signiert
  - Hash befindet sich als Whitelist in Authorized DB
- Blacklist auch möglich
  - Option ROM (Driver) mit Vulnerability
  - Hash in DBX

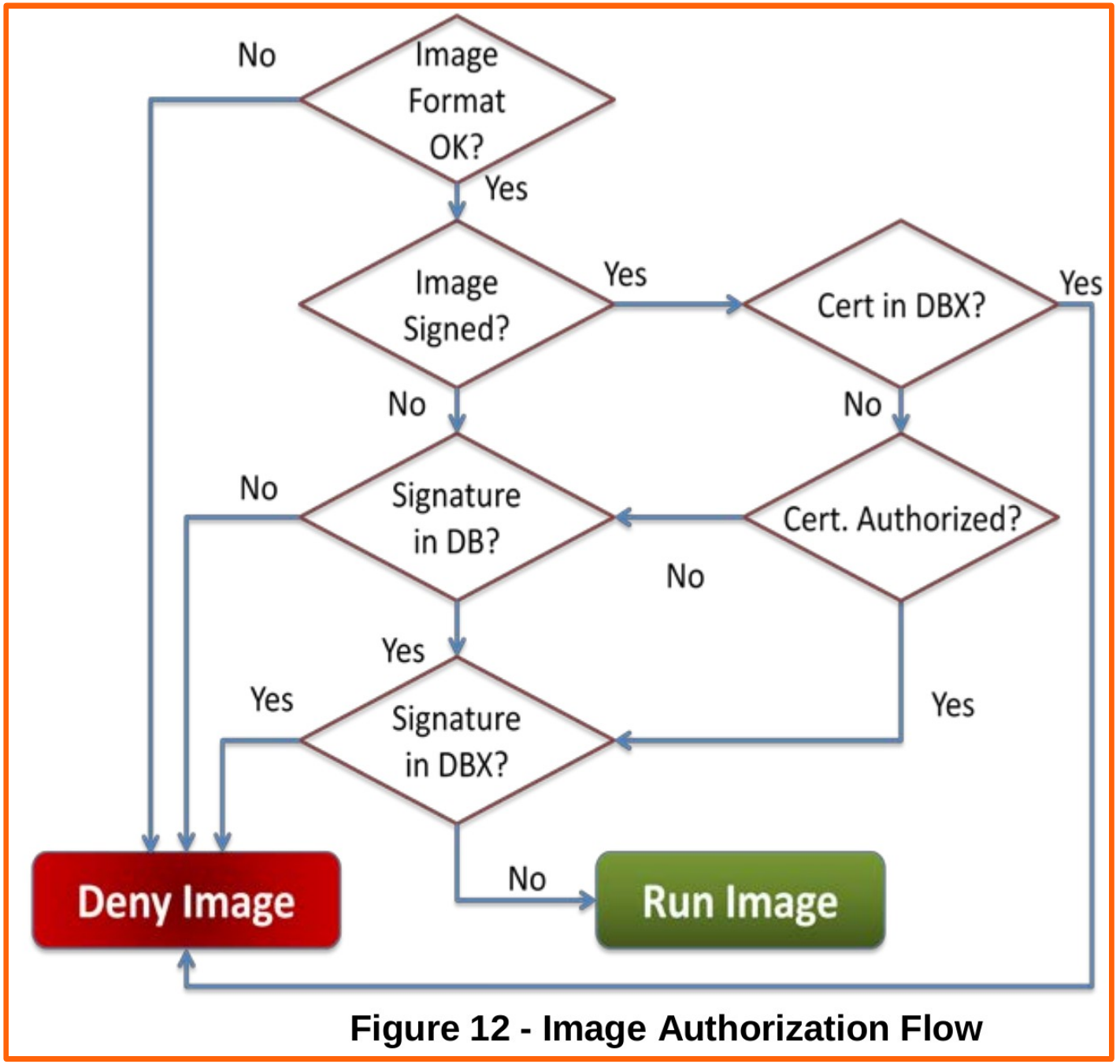


Figure 12 - Image Authorization Flow

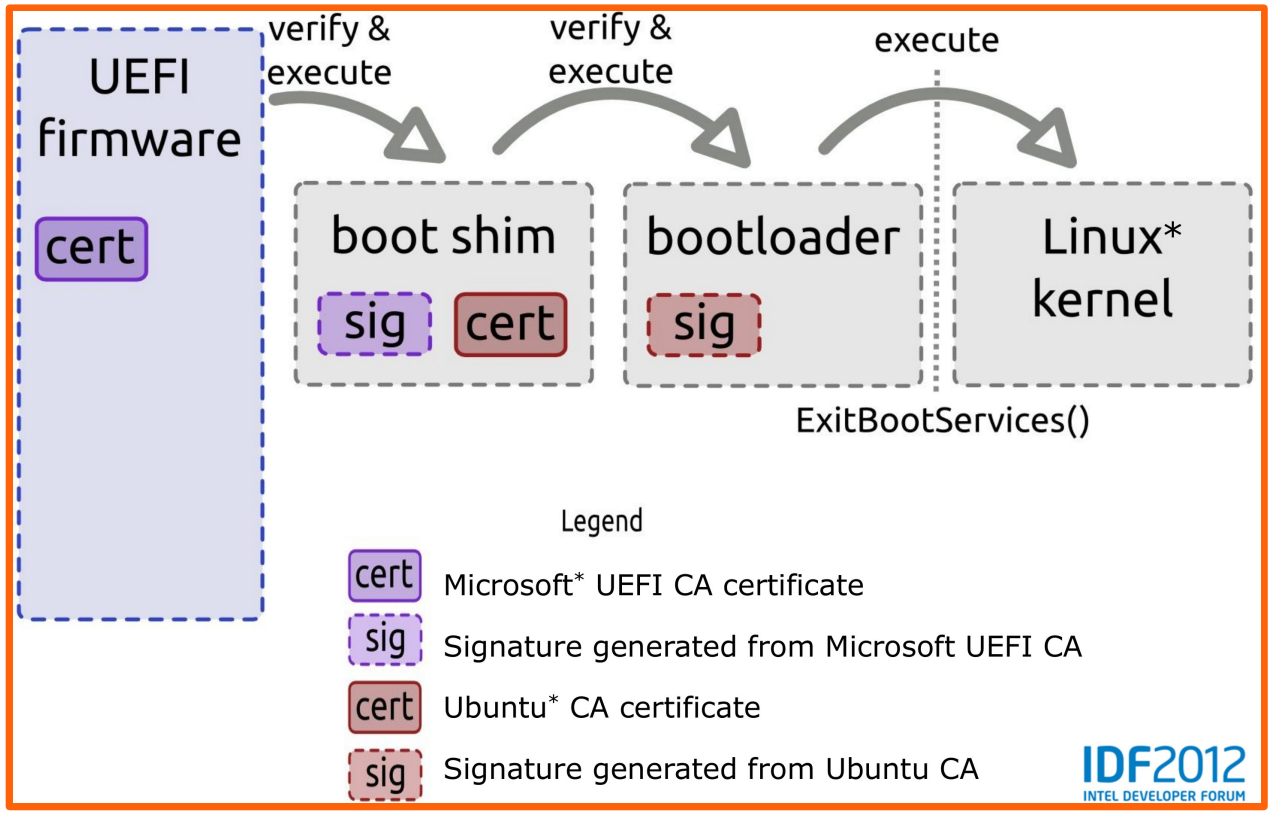
6) Secure Boot

Thomas-Krenn.AG®
The server experts

- Windows 8/Server 2012 Logo Zertifizierung verlangt
  - UEFI
  - Aktiviertes Secure Boot
    - Note II: Kann für Server deaktiviert werden
  - Mit Secure Boot kein CSM (Legacy BIOS Modus)
- Ubuntu

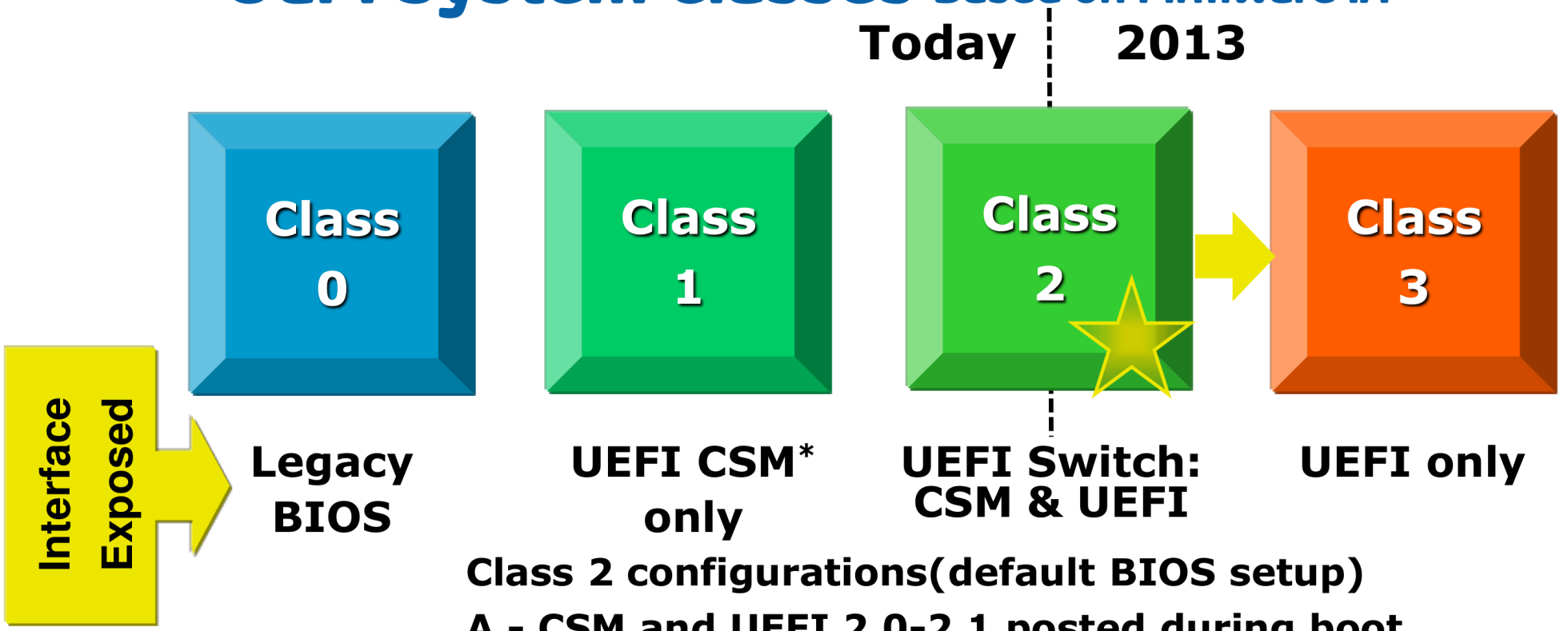
6) Secure Boot

- Linux
  - Option: Deaktivieren – Fördert nicht Sicherheit, Akzeptanz von Linux
  - Lösungsweg:[1]



1 IDF2012 - Developing UEFI Support for Linux*, Folie 11

UEFI System Classes Based on Firmware I/F



Class 2 configurations(default BIOS setup)

A - CSM and UEFI 2.0-2.1 posted during boot

B - UEFI 2.0-2.1 only posted during boot, CSM disabled

C - UEFI 2.3.1 only posted during boot, CSM disabled, secure boot enabled – only signed modules executed

A,B Shipping today (2012)

C Required by Windows 8 logo

***-CSM : Compatibility Support Module or Legacy BIOS written as an UEFI driver**

7) Fazit

Thomas-Krenn.AG®
The server experts

1. UEFI & GPT sind da
2. OS Support am kommen
3. Class 3 wird kommen

Einzelnachweise

- UDK2010 Präsentationen Base Training
  - UEFI-EDKII-Presentations.zip
- Linux Plumbers Conference
  - UEFI Tutorial – Harry Hsiung
- A Tour Beyond BIOS into UEFI Secure Boot
- Bilder
  - UEFI Logo
    - http://www.uefi.org/about/logo/
  - Kapitel-Folien-Bild
    - File:Old book - Basking Ridge Historical Society (1).jpg
  - http://openclipart.org/detail/16878/death-by-porota