U E F I
das neue
B I O S

Eine Ausarbeitung von Hans-Joachim Karnoll
von den Rutesheimer Onlinern

B I O S

- **Name:**
  - » **B**asic
  - » **I**nput and
  - » **O**utput
  - » **S**ystem

- **In Deutsch:**
  - » Grundlegendes
  - » Eingabe und
  - » Ausgabe
  - » System

B I O S

- **BIOS-Hersteller**

  Eine Auswahl von Herstellern von BIOSen für IBM-kompatible PCs:

  - American Megatrends
  - Phoenix/Award – Award und Phoenix haben 1998 fusioniert. Award wird von dem Unternehmen als Desktop-Produkt geliefert. Die Phoenix-Produktreihe wird hingegen bei Servern und Laptops eingesetzt.
  - MR BIOS
  - ATI Technologies
  - IBM
  - Insyde

B I O S

- **Aufgaben:**

  - » P.O.S.T. = Power On Self Test
  - » Initialisierung der Hardware
  - » Aufforderung zur Eingabe eines BIOS-Passworts (falls konfiguriert)
  - » Aufforderung zur Eingabe eines Festplatten-Passworts (falls konfiguriert)
  - » Darstellung eines Startbildschirms
  - » Möglichkeit, ein BIOS-Konfigurationsmenü („BIOS-Setup“) aufzurufen

B I O S

- Aufrufen von BIOS-Erweiterungen einzelner Subsysteme, die entweder auf Steckkarten untergebracht sind oder direkt auf dem Mainboard integriert sind, z. B.:
  - Grafikchip
  - Netzwerkchip
  - SCSI-Controller
  - RAID-Controller
- Feststellen, von welchem Datenträger gebootet werden kann und soll
- Laden des Bootsektors; meistens ist das ein Bootloader

B I O S

- **Zusätzliche Aufgaben:**

  » Kommunikation für das Betriebssystem mit diverser Hardware, z. B.:

  - Tastatur
  - Serielle und parallele Schnittstellen
  - Systemlautsprecher
  - Grafikkarte
  - Diskettenlaufwerke
  - Festplattenlaufwerke

B I O S

- **Einschränkungen:**

  Andere, moderne Arten von Hardware werden vom BIOS nicht bedient. Zur Ansteuerung beispielsweise einer Maus ist unter DOS ein spezieller Hardwaretreiber nötig. Neuere, treiberbasierte Betriebssysteme wie beispielsweise Linux oder Microsoft Windows nutzen diese BIOS-Funktionen nicht. Sie laden für jede Art von Hardware einen speziellen Treiber. Jedoch müssen sie am Anfang ihres Startvorgangs noch kurz auf die BIOS-Funktionen zur Ansteuerung der Festplatten zurückgreifen, um ihren Festplattentreiber zu laden.

B I O S

- **Kritik:**
  - Eine Firmware-Schnittstelle wie BIOS und UEFI ist sehr tief im System verankert und daher eine potenziell sicherheitskritische Komponente. Punkte, die zu einer kritischen Betrachtung eines herstellerabhängigen BIOS führen:
  - Proprietärer Code: Absichtliche oder unabsichtliche Sicherheitslücken entziehen sich der öffentlichen Kontrolle (Möglichkeit der Ausspähung, Manipulation und Industriespionage) - die NSA erarbeitete 2010 dazu eine Durchführbarkeitsstudie.
  - Die Einstufung der Vertrauenswürdigkeit von Software unterliegt beim BIOS-Nachfolger UEFI allein der Firma Microsoft.
  - Es gibt nur zwei große BIOS-Produzenten, beide residieren in den USA und unterliegen deren Bestimmungen.
  - UEFI erfüllt nicht die Anforderungen zur Computersicherheit der deutschen Bundesregierung.
  - Mögliche feste Implementation von Nutzungseinschränkungen, etwa Digital Rights Management.

U E F I

- **Name:**
  - » **U**nified
  - » **E**xtensible
  - » **F**irmware
  - » **I**nterface

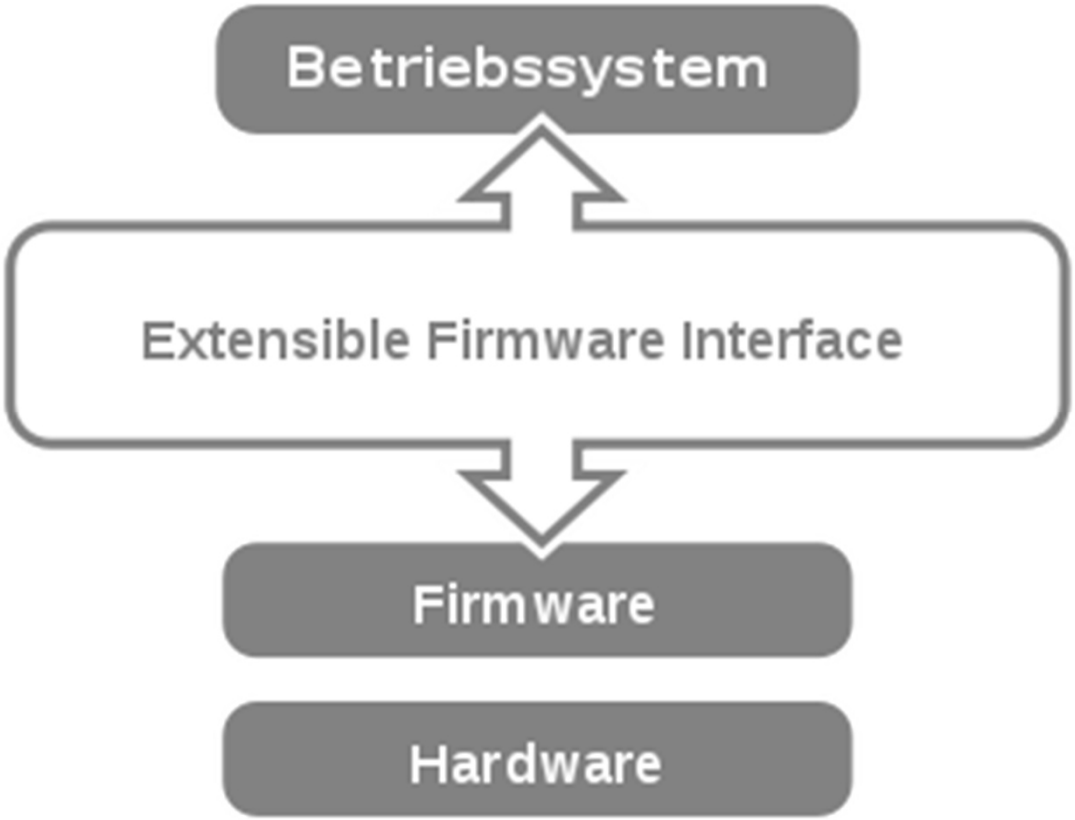
- **In Deutsch:**
  - » Vereinheitlichte
  - » erweiterbare
  - » Firmware
  - » Schnittstelle

U E F I

- **aus Wikipedia, der freien Enzyklopädie:**

  Das **Unified Extensible Firmware Interface** (kurz **UEFI**, und dessen Vorgänger **Extensible Firmware Interface** (kurz **EFI** genannt) beschreiben die zentrale Schnittstelle zwischen der Firmware, den einzelnen Komponenten eines Rechners und dem Betriebssystem. Es sitzt logisch gesehen unterhalb des Betriebssystems und ist der Nachfolger des PC-BIOS, mit Fokus auf 64-Bit-Systeme. Ein Bestandteil aktueller UEFI-Versionen ist **Secure Boot**, das das Booten auf vorher signierte Bootloader beschränkt und so Schadsoftware oder andere unerwünschte Programme am Starten hindert.

UEFI


Betriebssystem
Extensible Firmware Interface
Firmware
Hardware

U E F I

- **Entstehung:**

  Intel und Microsoft wollen das fast 35 Jahre alte (Stand 2015) x86-BIOS durch das *Extensible Firmware Interface* (EFI) ersetzen, weil dieses bessere Voraussetzungen für zukünftige Computergenerationen bieten soll. Im März 2006 kündigte Microsoft jedoch an, dass Vista EFI zunächst nicht unterstützen soll und es später nur für die 64-bit-Varianten nachgerüstet wird. Heute wird es als Unified Extensible Firmware Interface (UEFI) verwendet, beispielsweise bei Windows 8. Im Januar 2006 stellte Apple die Architektur der Macintosh-Rechner von PowerPC auf Core-Prozessoren von Intel um. Als erstes Modell kam der iMac der vierten Generation mit EFI auf den Markt und war somit auch der erste x86-Computer mit EFI.

U E F I

- **Ziel:**
  - UEFI soll einfacher zu bedienen sein als herkömmliche BIOS-Implementierungen.
  - Zudem sollen die Anwender beim Systemstart auswählen können, welche Bestandteile des verwendeten Betriebssystems geladen werden sollen, beispielsweise könnten fehlerhafte Treiber deaktiviert werden.
  - Auch soll von den grafischen Möglichkeiten moderner Hardware Gebrauch gemacht werden, und es soll möglich werden, Fehler mit Hilfe von Netzwerkverbindungen zu diagnostizieren.
  - Das ursprüngliche PC-BIOS erschien 1981 mit dem ersten IBM-PC und wird trotz vieler späterer Erweiterungen den Anforderungen moderner Hardware und Betriebssysteme schon seit einiger Zeit nicht mehr gerecht.

U E F I

- Insbesondere ist es nicht 64-bit-tauglich, und weitere „Flickschusterei-en“ in dieser Richtung erschienen Hardware-Herstellern (wie Intel oder AMD) nicht mehr tragbar.
- Maßgeblich für die Neuentwicklung EFI war eine Initiative von Intel, um einen Ersatz für das BIOS zur Verwendung in der IA64-Architektur zu finden.
- In dem 1998 gegründeten *Intel Boot Initiative (IBI)-Programm* wurde die Idee spezifiziert.
- Der eigentliche Nachfolger für das BIOS ist der *Firmware Foundation Code*, der zu den Bedingungen der CPL (Common Public License) freigegeben wird und das Extensible Firmware Interface implementiert.

U E F I

- **Unified EFI (UEFI):**
  - Zur Werbung und Weiterentwicklung von EFI wurde 2005 das *Unified EFI Forum* gegründet. Daran sind außer Intel auch AMD, Microsoft, Hewlett-Packard und viele andere PC- und BIOS-Hersteller beteiligt, so dass die nun als *Unified EFI* (UEFI) bezeichnete Schnittstelle nicht mehr allein von Intel festgelegt wird.
  - Im Januar 2006 wurde die EFI-Version 2.0 freigegeben.
  - Mit der Einführung von Windows 8 im Jahr 2012 wurde das UEFI in der Version 2.3.1 mit einem Secure-Boot-Mechanismus verstärkt eingeführt, der das Booten auf vorher signierte Bootloader beschränkt. Dies erhöht die Sicherheit beim Systemstart, indem Schadsoftware am Starten gehindert wird.

U E F I

- Andererseits wird der Aufwand für die Nutzung von z. B. Linux-Distributionen erhöht, da entweder *Secure Boot* deaktiviert oder ein signierter Kernel genutzt werden muss.
- Allerdings ist das Signieren eines Kernels mit Kosten verbunden, die die wenigsten Distributoren tragen wollen.
- Wie Forscher der Mitre Corporation Mitte 2014 bekannt gegeben haben, weist die Intel-Referenzimplementierung von UEFI eine Sicherheitslücke auf, die das dauerhafte Einschleusen von Malware ermöglicht. Genutzt wird hierfür eine fehlerhafte Update-Funktion, durch die es zu Integer-Overflows kommt und Schadcode ausführbar macht. Viele nehmen den Code der Intel-Referenzimplementierung als Basis für ihr UEFI.

U E F I

- **Techniken und Möglichkeiten:**

  Die EFI-Schnittstelle soll die Nachteile des seit den 1980er Jahren verbreiteten BIOS beseitigen und neue Möglichkeiten eröffnen. Dazu gehören laut EFI-Spezifikationen:

  – Einfache Erweiterbarkeit (z. B. für Digital Rights Management)
  – Eingebettetes Netzwerkmodul (zur Fernwartung)
  – Preboot Execution Environment (universelles Netzwerkboot-system)
  – Unterstützung für hochauflösende Grafikkarten schon beim Start des Computers

U E F I

- BIOS-Emulation (für Kompatibilität zu alten Betriebssystemen die UEFI nicht unterstützen und zu manch alter Firmware) durch ein „Compatibility Support Module“ (CSM) eine Shell, über die beispielsweise EFI-Applikationen (*.efi) aufgerufen werden können
- Treiber können als Modul in das EFI integriert werden, so dass sie nicht mehr vom Betriebssystem geladen werden müssen. Damit sind, wie bei Open Firmware, systemunabhängige Treiber möglich.
- Das System kann in einem Sandbox-Modus betrieben werden, bei dem Netzwerk- und Speicherverwaltung auf der Firmware laufen anstatt auf dem Betriebssystem.
- Das EFI bietet eine Auswahlmöglichkeit für die auf dem System installierten Betriebssysteme und startet diese; damit sind (den Betriebssystemen vorgeschaltete) Boot-Loader überflüssig.

U E F I

- Mit der GUID Partition Table (GPT) führt es einen flexibleren Nachfolger für auf dem Master Boot Record basierende Partitionstabellen ein. Die GPT ist not-wendig, um von einer Festplatte > 2 TB booten zu zu können bzw. Partitionen > 2 TB anlegen und verwalten zu können.

U E F I

- **UEFI und Secure Boot:**

  Aus Thomas-Krenn-Wiki:

  Secure Boot ist ein Teil der UEFI-Spezifikation, der die Echtheit bzw. Unverfälschtheit von wichtigen Software-Teilen der Firmware garantieren soll. Kritische Teile der Firmware, wie der OS-Loader, sollen nur mehr dann ausgeführt werden, wenn sie zuvor durch eine vertrauenswürdige Institution dazu autorisiert wurden. Dadurch werden unter anderem Rootkits ausgeschlossen, die sich schon vor dem Boot des Betriebssystems (OS) einnisten.

U E F I

Durch kryptografische Mechanismen wird verhindert, dass nicht vertrauenswürdige Software-Teile ausgeführt werden. Die Schlüssel in der UEFI-Firmware prüfen die Authentizität von z.B. Bootloadern. Ein Bootloader wird nur dann ausgeführt, wenn er eine gültige "Unterschrift" vorweist. Kann eine Unterschrift nicht überprüft werden bzw. ist sie nicht gültig wird das System am Starten gehindert. Entspricht z.B. die Unterschrift des Bootloaders nicht der, die die UEFI-Firmware erwartet, startet das System nicht.

Aktuelle Informationen:

UEFI Secure Boot - Where we stand (LCA2013, James Bottomley) (blog.hansenpartnership.com)

UEFI Secure Boot - The story behind and where Linux stands (LinuxTag 2013, Dr. Udo Seidel) (linuxtag.org)

UEFI

- **Vorteile von Secure Boot:**

  – Schutz vor Malware: Vor allem Rootkits, die sich in kritische Betriebssystemteile vor dem eigentlichen Boot einhängen, werden durch Secure Boot aufgedeckt.

  – Durch das Signatur-System kann Software gezielt ausgeschlossen werden und nur gewünschte Software zum Einsatz kommen.

UEFI

- **Nachteile von Secure Boot:**

  – Vor allem, dass sich der Platform Key (PK) nicht unter der Kontrolle des Endkunden befindet, entpuppt sich als Nachteil.

  – Für Secure Boot müssen alle Software-Teile entsprechend signiert werden. Auch zugehörige Hardware-Treiber für die Firmware. Für den nachträglichen Einbau von Hardware in Systemen muss sicher gestellt sein, dass sich der Key des Hardware-Herstellers des neuen Bauteils auf dem System befindet.

U E F I

- **Wahl des Betriebssystems:**

  – Alternative Betriebssysteme bzw. Dual-Boot-Konfigurationen werden durch Secure Boot erschwert. Die Tatsache, dass Linux-Installationen nur mehr nach einer manuellen Deaktivierung von Secure Boot in der UEFI-Firmware vorgenommen werden können, ergeben ein weiteres Hindernis beim Einsatz von Linux.

  – Beim Dual-Boot müsste sogar ständig zwischen Secure und Nicht-Secure Boot gewechselt werden, um signierte und nicht signierte Betriebssysteme zu starten.

U E F I

- **Alternativen:**

  Für PowerPC-und SPARC-Rechner wurde vor geraumer Zeit bei Unix-Workstations und Servern der plattform- und prozessor-unabhängige Forth-basierte Industriestandard Open Firmware (IEEE-1275) spezifiziert. Wesentliche technische Vorteile von Intels Eigenentwicklung EFI gegenüber Open Firmware, abgesehen von wesentlich gesteigerter Ausführungsgeschwindigkeit (Vergleich Mac mit Open Firmware zu Mac (gleicher Jahrgang) mit EFI), sind nicht bekannt.

  Eine weitere Alternative ist die unter der GPL-Lizenz stehende Firmware coreboot (ehemals *LinuxBIOS*). Coreboot ist ein Minimalsystem, das lediglich die Hardware soweit initialisiert, dass ein anderes Programm (eine sogenannte *Payload*) aufgerufen werden kann, etwa ein Linux-Kernel, ein Bootloader wie etwa GRUB, Open Firmware oder diverse andere.

UEFI

- **Betriebssysteme – x86-Windows:**
  - Seit Windows 2000 gibt es Versionen von Windows für die IA64 Architektur. Da EFI ein zwingender Bestandteil dieser Plattform ist, unterstützt jede IA64-Version von Windows somit auch EFI.
  - Für Endanwender unterstützt Windows EFI ausschließlich in den 64-Bit-Varianten ab Windows Vista mit integriertem Service Pack 1 bzw. Windows Server 2008.
  - Für den Windows-7-Nachfolger Windows 8 wird EFI 2.x empfohlen. Systeme mit Systemplatten größer als 2 Terabyte und Systeme mit ARM-Prozessor benötigen EFI zwingend.
  - Alle vorherigen Windows-Versionen für die x86-Architektur funktionieren nur, wenn eine BIOS-Kompatibilitätsschicht (CSM) vorhanden ist.

U E F I

- **Betriebssysteme – Linux:**

  EFI wird auch von Linux unterstützt. Der stabile Zweig des Linux-Kernels bietet seit Version 2.6.25 auch für die x86-Architektur Unterstützung für EFI. Seit dem Erscheinen der ersten Itanium-Systeme entwickelt HP den Bootloader *elilo*. Dieser ist zwar für IA-64 ausgelegt, lässt sich aber ebenfalls auf IA-32 verwenden – eine Portierung von elilo auf x86-64 befindet sich aber noch im Beta-Stadium. Als Alternative zu elilo kann auch GRUB 2 für EFI-PCs verwendet werden. Fedora unterstützt ab Version 17 EFI in der Installation und richtet das System entsprechend ein, um mit EFI arbeiten zu können. Debian unterstützt EFI seit Version 7.0 *Wheezy* mit einem eigenen Bootloader.

U E F I

- **Betriebssysteme – OS X:**

  Die im Januar 2006 vorgestellten und alle nachfolgenden Apple Macintosh-Rechner mit OS X, die auf Intel-CPUs und Chipsätzen basieren, verwenden ebenfalls EFI als Firmware. Damit sind sie – zusammen mit einigen Media-Center-PCs wie etwa dem Gateway 610 aus dem Jahr 2003 – die ersten EFI-basierten Massenmarkt-computer. Die ausschließliche Nutzung des EFI ohne die optionale BIOS-Kompatibilitätsschicht verhinderte zunächst das Booten von Windows XP auf Intel-basierten Macintosh-Rechnern. Bald wurde aber durch das Projekt *xom* eine BIOS-Emulation implementiert, die das Starten von Windows ermöglichte.

  Apple rüstete den „BIOS Layer“ nach einigen Monaten durch eine Firmware-Aktualisierung nach und bot bis Mitte Oktober 2007 eine kostenlose, „Boot Camp“ genannte Lösung an, die es ermöglicht, OS X und Windows XP auf zwei Partitionen desselben Rechners

U E F I

zu installieren und durch Neustart (Booten) zwischen den Betriebssystem hin- und herzuwechseln („Dualboot-Lösung“).

Seit Erscheinen von Mac OS X 10.5 (Leopard) ist Boot Camp standardmäßig auf allen Intel-Macs vorinstalliert. Die Beta-Version von Boot Camp, die auch auf Mac OS X 10.4 lief, ist inzwischen offiziell nicht mehr lauffähig.

Mit EFi-X erschien im Sommer 2008 nachrüstbare Firmware für PCs, mit der die Installation von OS X von einer unmodifizierten, handelsüblichen Original-DVD auf ausgewählter Hardware anderer Hersteller ermöglicht wird, die sich hauptsächlich aus einer Kombination von Gigabyte-Hauptplatinen mit bestimmten Nvidia- und ATI-Grafikkarten zusammensetzt. Die *EFi-X*-Firmware ist dabei auf einem USB-Dongle untergebracht, der auf einen internen USB-Steckplatz der Hauptplatine gesteckt wird. Beim Systemstart werden daraufhin eine EFI-Emulation und ein „Multiboot-Manager“

U E F I

geladen, über den neben OS X auch Windows XP, Vista oder Linux gestartet werden können.

Mittlerweile gibt es auch den Bootloader *Chameleon*, mit dem der OS X-Kernel direkt geladen werden kann, oder *Clover*, welcher ein Macintosh-EFI vollständig softwareseitig emuliert.

Ebenso gibt es ozmosis was einen Platform-Treiber für OSX darstellt. Ein Dualbios wie auf Gigabyte Mainboards wird empfohlen da dort die Gefahr des "bricken" minimiert ist. Mac OS lässt sich von einem solchen PC direkt starten.

U E F I

- **Kritik:**

  EFI wurde dafür kritisiert, mehr Komplexität ins System zu bringen, ohne nennenswerte Vorteile zu bieten, und das vollständige Ersetzen mit einem Open-Source-BIOS wie OpenBIOS und coreboot unmöglich zu machen. Es löse nicht eines der langjährigen Probleme des BIOS – nämlich, dass die meiste Hardware zwei unterschiedliche Treiber benötigt. Es sei nicht klar, warum es nützlich sein soll, zwei komplett unterschiedliche Betriebssysteme gleichzeitig in Betrieb zu haben, die im Grunde dieselben Aufgaben erledigen, oder warum ein neues Betriebssystem von Grund auf neu geschrieben werden müsste.

U E F I

EFI gilt einem Entwickler von coreboot zufolge in sicherheits-kritischen Einsatzumgebungen – wie etwa in Banken – als ein mögliches Sicherheitsrisiko, da etwa mit dem implementierten Netzwerkstack die theoretische Möglichkeit bestünde, Daten unbemerkt vom Betriebssystem an eine beliebige Adresse zu senden. Der eigene Netzwerkstack für TCP/IP, der „unterhalb“ vom Betriebssystem direkt und unabhängig auf der Hauptplatine läuft, ermöglicht es, das System zu manipulieren, zu infizieren oder zu überwachen, ohne dass man es betriebssystemseitig kontrollieren oder einschränken könnte. Auch für DRM-Zwecke könnte EFI benutzt werden, um etwa den I/O-Datenstrom auf digitale Wasserzeichen hin zu überwachen. Aus diesen Gründen plädieren einige Anwender für ein quelloffenes System wie coreboot (ehemals *LinuxBIOS*).

U E F I

Fehlerhafte Implementationen von UEFI haben bei mehreren Herstellern zu irreparablen Schäden an Systemen geführt. Im Juni 2013 wurden Notebooks von Samsung beim Bootvorgang mit Linux eingefroren, sobald das Betriebssystem schreibend auf die UEFI-Firmware zugriff. Das Mainboard wurde dadurch unlösbar blockiert. Anfang 2014 trat das gleiche Problem bei Geräten von Lenovo auf und Ende 2015 bei Geräten von ASUS.

U E F I

Für das Treffen des Kreisseniorenrats Landkreis Böblingen am 3. März 2016 in Bondorf habe ich mich bereit erklärt, dieses Referat zu Thema BIOS / UEFI zu halten. Neben persönlichen Kenntnissen und Erfahrungen habe ich die vorliegenden Informationen überwiegend aus dem Internet bezogen.

Folgende Quellen habe ich „angezapft“:

Wikipedia	de.wikipedia.org
Microsoft	windows.microsoft.com/de
Thomas Krenn	www.thomas-krenn.com
Wintotal	www.wintotal.de
PC Magazin	www.pc-magazin.de

Der Ordnung halber möchte ich darauf hinweisen, dass ich keinen Anspruch auf Vollständigkeit und Richtigkeit erhebe und dass ich für Fehlinformationen nicht hafte.

Hans-Joachim Karnoll
09.02.2016

UEFI, das neue BIOS

E n d e