## PC-Start in 7 Sekunden

# Alles über UEFI 2.3.1

Quelle: com!-Magazin von Oliver Ehm - 01.08.2013


1. Teil: Alles über UEFI 2.3.1
2. Teil: Secure Boot und Measured Boot
3. Teil: Early Launch Anti-Malware

**Das UEFI-BIOS hat längst das klassische BIOS abgelöst. Die neue Version 2.3.1 verkürzt den PC-Start auf bis zu sieben Sekunden und enthält verschiedene Techniken zum Schutz vor Boot-Viren.**

Im Juni 2012 wurde die UEFI-Spezifikation 2.3.1 vom Unified EFI Forum verabschiedet. Alle PCs und Notebooks, die mit Windows 8 ausgeliefert werden, sind bereits mit dieser neuesten Version des UEFI-BIOS ausgerüstet.

Gegenüber den vorhergehenden Spezifikationen des UEFI-BIOS sind in der aktuellen Version fünf Neuerungen hinzugekommen, von denen Besitzer von Windows 8 besonders profitieren.

Diese fünf Techniken verkürzen etwa die Boot-Zeit von Windows 8 auf bis zu sieben Sekunden oder verhindern, dass Windows 8 von einem Bootkit oder Rootkit kompromittiert wird.

In dem folgenden Artikel lesen Sie, was hinter den Techniken Seamless Boot, Fast Boot, Secure Boot, Measured Boot und Early Launch Anti-Malware steckt und wie diese Techniken funktionieren.
Weitere Informationen zur Funktionsweise von UEFI lesen Sie im Artikel „So funktioniert UEFI“.

## Seamless Boot

Der klassische Boot-Vorgang erfolgte bislang in drei Phasen, die sich am Bildschirm verfolgen ließen.

Beim PC-Start wurde zunächst das BIOS geladen, das die Hardware initialisiert – etwa die Festplatten. Diese Phase ist am Monitor an den Meldungen des BIOS beziehungsweise an dem Logo des PC- oder Mainboard-Herstellers zu erkennen.

Im zweiten Schritt wird das Betriebssystem gestartet und man sieht die Boot-Animation von Windows. Am Ende des Boot-Vorgangs erscheint schließlich der Desktop.

Seamless Boot soll nun diese Phasen zusammenführen und einen grafisch einheitlichen Startprozess ermöglichen. So zeigen aktuelle PCs und Notebooks mit Windows 8 vom Anfang des Boot-Vorgangs bis zum Ende nur noch das Hersteller-Logo zusammen mit einer kleinen Boot-Animation an. Die drei Phasen verschmelzen so optisch zu einer einzigen.

## Fast Boot


***Turbostart:*** *Wählen Sie im UEFI-BIOS die Option „Ultra Fast“ aus. Die Startzeit von Windows 8 verkürzt sich dann auf bis zu sieben Sekunden*

PCs mit einem frisch installierten Windows starten in rund 37 Sekunden – zuzüglich der Zeit, die der PC für den Start des BIOS benötigt. Bis Sie mit Windows arbeiten können, vergeht so rund eine Minute.

PCs mit dem neuen UEFI-BIOS und einem installierten Windows 8 nutzen für den Start die Technik Fast Boot. Nach Angaben von Microsoft benötigt Windows 8 dann nur noch sieben Sekunden für den Start, wenn eine SSD eingebaut ist. Fast Boot wird im UEFI-BIOS aktiviert. Beim Mainboard-Hersteller Gigabyte zum Beispiel finden Sie die Funktion in den erweiterten Einstellungen auf der Registerkarte „BIOS Funktionen“. Wählen Sie hier bei „Schnelles Booten“ den Eintrag „Ultra Fast“ aus.

Speichern Sie die Einstellungen ab. Das UEFI-BIOS übernimmt jetzt die vollständige Kontrolle über die Hardware im PC und verwendet für den Start integrierte, standardisierte UEFI-Treiber. Auf diese Weise wird der klassische Initialisierungsprozess des BIOS drastisch verkürzt und Windows startet nach dem Einschalten des PCs fast augenblicklich.

Voraussetzung für den Turbostart ist eine UEFI-kompatible Grafikkarte. UEFI-kompatible Grafikkarten werden bislang nur vereinzelt angeboten. Manche Hersteller wie MSI, Asus oder Power Color stellen auf Anfrage auch für vereinzelte Modelle ein UEFI-kompatibles BIOS für Grafikkarten zur Verfügung, mit dem sich die Grafikkarte flashen lässt.

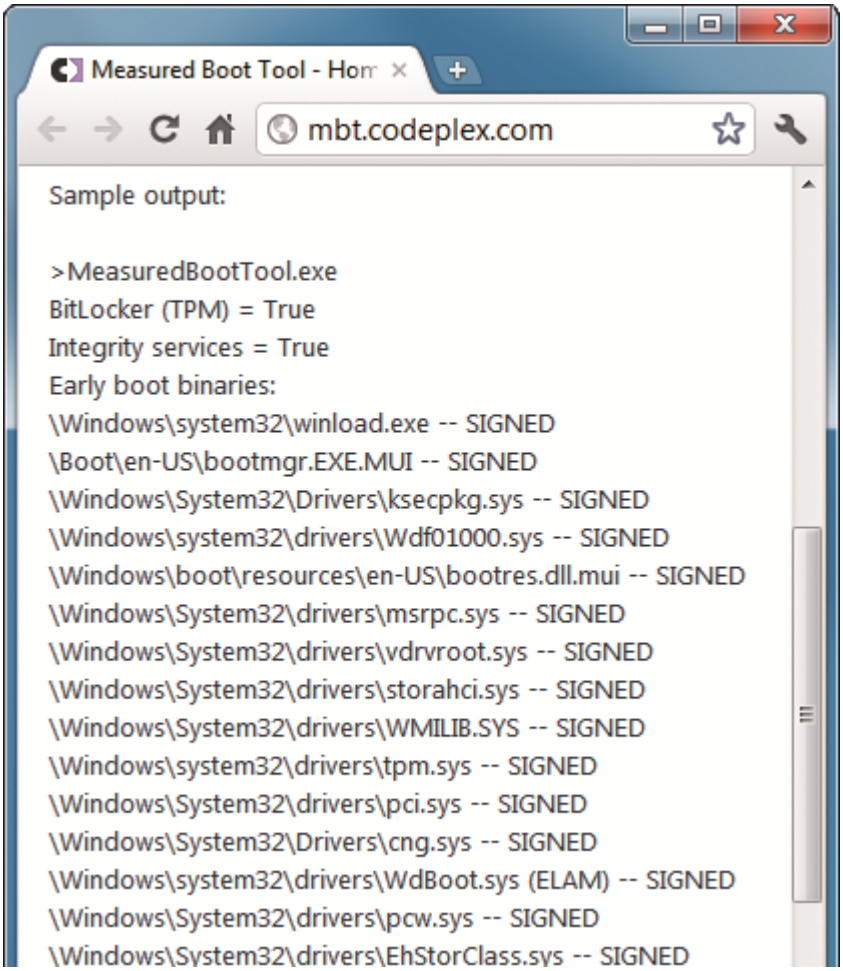
Die bislang einzigen Grafikkarten, die bereits UEFI-fähig sind, sind die in den Prozessor Ivy Bridge integrierten Grafikkerne von Intel.

Sie sollten mit Fast Boot nicht herumspielen, denn wenn die Grafikkarte nicht UEFI-kompatibel ist, dann bleibt der Bildschirm schwarz und Sie kommen nicht mehr ins UEFI-BIOS. In diesem Fall müssen Sie das UEFI-BIOS zurücksetzen. Auf Mainboards existiert dafür in der Regel der Jumper mit der Bezeichnung CLR_CMOS, den Sie kurzschließen müssen. Nehmen Sie dazu einen Schraubendreher oder einen gewöhnlichen Jumper. Nach der Überbrückung lässt sich das Setup des UEFI-BIOS wieder starten.

# Secure Boot und Measured Boot

von Oliver Ehm - 01.08.2013

## Secure Boot




***Measured Boot:*** *Die Technik erstellt ein Boot-Protokoll aller Treiber, die beim Start von Windows geladen werden – hier ein Auszug*

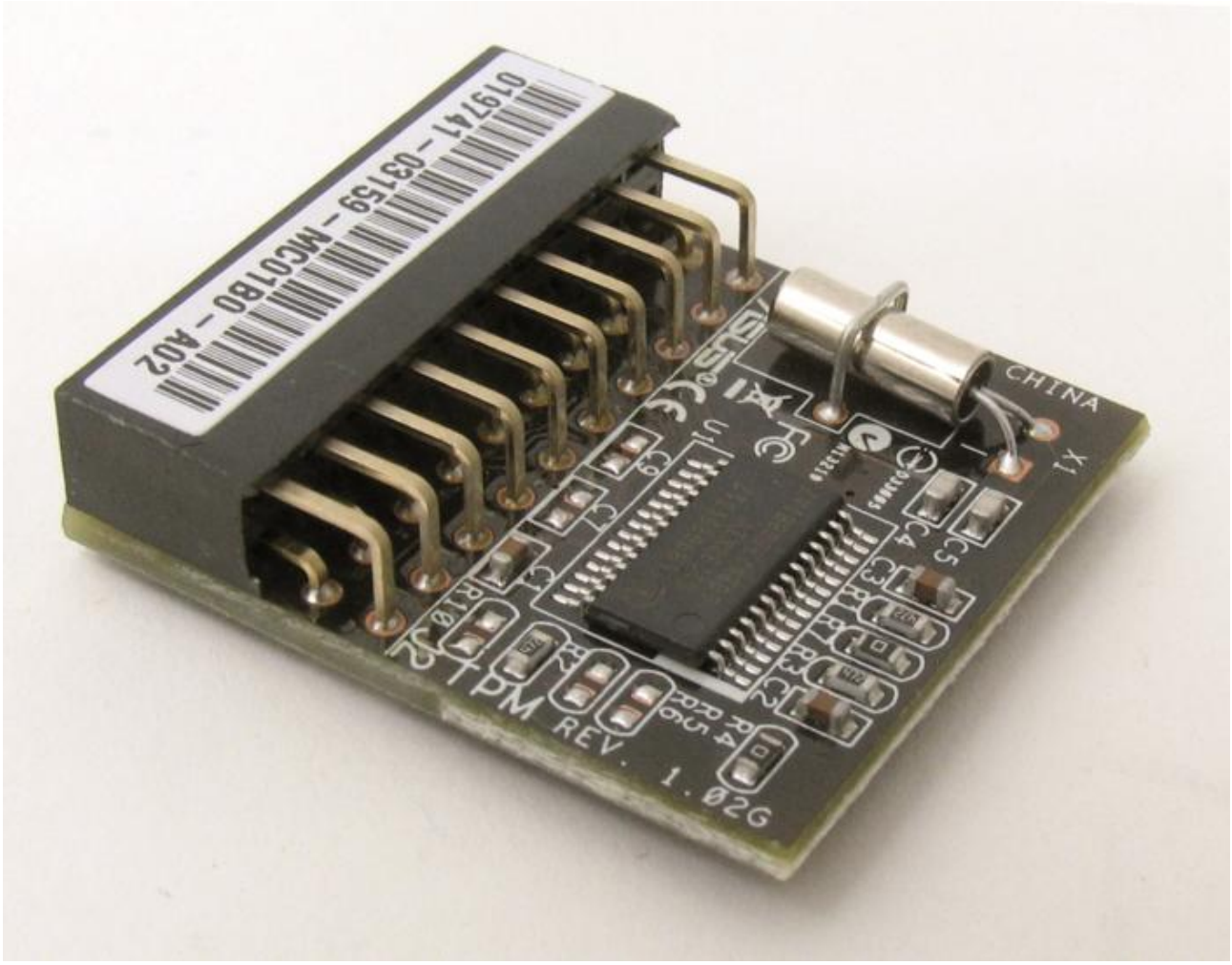
Die Sicherheitstechnik Secure Boot soll verhindern, dass ein Betriebssystem gestartet wird, das von einem Virus infiziert wurde.

Dazu prüft das UEFI-BIOS vor dem Start den Bootloader des Betriebssystems. Verläuft die Überprüfung erfolgreich, stellt das UEFI-BIOS das System als Boot-Option zur Verfügung.

Scheitert die Überprüfung, wird der Datenträger im Boot-Menü des UEFI-BIOS entweder gar nicht angezeigt oder der Boot-Prozess wird unmittelbar nach dem Start gestoppt und der Anwender erhält einen Hinweis.

## Measured Boot

In Verbindung mit einem TPM-Chip (Trusted Platform Module) lässt sich Measured Boot nutzen. Der Chip enthält Schlüssel für den Bootloader, den Kernel oder das UEFI-BIOS.




***TPM-Chip:*** *Um Measured Boot nutzen zu können, benötigen Sie ein solches Sicherheitsmodul*

Beim Start von Windows protokolliert Measured Boot den Start, vergleicht die Werte mit denen, die im TPM-Chip gespeichert sind, und erstellt daraus ein Protokoll.

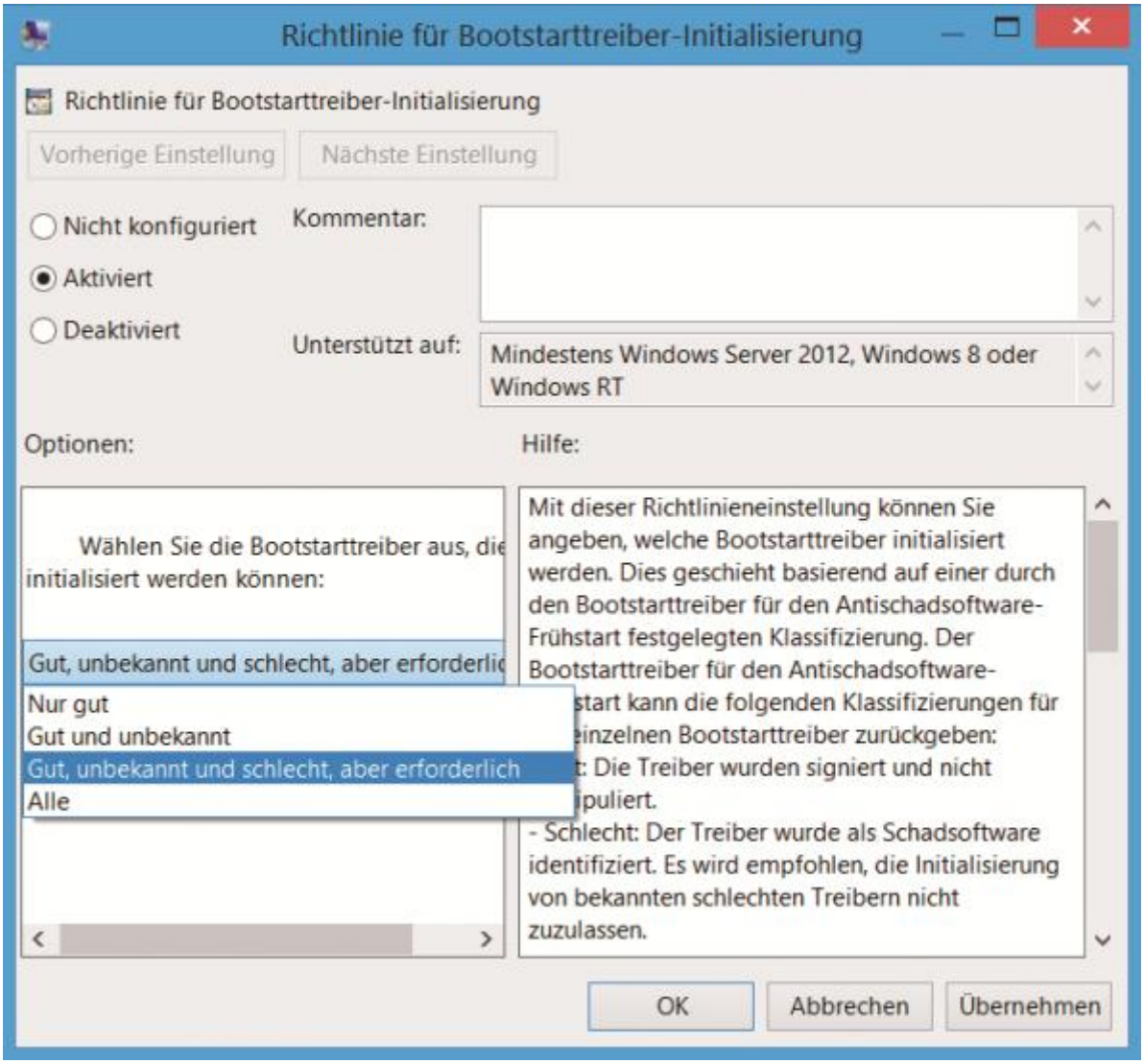
Das Protokoll übergibt Measured Boot an den Virenscanner und lässt von ihm prüfen, ob alles mit rechten Dingen zugegangen ist.

Das Protokoll speichert die Antivirensoftware im TPM-Chip ab. Es dient fortan als Referenz für die Kontrolle künftiger PC-Starts.

Der TPM-Chip lässt sich auf manchen Mainboards bereits für 11 Euro nachrüsten.

# Early Launch Anti-Malware

von Oliver Ehm - 01.08.2013
Bei der Sicherheitstechnik Early Launch Anti-Malware – kurz ELAM-Treiber – handelt es sich um einen Virenscanner, der nach Rootkits sucht. Der ELAM-Treiber ist Bestandteil von Windows 8 und wird unmittelbar nach dem Windows-Kernel gestartet. So kann er alle weiteren Treiber überprüfen, die Windows 8 beim Start lädt. Der ELAM-Treiber wird normalerweise beim Start vom UEFI-BIOS und – falls vorhanden – vom TPM-Chip überprüft, ob er eventuell selbst korrumpiert wurde.



***Virenschutz beim PC-Start:*** *Im Gruppenrichtlinien-Editor von Windows 8 können Sie das Verhalten des ELAM-Treibers individuell konfigurieren*

Der ELAM-Treiber ist Teil des in Windows 8 integrierten Virenscanners Defender. Wenn Sie eine andere Antivirensoftware installieren – etwa von Kaspersky oder Avast – wird der integrierte ELAMTreiber durch den der neuen Antivirensoftware ausgetauscht. Einzige Bedingung: Der Hersteller des Antivirenprogramms muss von Microsoft zertifiziert sein.

Die Funktionsweise des ELAM-Treibers ist recht eingeschränkt. So prüft er die geladenen Softwarekomponenten und Hardware-Treiber nur anhand von hinterlegten Prüfsummen und spürt so Bootkits oder Rootkits auf. Stimmen die gespeicherten Prüfsummen mit den aktuell ermittelten

nicht überein, wird der zu ladende Treiber blockiert. Die einzige Stelle, an der Sie den ELAMTreiber in Windows sehen können, ist der Gruppenrichtlinien-Editor. Unter „Computerkonfiguration, Administrative Vorlagen, System, Antischadsoftware-Frühstart“ nennt ihn Microsoft dort „Bootstarttreiber“.

## BIOS-Nachfolger

# So funktioniert UEFI

von Oliver Ehm - 27.06.2013

PCs haben heute kein BIOS mehr. Stattdessen wird der BIOS-Nachfolger UEFI verwendet. UEFI kann deutlich mehr als das alte BIOS. Viele PC-Anwender nutzen die Vorteile aber gar nicht.

Das Basic Input/Output System (BIOS) hat vor über 30 Jahren das Licht der Welt erblickt. Seitdem hat es sich optisch kaum verändert. Charakteristisch für das BIOS sind der blaue Hintergrund, die Klötzchenschrift und die mehr oder weniger kryptischen Optionen.

Der BIOS-Nachfolger UEFI ist nicht nur leichter zu bedienen, er leistet auch technisch deutlich mehr.

### Was bedeutet UEFI?


***UEFI in Aktion:*** *Der BIOS-Nachfolger ist in den meisten Fällen grafisch aufwendig gestaltet und lässt sich mit der Maus bedienen. Hier sehen Sie das UEFI des Mainboard-Herstellers Asus*

UEFI steht für Unified Extensible Firmware Interface. Wörtlich übersetzt heißt das etwa vereinheitlichte erweiterte Firmware-Schnittstelle. Gemeint ist damit eine leistungsstarke Schnittstelle zwischen Hardware und Betriebssystem.

## Was heißt „vereinheitlicht“?

Das klassische BIOS wurde seit der Einführung immer wieder von den PC- und Mainboard-Herstellern an die neuen Hardware-Gegebenheiten angepasst. Dabei wurde aber kein einheitlicher Weg verfolgt. Die Folge: Die BIOS-Versionen der Hersteller enthielten sehr unterschiedliche Einstelloptionen.

Bei UEFI ist das anders. Das UEFI-Forum – ein Zusammenschluss mehrerer Hardware-Hersteller wie Intel, AMD oder IBM – verabschiedet Spezifikationen, die den Rahmen abstecken, in dem sich die Hersteller bewegen dürfen.

## UEFI — das neue BIOS

Ähnlich wie beim Betriebssystem eines Smartphones sind damit grundlegende Funktionen vorgegeben, die jeder Hersteller einhalten muss. Der Artikel „Alles über UEFI 2.3.1“ beschreibt die allgemeinverbindlichen Funktionen der neusten UEFI-Version.

Darüber hinaus können die Hersteller aber ihre UEFI-Version auch individuell anpassen.

*zum Anfang*