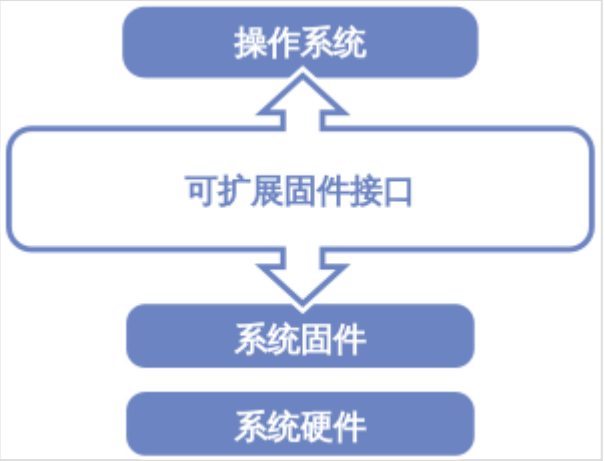
統一可延伸韌體介面

統一可延伸韌體介面（英語：Unified Extensible Firmware Interface，缩写**UEFI**）是一种個人電腦系统規格，用來定義作業系統與系統固件之間的軟件界面，作為BIOS的替代方案[1]。可扩展固件接口負責加電自檢（POST）、联系作業系統以及提供連接作業系統與硬體的介面。



可扩展固件接口在软件层次中的位置

UEFI的前身是Intel在1998年开始開發的Intel Boot Initiative，后来被重命名为**可延伸韌體介面**（Extensible Firmware Interface，缩写**EFI**）。Intel在2005年将其交由统一可扩展固件接口论坛（Unified EFI Forum）來推廣與發展，為了凸顯這一點，EFI也更名為UEFI（Unified EFI）。UEFI论坛的創始者是11家知名電腦公司，包括Intel、IBM等硬件廠商，軟件廠商Microsoft，及BIOS廠商安邁科技、Insyde、Phoenix。

規格

可延伸韌體介面（EFI）最初是由英特尔开发，于2002年12月英特尔释出其订定的版本——1.1版，之后英特尔不再有其他关于EFI的规范格式发布。有关EFI的规范，英特尔已于2005年将此规范格式交由UEFI论坛来推广与发展，后来并更改名称为**Unified EFI**（UEFI）。UEFI论坛于2007年1月7日释出并发放2.1版本的规格，其中较1.1版本增加与改进了加密编码（cryptography）、网络认证（network authentication）与用户接口架构（User Interface Architecture）。

相关方面的制定

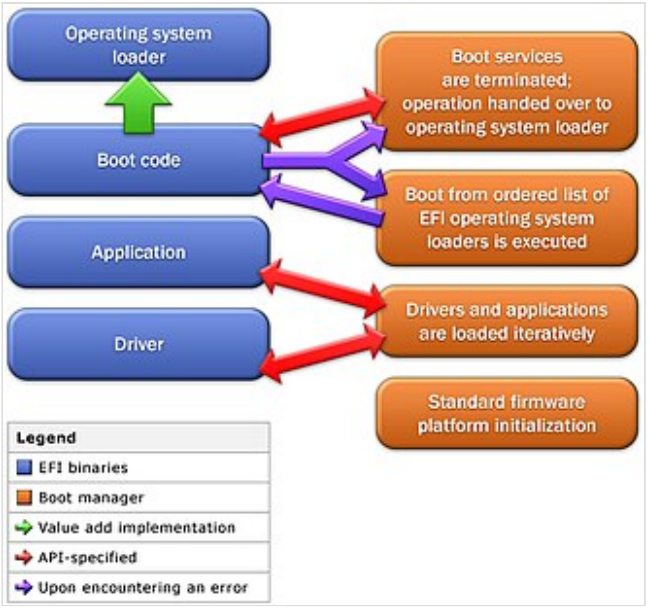
2009年5月9日，发布2.3版本。截至今日为止，2.9版是最新的公开的版本。

产生

众所周知，英特尔在近二十年来引领以x86系列处理器为基础的PC技术潮流，其产品如CPU，芯片组等在PC生产线中占据绝对领导的位置。因此，不少人认为此舉显示英特尔公司欲染指固件产品市场的野心。事实上，EFI技术源于英特尔安腾处理器（Itanium）平台的推出。安腾处理器是英特尔瞄准服务器高端市场投入近十年研发力量设计产生的与x86系列完全不同的64位新架构。在x86系列处理器进入32位的时代，由于相容性的原因，新的处理器（80386）保留16位的运行方式（实模式），此后多次处理器的升级换代都保留这种运行方式。甚至在包含EM64T技術的至强系列处理器中，处理器加电启动时仍然会切换到16位的实模式下运行（BIOS）。英特尔将这种情况归咎于BIOS技术的发展缓慢。自从IBM PC兼容机厂商通过净室的方式复制出第一套BIOS源程序，BIOS就以16位汇编代码，寄存器参数调用方式，静态链接，以及1MB以下内存固定编址的形式存在十几年。虽然由于各大BIOS厂商近年来的努力，有许多新元素添加到产品中，如PnP

BIOS、ACPI、传统USB设备支援等等，但BIOS的根本性质没有得到任何改变。这迫使英特尔在开发新的处理器时，都必须考虑加进使效能大大降低的相容模式。用一個比喻來講：这就像保时捷新一代的全自排跑车，被人套上去一个蹩脚打檔器。

然而，安腾处理器并没有这样的顾虑，它是一个新生的处理器架构，系统固件和操作系统之间的接口都可以完全重新定义。并且这一次，英特尔将其定义为一个可扩展的，标准化的固件接口规范，不同于传统BIOS的固定的，缺乏文档的，完全基于经验和晦涩约定的一个事实标准。基于EFI的第一套系统产品的出现至今已经有五年的时间，如今，英特尔试图将成功运用在高端服务器上的技术推广到市场占有率更有优势的PC产品线中，并承诺在2006年间会投入全力的技术支持。



EFI開機管理員與 EFI drivers的溝通方式

与BIOS的比较

二者显著的区别就是UEFI是用模块化，C语言风格的参数堆栈传递方式，动态链接的形式构建的系统，较BIOS而言更易于实现，容错和纠错特性更强，缩短了系统研发的时间。它可以執行於x86-64、IA32、ARM等架構上（在個人電腦上通常是x86-64平台），突破传统16位代码的寻址能力，达到处理器的最大寻址。它利用加载UEFI驱动程序的形式，识别及操作硬件，不同于BIOS利用挂载真实模式中断的方式增加硬件功能。后者必须将一段类似于驱动程序的16位代码（如RAID卡的Option ROM）放置在固定的0x000C0000至0x000DFFFF之间存储区中，运行这段代码的初始化部分，它将挂载实模式下约定的中断向量向其他程序提供服务。例如，VGA图形及文本输出中断（INT 10h），磁盘存取中断服务（INT 13h）等等。BIOS以真實模式執行，因此这段記憶體空間很有限（在真實模式下僅能尋址最多1MB的記憶體），BIOS对于所需放置的驱动程序代码大小超过空间大小的情况无能为力。另外，BIOS的硬件服务程序都以16位代码的形式存在，这就给运行于保護模式或長模式的操作系统访问其服务造成了困难。因此BIOS提供的BIOS中斷呼叫在现实中只能提供给作業系統的啟動程式或MS-DOS类操作系统使用[2]。而UEFI系统下的驱动程序可以由EFI Byte Code（EBC）编写而成，EFI Byte Code是一组专用于EFI驱动程序的虚拟机器语言，必须在UEFI驱动程序运行环境（Driver Execution Environment，DXE）下被解释运行。由于UEFI驱动程序开发简单，所有的PC部件提供商都可以参与，情形非常类似于现代操作系统的开发模式，这个开发模式曾使Windows在短短的两三年时间内成为功能强大，性能优越的操作系统。基於UEFI驅動模型（UEFI driver model，UDM）可以使UEFI系統接觸到所有的硬體功能，在作業系統執行以前瀏覽全球資訊網站，實現圖形化、多語言的BIOS設定界面，或者無需執行作業系統即可線上更新BIOS等等不再是天方夜譚，甚至实现起来也非常简单。这对基于传统BIOS的系统来说是件难以实现的任务，在BIOS中添加几个简单的USB设备支持都曾使很多BIOS设计师痛苦万分，更何况除了添加对无数网络硬件的支持外，还得凭空构建一个16位模式下的TCP/IP协议栈。

一些人认为BIOS只不过是由于兼容性问题遗留下来的无足轻重的部分，不值得为它花费太大的升级努力。而反对者认为，当BIOS的出现约制了PC技术的发展时，必须有人对它作必要的改变。

与操作系统的关系

UEFI在概念上类似于一个低阶的操作系统，并且具有操控所有硬件资源的能力。不少人感觉它的不断发展将有可能代替现代的操作系统。事实上，EFI的缔造者们在第一版规范出台时就将EFI的能力限制于不足以威胁操作系统的统治地位。首先，它只是硬件和预启动软件间的接口规范；其次，UEFI环境下不提供中断的机制，也就是说每个UEFI驱动程序必须用轮询（polling）的方式来检查硬件状态，并且需要以解释的方式运行，较操作系统下的机械码驱动效率更低；再则，UEFI系统不提供复杂的缓存器保护功能，它只具备简单的缓存器管理机制，具体来说就是指运行在x64或x86处理器的長模式或保护模式下，以最大寻址能力为限把缓存器分为一个平坦的段（Segment），所有的程序都有权限存取任何一段位置，并不提供真实的保护服务。当UEFI所有组件加载完毕时，便會啟動作業系統的啟動程式，如果UEFI韌體內建UEFI Shell，也可以启动UEFI Shell命令提示。UEFI應用程式（UEFI Application）和UEFI驅動程式（UEFI driver）是PE格式的.efi檔案，可用C語言編寫。在UEFI開機模式下，作業系統的啟動程式也是UEFI應用程式，啟動程式的EFI檔案儲存在EFI系統分區（ESP）上[3]。

UEFI韌體區分架構，在UEFI開機模式下，通常只能執行特定架構的UEFI作業系統和特定架構的EFI應用程式（EBC程式除外）。比如，採用64位元UEFI韌體的PC，在UEFI開機模式下只能執行64位元作業系統啟動程式；而在Legacy開機模式（即BIOS相容開機模式）下，既可以執行16位元的作業系統（如DOS），也可以執行32位元作業系統和64位元作業系統。

组成

一般认为，UEFI由以下几个部分组成：

1. Pre-EFI初始化模块（PEI）
2. UEFI驱动程序执行环境（DXE）
3. UEFI驱动程序（UEFI driver）
4. 兼容性支持模块（CSM）
5. UEFI高层应用（UEFI Application）
6. GUID磁盘分区表
7. 系統管理模式（SMM）

Pre-EFI初始化程序在系统开机的时候最先得到执行，它负责最初的CPU，晶片組及主記憶體的初始化工作，紧接着载入UEFI的驱动程序执行环境（DXE）。当DXE被载入运行时，系统便具有了枚举并加载其他UEFI驱动程序的能力。DXE枚举并加载各种总线（包括PCI、SATA、USB、ISA）及硬體的UEFI驱动程序。例如一个具PCI-E总线接口的RAID存储适配器，其UEFI驱动程序一般会放置在这个设备的Option ROM中。在UEFI规范中，一种突破传统MBR磁盘分区结构限制的GUID磁盘分区系统（GPT）被引入，新结构中，磁盘的主分区数不再受限制（在MBR结构下，只能存在4个主分区），另外UEFI+GPT结合还可以支持2.1 TB以上硬盘。在众多的分区类型中，EFI系统分区可以被UEFI固件存取，可用于存放操作系统的引导程序。UEFI韌體通過執行EFI系統分區中的啟動程式啟動作業系統。CSM是在x86平台UEFI系统中的一个特殊的模块，它将为不具备UEFI引导能力的操作系统以及16位的传统Option ROM提供类似于传统BIOS的系统服务。在載入作業系統後，UEFI的SMM程式繼續執行，提供ACPI等服務[4]。

发展

英特尔无疑是推广EFI的积极因素，近年来由于业界对其认识的不断深入，更多的厂商正投入这方面的研究。包括英特尔，AMD在内的一些PC生产厂家联合成立了UEFI论坛。另外各大BIOS提供商如Insyde，Phoenix，AMI等，他们原先被认为是EFI发展的阻碍力量，现在也不断的推出各自的解决方案。分析人士指出，这是由于BIOS厂商在EFI架构中重新找到了诸如Pre-EFI启动环境之类的市场位置，然而随着EFI在PC系统上的成功运用，以及英特尔新一代芯片组的推出，这一部分市场份额将会不出意料的在英特尔的掌控之中。2011年以後生產的零售主機板大多數採用UEFI技術。隨後，微軟又要求，預裝Windows 8的電腦，必須採用UEFI開機模式，以及Secure Boot。部分採用EFI技術的BIOS並不支援EFI開機。

作業系統支援

Linux內核自2000年開始，已經支援EFI啟動。早期使用ELILO作為EFI下的啟動程式。現在，GRUB的EFI版本已代替ELILO，大多數Linux發行版已使用GRUB作為UEFI下的啟動程式。從Linux版本3.15起，來自英代爾的工程師Matt Fleming將64位元核心提供了支援32位元UEFI韌體的可能，前提只需要UEFI作業系統啟動程式支援EFI handover協定[5]，譬如流行的GRUB2。同樣流行的32位元版Linux，譬如Ubuntu 16.04.3 LTS，也可以使用這類啟動程式在64位元版UEFI韌體的機器上使用。

安騰版本的Windows 2000已於2002年加入對EFI 1.10的支持。安騰版本的Windows Server 2003和Windows XP 64-Bit Edition（以IA-64架構作為執行平台）已支援EFI。

從Windows Vista SP1開始，x86-64架構的Windows作業系統已支援UEFI。但是，若在UEFI模式下安裝和啟動Windows Vista SP1或Windows 7，需要在UEFI韌體設定中開啟CSM[6]，因為在Windows 8之前的版本中，均不支援UEFI標準的“圖形輸出協議”（GOP），只支持用於傳統BIOS的VESA BIOS Extension。32位元的Windows Vista和Windows 7不支援UEFI啟動。從Windows 8開始，支援Secure Boot，UEFI模式下的啟動亦無須CSM。

現在，x86-64架構的FreeBSD、OpenBSD和NetBSD已支援UEFI。

虛擬機器對UEFI的模擬

VMware Workstation支援對UEFI的模擬，但是在VMware Workstation 11以前，VMware Workstation並未正式支援UEFI，需要手動編輯虛擬機的.vmx檔案以開啟虛擬機器的UEFI。VMware Workstation 11及以後的版本正式支援對UEFI的模擬。從VMware Workstation 14開始支援Secure Boot。

VirtualBox支援對UEFI的模擬，但是VirtualBox的UEFI並不支援Windows Vista和Windows 7。

QEMU/KVM可通過OVMF支援對UEFI的模擬。

微軟Hyper-V的第二代虛擬機器支援對UEFI的模擬，以及Secure Boot。

Parallels Desktop不僅提供全規格的UEFI支援，並支援在作業系統不支援“圖形輸出協議”（GOP）的情況下回退至傳統BIOS

採用UEFI韌體的x86/x64系統類別

類別0，這類系統使用x86 BIOS韌體，只支援傳統作業系統。

類別1，這類系統採用支援UEFI和Pi規範的韌體，啟用CSM層功能，只支援傳統作業系統。

類別2，這類系統採用支援UEFI和Pi規範的韌體，啟用CSM層功能，同時支援傳統和UEFI啟動的作業系統。

類別3，這類系統採用支援UEFI和Pi規範的韌體，不再提供或完全關閉CSM層功能，只支援由UEFI啟動的作業系統。

類別3+，在類別3的系統基礎上提供並啟用Secure Boot功能。

微軟公司的Windows 11僅可用於類別3+型電腦[7]，Windows 8及Windows 10適用於上述所有類別的電腦，x64型版的Windows Vista SP1和Windows 7，以及不支援UEFI韌體的作業系統僅可用於類別0至類別2型電腦。所有支援UEFI啟動的Linux作業系統適用於類別0至類別3型電腦，多數現行分發版也支援類別3+中的Secure Boot功能，譬如Ubuntu等。 Intel计划将于2020年推出的UEFI Class 3规范中，将CSM層功能舍弃，不再支援由當年IBM公司制定的BIOS平台，Intel旗下的所有产品将遵循UEFI類別3（有一部分产品可能是3+）型規範[8]。

批評

Ronald G. Minnich（coreboot的共同作者）和科利·多克托羅和數位權利運動者批評EFI是企圖藉由禁止使用者完整控制他們的電腦，來保護智慧財產權。[9][10]它並沒有解決BIOS長期以來對多數硬體需要兩種不同驅動程式的問題－－一個給韌體，一個給作業系統。[11]

TianoCore（一個提供製作基於UEFI自由韌體工具的開放原始碼專案）[12]缺乏用來啟動晶片組的專門的驅動程式，因此需要晶片組廠商提供額外的功能。TianoCore是coreboot的一個附加選項，它包含了啟動晶片組的程式碼。

由於UEFI比起原先的BIOS技術可以對遠端網路開機提供更高的彈性，因此在標準的安全規定有一些疑慮。[13]

Secure Boot

中文名又译作“**安全启动**”，该协议定义在UEFI 2.3.1 Errata C規範中。Secure Boot只允許載入有適當數位簽章的EFI驅動程式和EFI啟動程式，因此Secure Boot可讓開機過程更安全。

但是Red Hat開發者Matthew Garrett在他的文章"UEFI secure booting"中憂慮UEFI的Secure Boot功能可能會影響Linux（貼有Windows 8認證貼紙的機器，預設Secure Boot啟動，只預載了OEM和微軟金鑰，可能無法以Linux開機）。[14][15]微軟回應稱顧客可以停用UEFI韌體中的secure boot。[16][17]然而，某些OEM廠商仍然可能在其產品中省略這項功能。不久，報告指出微軟顯然禁止在ARM系統上實作停用Secure Boot的功能。[18][19]

自由軟體基金會（FSF）的Josh Gay對UEFI的"Secure Boot"實作提出憂慮，並發表公開聲明及連署說：

> 我們—連署者—敦促所有實作了UEFI中稱為"Secure Boot"的電腦製造商立即允許自由的作業系統可以被安裝。基於尊重使用者的自由權以及確切保護使用者安全，製造商必須允許電腦擁有者停用開機限制，或是提供一個確切可能的方法讓他們安裝並執行自由的作業系統。我們承諾我們將不會購買、也不會推薦剝奪使用者重要自由的電腦，並且，我們將積極地敦促社會大眾避免如此禁錮使用者的系統。[20][21]

2012年1月，微軟釋出一份關於OEM硬體認證的文件，指出所有的x86和x86-64裝置應該將UEFI Secure Boot啟動，不過可以改用一個可讓使用者增加數位簽章的自訂Secure Boot模式。然而，无法在运行Windows的ARM设备上修改或禁用Secure Boot。[18]。這份稱為Windows硬體認證需求（英語：Windows Hardware Certification Requirements）[22]證實了執行Windows 8、基於ARM的裝置被禁止了任何安裝其他作業系統的可能性。現在，Ubuntu、Fedora、openSUSE、RHEL（從RHEL 7開始）、CentOS（從CentOS 7開始）、Debian（从Debian 10开始）等Linux發行版已經支援Secure Boot。Windows 8、Windows 8.1、Windows 10支援Secure Boot。

注釋

1. Kinney, Michael. Solving BIOS Boot Issues with EFI (PDF). Intel DeveloperUPDATEMagazine: 1. [2008-02-18]. （原始内容存档 (PDF)于2007-11-28）.
2. 存档副本. [2020-09-12]. （原始内容存档于2021-04-17）.
3. 存档副本. [2020-09-12]. （原始内容存档于2021-04-17）.
4. 存档副本. [2020-09-12]. （原始内容存档于2017-05-26）.
5. Linux kernel 3.15, Section 1.3. EFI 64-bit kernels can be booted from 32-bit firmware. kernelnewbies.org. 2014-06-08 [2014-06-15]. （原始内容存档于2018-06-11）.
6. UEFI 的 Windows 支援, Microsoft, [2017-11-25], （原始内容存档于2017-12-01）
7. Windows 11 規格 - Microsoft. Windows. [2021-07-08]. （原始内容存档于2021-11-18） （中文（臺灣））.
8. Richardson, Brian. "Last Mile" Barriers to Removing Legacy BIOS (PDF). 30 October 2017 [22 November 2017]. （原始内容存档 (PDF)于2019-02-01）.
9. Interview: Ronald G Minnich. Fosdem. 2007-02-06 [2010-09-14]. （原始内容存档于2011-01-29）.
10. Cory Doctorow, The Coming War on General Purpose Computation, 2011-12-27 [2013-07-11], （原始内容存档于2013-02-10）
11. coreboot (aka LinuxBIOS): The Free/Open-Source x86 Firmware. YouTube. 2008-10-31 [2010-09-14]. （原始内容存档于2020-11-21）.
12. Welcome, TianoCore, SourceForge, （原始内容存档于2012-04-23）.
13. Risks, UK: NCL, [2012-01-19], （原始内容存档于2021-03-14）.
14. Garrett, Matthew. UEFI secure booting. [2011-09-20]. （原始内容存档于2021-04-27）.
15. Garrett, Matthew. UEFI secure booting. [2011-09-23]. （原始内容存档于2021-04-27）.

16. MS denies secure boot will exclude Linux. The Register. 2011-09-23 [2011-09-24]. （原始内容存档于2020-04-22）.
17. Protecting the pre-OS Environment with UEFI. Microsoft. 2011-09-22 [2011-09-24]. （原始内容存档于2012-08-10）.
18. 存档副本. [2012-01-19]. （原始内容存档于2021-04-19）.
19. 存档副本. [2017-03-07]. （原始内容存档于2012-03-09）.
20. Gay, Josh. Will your computer's "Secure Boot" turn out to be "Restricted Boot"?. www.fsf.org. Free Software Foundation. [2011-10-25]. （原始内容存档于2021-04-27）.
21. Stand up for your freedom to install free software. www.fsf.org. Free Software Foundation. [2011-10-25]. （原始内容存档于2021-04-19）.
22. 存档副本 (PDF). [2014-04-24]. （原始内容 (PDF)存档于2014-06-11）.

參見

- BIOS
- ACPI
- SMBIOS
- x86-64
- 统一可扩展固件接口论坛

外部链接

- 官方网站 (https://uefi.org/) （页面存档备份 (https://web.archive.org/web/20100105051711/http://www.intel.com/technology/efi/)，存于互联网档案馆）
- 统一可扩展固件接口论坛 (http://www.uefi.org) （页面存档备份 (https://web.archive.org/web/20080905205125/http://www.uefi.org/)，存于互联网档案馆）
- 英特尔公司对EFI的标准实现：Intel EFI创新架构 (http://www.intel.com/technology/framework/) （页面存档备份 (https://web.archive.org/web/20110821043030/http://www.intel.com/technology/framework/)，存于互联网档案馆）
- 英特尔公司发起的EFI核心实现的一个半开源的计划TianoCore (http://www.tianocore.org) （页面存档备份 (https://web.archive.org/web/20210428095130/http://www.tianocore.org/)，存于互联网档案馆）