

UEFI

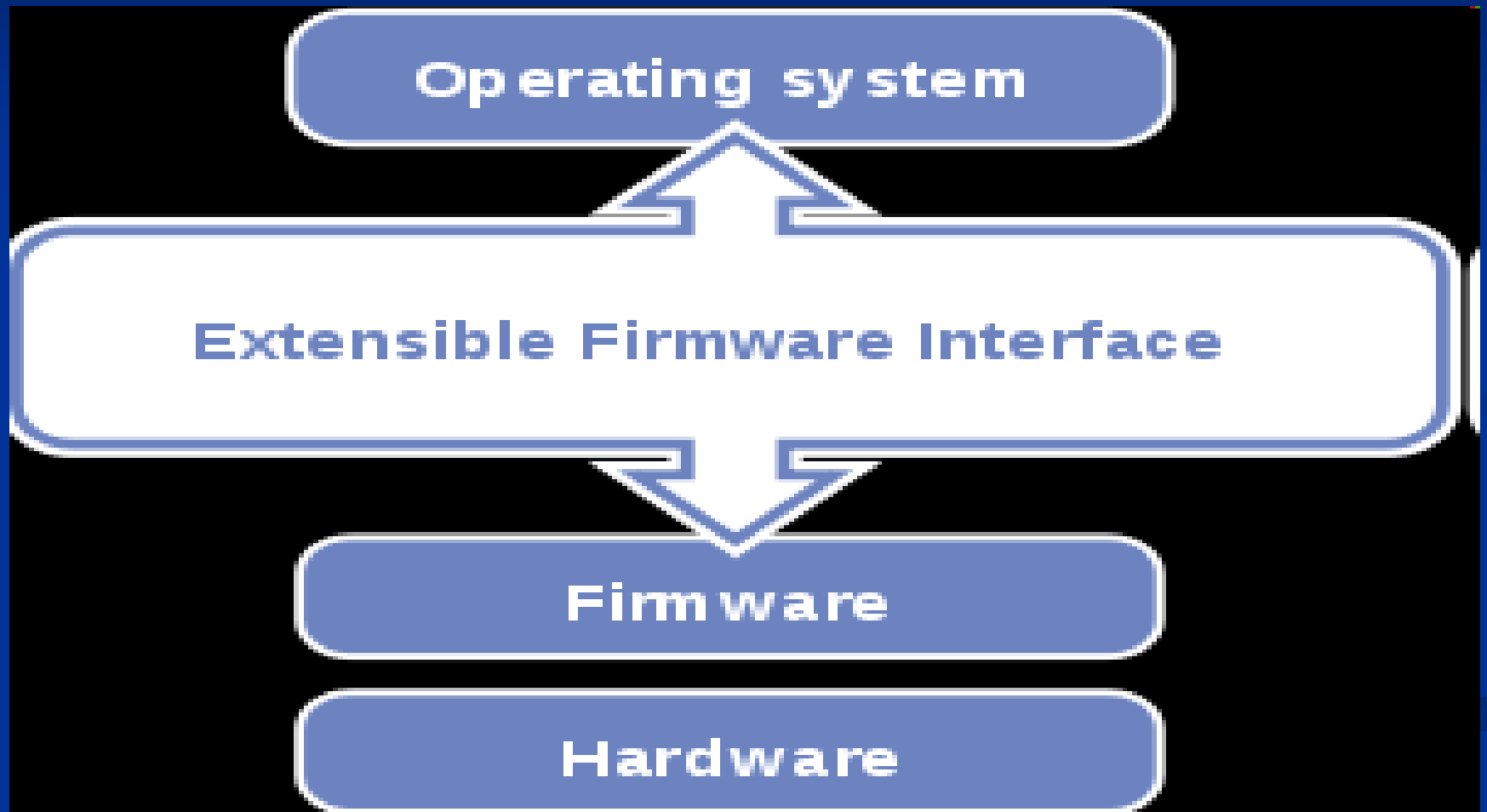
Důvod nástupce BIOSU

- BIOS má 2 základní nedostatky:
 - Je založen na 16 bitovém assembleru
 - nemůže tedy využít moderní 64b HW
 - Neexistuje jednotná specifikace
 - Každý výrobce si vše udělá podle sebe
- UEFI standard byl vytvořen více než 140 technologickými společnostmi pracujícími v rámci konsorcia UEFI (skupina Platform Initialization – PI)

Extensible Firmware Interface

- **Extensible Firmware Interface (EFI**, v překladu *rozšiřitelné firmwarové rozhraní*) je specifikace, která definuje softwarové rozhraní mezi OS a firmwarem použitého HW
- **EFI** je určeno jako významně vylepšená náhrada zastaralého firmwarového rozhraní BIOS, které se používalo během celé historie tzv. IBM kompatibilních PC – to je již 30 let

EFI



Historie EFI

- Původní záměr vytvořit EFI vznikl v počátcích vývoje prvních systémů Intel-HP Itanium v polovině 90. let 20. století. Omezení PC BIOSu (16bitový režim procesoru, 1 MB adresovatelného místa aj.) byla považována za nepřijatelná pro platformu větších serverů, na které se Itanium zaměřovalo. Původní pokus o řešení těchto problémů se nejprve nazýval **Intel Boot Initiative** a později byl přejmenován na Extensible Firmware Interface.
- EFI specifikace verze 1.02 byla vydána Intelem 12. prosince 2000.
- EFI specifikace verze 1.10 byla vydána Intelem 1. prosince 2002. Oproti 1.02 zahrnovala ovladačový model EFI a mnoho menších vylepšení.
- V roce 2005 Intel poskytl specifikaci UEFI Foru, které je nyní zodpovědné za vývoj a propagaci EFI. To bylo přejmenováno na Unified EFI (UEFI), ale ve většině dokumentace jsou oba termíny zaměnitelné.
- UEFI Forum vydalo 7. ledna 2007 UEFI specifikaci verze 2.1. Ta přidala a vylepšila šifrování, sít'ovou autentizaci a architekturu uživatelského rozhraní.

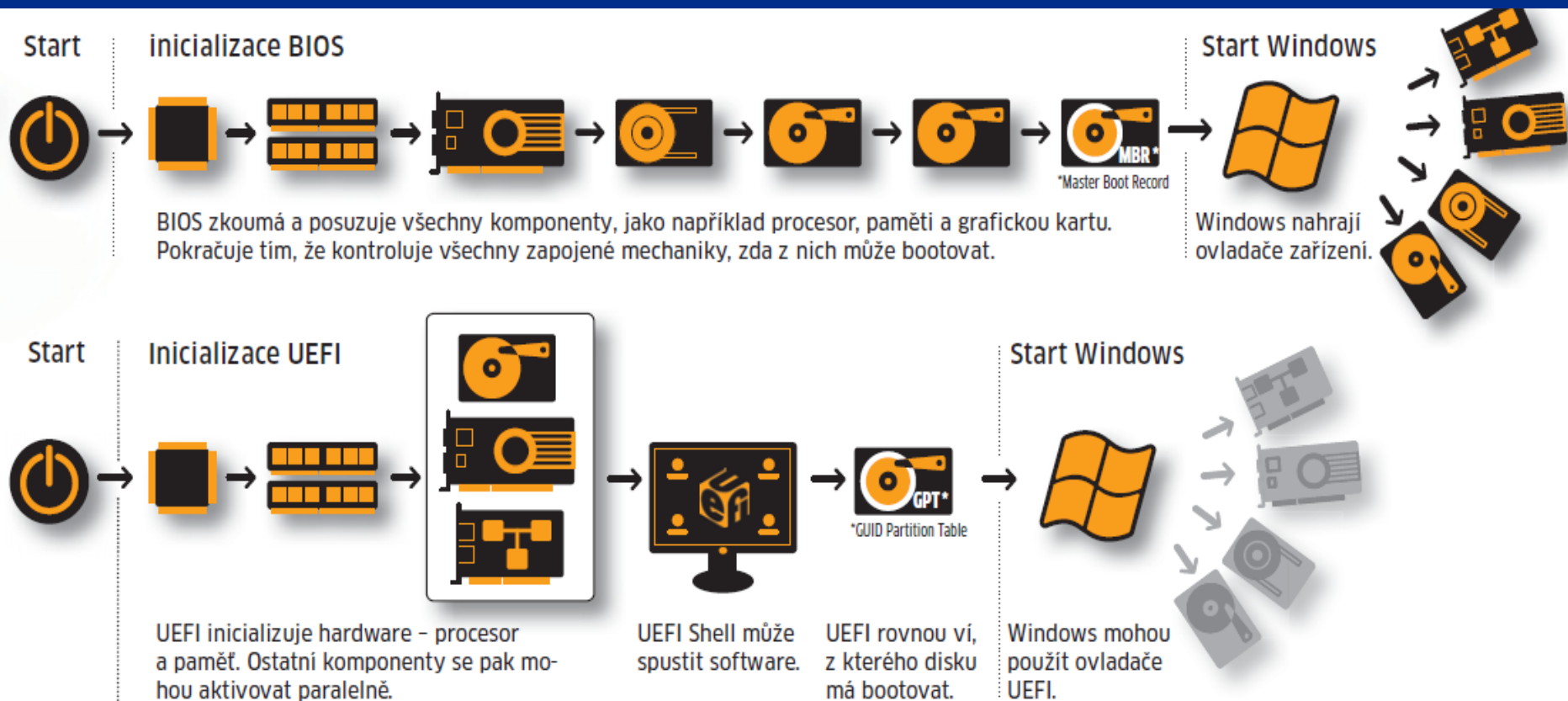
Operační systémy a EFI

- Operační systém, který podporuje bootování z (U)EFI, je podle (U)EFI specifikace nazýván **(U)EFI-aware OS** (tj. OS uvědomující si UEFI). Termín *bootování z (U)EFI* označuje přímé bootování systému s použitím **(U)EFI OS loaderu** uloženého na jakémkoli nosiči dat.
- Linuxové systémy jsou schopné používat EFI pro bootování již od roku 2000 pomocí EFI bootloaderu ELILO nebo později EFI verzí GRUBu.
- HP-UX používá od roku 2002 (U)EFI jako způsob bootování na systémech IA-64.
- HP OpenVMS používá (U)EFI od svého počátečního ověřovacího vydání v prosinci 2003 a pro produkční vydání od ledna 2005.
- Apple adoptoval EFI pro svoji linii počítačů Macintosh používající procesory Intel. Mac OS X verze 10.4 Tiger pro Intel a Mac OS X verze 10.5 Leopard podporují EFI verze 1.10 ve 32bitovém režimu, i s 64bitovými procesory. (Novější Macy mají 64bitové EFI.)
- Itanium ve verzích pro Windows 2000 (Advanced Server Limited Edition a Datacenter Server Limited Edition) podporovalo v roce 2002 EFI 1.10. Jako požadavek platformy podle specifikace DIG64 podporují EFI Windows Server 2003 pro IA-64, Windows XP 64-bit Edition a Windows 2000 Advanced Server Limited Edition, vydané pro rodinu procesorů Intel Itanium.
- Microsoft zavedl podporu UEFI pro operační systém Windows na platformě x64 ve verzích Windows Server 2008 a Windows Vista Service Pack 1.

Fáze bootování UEFI

- Přesně definované skupinou PI:
 - Pre EFI Initialization (PEI) – aktivuje se procesor, paměť a čipová sada
 - Driver Execution Environment (DXE) – inicializuje se zbytek HW a to i paralelně

Rozdíly při bootování s BIOS a s UEFI



Výhody UEFI

- Rychlejší bootování
- Rychlejší obnovení z režimu hibernace
- Podpora disků větších než 2,2 terabajtu (TB)
- Podpora moderních ovladačů zařízení s 64bitovým firmwarem, které systém může používat k adresování více než 17,2 miliard gigabajtů (GB) paměti při spouštění
- Možnost používat systém BIOS s hardwarem UEFI
- Lepší zabezpečení díky tomu, že pomáhá chránit proces před spuštěním proti útokům rootkitů

Výhody UEFI

- Muže v sobě integrovat různé ovladače (nezávislé na OS)
 - Síťové karty (bootování, dálková správa...)
 - Grafické karty (přívětivé grafické rozhraní...)
 - Nevyhledává se bootovatelný disk – je určen v UEFI
- Možnost vytvoření samostatných EFI oddílu na HDD (pro diagnostické nástroje, antivirové programy, SW pro správu systému, aplikace...)
- Součástí standardu je GPT



Co je to GPT ?



GUID Partition Table

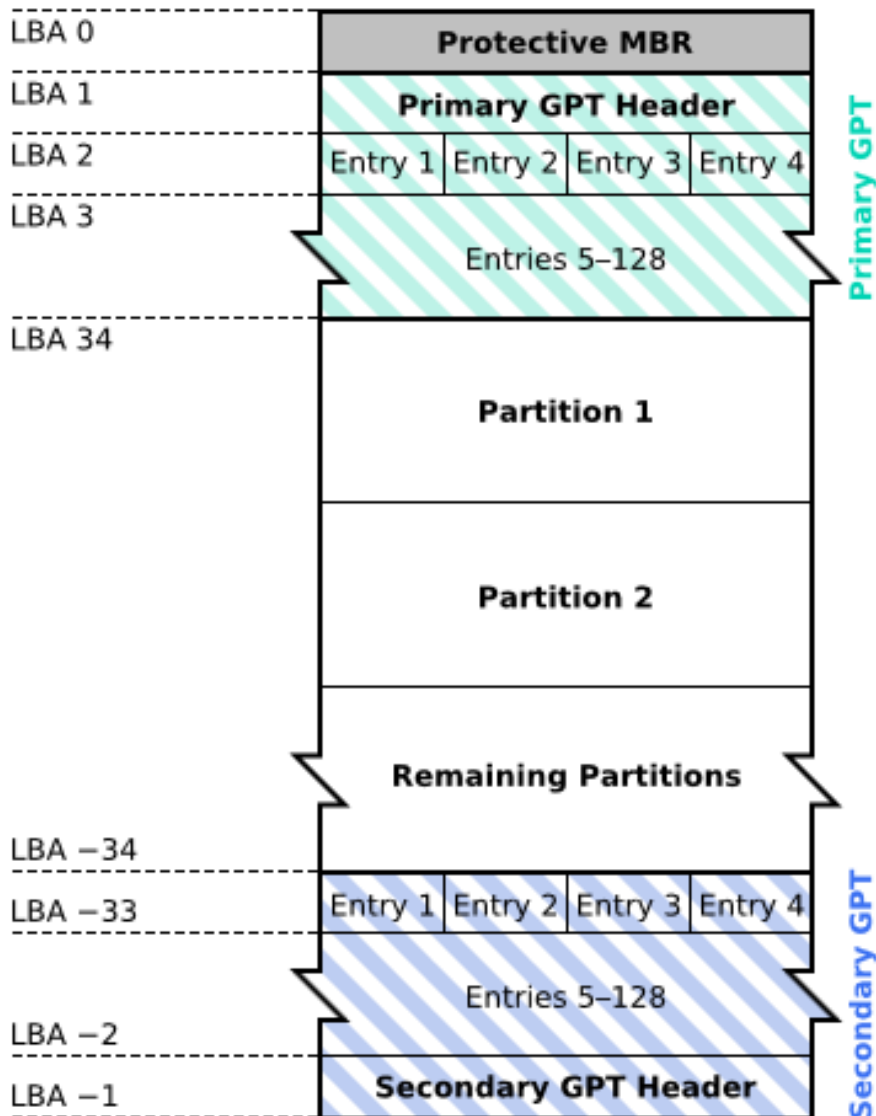
■ GUID Partition Table (GPT)

- je v standard pro popis členění HDD na oddíly.
(**G**lobaly **U**nique **I**dentifier)
- GPT je součástí standardu UEFI od firmy Intel, který by měl nahradit v počítačích klasický BIOS.
- Nahrazuje starší tabulku PaT typu MBR, která neumožňuje použít disk větší, než 2 TiB.
- Na discích s MBR lze vytvořit maximálně čtyři primární oddíly, nebo tři primární oddíly a jeden rozšířený oddíl a neomezený počet logických jednotek.
- Na discích GPT (GUID Partition Table) lze vytvořit až 128 primárních oddílů.

Další hlavní rozdíly oproti MBR:

- zcela opouští dělení disku na cylindry, hlavy a sektory, pracuje pouze s LBA
- záložní kopii tabulky ukládá na konci disku

GUID Partition Table Scheme



Umístění GPT na pevného disku, kde každý logický blok (LBA) má velikost 512 bajtů a každá položka pro jednotlivé diskové oddíly má 128 bajtů.

Záporné hodnoty vyjadřují umístění položek na konci disku.

Jak funguje UEFI

- Počítače s UEFI startují stejně až do začátku bootování, poté už vše probíhá úplně jinak:
 - UEFI disponuje vlastním zaváděčem OS, do kterého se integrují boot managery instalovaných operačních systémů.
 - Pro tento boot loader je na pevném disku vyhrazen malý oddíl (100 až 250 MB), naformátovaný systémem FAT32, který se nazývá Extensible Firmware Interface System Partition (ESP).
 - Zjednodušeně řečeno dokáže UEFI kromě DVD disku načíst operační systém pouze z média naformátovaného souborovým systémem FAT32.
 - ESP obsahuje ovladače hardwaru, ke kterým během načítání přistupuje operační systém. Například systémy Windows 7 a 8 ukládají do ESP celou Hardware Abstraction Layer.



Efficient, Flexible, Intelligent

Language



Boot



Game



Setting



Eco



Utility

Select an option with Up/Down key or cursor; press Enter or left click to confirm. Right click to go to previous menu; left click twice to enter sub-menu.



MSI
MOOD • BEAT • EXCEED



Efficient, Flexible, Intelligent

www.cdr.cz



System Status



Chipset Setting



Password Setting



Boot Setting



Save & Exit

Select an option with Up/Down key or cursor; press Enter or left click to confirm. Right click to go to previous menu; left click twice to enter sub-menu.



MSI
Micro-Star International Co., Ltd.

17:30

Wednesday [04/25/2012]

P8Z77 WS

BIOS Version : 0601

CPU Type : Intel(R) Core(TM) i5-2500K CPU @ 3.30GHz

Speed : 3310 MHz

Total Memory : 4096 MB (DDR3 2133MHz)

English

Temperature

CPU +109.4°F/+43.0°C

MB +95.0°F/+35.0°C

Voltage

CPU 1.130V 5V 5.120V

3.3V 3.408V 12V 12.000V

Fan Speed

CPU_FAN 957RPM CPU_OPT_FAN N/A

CHA_FAN1 N/A CHA_FAN2 N/A

System Performance

Quiet

Performance

Energy Saving

Normal

Boot Priority



Use the mouse to drag or keyboard to navigate to decide the boot priority.

Shortcut (F3)

Advanced Mode (F7)

Boot Menu (F8)

Default (F5)



Main



Ai Tweaker



Advanced



Monitor



Boot



Tool

Target CPU Speed : 2600MHz

Target DRAM Speed : 1333MHz

Ai Overclock Tuner

Auto

ASUS MultiCore Enhancement

Enabled

Memory Frequency

Auto

iGPU Max. Frequency

Auto

EPU Power Saving Mode

Disabled

> OC Tuner

> DRAM Timing Control

> CPU Power Management

> DIGI+ URM

CPU Voltage

1.048V

Offset Mode

CPU Offset Mode Sign

+

[X.M.P.]

When XMP mode is enabled, the
CPU ratio, BCLK frequency,
and memory parameters
will be optimized automatically.

[Manual]

When Manual mode is enabled, the
CPU ratio and BCLK frequency
will be optimized automatically.

←→: Select Screen

↑↓: Select Item

Enter: Select

+/-: Change Opt.

F1: General Help

F2: Previous Values




F3: Shortcut

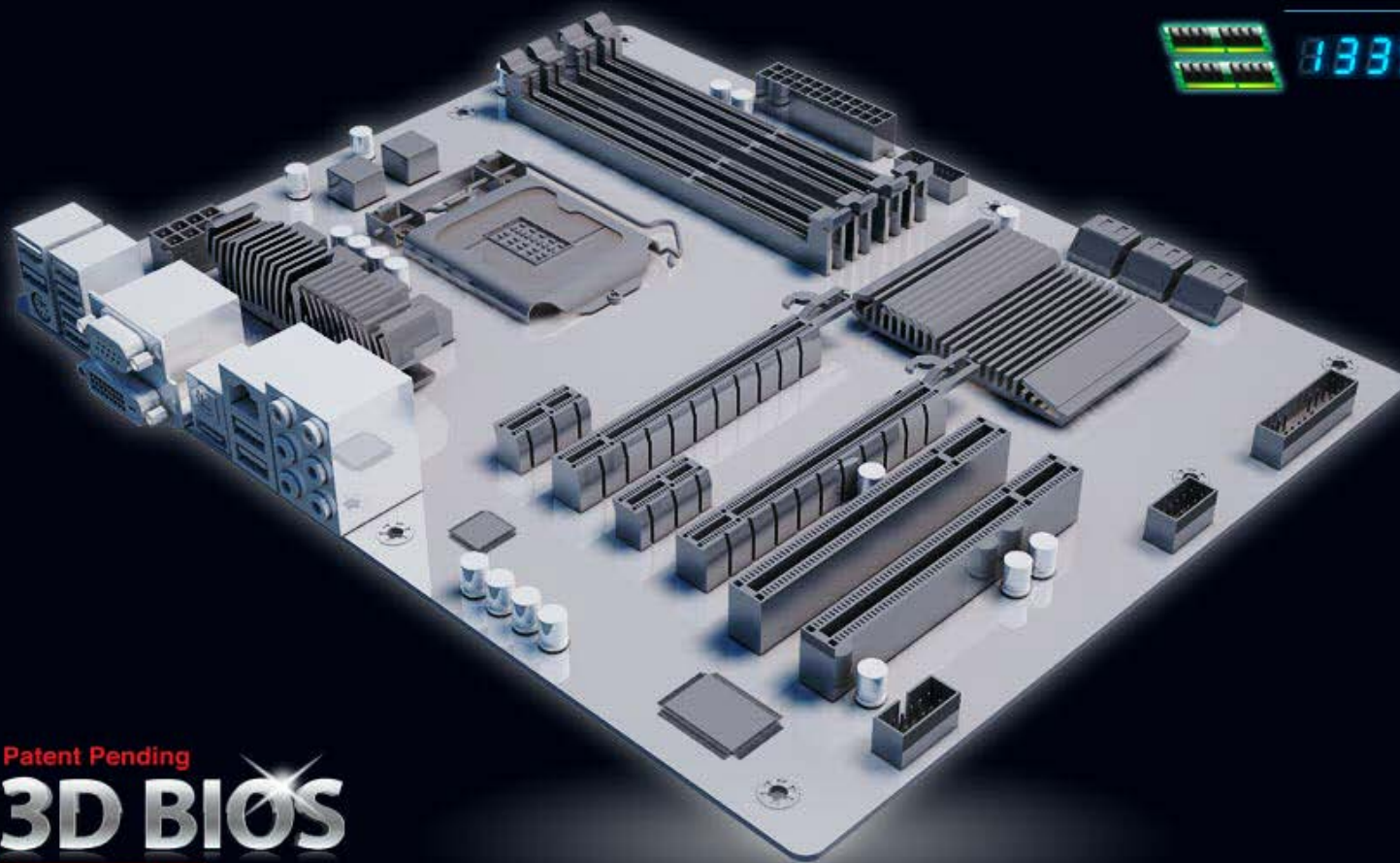
F5: Optimized Defaults

F10: Save ESC: Exit

F12: Print Screen

GIGABYTE™

 2603.29 MHz
 8100.12 MHz
 1335.02 MHz



Patent Pending
3D BIOS
Dual UEFI BIOS™



The above photos are reference only



Advanced



Boot



Language



Fan Control



Time






Load Defaults



Save & Exit

GIGABYTE™

 2603.20 MHz
 1100.12 MHz
 1334.97 MHz

Expansion Slots

Check connected PCIe device bus speeds with options to enable or disable individual PCIe and PCI expansion slots. Also includes additional options for VGA card boot priority.

Patent Pending
3D BIOS
Dual UEFI BIOS™



The above photos are reference only



Advanced



Boot



Language



Fan Control



Time



Load Defaults



Save & Exit

Použité zdroje:

- WIKIPEDIE. *Extensible Firmware Interface* [online]. [cit. 15.2.2013]. Dostupný na WWW: http://cs.wikipedia.org/wiki/Extensible_Firmware_Interface
- LITTSCHWAGER, Thomas. *UEFI: Nový a lepší BIOS* [online]. [cit. 15.2.2013]. Dostupný na WWW: <http://earchiv.chip.cz/cs/earchiv/vydani/r-2011/chip-02-2011/uefi.html>
- ŠIMONEK, Michal. *Klasický BIOS je přežitek – srovnání UEFI od tří výrobců* [online]. [cit. 15.2.2013]. Dostupný na WWW: <http://pctuning.tyden.cz/hardware/zakladni-desky/23428-klasicky-bios-je-prezitek-srovnani-uefi-od-tri-vyrobcu?start=5>
- MICROSOFT. *Co je UEFI?* [online]. [cit. 15.2.2013]. Dostupný na WWW: <http://windows.microsoft.com/cs-CZ/windows-8/what-uefi>
- LANK, Vojtěch. *Dosavadním BIOSům odzvonilo - přichází EFI* [online]. [cit. 15.2.2013]. Dostupný na WWW: http://pctuning.tyden.cz/index.php?option=com_content&view=article&id=15675&catid=1&Itemid=57
- MANDAU, Markus. *Chaos místo BIOS* [online]. [cit. 16.10.2013]. Dostupný na WWW: <http://www.chip.cz/casopis-chip/earchiv/vydani/rocnik-2013/chip-06-2013/chaos-bios/>
-