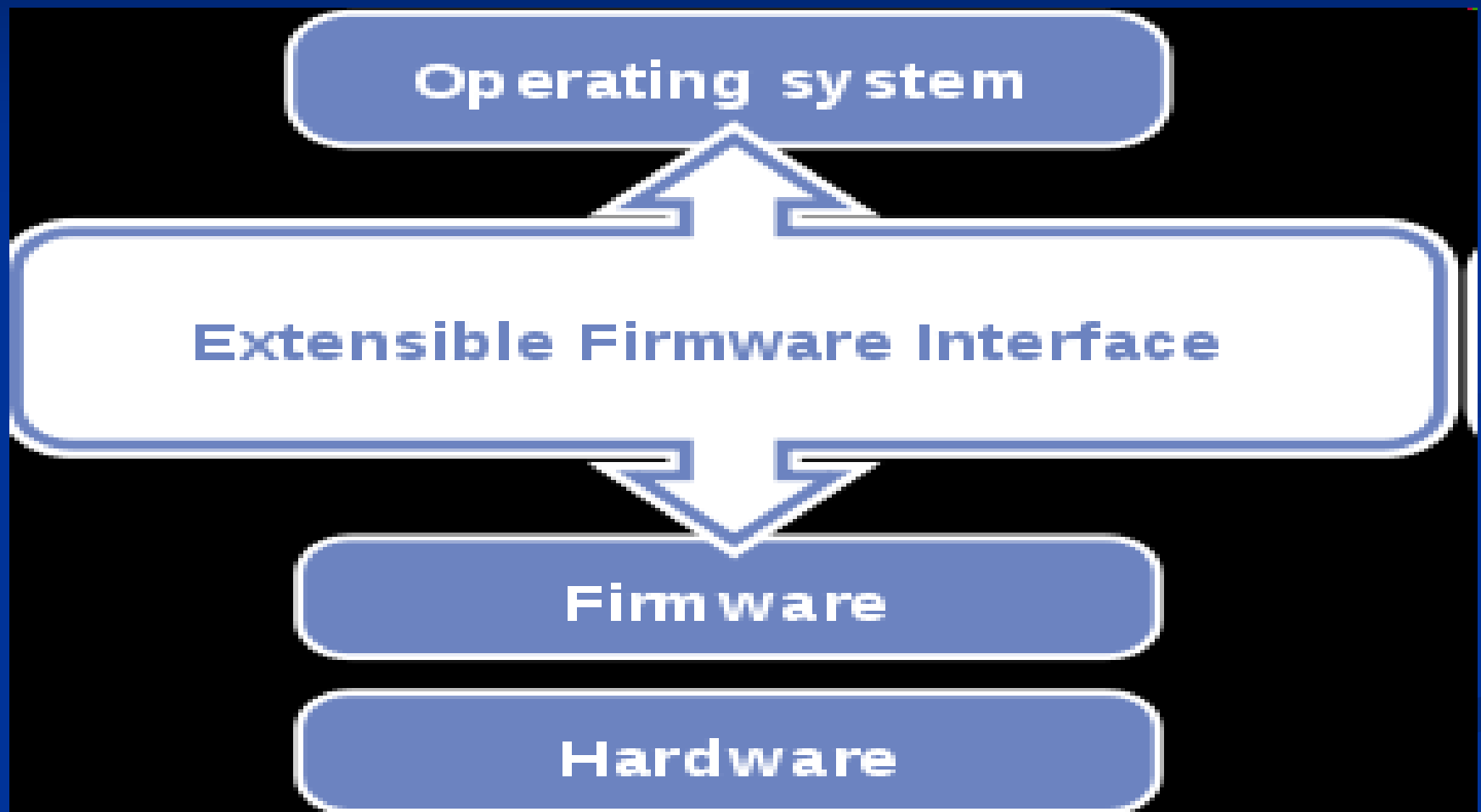
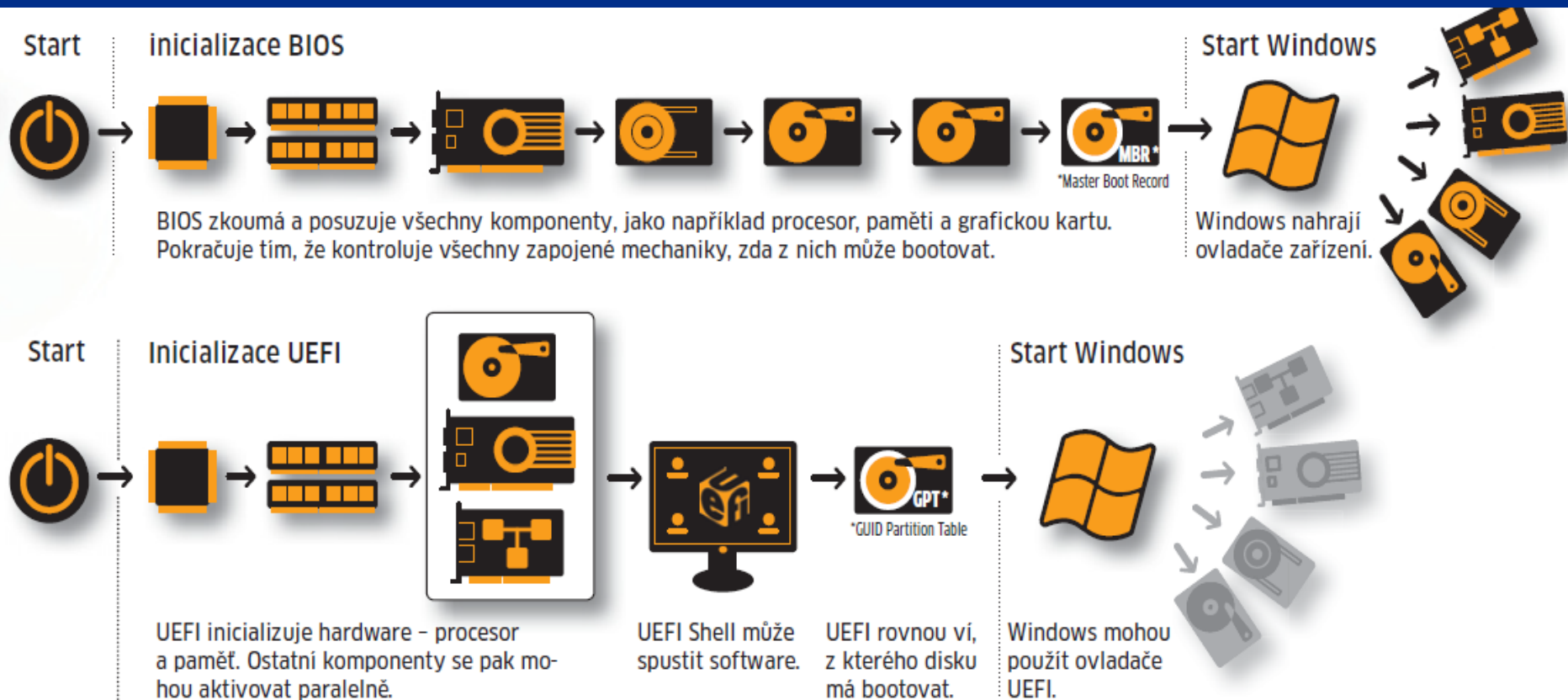
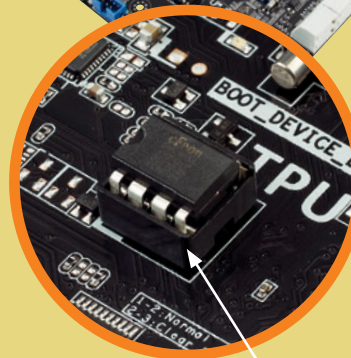
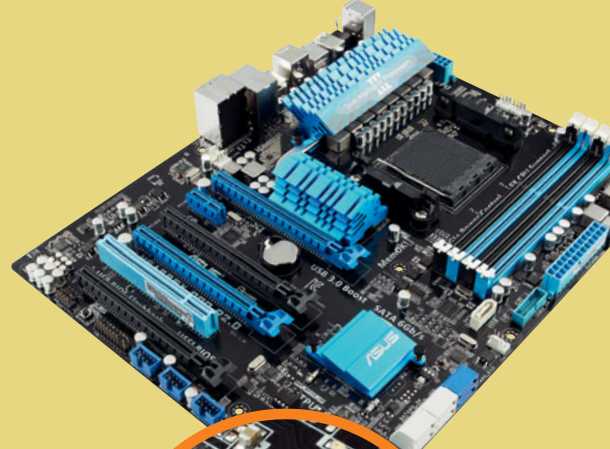


EFI



Výhody UEFI



**INICIALIZACE PLATFORMY****ZAPNUTÍ POČÍTAČE**

Uživatel stiskne zapínací spínač počítače. Ke komponentám začíná proudit elektřina.

FIRMWARE AKTIVUJE KOMPONENTY

Po dokončení sekvence POST (Power On Self Test) postupně spouští firmware UEFI nejdůležitější komponenty počítače (základní deska, CPU, paměti).

SPOUŠTÍ SE UEFI

Načítají se základní rutiny UEFI včetně tabulek pro spuštění příkazů, které mají být provedeny.

POSTUP NAČÍTÁNÍ UEFI**SPOUŠTÍ SE UEFI BOOT MANAGER**

V rámci Boot Manageru pracují centrální komponenty, které vykonávají příkazy a aplikace UEFI.

MANAGER NAČÍTÁ BOOTOVACÍ NASTAVENÍ

NVRAM paměť na základní desce obsahuje všechna základní nastavení pro start systému, která používá i Boot Manager.

MANAGER AKTIVUJE BOOTOVACÍ DISK

Boot Manager UEFI určuje, ze kterého pevného disku, flash disku nebo optické mechaniky se bude bootovat operační systém.

MANAGER NAČÍTÁ OBSAH DISKOVÉHO ODDÍLU UEFI

Manager zkontroluje certifikáty ovladačů a aplikací UEFI, které jsou umístěny v diskovém oddílu UEFI. Pokud odpovídají, tak je načte.

MANAGER SPOUŠTÍ APLIKACE UEFI

Spouští se aplikace UEFI, jako například síťové připojení a shell. Jako poslední UEFI aplikace se spouští zavaděč operačního systému.

ZAVADEČ SPUSŘÍ NAČÍTÁNÍ OPERAČNÍHO SYSTÉMU

Dojde-li ke shodě podpisových klíčů startovacího kódu nebo Boot Manageru, spustí zavaděč načítání OS.

Načítání

NVRAM

Start

Načítání

Kop

PLATFORM KEY (PK)

PK od výrobce hardwaru umožňuje aktualizace UEFI a změny v seznamu KEK.

KEY ENROLLMENT KEY (KEK)

KEK seznam výrobce operačního systému (Microsoft) umožňuje změny v obou databázích

Measured Boot

Windows 10 budou v budoucnu vyžadovat TPM 2.0, šifrovací čip nezbytný pro tzv. Measured Boot. Díky němu budou všechny moduly nahrávané při startu Windows ověřovány důvěryhodným serverem.

Start Windows s kontrolou UEFI

Pro opravdu bezpečný start si Windows nevystačí s vlastními prostředky. Microsoft spoléhá na dva pomocníky: UEFI Secure Boot a TPM čipy.

Říjen 2012

Windows 8 podporují Secure Boot a Measured Boot (musí být přepínatelný).

Červenec 2015

Nová zařízení s Windows 10 musí obsahovat TPM 1.2 nebo 2.0. Secure Boot lze volitelně přepnout.

Červenec 2016

TPM 2.0 budou potřebovat i počítače s Windows 10.



TPM čipy jsou malé šifrovací moduly využívané již několik let. Windows 10 je budou vyžadovat povinně.



Fáze 1: Secure Boot

Stejně jako předchozí verze využívají i Windows 10 Secure Boot – funkci UEFI. Proto nahraje firmware pouze podepsaný zavaděč operačního systému (bootloader). Platný podpis vyžadují také další nahrávané komponenty.

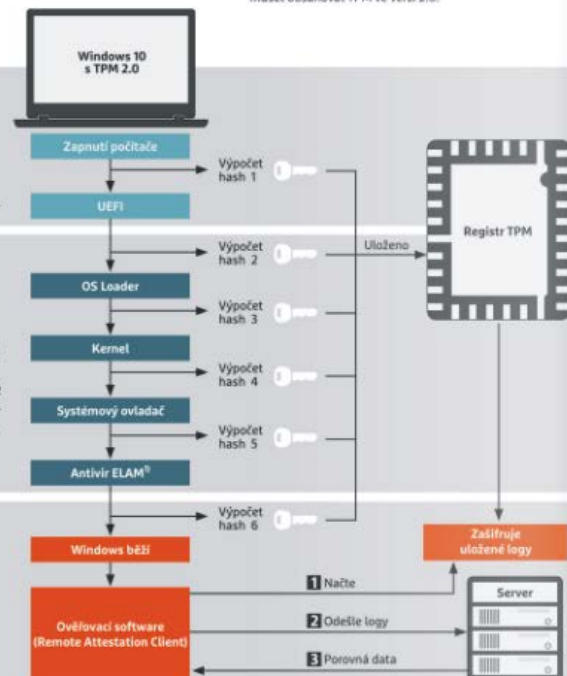
Fáze 2: Trusted Boot

Další fáze se jmenuje Trusted Boot a je speciální bezpečnostní funkcí Windows. Nahraje se pouze digitálně podepsané komponenty startovacího procesu. Pro Measured Boot jsou navíc vypočteny hash hodnoty nahrávaných modulů. Tyto hash hodnoty jsou v zašifrované podobě uloženy do registru TPM. TPM čip proto vytvoří tzv. Platform Configuration Register s hodnotami od 0 do 7.

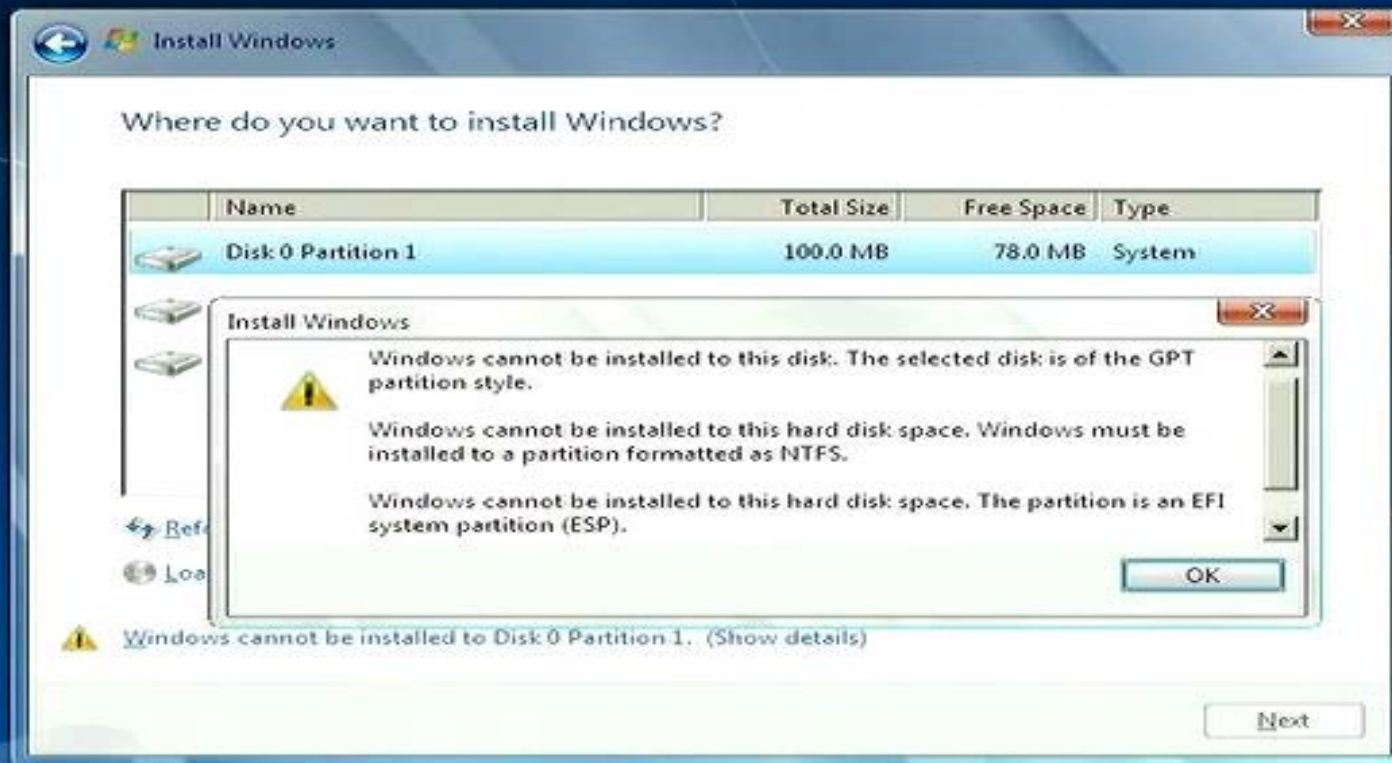
1) EARLY LAUNCH ANTIMALWARE

Fáze 3: Measured Boot

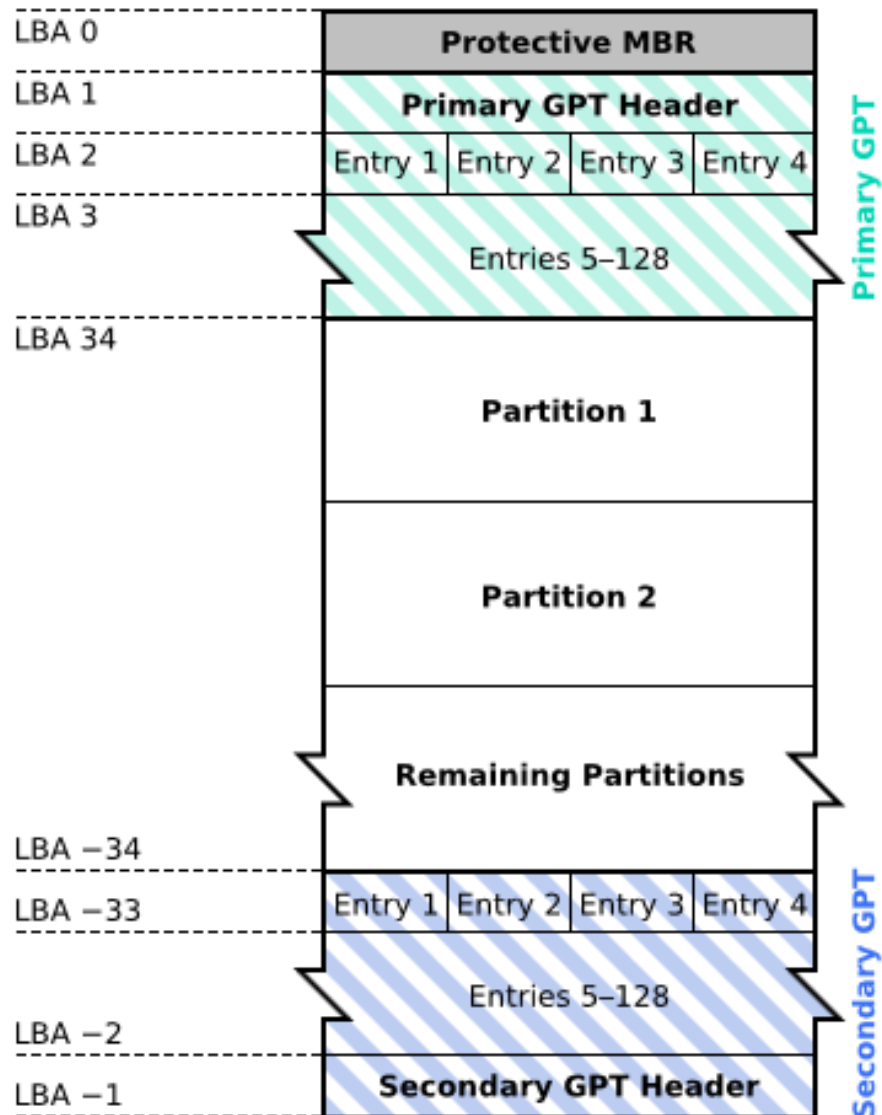
Measured Boot porovnává získané hash hodnoty s externí instancí. Remote Attestation Client 1 vezme zašifrované hodnoty z TPM a odešle je na ověřovací server 2. Ten data porovná 3 a pošle varování, pokud něco nesedí.



Co je to GPT ?



GUID Partition Table Scheme





Efficient, Flexible, Intelligent

Language



00



Game



Setting



600



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 • STAR • INTERNATIONAL



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

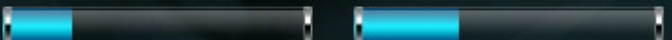


MB +95.0°F/+35.0°C



Voltage

CPU 1.130V 5V 5.120V

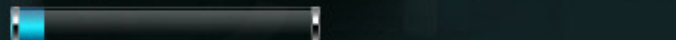


3.3V 3.408V 12V 12.000V



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

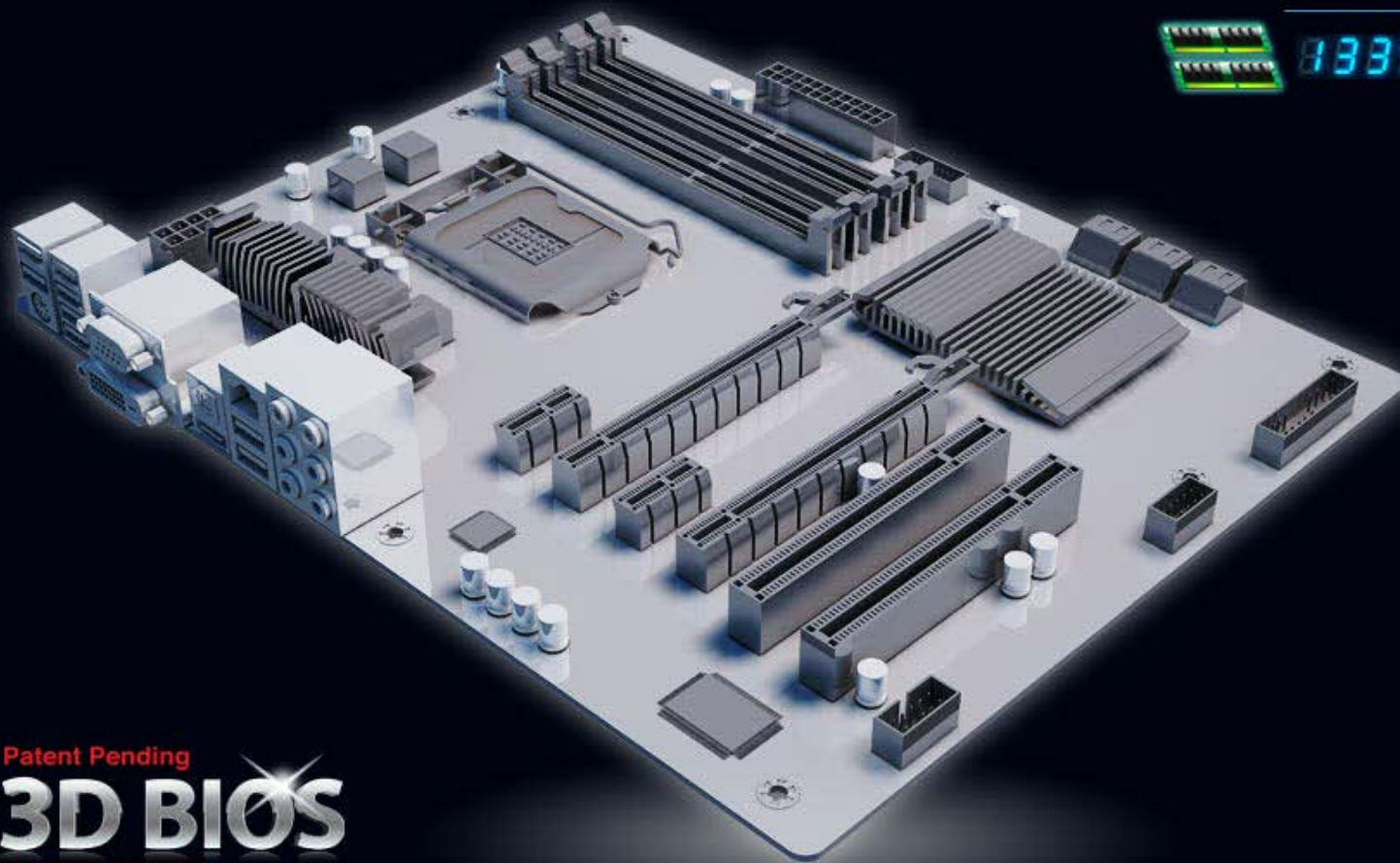
F5: Optimized Defaults

F10: Save ESC: Exit

F12: Print Screen

GIGABYTE™

 2603.29 MHz
 1100.12 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
 8100.12 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