



Comparing BIOS, UEFI and Boot Loader Solutions

Understanding the advantages of
UEFI over embedded boot loaders

Updated 2011-02-10

LEGAL

Disclaimer

- This publication contains proprietary information which is protected by copyright. No part of this publication may be reproduced, transcribed, stored in a retrieval system, translated into any language or computer language, or transmitted in any form whatsoever without the prior written consent of the publisher, American Megatrends, Inc. American Megatrends, Inc. retains the right to update, change, modify this publication at any time, without notice.

For Additional Information

- Call American Megatrends, Inc. at 1-800-828-9264 for additional information.

Limitations of Liability

- In no event shall American Megatrends be held liable for any loss, expenses, or damages of any kind whatsoever, whether direct, indirect, incidental, or consequential, arising from the design or use of this product or the support materials provided with the product.

Limited Warranty

- No warranties are made, either express or implied, with regard to the contents of this work, its merchantability, or fitness for a particular use. American Megatrends assumes no responsibility for errors and omissions or for the uses made of the material contained herein or reader decisions based on such use.

Trademark and Copyright Acknowledgments

- Copyright ©2011 American Megatrends, Inc. All Rights Reserved.
- American Megatrends, Inc., 5555 Oakbrook Parkway, Suite 200, Norcross, GA 30093
- All product names used in this publication are for identification purposes only and are trademarks of their respective Companies.

BIOS OR BOOT LOADER?

- Customers in embedded computing have often used boot loaders for system startup
- When moving into x86 architecture, there is some confusion over the role of the simple boot loader versus the PC BIOS firmware
- BIOS offers advantages over boot loaders, including enhancements based on UEFI

BOOT LOADER

- Does minimum silicon/platform bring-up
- Little or no runtime environment
- Platform management done mostly at OS level
- Suitable for smaller, less complex systems
- Leaves most hardware initialization to OS
 - Requires OS to be customized for the hardware

LESSONS LEARNED: BOOT LOADERS

- Boot loaders bring a *lack of flexibility* to platforms
 - Changing OS needs porting in firmware and OS kernel
 - Boot loaders are typically not based on standards and can be difficult to extend
- Traditional boot loader firmware model is *D.I.Y.*
 - Chip vendors might deliver source code, but often without the right training, tools or developer support
- These issues are addressed using BIOS & UEFI

EXAMPLE: SMARTPHONES



- Almost all smart phones use the boot loader model
 - Android, iOS, BlackBerry
- Phone OS port is specific to the hardware config
- Boot loader won't load other OS versions

THE DOWNSIDE ...

- Customers can't easily change OS
 - Requires a hacked OS, a hacked bootloader and voiding the warranty
 - “Rooting” the phone is required
- This model works if the hardware manufacturer wants to lock the OS
- The bootloader model is *not good for general purpose systems* using an off-the shelf operating system



BIOS = BASIC INPUT/OUTPUT SYSTEM

- ✔ Initializes platform before the OS loads
 - Configures silicon for advanced operating modes
 - Performs bus and peripheral enumeration
- ✔ Set up runtime environment for OS and applications
 - Enables OS directed platform & power management
- ✔ Enables pre-boot services for OS loader & recovery
- ✔ Suitable to a wide range of platform implementations
- ✔ Supports the full platform product cycle
 - Support from chipset power-on through “end of life”

BIOS ENABLES OFF THE SHELF OS



- A great strength of the PC is *access to many OS versions*
 - Install an OS “out of the box”
 - Allows developers to pick the best OS for the market
 - Removes CPU dependencies
- This *flexibility and rapid innovation* depends on the services of BIOS and UEFI
 - Documented interfaces
 - Standards based compatibility

BIOS ADVANTAGES

- BIOS provides a true compatibility layer
 - User setup interface
 - Multiple boot devices
 - Rapidly change OS
 - OEM differentiation
- *AMI uses UEFI to further improve this model ...*



MOVING FROM BIOS TO UEFI

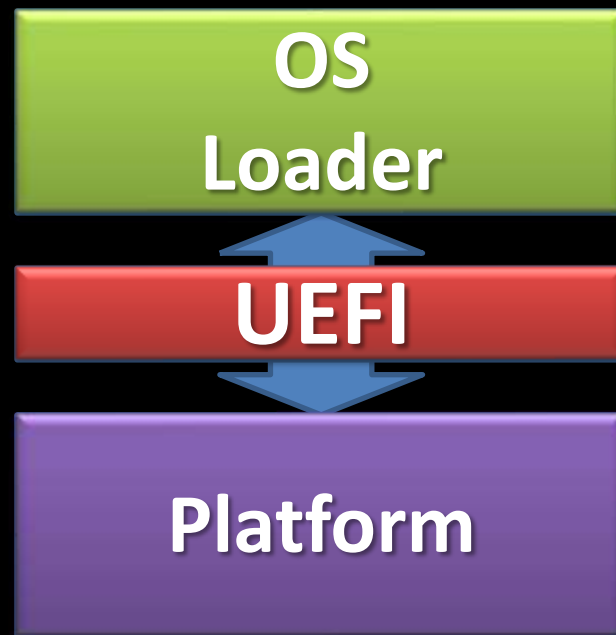
- The term BIOS is often associated with old 16-bit code for x86 CPUs
- While “BIOS” still has the same job, several legacy limitations have been removed ... *underlying code has been upgraded to the UEFI standard*



UEFI HIGHLIGHTS

Unified Extensible Firmware Interface (UEFI)

- OS-to-Firmware interface specification
- Abstracts platform from OS
- Includes modular driver model
- Compatible by design
- Modular and extensible
- Complements existing firmware & OS interfaces



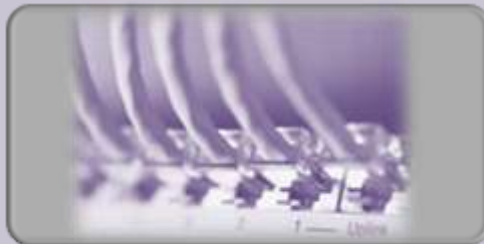
UEFI IMPROVES THE BIOS MODEL



Drive Size Limitations

UEFI removes 2.2TB
MBR partition limits
using GPT ...

Now supporting drives
up to 9.8 zettabytes



Networking

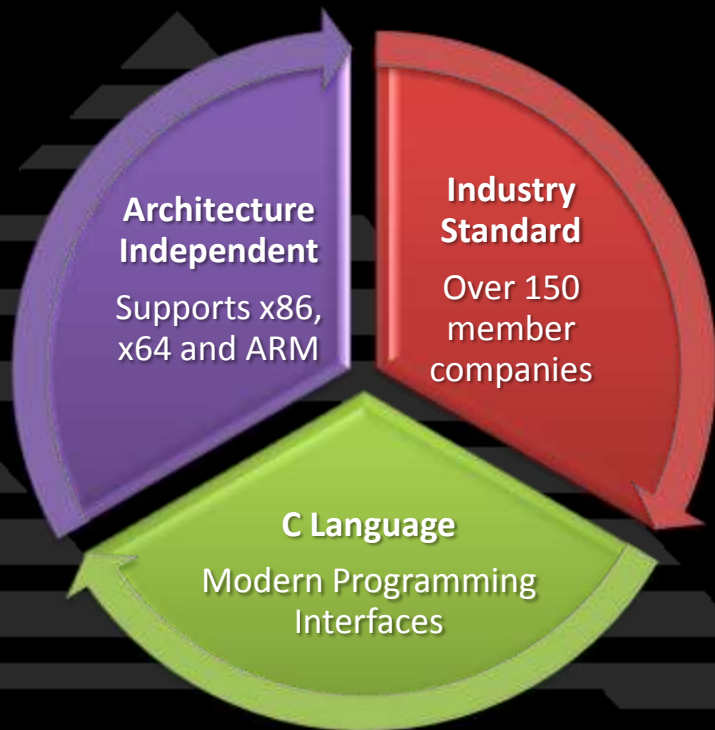
The UEFI specification
supports IPv4 and IPv6
networking ... *without
booting to the OS*



Pre-Boot Applications

GUI or text tools for
provisioning, recovery
and diagnostics ...
without the OS

LEVERAGING UEFI ADVANTAGES



- BIOS providers like AMI have made the move to UEFI because it offers numerous advantages
 - Standards based
 - Driver model
 - Multiple CPU Architectures



AMI PRODUCTS LEVERAGING UEFI



Aptio

UEFI Solution for
any x86 BIOS
application

AMI Provisioning

GUI pre-boot
apps, based on
UEFI

AMIDIag for UEFI

Pre-boot
diagnostics for test
and burn-in
without an OS

BIOS - KEY TO A SOLID PLATFORM

BIOS offers the compatibility between the hardware & operating system that makes the x86 platform today's most flexible computing architecture.



*Platform
Initialization*

*Maximum
OS-to-BIOS
Compatibility*

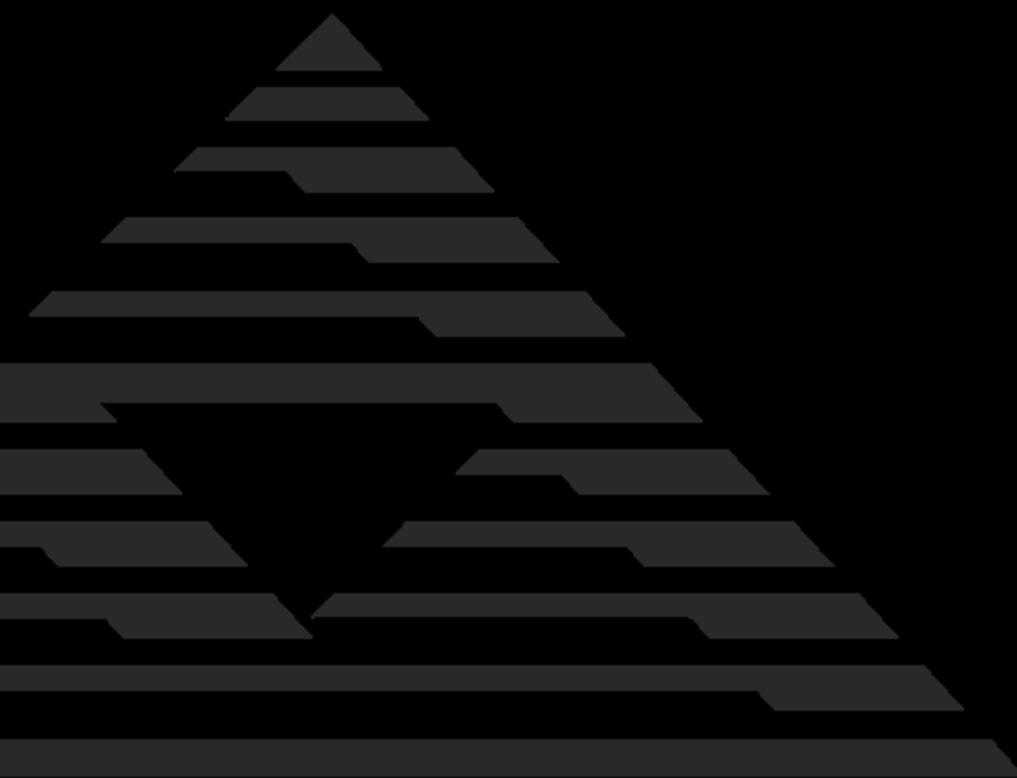
*Pre-boot
Value Add*



UEFI brings modern software methods and C-based programming to the BIOS world using industry standards.

RESOURCES

- The Unified EFI Forum – www.uefi.org
- [The UEFI Primer @ uefi.org](http://www.uefi.org)
- [Learning Center @ uefi.org](http://www.uefi.org)
- [Aptio](http://www.ami.com) information @ www.ami.com
- [AMIDiag for UEFI](http://www.ami.com) information @ www.ami.com
- [AMI Provisioning](http://www.ami.com) information @ www.ami.com
- “Ask a BIOS Guy” on Twitter [@askabiosguy](https://twitter.com/askabiosguy)



**5555 Oakbrook Parkway
Suite 200
Norcross, GA 30093**

www.ami.com