

presented by



UEFI State of the Union

Ecosystem enabling update

UEFI Summer Plugfest – July 6-9, 2011

Mark Doran

Bailey Cross

Intel Corporation

Agenda



- UEFI Forum Update
- Intel UEFI Ecosystem Enabling Update



About 10 years ago,
Intel committed to ...



*Establish an industry standard
framework for platform innovation and
delivering interoperable firmware binary
modules on Intel platforms*



Industry BIOS Transition



Pre-2000

All Platforms BIOS were proprietary

2000

Intel invented the Extensible Firmware Interface (EFI) and provided sample implementation under free BSD terms

2004

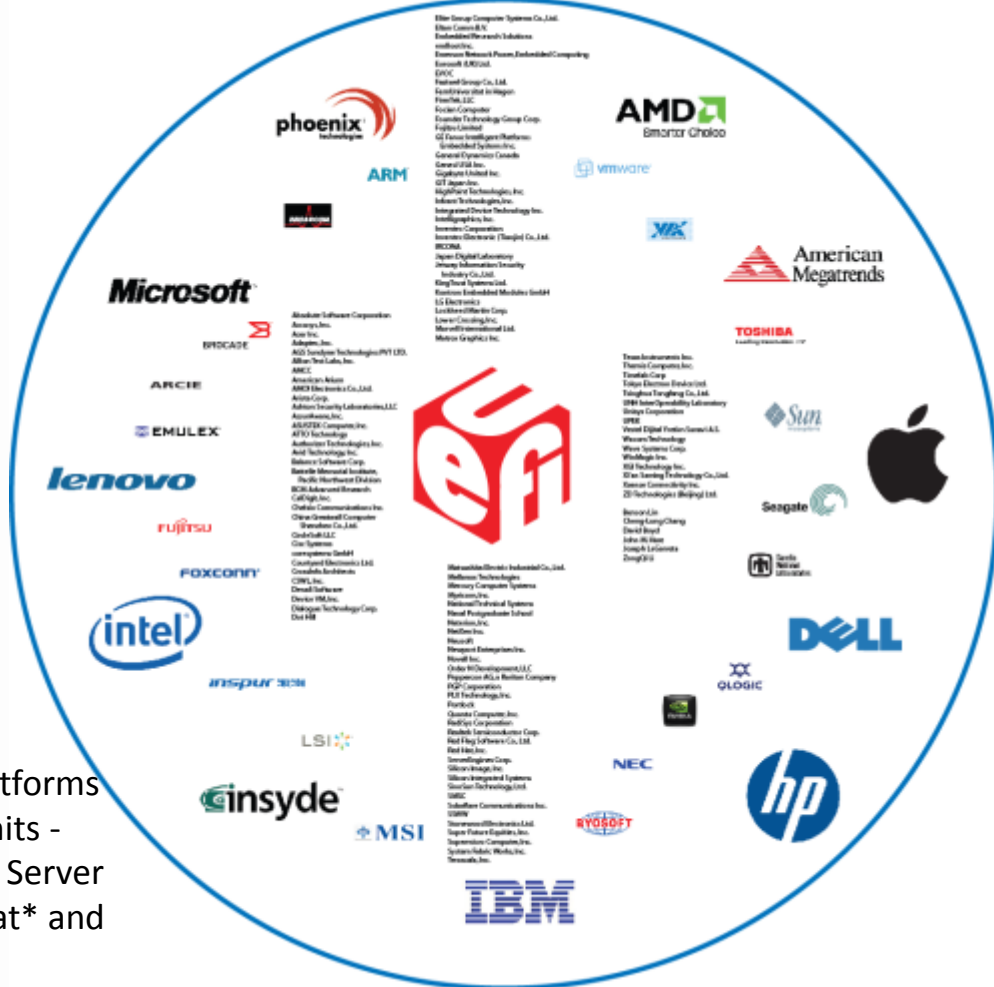
tianocore.org, open source EFI community launched

2005

Unified EFI (UEFI)
Industry forum, with 11 members, was formed to standardize EFI

2011

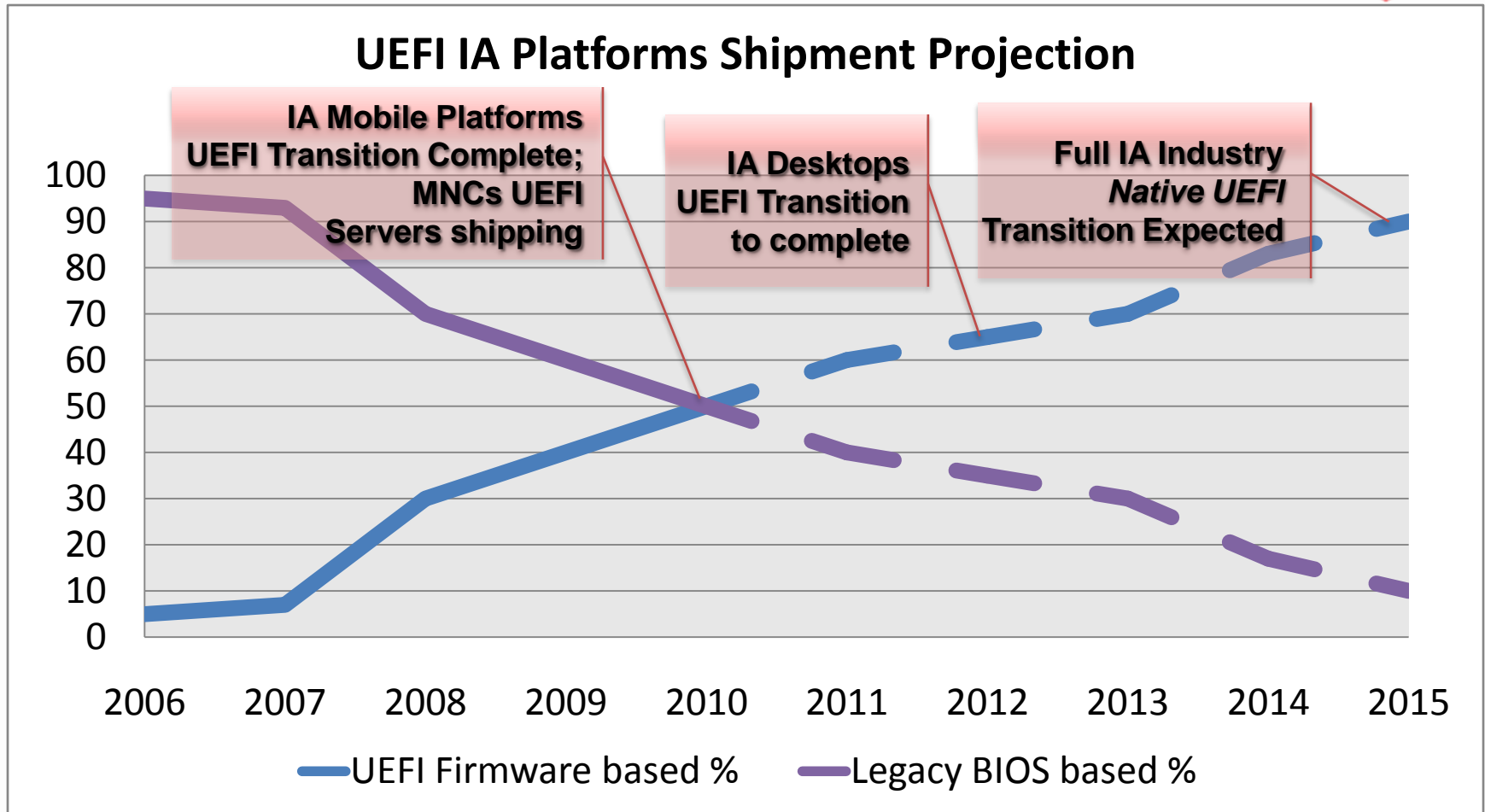
183 members and growing!
Major MNCs shipping - UEFI platforms crossed 50% of IA worldwide units -
Microsoft* UEFI x64 support in Server 2008, Vista* and Win7* - RedHat* and Novell* OS support



UEFI Firmware Deployments



Over 50% of worldwide IA units in 2010 and expected to reach 90% by 2015



UEFI Operating Systems



 Windows® 7

 Windows® Azure™


Windows Server® 2008 R2
Microsoft®
Hyper-V™ Server 2008 R2

 Windows® Storage Server 2008 R2
Enterprise

CANONICAL  ubuntu

MeeGo™



 RED HAT®
ENTERPRISE
LINUX

fedora 



SUSE® Linux Enterprise 11
Novell.



vmware®



Recognition of our accomplishments

“Without UEFI and the common code model it supports, we would not have been able to execute and achieve time to market delivery of multiple server offerings concurrently” -Akhtar Ali Vice President, Blades & Modular Software Development for IBM Systems and Technology Group



“Say Bye to BIOS and Hello to PCs that Boot in Seconds With UEFI”

– DailyTech, October 2010

DAILY TECH

“Change to 'Bios' will make for PCs that boot in seconds...Bios' replacement, known as UEFI, will predominate in new PCs by 2011”
- BBC News Technology, October 2010

“Seagate: 3TB HDD requires modern 64-bit OS and UEFI”

Dark Vision Hardware, May'10

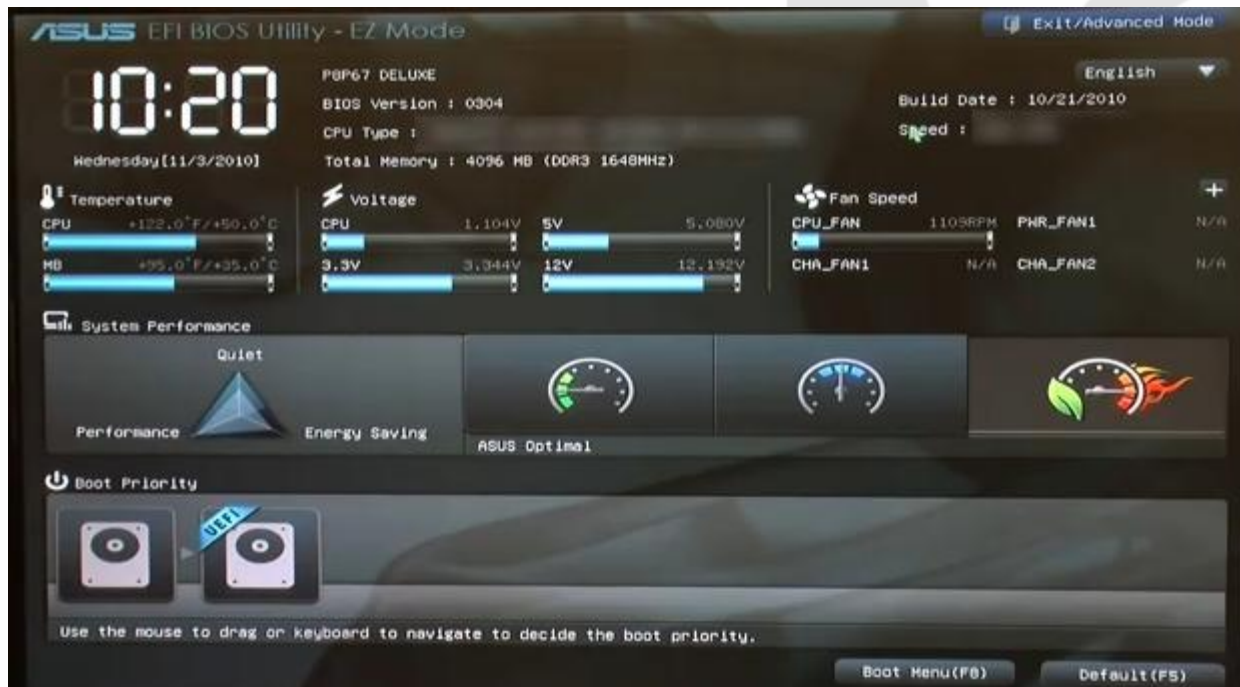
**DarkVision
Hardware**

**BBC
NEWS**

UEFI Goes Mainstream

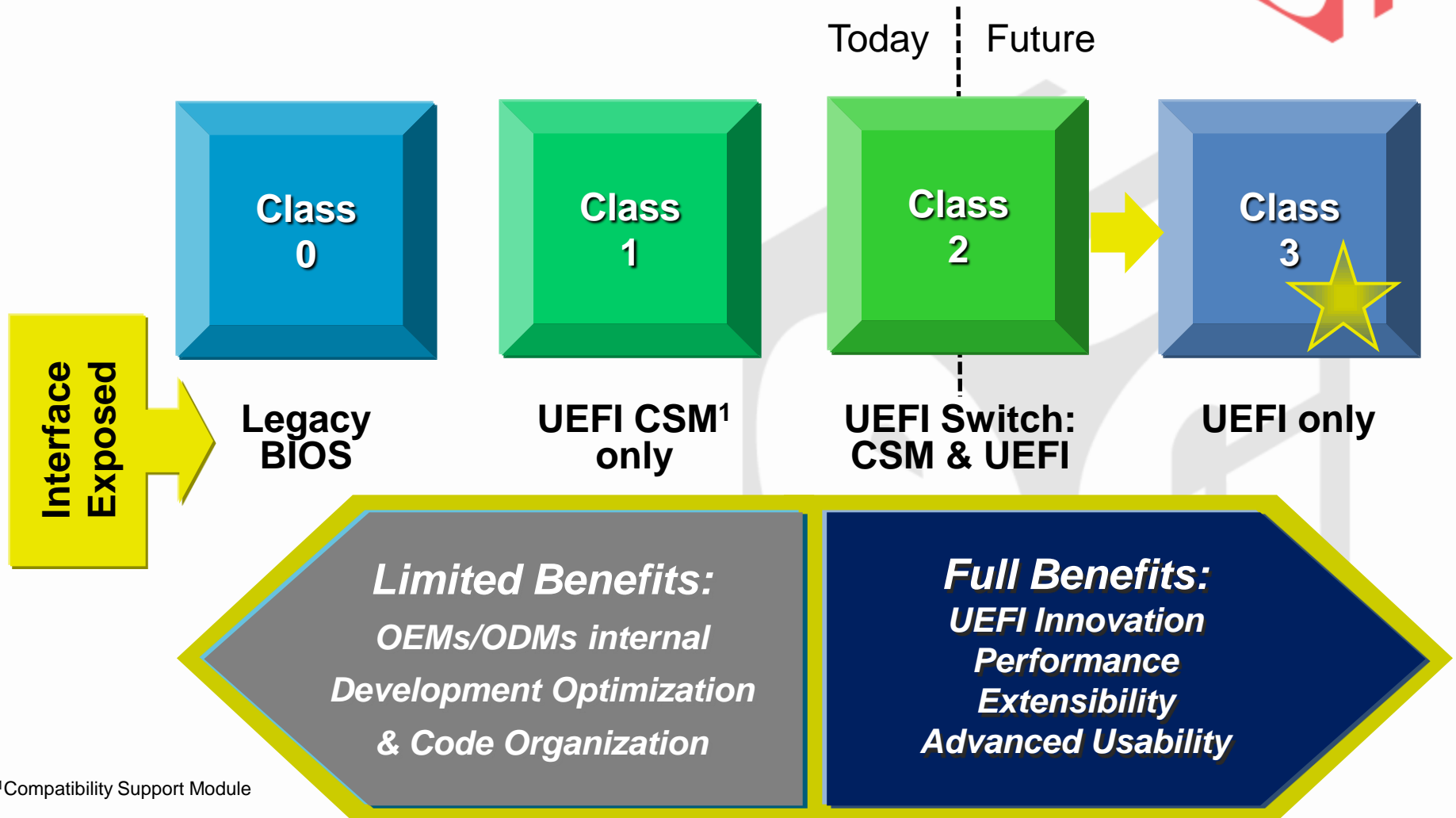


- Asus UEFI BIOS Ad
- Asus “EZ Mode” UEFI Setup



UEFI System Classes

Based on Firmware I/F



¹Compatibility Support Module

UEFI Vision Timeline & Progress



2000-2004

2005-2010

2011-2015

2015+

Technology Creation

Industry Transition

Industry Wide Adoption

- Standard Common Firmware Foundation & Interoperable Packages Technology will free up more OEMs/IBVs resources for differentiation
- Rich pre-boot environment will enable more Optimization and integration of new capabilities

Early Adoption led by MNCs:
Apple, Dell, HP, IBM

- Key Factors fueling wide UEFI adoption:
- Major OEMs making UEFI a design requirement
 - Industry mandate for Fast Boot performance & Support for large hard drives (> 2.2 TB)
 - Intel convergence on common UEFI code base; No BIOS legacy support from Intel

Increased Innovation Differentiation

UEFI-based Value-Add & Innovation



Pre-OS Security & Rich Networking

- IPV6/IPSec; Authenticode signature for firmware modules; protected updates; TPM & S-RTM



Manageability

- Enhanced Diagnostics; Intelligent & efficient platform updates; Flexible OS deployment; Consistent look & feel; Improved UI usability and OOB mgmt capabilities



Power Management

- Power metering, power capping, power saving

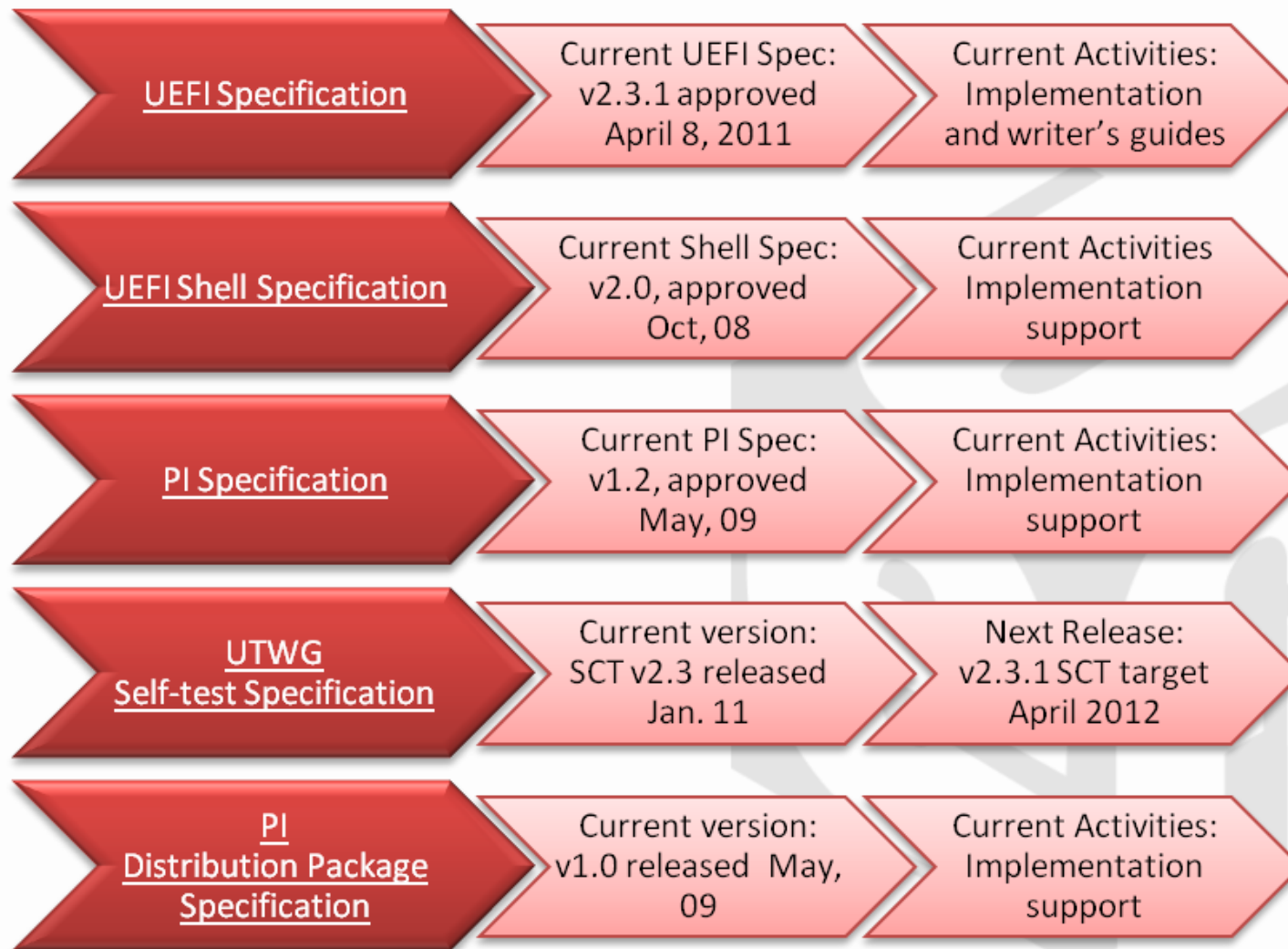


Optimized Boot & Modern Look

- Fast boot and resume response; High resolution graphics; System boot from large drives >2.2 TB



UEFI Specification Roadmap



UEFI 2.3.1 Specification Update

Security

- Authenticated Variable & Signature Database
- Key Management Service (KMS)
- Storage Security Command Protocol for encrypted HDD

Network

- Netboot6 client use DUID-UUID to report platform identifier

Interoperability

- New FC and SAS Device Path
- FAT32 data region alignment
- HII clarification & update
- HII Modal Form

Performance

- Non-blocking interface for BLOCK oriented devices

Technology

- USB 3.0

Maintenance

- User Identifier, etc.

UEFI 2.3.1 Enables More Security Support

Getting ahead: our imperatives

- Distill: refactor complexity for SoCs
- Expedite: the “shift left” for F/W
- Lead: SoC platform readiness
- Innovate: work with OS ecosystem dynamics
- Verify: strive for better quality
- Enable: port of choice starts with F/W
- Re-use: efficiently leverage our F/W assets



Unprecedented opportunity to DELIVER fundamental building blocks for the Compute Continuum



Intel UEFI Ecosystem Enabling Update

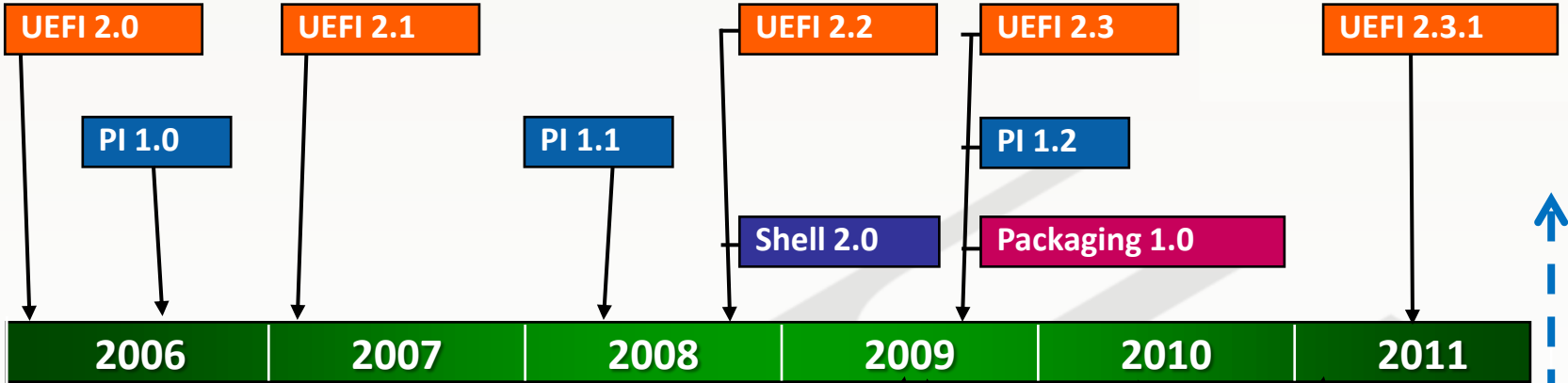
Topics

- Tiano Reference Implementation Timeline
- Intel® UEFI Development Kit 2010 (Intel® UDK2010)
- Intel firmware development platform “Tunnel Mountain”
- Intel UEFI Enabling Calendar
- UEFI Resources

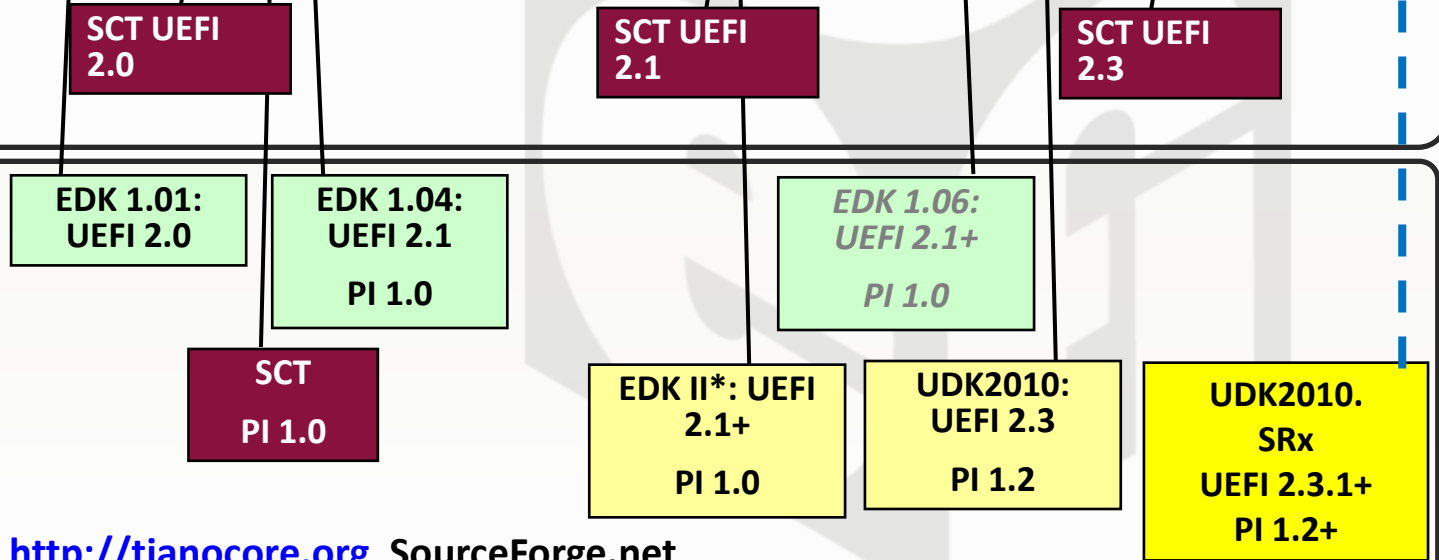
UEFI Specification & Tiano Reference Implementation Timeline

<http://uefi.org>

Specifications



Implementation



<http://tianocore.org> SourceForge.net

All products, dates, and programs are based on current expectations and subject to change without notice.

* EDK II is same code base as UDK2010

Intel® UDK2010 Key Features

Intel® UEFI Development Kit 2010 (Intel® UDK2010)



Industry Standards Compliance

- UEFI 2.0, UEFI 2.1, UEFI 2.2, UEFI 2.3; PI 1.0, PI 1.1, PI 1.2

Extensible Foundation for Advanced Capabilities

- Pre-OS Security
- Rich Networking (IP4/6, UDP4/6, TCP4/6, DHCP4/6, VLAN, IPsec, SAN/Datacenter boot: TCP-based iSCSI)
- Manageability

Support for UEFI Packages

- Import/export modules source/binaries to many build systems

Maximize Re-use of Source Code¹

- Platform Configuration Database (PCD) provides “knobs” for binaries
 - ECP provides for reuse of EDK1117 (EDK I) modules
 - Improved modularity, library classes and instances
 - Optimize for size or speed

Multiple Development Environments and Tool Chains¹

- Windows*, Linux*, OSX*
- VS2003, VS2005, WinDDK, Intel, GCC

Fast and Flexible Build Infrastructure¹

- 4X+ Build Performance Improvement (vs EDKI)
 - Targeted Module Build Flexibility

¹ benefit of EDK II codebase

Key Intel® UDK2010 Features



- UEFI Packaging
 - Enabling fast delivery of advanced capabilities to market
- Health and Management
 - Driver Health Protocol allows for self-healing / correcting devices
 - Firmware Management Protocol is a consistent way for driver adapters and system board to allow for updates
- Networking and Security
 - IP4/6, UDP4/6, TCP4/6, DHCP4/6, VLAN, IPsec, SAN/Datacenter boot: TCP-based iSCSI, Cryptographic logon, Multi-path/fail-over
 - Compliance with US Government requirements for IPV6 transition (<http://www.antd.nist.gov/usgv6/usgv6-v1.pdf>)
 - Compliance: Internet Engineering Task Force IETF RFC 5970, and IPV6 certified logo!
- UEFI Image Signing
 - Adds policy around UEFI and its 3rd party image extensibility
- UEFI User Identity
 - A standard framework for user-authentication devices that ensures the 'right' party applies policy/changes
- UEFI Shell 2.0



Intel® UDK2010 firmware development platform “Tunnel Mountain”



- Enables developers to write, debug, and validate drivers and applications on UEFI 2.3*
- Benefits
 - All H/W commercially available, NDA not required
 - Build platform yourself or purchase an pre-assembled platform
 - UDK2010 Compatible, supports UEFI 2.3+
 - Long lifetime hardware platform support from Intel
- It's easy to build: Purchase Parts from supported H/W list, assemble, download UEFI 2.3. BIOS Image, and flash BIOS to motherboard using a SPI Flash programmer
- Pre-assembled systems available at HDNW, visit <http://www.tunnelmountain.net/> or (425) 943-5515 ext 4223

Visit www.intel.com/technology/efi for the latest

Intel UEFI Enabling Calendar



Events

IDF Beijing
April 12-13

IDF San Francisco
Sep 13-15

IDF PRC
April 12-13

Training

Q1 Base Training Oregon

Q1 Base Training Oregon

Q2 Base Training Beijing, Chi

Q2 Base Training May 2-4 OR

Q3 Base July 13-15th

Q4 Base Training

Q1 Base Training Oregon

Q1 Base Training Oregon

Q2 Base Training China

Plugfest

Redmond, WA
UEFI Summer Plugfest
July 6-9thnd

Taipei, Taiwan
UEFI Fall Plugfest
Oct 24-27
Insyde Hosting

US
UEFI Plugfest

Q1

Q2

Q3

Q4

Q1

Q2

2011

2012

UEFI Industry Resources

UEFI Forum

Welcome What's New: UEFI Specifications Update!

- UEFI 2.3** - Current UEFI Spec: v2.3 approved May 09 - Current Activities: Implementation and writer's guide
- UEFI 2.5** - Current UEFI Spec: v2.5 approved Oct 08 - Current Activities: Implementation support
- UEFI 2.6** - Current UEFI Spec: v2.6 approved May 09 - Current Activities: Implementation support
- UEFI 2.7** - Current version: v2.7 released May 09 - Next Release: v2.8 - SCT target mid 2010
- UEFI 2.8** - Current version: v2.8 released May 09 - Current Activities: Implementation support

www.uefi.org

UEFI Open Source

Introducing UDK2010

Component	Architecture	Development platform	Platform
UEFI for ARM	ARM	ARM	ARM
UEFI for IA32	IA32	IA32	IA32
UEFI for IA64	IA64	IA64	IA64
UEFI for MIPS	MIPS	MIPS	MIPS
UEFI for PowerPC	PowerPC	PowerPC	PowerPC
UEFI for SBC	SBC	SBC	SBC
UEFI for x86_64	x86_64	x86_64	x86_64

www.tianocore.org

Intel UEFI Resources

Extensible Firmware Interface (EFI) and Unified EFI (UEFI)

Background

The Unified EFI (UEFI) specification (previously known as the EFI specification) defines an interface between an operating system and platform firmware. The interface consists of data layers that contain platform-related information, boot service calls, and runtime service calls that are available to the operating system and its loaded modules. These provide a standard environment for booting an operating system and running pre-boot applications.

The UEFI specification was primarily intended for the next generation of IA architecture-based computers, and is an extension of the "Intel® Base Initiative" (BI) program that began in 1996. Intel's original version of the specification was publicly released in 1997 along with the EFI 1.0 revision. In 2005 the Unified EFI forum was formed as an industry-wide organization to promote adoption and continue the development of the EFI specification. Using the EFI 1.10 specification as the starting point, the industry group released the Unified EFI specification in 2008. The current version of the UEFI specification can be found at the UEFI web site.

More information

Specifications

The latest version of the UEFI specification is available from the UEFI web site.

<http://developer.intel.com/technology/efi>

Intel EBC Compiler

Intel C Compiler for EFI Byte Code

<http://software.intel.com/en-us/articles/intel-software-evaluation-center/#compilers>

UEFI Books

Harnessing the UEFI Shell: Playing the platform beyond BIOS

Beyond BIOS: Developing with the Unified Extensible Firmware Interface

www.intel.com/intelpress

Training/IHVs Contact

Laurie Jarlstrom

- Intel UEFI Training
- Laurie.Jarlstrom@intel.com

Bailey Cross

- Intel IHVs UEFI Support
- Bailey.T.Cross@intel.com

Thanks for attending the
UEFI Summer Plugfest 2011



For more information on
the Unified EFI Forum and
UEFI Specifications, visit
<http://www.uefi.org>



presented by



But wait, there's more ...

Wed
(July 6)

- UEFI State of the Union (10:30am, Intel)
- Implementing a Secure Boot Path with UEFI 2.3.1 (1:00pm, Insyde)
- UEFI SCT Overview (2:30pm, HP/Intel)

Thu
(July 7)

- Replacing VGA: GOP Implementation in UEFI (10:30am, AMD)
- UEFI prototyping using a Windows-hosted UEFI environment (1:00pm, Phoenix)
- EFI Shell Lab (2:00-4:00pm, “Thunder”, Intel)
- GOP Enabling & Testing Lab (4:30—5:30pm, “Thunder”, Intel)

Fri
(July 8)

- Best Practices for UEFI Option ROM Developers (10:30am, AMI)

Download presentations after the plugfest at www.uefi.org