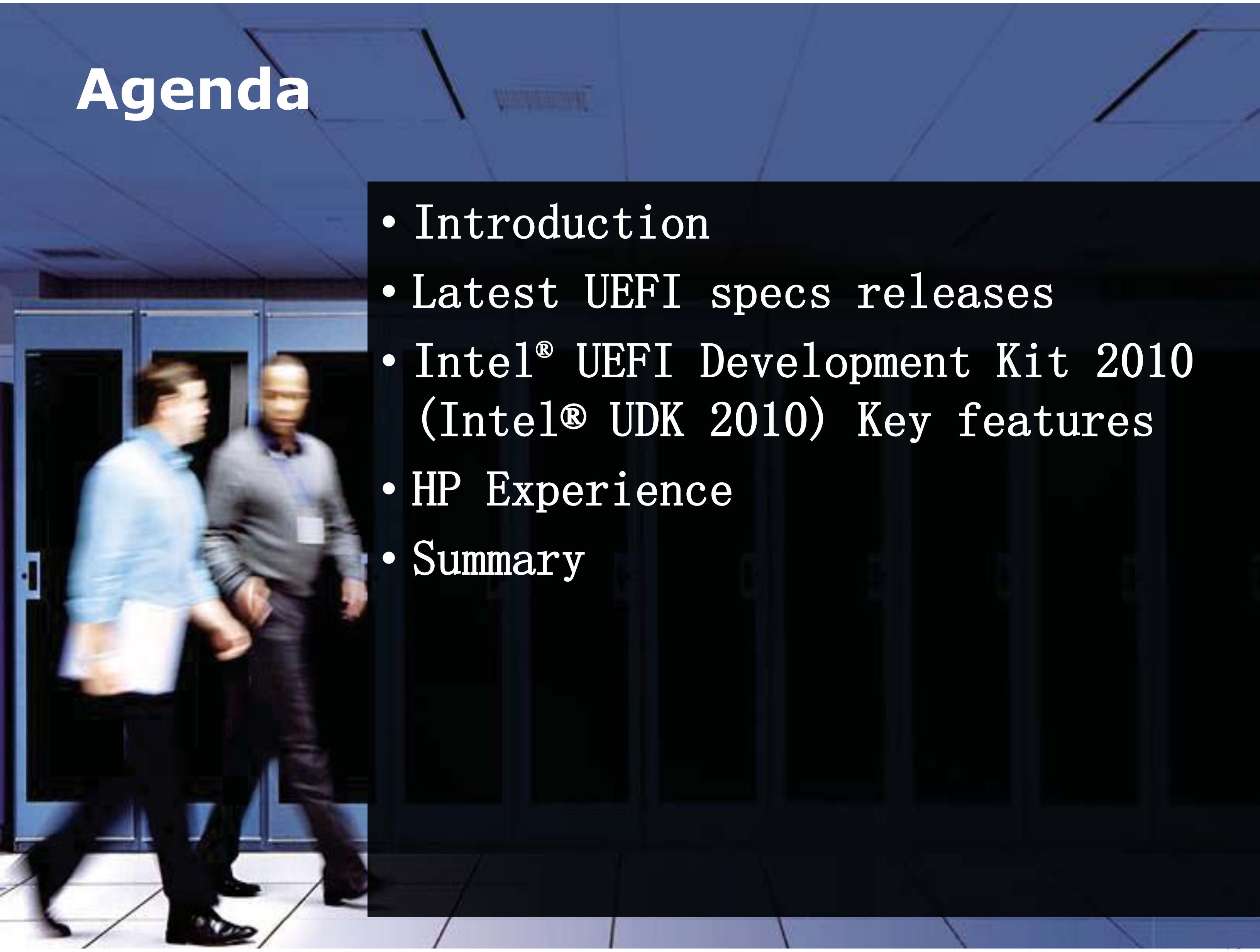
UEFI Technical Updates & Platform Innovations

Dong Wei - HP
魏东
Vincent Zimmer - Intel

Agenda



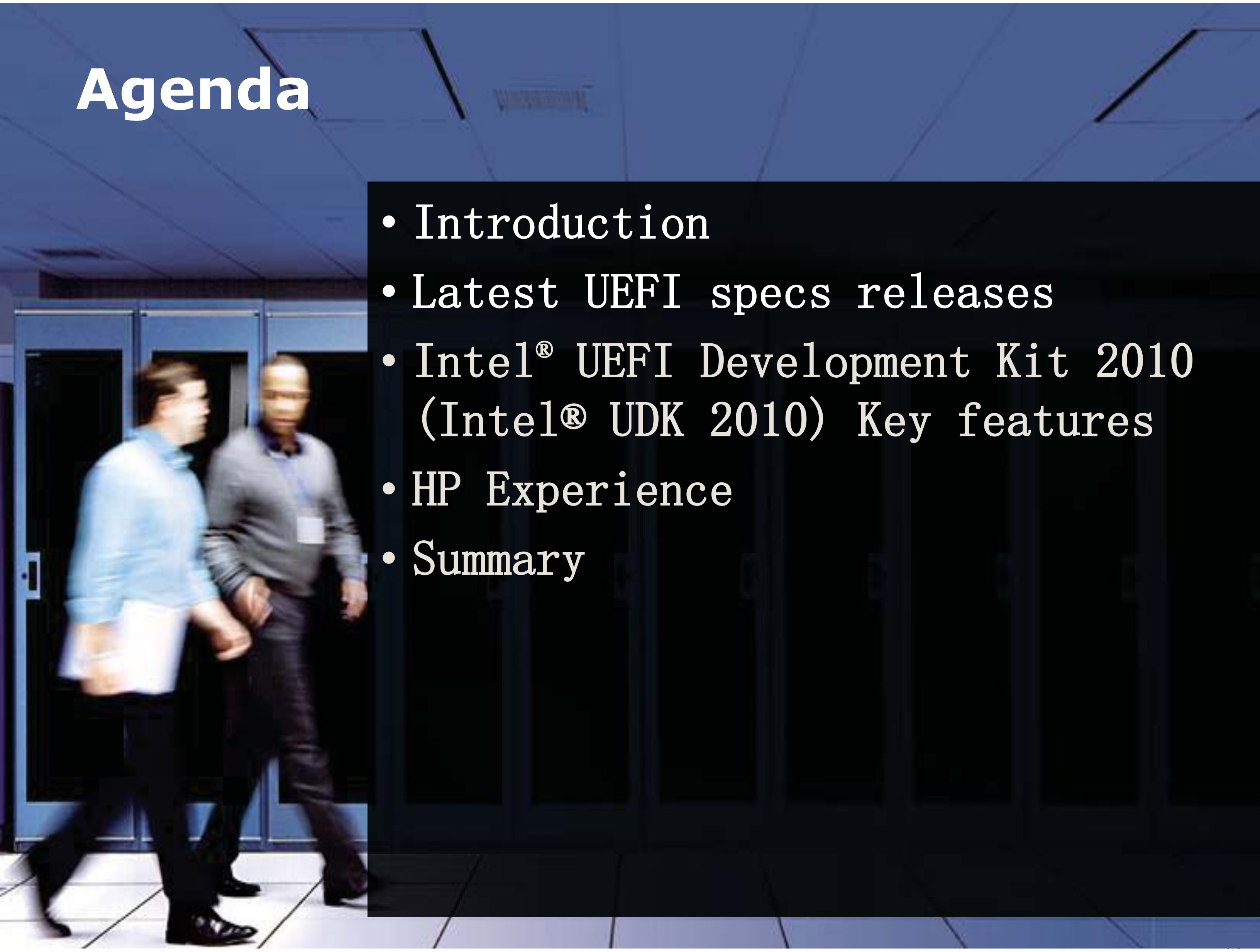
- Introduction
- Latest UEFI specs releases
- Intel® UEFI Development Kit 2010 (Intel® UDK 2010) Key features
- HP Experience
- Summary

INTRODUCTION – Dong Wei

- Distinguished Technologist/Strategist, HP
- Senior Member, IEEE
- Executive MBA
- Vice President, the UEFI Forum
- Secretary, the ACPI SIG
- Chair, PCI SIG Firmware WG

INTRODUCTION - Vincent Zimmer

- Principal Engineer, Intel
- Member IEEE, ACM
- BS EE Cornell University,
  MS CS University of Washington
- Lead of PI Security Subteam & Network Subteam in UEFI Forum
- 200+ issued patents, lead/co-author on 3 books, 2 book chapters, 10+ conference papers, 1 RFC

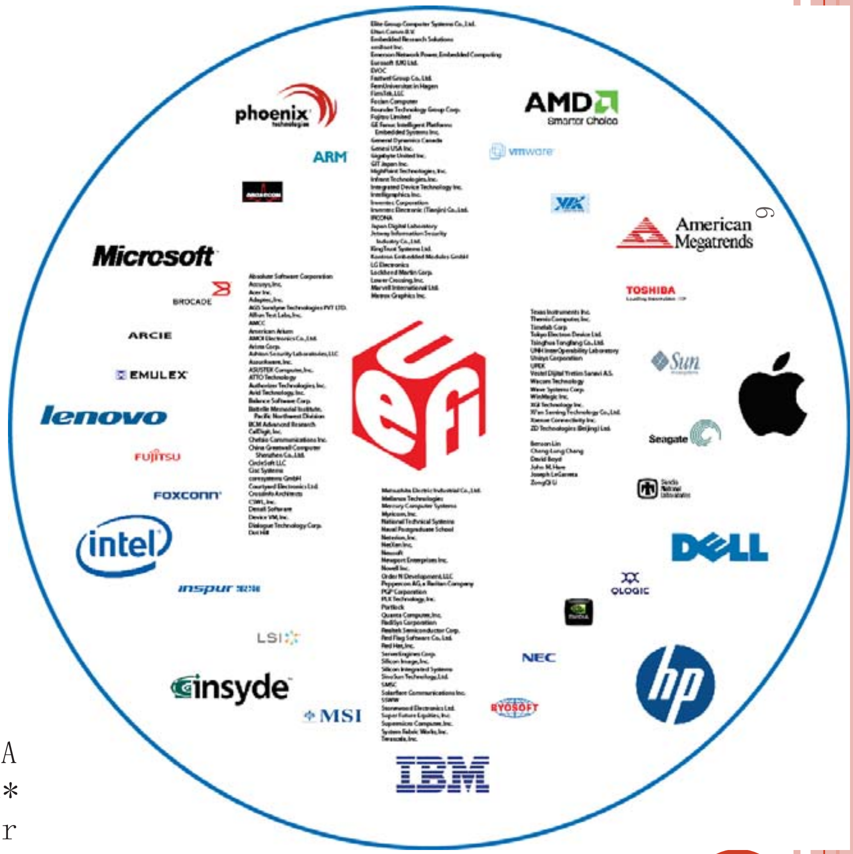


Agenda

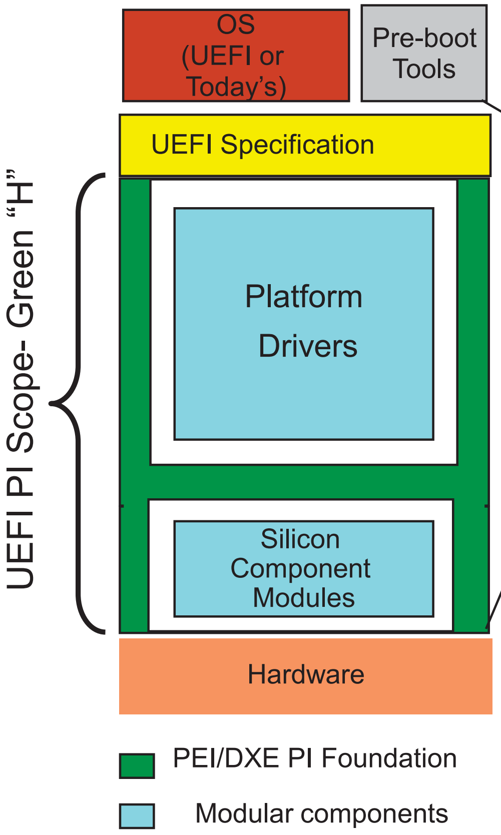
- Introduction
- Latest UEFI specs releases
- Intel® UEFI Development Kit 2010 (Intel® UDK 2010) Key features
- HP Experience
- Summary

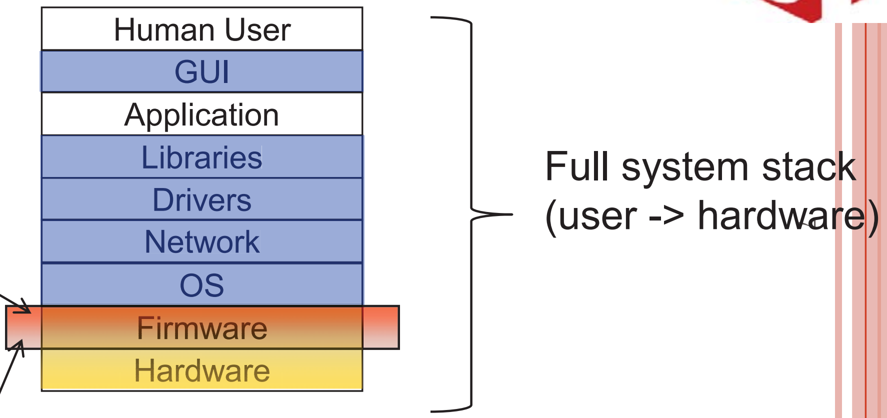
Industry BIOS Transition

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
2010	160 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



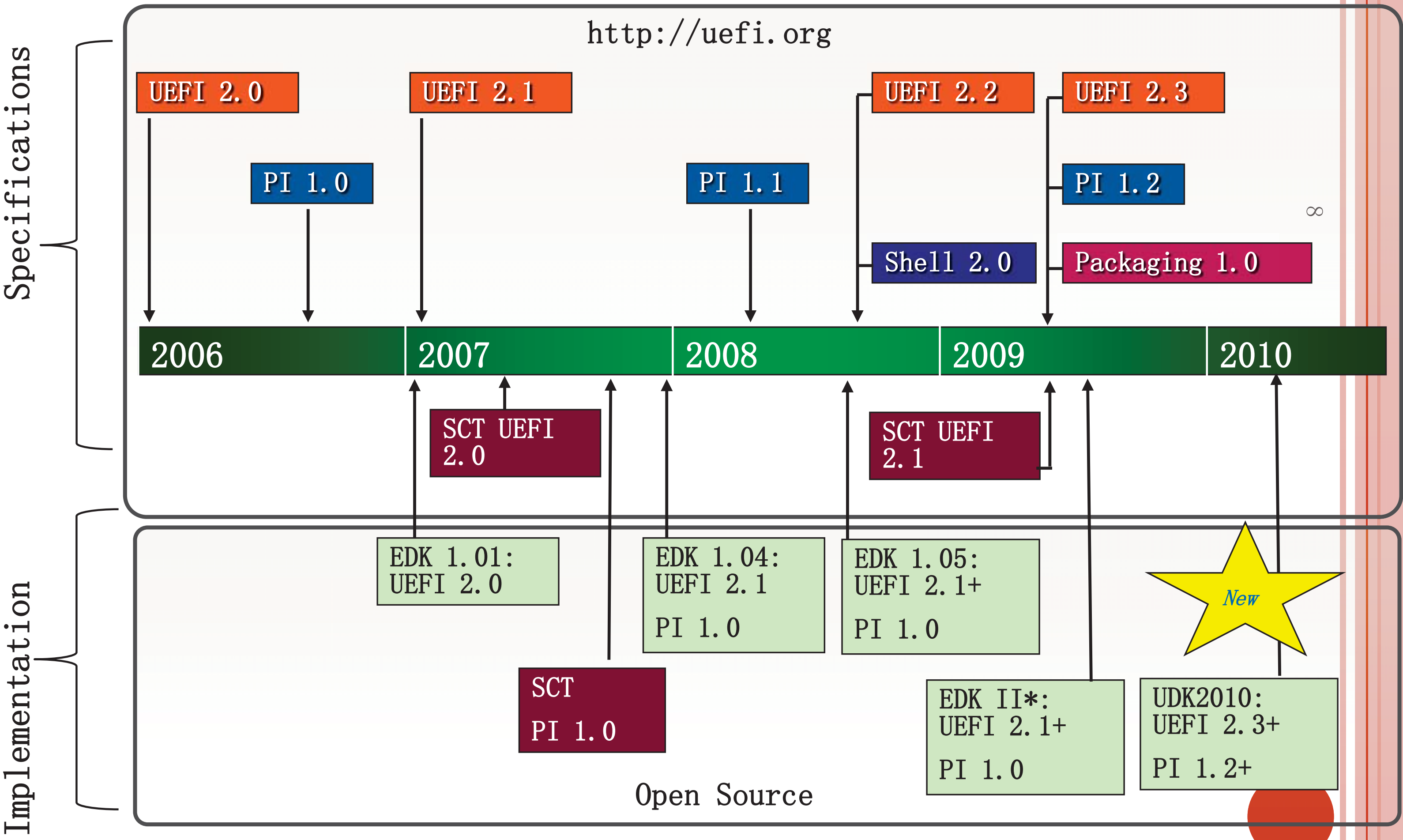
UEFI Platform Initialization Overview





- UEFI 2.3 specifies how firmware boots OS loader
- UEFI's Platform Initialization (PI) 1.2 Architecture specifies how Driver Execution Environment (DXE) Drivers and Pre-EFI Initialization (PEI) Modules (PEIMs) initialize SI and the platform
- DXE is preferred UEFI Implementation
- PEIMs, UEFI and DXE drivers implements networking, Update, other security features

UEFI Specification Timeline



Specifications

http://uefi.org

UEFI 2.0

PI 1.0

UEFI 2.1

PI 1.1

UEFI 2.2

Shell 2.0

UEFI 2.3

PI 1.2

Packaging 1.0

2006

2007

2008

2009

2010

SCT UEFI 2.0

SCT UEFI 2.1

Implementation

EDK 1.01: UEFI 2.0

SCT PI 1.0

EDK 1.04: UEFI 2.1 PI 1.0

EDK 1.05: UEFI 2.1+ PI 1.0

EDK II*: UEFI 2.1+ PI 1.0

New

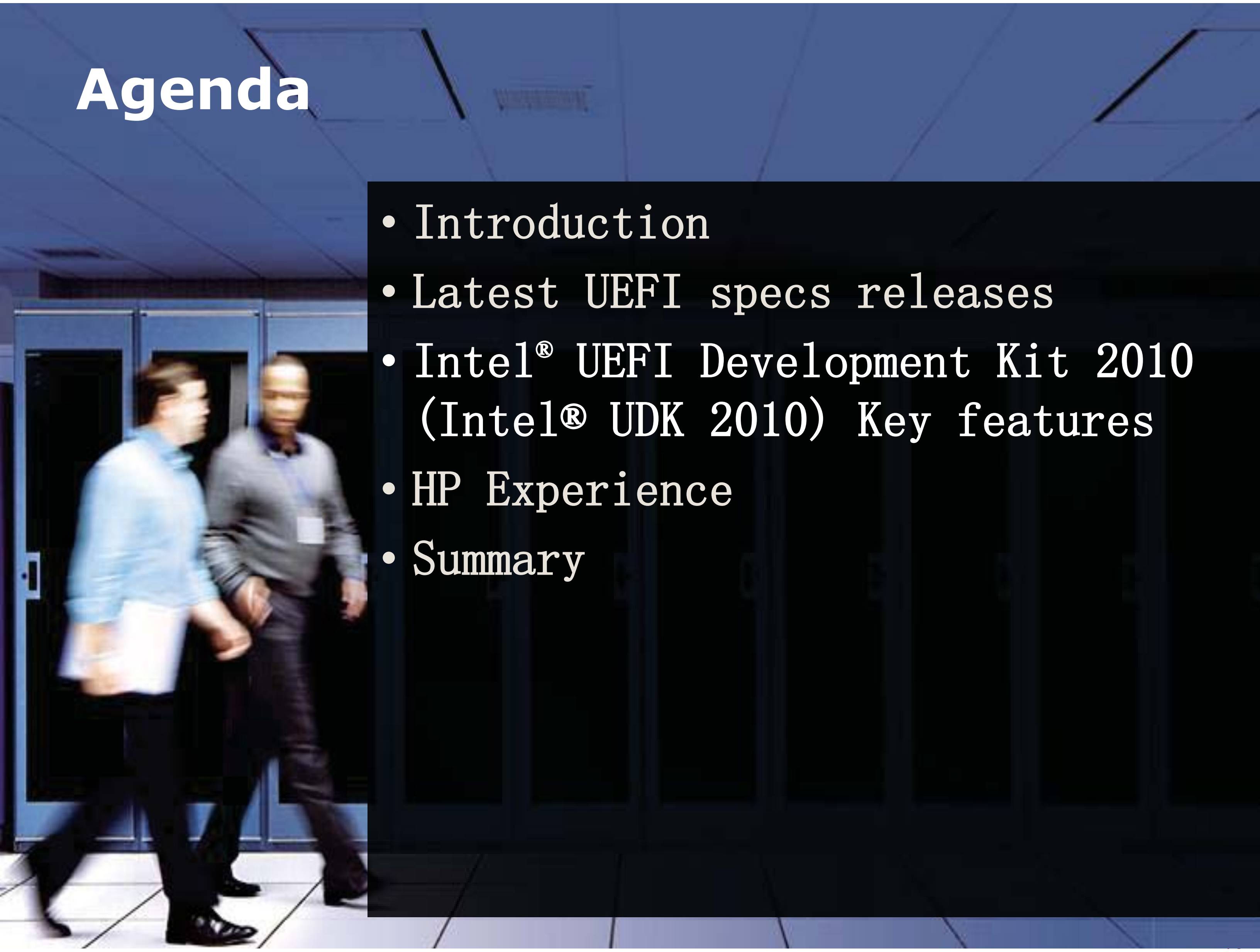
UDK2010: UEFI 2.3+ PI 1.2+

Open Source

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

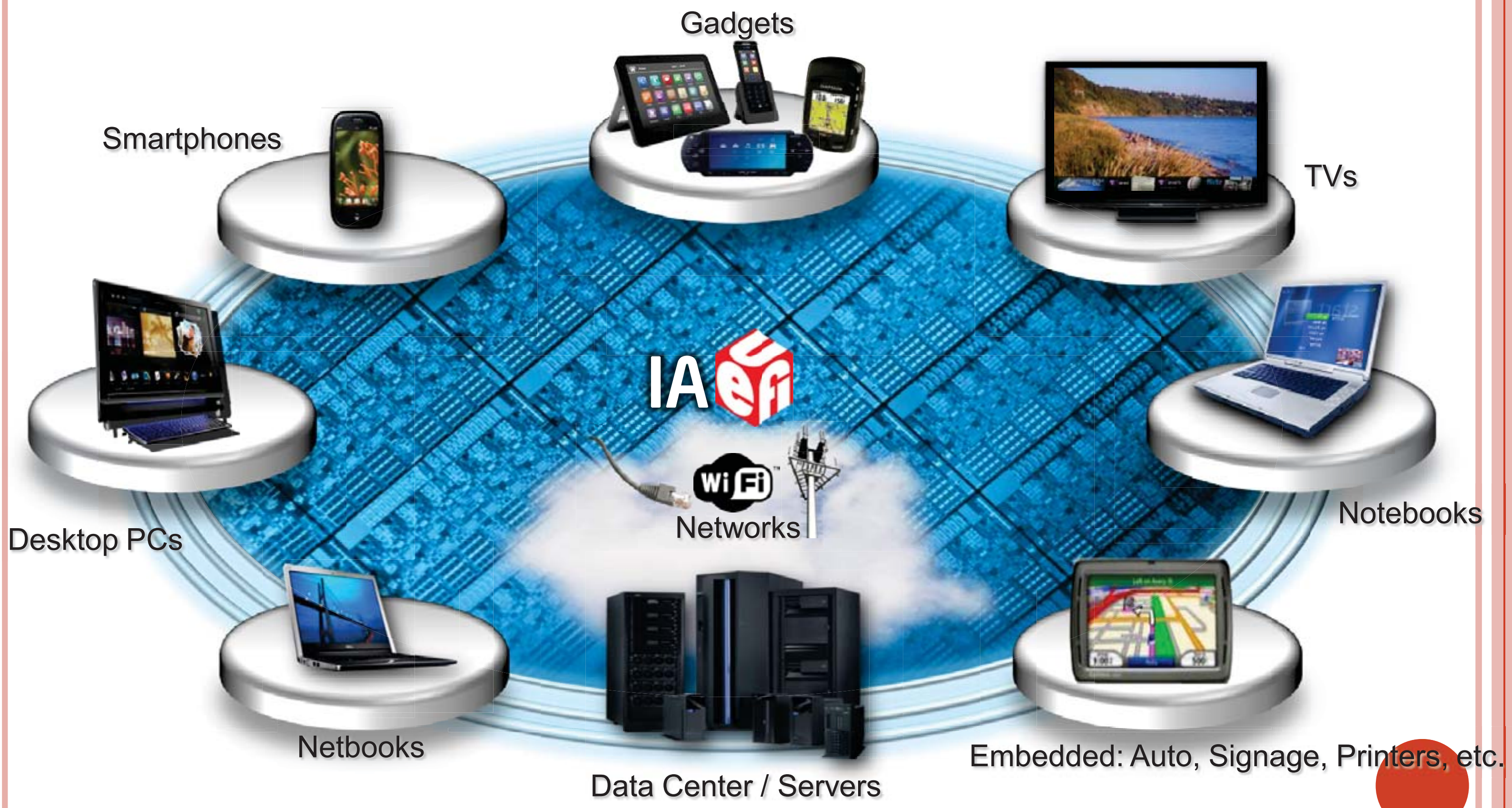
*** EDK II is same code base as UDK2010**

Agenda



- Introduction
- Latest UEFI specs releases
- Intel® UEFI Development Kit 2010 (Intel® UDK 2010) Key features
- HP Experience
- Summary

Intel® UDK2010 enables a common firmware development foundation across the compute continuum



Intel® UDK2010 Key Features

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
- Manageability

Support for UEFI Packages

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

Maximize Re-use of Source Code**

- 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 Chains**

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

Fast and Flexible Build Infrastructure**

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

*** benefit of EDK II codebase*

Intel® UDK2010 Value Proposition

OEMs/ODMs

- Reduced Development costs (code sharing)
- Fast TTM (quick integration, fast build, ref code)
- Flexibility to use modules from different suppliers
- Quality and Rich Development Foundation
- Easy to Innovate and Differentiate

End Users

- New standard-based Features (e.g. IPV6/IPSec)
- Advanced OEMs Innovative Capabilities
- Easy to use and configure systems
- Improved UI; Consistent Look & Feel
- Intelligent, Efficient and Secure Updates

IBVs

- Common scalable solutions
- Improved module deployment efficiency
- Support multiple customers efficiently
- Alignment with Intel dev foundation direction

OSVs

- Optimized Boot with Modern Look
- Pre-OS system software verification
- Enhanced network protocols for deployment
- System Boot from large capacity hard drives

SI Vendors/IHVs

- IP Protection/Binary Modules deployment oppty
- Reduced Development costs
- Improved Validation and Debug-ability
- Comply with OEMs requirements
- Multi-Tier Customers Enabling

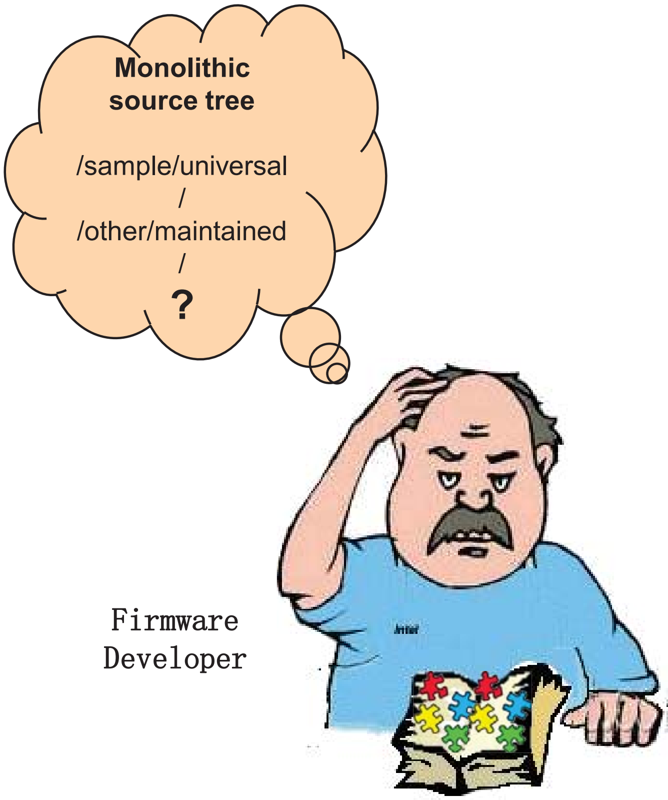
ISVs

- New opportunities for innovation (UEFI apps)
- Advanced Secure Pre-Boot App environment

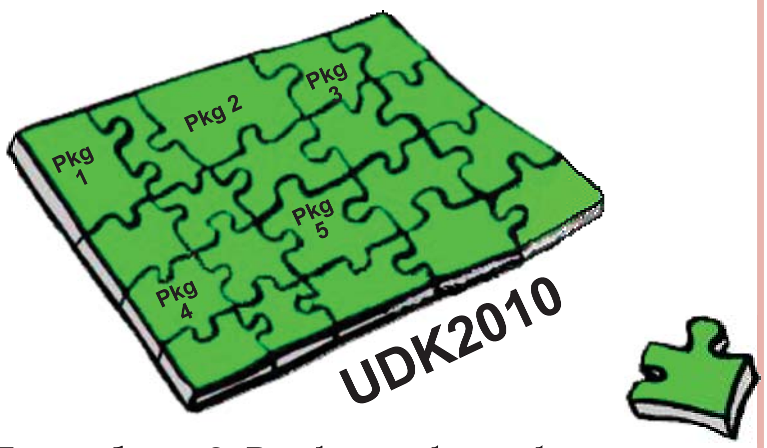
Spotlight on Select Intel® UDK2010 Features

- Packaging
- Driver Health
- Firmware Management protocol
- IP6 Networking
- UEFI Image signing
- UEFI User Identity

Packaging: Enabling fast delivery of advanced capabilities to market



Firmware Developer

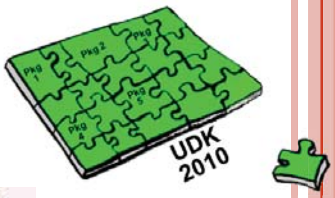


Example of Package-based deployment

- Package 1 Industry standard modules and drivers
- Package 2 Chipset PEIM’ s and DXE drivers
- Package 3 System board code
- Package 4 OEM Value-add

UDK2010 enables all the pieces to fit together and work!

Health and Management



- Driver Health Protocol
  - Allow for self-healing / correcting devices
  - Drivers and platform boot manager work in concert to correct & diagnose issues
  - Moving more autonomics into the platform

- Firmware Management Protocol
  - Consistent way for driver adapters and system board to allow for updates
  - More manageable elements that can
    - Update from error/bug
    - Fix field issue
    - Prevent roll-back to ‘bad’ image
  - Extend component manageability

CPU Caches Mainboard Memory SPD About

Motherboard

Manufacturer Gigabyte Technology Co., Ltd

Model [illegible]

Chipset Intel [illegible] Rev. [illegible]

Southbridge Intel [illegible]

LPCIO [illegible]

BIOS

Brand [illegible]

Version [illegible]

Date [illegible]

Graphic Interface

Version PCI-Express

Link Width x16 Max. Supported x16

Version [illegible]

OK

Rich set of features for package-driven deployment

IP6 Networking

- UEFI 2.3 network stack infrastructure
  - SAN/Datacenter boot
    - TCP-based iSCSI
    - Cryptographic logon
    - Multi-path/fail-over
  - IPsec for end-to-end security
  - Supports US Government requirements for IPV6 transition

http://www.antd.nist.gov/usgv6/usgv6-v1.pdf

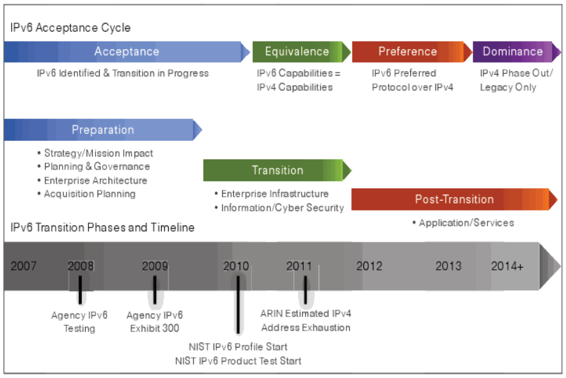
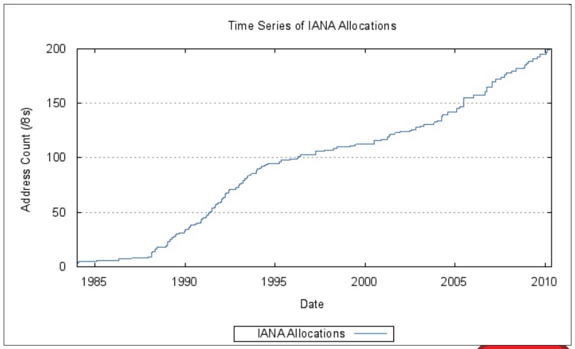

IPv6 Acceptance Cycle
Acceptance
IPv6 Identified & Transition in Progress
Equivalence
IPv6 Capabilities = IPv4 Capabilities
Preference
IPv6 Preferred Protocol over IPv4
Dominance
IPv4 Phase Out/ Legacy Only
Preparation
• Strategy/Mission Impact
• Planning & Governance
• Enterprise Architecture
• Acquisition Planning
Transition
• Enterprise Infrastructure
• Information/Cyber Security
Post-Transition
• Application/Services
IPv6 Transition Phases and Timeline
2007
2008
2009
2010
2011
2012
2013
2014+
Agency IPv6 Testing
Agency IPv6 Exhibit 300
ARIN Estimated IPv4 Address Exhaustion
NIST IPv6 Profile Start
NIST IPv6 Product Test Start

Figure 2: Federal IPv6 Transition Phases and Timelines

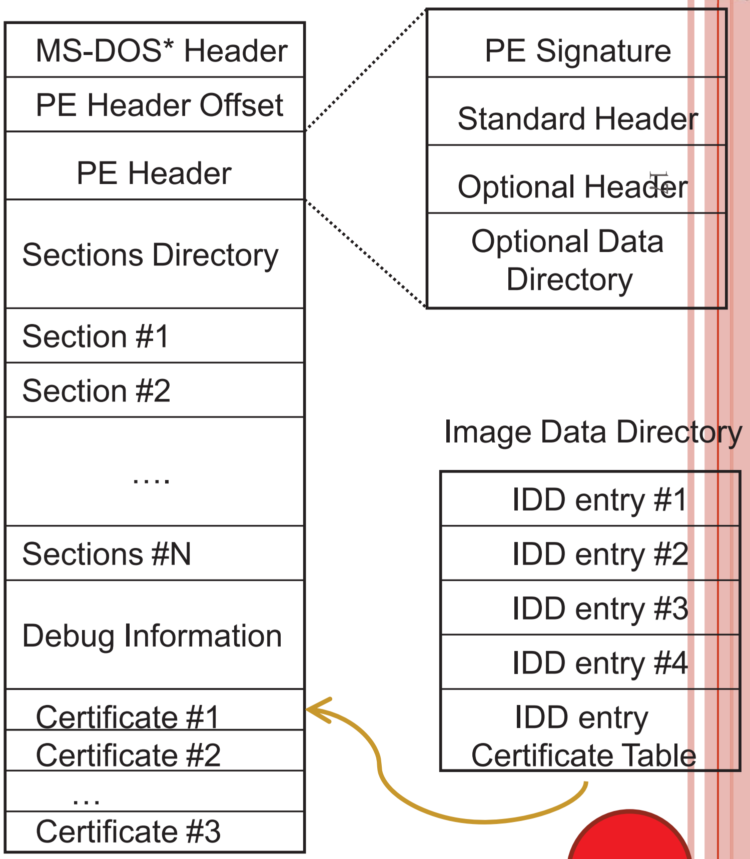
- Technology includes
  - IP4/6, UDP4/6, TCP4/6, DHCP4/6, VLAN, IPsec
    - Allows for concurrent network applications via design based upon MNP
    - Features dual stack: IP4, IP6, or both
  - Evolution of network boot to IPV6
    - Defined in IETF RFC 5970



US Government moving to IPV6 for equipment procurement

UEFI DRIVER SIGNING

- Adds policy around UEFI and its 3rd party image extensibility
  - Admixture of OS loaders, apps, and drivers in system
  - Gives IT control around these executables
  - Detects/prevents malware
- Technology includes
  - Supports "known-good" and "known-bad" signature databases
  - Policy-based updates to list
  - Rich signature types
    - SHA-1, SHA-256, RSA2048/SHA-1, RSA2048/SHA-256 & Authenticode*



MS-DOS* Header

PE Header Offset

PE Header

Sections Directory

Section #1

Section #2

….

Sections #N

Debug Information

Certificate #1

Certificate #2

…

Certificate #3

PE Signature

Standard Header

Optional Header

Optional Data Directory

Image Data Directory

IDD entry #1

IDD entry #2

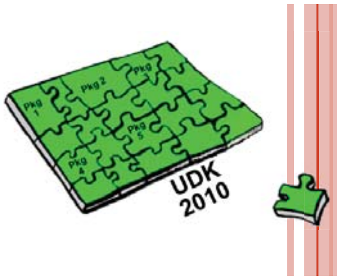
IDD entry #3

IDD entry #4

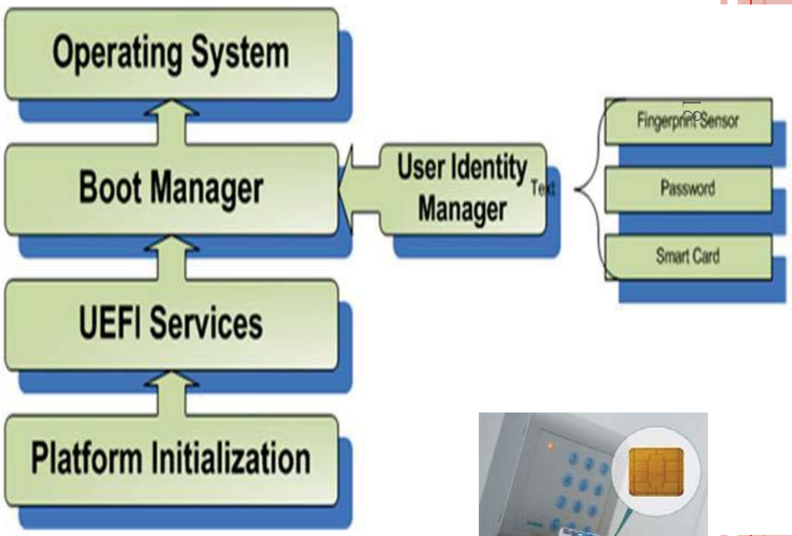
IDD entry Certificate Table

Extensible integrity architecture

UEFI User Identification

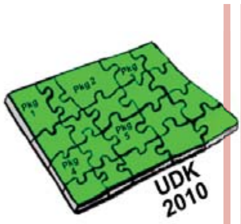


- Facilitates appropriate user and platform administrator existence
  - Ensures 'right' party applies policy/changes
  - Keeps out hacker/unlawful user
- Technology includes
  - Uses UEFI Human Interface Infrastructure (HII) to display information to the user
  - Introduces optional policy controls for connecting to devices, loading images and accessing setup pages
  - A standard framework for user-authentication devices
    - Network auth protocols, Smart cards, smart tokens & fingerprint sensors



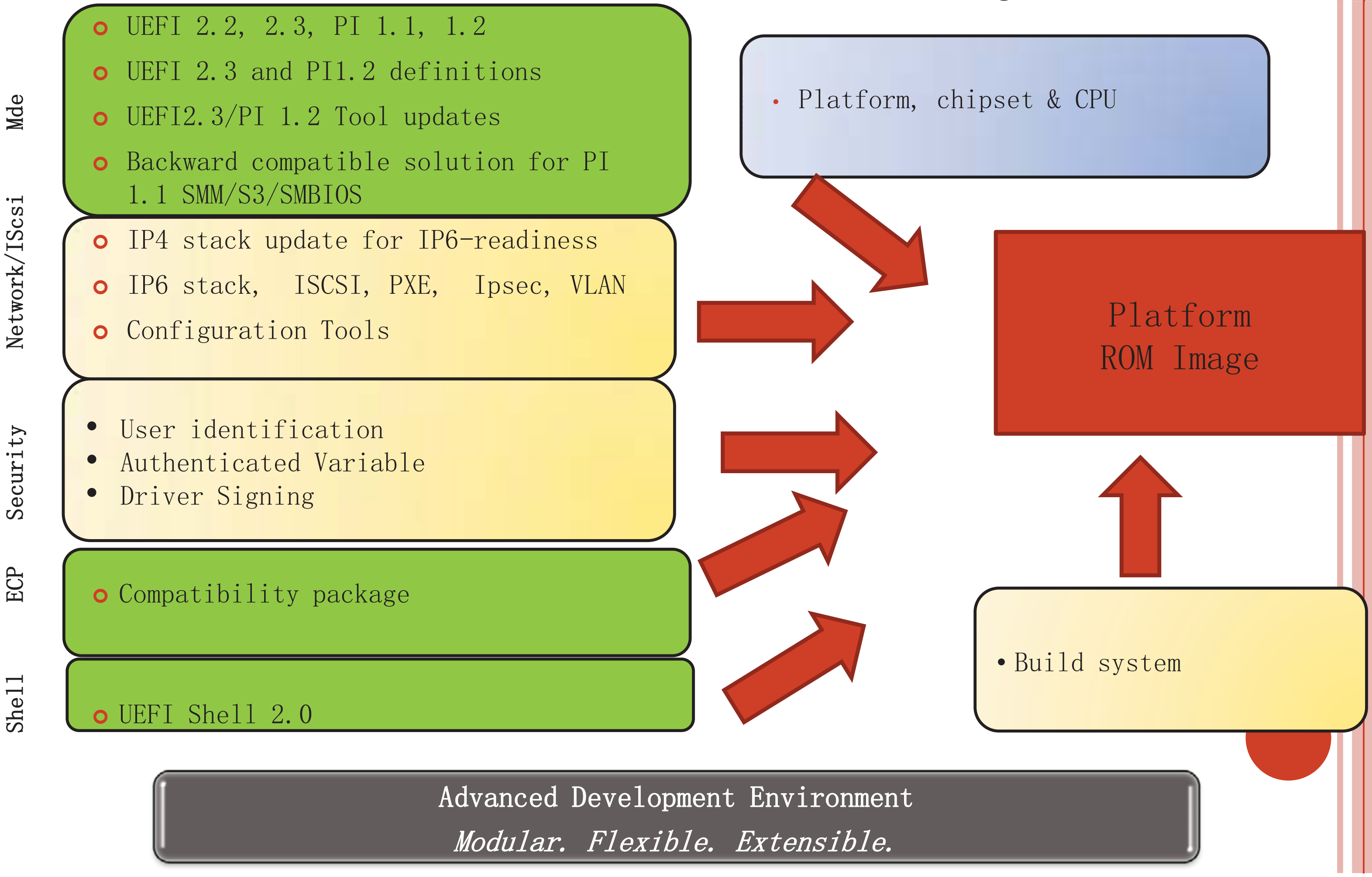
Support for various pre-boot authenticators

Intel® UDK2010 Putting it All together



UDK2010 Packages

Silicon Packages



Mde

- UEFI 2.2, 2.3, PI 1.1, 1.2
- UEFI 2.3 and PI1.2 definitions
- UEFI2.3/PI 1.2 Tool updates
- Backward compatible solution for PI 1.1 SMM/S3/SMBIOS

Network/IScsi

- IP4 stack update for IP6-readiness
- IP6 stack, ISCSI, PXE, Ipsec, VLAN
- Configuration Tools

Security

- User identification
- Authenticated Variable
- Driver Signing

ECP

- Compatibility package

Shell

- UEFI Shell 2.0

- Platform, chipset & CPU

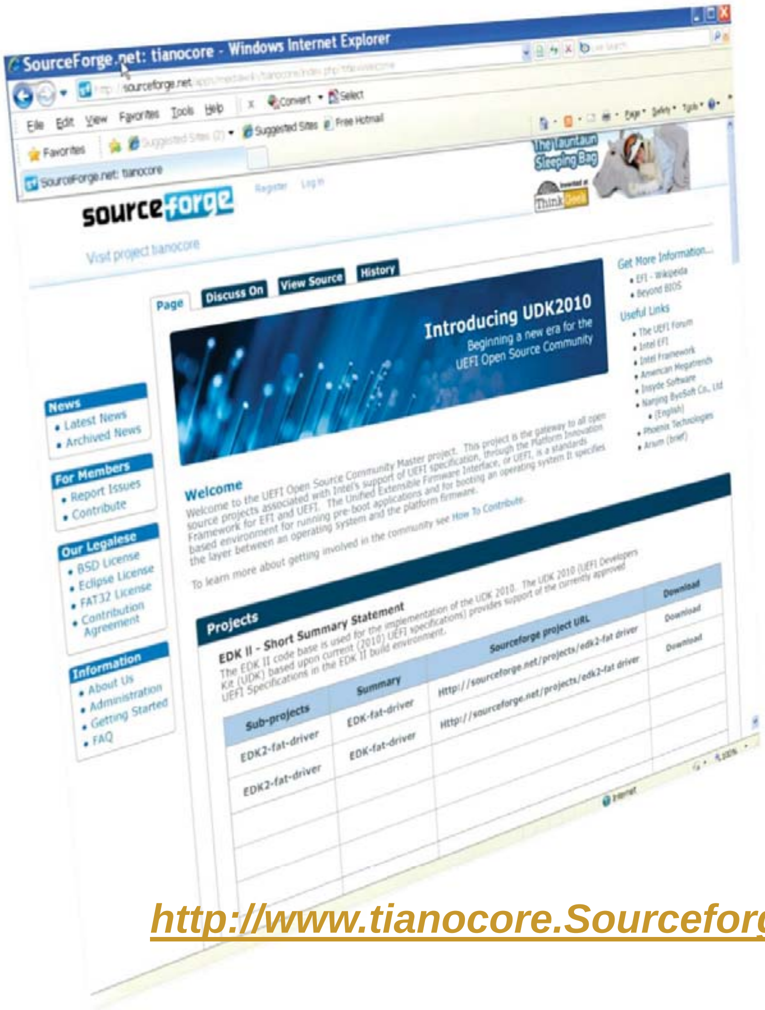
Platform ROM Image

- Build system

Advanced Development Environment

Modular. Flexible. Extensible.

UDK2010: AVAILABLE AT TIANOCORE.ORG



Introducing UDK2010
Beginning a new era for the
UEFI Open Source Community

Get More Information...
- EFI - Wikipeida
- Beyond BIOS

Useful Links
- The UEFI Forum
- Intel EFI
- Intel Framework
- American Megatrends
- Insyde Software
- Nanjing ByoSoft Co., Ltd
  - (English)
- Phoenix Technologies
- Arium (brief)

News
- Latest News
- Archived News

For Members
- Report Issues
- Contribute

Our Legalese
- BSD License
- Eclipse License
- FAT32 License
- Contribution Agreement

Information
- About Us
- Administration
- Getting Started
- FAQ

Welcome

Welcome to the UEFI Open Source Community Master project. This project is the gateway to all open source projects associated with Intel's support of UEFI specification, through the Platform Innovation Framework for EFI and UEFI. The Unified Extensible Firmware Interface, or UEFI, is a standards based environment for running pre-boot applications and for booting an operating system It specifies the layer between an operating system and the platform firmware.

To learn more about getting involved in the community see How To Contribute.

Projects

EDK II - Short Summary Statement

The EDK II code base is used for the implementation of the UDK 2010. The UDK 2010 (UEFI Developers Kit (UDK) based upon current (2010) UEFI specifications) provides support of the currently approved UEFI Specifications in the EDK II build environment.

Sub-projects	Summary	Sourceforge project URL	Download
EDK2-fat-driver	EDK-fat-driver	Http://sourceforge.net/projects/edk2-fat driver	Download
EDK2-fat-driver	EDK-fat-driver	Http://sourceforge.net/projects/edk2-fat driver	Download

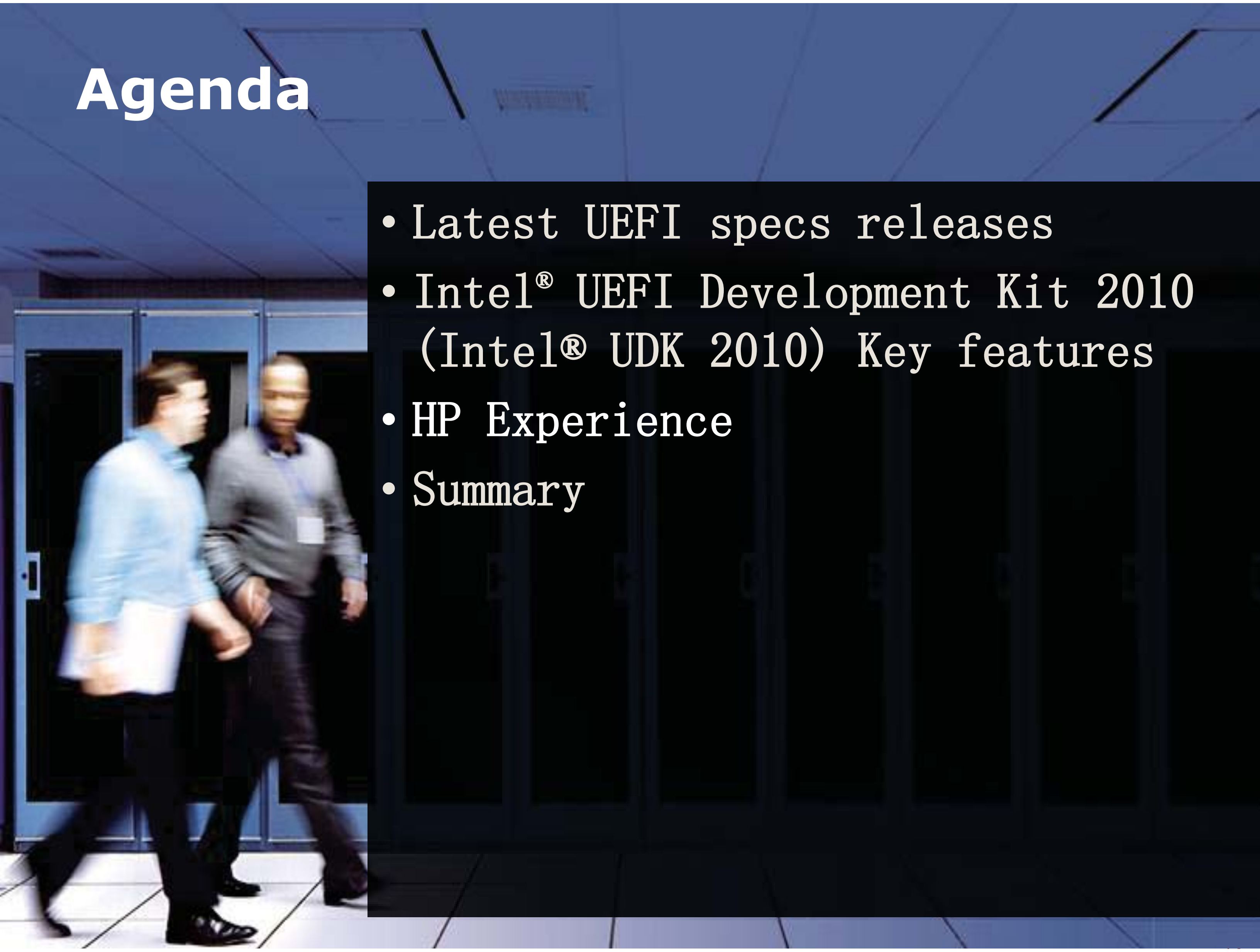
http://www.tianocore.Sourceforge.net

tianocore.org

UDK2010
Open Source
UEFI Development Kit

Develop. Contribute. Advance.

Agenda



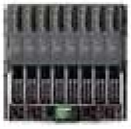
- Latest UEFI specs releases
- Intel® UEFI Development Kit 2010 (Intel® UDK 2010) Key features
- HP Experience
- Summary

UEFI DEVELOPMENT IN HP

Dong Wei

HP UEFI Support Status

- Integrity Business Critical Servers
  - Lead in the use of EDK II/UDK2010
- Printers/Scanners/Copiers/Laserjets
- Notebooks and Tablet PCs
  - HP innovating based on the UEFI technology: e.g., Diag, DayStarter
  - Commercial systems support UEFI boot



- Desktops and Workstations
  - Adopt a common UEFI codebase
  - Collaborate with Commercial Notebooks on HP features that provide enhanced manageability, security and ease of use
- Embedded: e.g., Storage, Network
  - Using UEFI to deliver next generation storage arrays

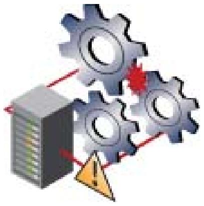
- UEFI/PI framework has enabled code sharing opportunities among business entities and with partners/vendors.
- HP supports UEFI in x64, ARM and Itanium architectures
  - UEFI provides opportunities of code sharing among systems based on different processor architectures

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

Mission-Critical Customer Challenges

Financial Services
Every minute of downtime = a minute of lost revenue!

Manufacturing and Distribution
Production comes to grinding halt



Healthcare
Patient outcomes depend on 24x7 access to data

Public Sector, and Communications, Media & Entertainment
Customer retention and fraud detection at risk

No tolerance for downtime

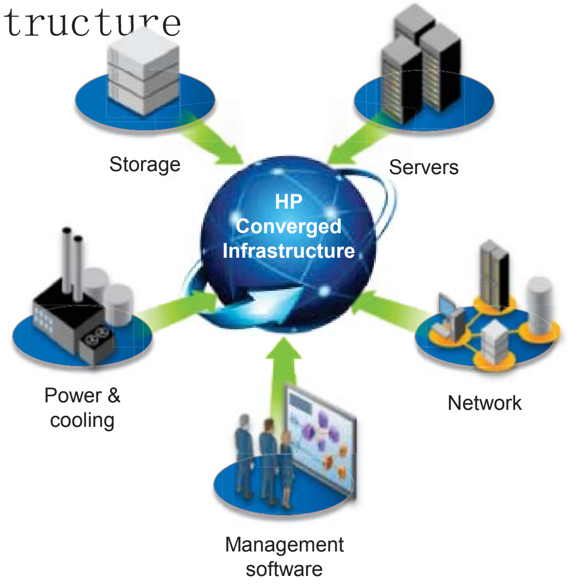
Increasing Service Level Agreements with decreasing budgets

Islands of legacy apps and monolithic systems

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

THE FIRST MISSION-CRITICAL CONVERGED INFRASTRUCTURE

- New Integrity systems optimized for the converged infrastructure



A common, modular architecture that simplifies, consolidates, and automates everything

A mission-critical infrastructure delivering the highest levels of reliability and flexibility

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

What HP looks for in Firmware

- HP Firmware Requirements
- Advanced Features support
  - Path to support network boot over IPv6, etc.
- HP Platform Innovations
  - Platform value-add modules
  - Protect intellectual property
- Improve Execution Excellence
  - Limited engineering resources
  - Faster time to market
  - Separate the hardware basic execution away from HP innovations
  - Reduced Integration & Validation Time
  - Used packaging supplied by Silicon driver modules from Silicon supplier
  - Maximize proper code reuse
  - Build-once, use by multiple platforms

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

INTEGRITY† LEADS HP EDK II TRANSITION

EDK II Enables HP Platform Innovation and Execution Excellence

Single Source Tree
For Superdome 2,
Blades and Rack
Servers

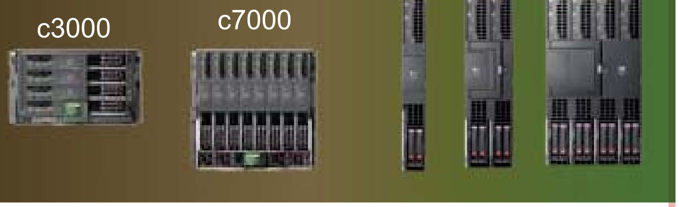
Superior Packages
Ability to reuse
Single module/solution
owner
Global visibility for bug fix

ECP Works Well
Reuse existing silicon
modules, applications

Superdome 2

The ultimate mission-critical consolidation platform

Integrity Server Blades

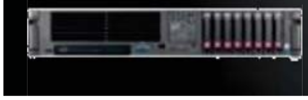


BladeSystem Matrix with HP-UX

First Converged Infrastructure platform for shared services, now mission-critical

Integrity 2s Rack Server

8-core scalability in 3x less compute density—without sacrificing RAS



Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

HP Contributions to EDK II

An Early Adopter

- Provided review/guidance that helped to refine EDK II to the present form
- Provided multiple feedback on simplification
- Recommended the use industry-standard tools instead of proprietary tools
- Provided fixes of build tool bugs
- Identified EDK II issues that arose when enabling compiler optimization with the Intel C compiler.
- Discovered multiple EDK II bugs
  - For example, a subtle design issue with the UEFI network stack that leads to severe performance degradation on large systems

HP Contributions benefited the entire open-source community

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

UEFI Transition Recommendations

Development Challenge

- Code development required large-scale source tree updates
  - Updates needed on average every 2-3 months
  - Expected in early adoption phase

UDK2010 addresses this challenge through *code base maturity, packaging technology, and catching up with the latest specs*

Developers Recommendation

- Pay close attention to the specifications/errata
- Parallel versions for different spec versions
- Maintain the infrastructure support and compatibility
  - Keep "deprecated" version of lib/include/PCD
  - Avoid changing build tools/lib/include/PCD
- Proactively communicate when a bug is fixed

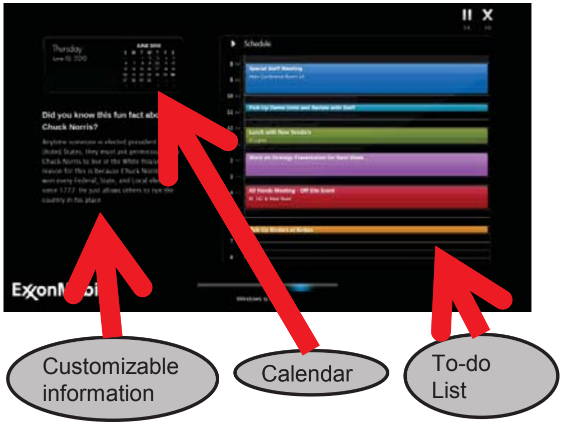
OEMs/IBVs Recommendation

- Take advantage of parallel versions if available
  - Get small-scale source updates needed
- Pull in the latest code at least every 2 months
- Use EDK II package solution
  - Create vendor-specific modules

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

HP DAYSTARTER: OUR APPROACH TO INSTANT-ON USER EXPERIENCE

A Better User Experience



Thursday

Schedule

Did you know this fun fact abo… Chuck Norris?

Special Staff Meeting

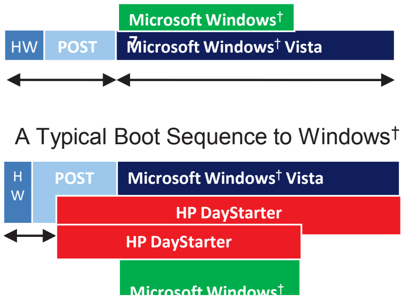
Lunch with New Vendors

Work on Strategy Presentation for Next Week

All Hands Meeting - Off Site Event

- Customer benefit:
  - Instant-on User Experience
  - displays user's info
    - calendar
    - to-do list
    - customizable info
  - before Windows† is booting.

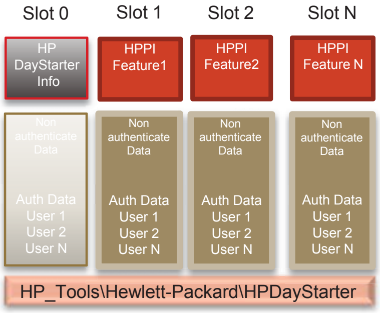
Boot Sequence Improvements



A Typical Boot Sequence to Windows†

The New HP Innovative Boot with DayStarter

Extensible Architecture



Innovative Technology

The main technology behind the HP DayStarter is for **UEFI** BIOS to locate the proper JPEG image and use the System Management Mode (SMM) to update the frame buffer content until Windows† is ready for system login.

At runtime, the HP DayStarter implements an Microsoft Outlook plug-in to capture the calendar information.

An HP Platform Innovation enabled by UEFI

Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

SUMMARY

- Intel® UDK2010 meets the OEMs advanced requirements for platform development and enables common firmware foundation across the compute continuum
- EDK II/UDK2010 enables HP Platform Innovations and Excellent Execution
- UDK2010 is available on tianocore.org