Introducing the New Intel® UEFI Development Kit: Industry Foundation for Platform Innovation

Vincent Zimmer, Principal Engineer, Intel

Nathan Skalsky, Advisory Engineer, IBM

Dong Wei, Distinguished Technologist/Strategist, HP

EFIS001

Sponsors of Tomorrow.™ (intel)

Agenda

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

Agenda

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

Industry BIOS Transition
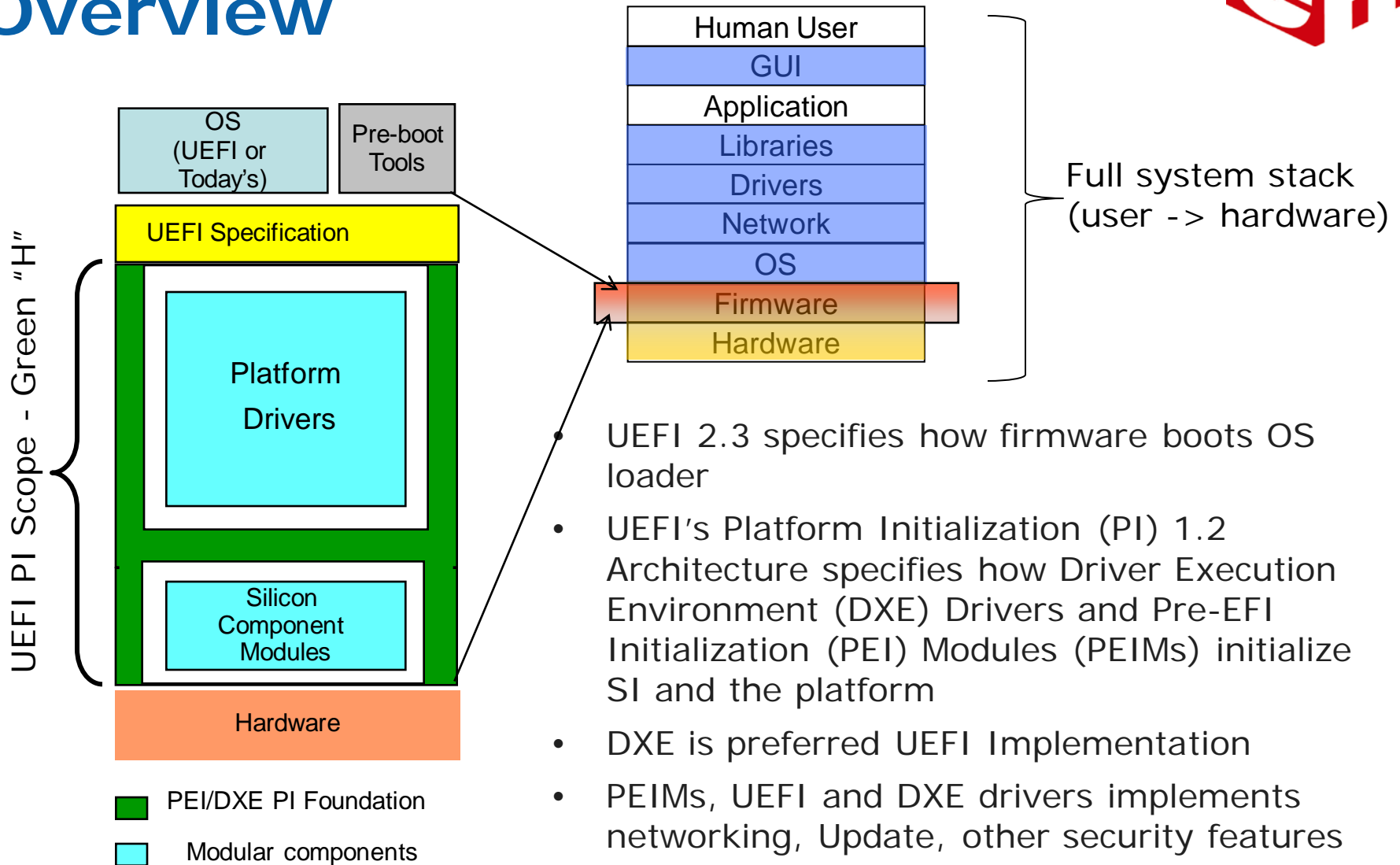
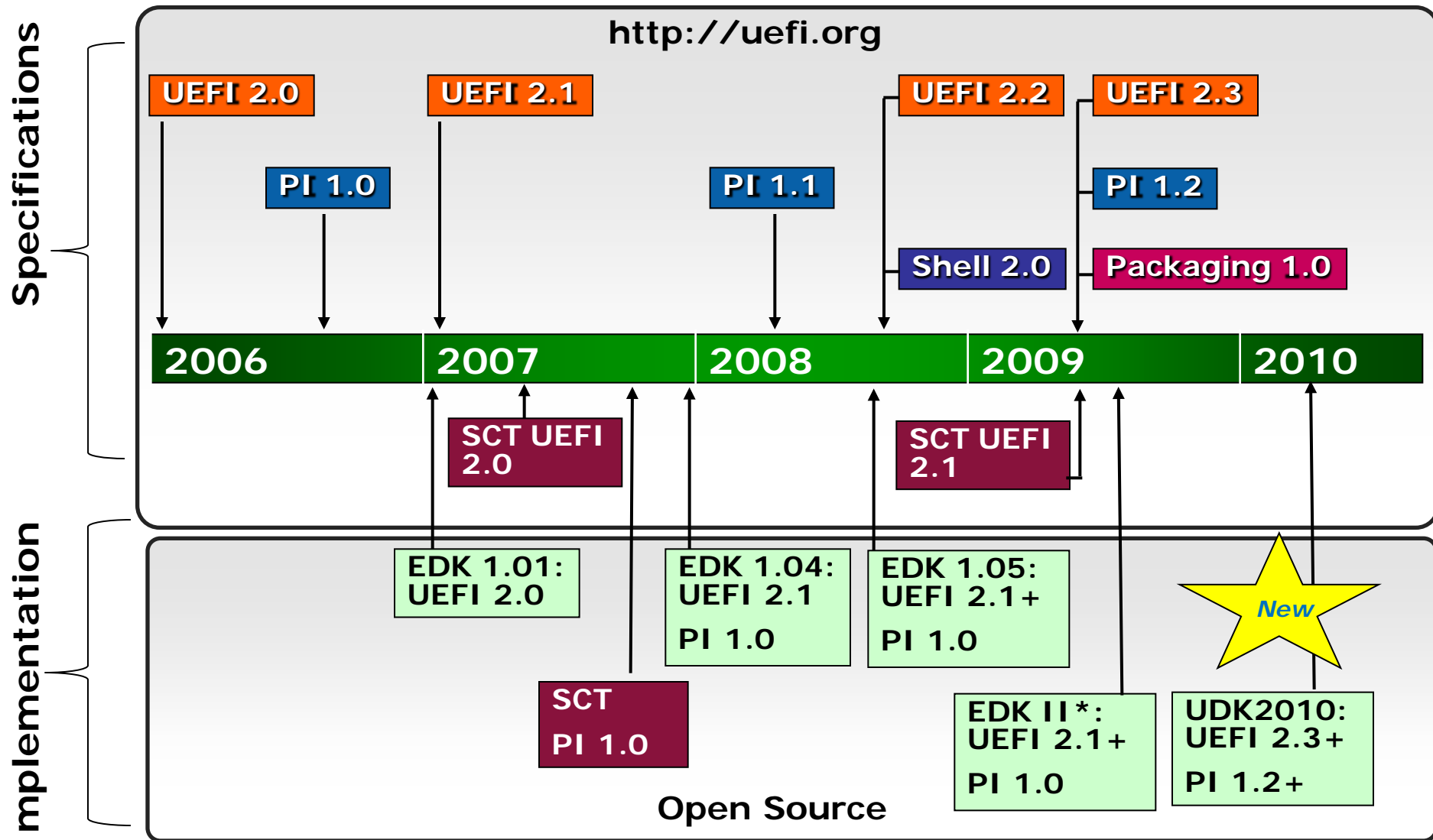**Pre-2000**
All Platforms BIOS were proprietary

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

4

UEFI Platform Initialization Overview

OS (UEFI or Today's)

Pre-boot Tools

UEFI Specification

UEFI PI Scope - Green "H"

Platform Drivers

Silicon Component Modules

Hardware

- PEI/DXE PI Foundation
- Modular components

Human User

GUI

Application

Libraries

Drivers

Network

OS

Firmware

Hardware

Full system stack (user -> hardware)

- 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

IDF2010
INTEL DEVELOPER FORUM

UEFI Specification Timeline

Specifications

http://uefi.org

| UEFI 2.0 | UEFI 2.1 | | UEFI 2.2 | UEFI 2.3 |

| PI 1.0 | | PI 1.1 | PI 1.2 |

| | | Shell 2.0 | Packaging 1.0 |

| 2006 | 2007 | 2008 | 2009 | 2010 |

SCT UEFI 2.0

SCT UEFI 2.1

Implementation

EDK 1.01: UEFI 2.0

EDK 1.04: UEFI 2.1 PI 1.0

EDK 1.05: UEFI 2.1+ PI 1.0

New

SCT PI 1.0

EDK II*: UEFI 2.1+ PI 1.0

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

IDF2010
INTEL DEVELOPER FORUM

Agenda

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

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

Gadgets

Smartphones

TVs

UEFI

Intel® UDK2010

Wi-Fi™

Networks

Notebooks

Desktop PCs

Netbooks

Data Center / Servers

Embedded: Auto, Signage, Printers, etc.

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

IDF2010
INTEL DEVELOPER FORUM

Intel® UDK2010 Key Features

Industry Standard Support:
UEFI 2.0, UEFI 2.1, UEFI 2.2, UEFI 2.3
PI 1.0, PI 1.1, PI 1.2

Delivery as Packages (with XML metadata):
- Import/export modules source/binaries to many build systems
- ECP provides reuse of EDK1117 modules

Maximize Reuse of Source Code:
- Platform Configuration Database (PCD)
- Library Classes/Instances
- Optimize for size or speed

Multiple Development OS:
Windows*, Linux*, OSX

Fast and Flexible Build Infrastructure:
- 4X+ Build Performance Improvement (vs EDKI)
- Targeted Module Build Flexibility

Multiple Tools Chains:
VS2003, VS2005, WinDDK, Intel, GCC

Extensible Foundation for Advanced Capabilities:
- Pre-OS Security, Rich Networking, Manageability, etc. (e.g. User Identity, Driver/Application signing, IPv6 networking, PXE, iSCSI)

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

IDF2010
INTEL DEVELOPER FORUM

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

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

IDF2010
INTEL DEVELOPER FORUM

Spotlight on Select Intel® UDK2010 Features

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

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

IDF2010
INTEL DEVELOPER FORUM

Packaging: Enabling Fast Delivery of Advanced Capabilities to Market

Monolithic source tree

/sample/universal
/
/other/maintained
/
?

Firmware Developer
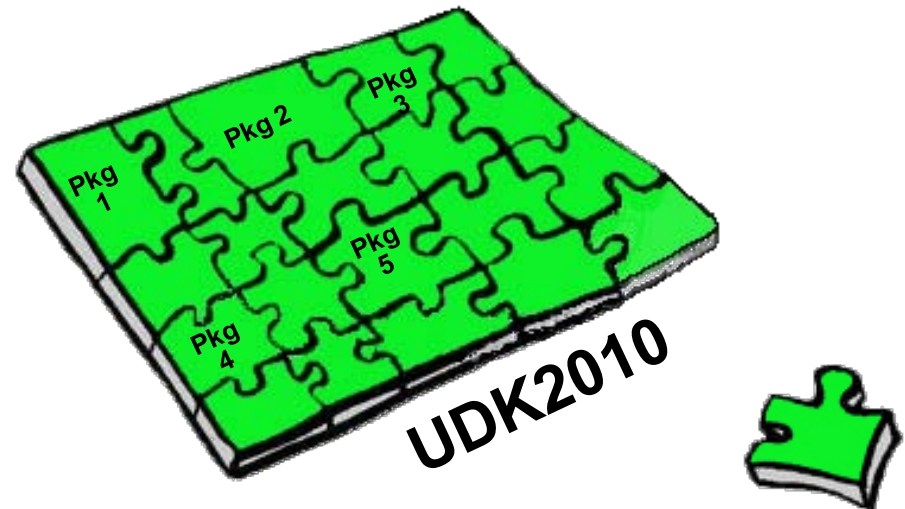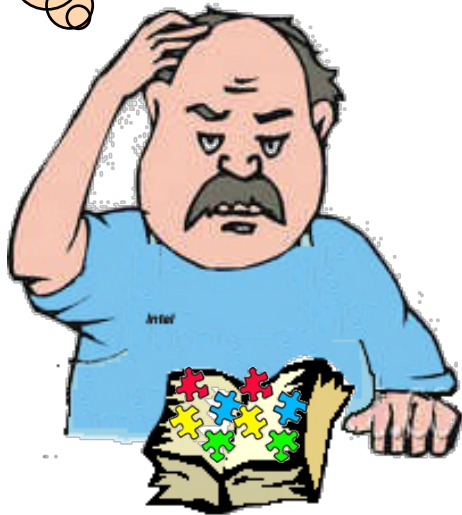
Example of Package-based deployment

- **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

UDK2010 enables all the pieces to fit together and work!

Health and Management

- Driver Health Protocol
  - Allows for self-healing / correcting devices
  - Drivers and platform boot manager work in concert to correct & diagnose issues
  - Moves more autonomics into the platform
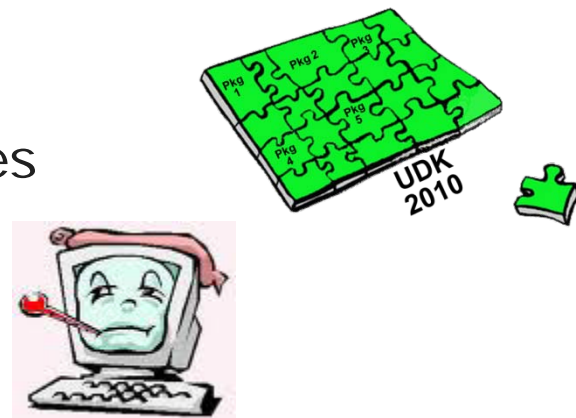
- Firmware Management Protocol
  - Consistent way for driver adapters and system board to allow for updates
  - More manageable elements that can
    - Update from error/bug
    - Fix field issue
    - Prevent roll-back to 'bad' image
  - Extends component manageability

Rich set of features for package-driven deployment

IDF2010

INTEL DEVELOPER FORUM

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

- 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
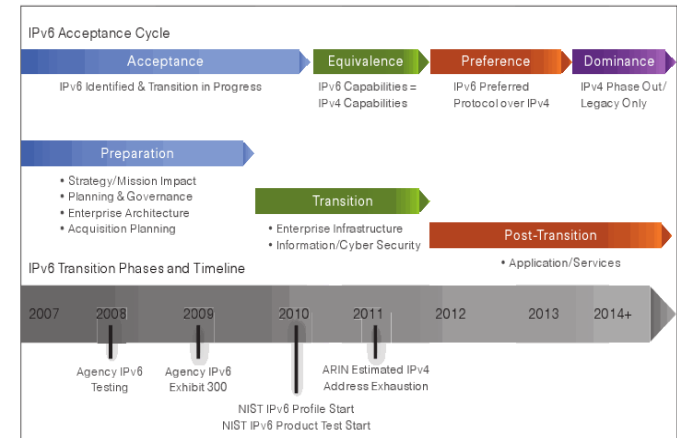
Figure 2: Federal IPv6 Transition Phases and Timelines

Time Series of IANA Allocations

US Government moving to IPV6 for equipment procurement

IDF2010
INTEL DEVELOPER FORUM
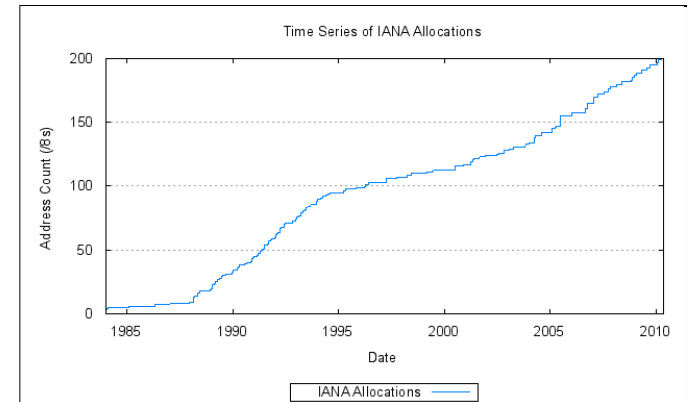
UEFI Driver Signing

- 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

UDK 2010

Extensible integrity architecture

IDF2010
INTEL DEVELOPER FORUM
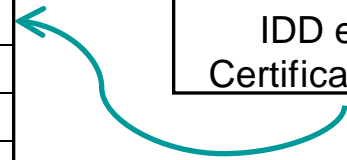
UEFI User Identification

- 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

Operating System

Boot Manager ← **User Identity Manager** Text

UEFI Services

Platform Initialization

Fingerprint Sensor

Password

Smart Card
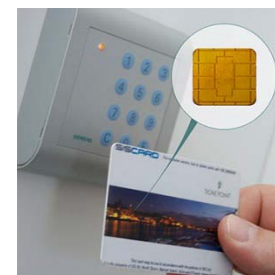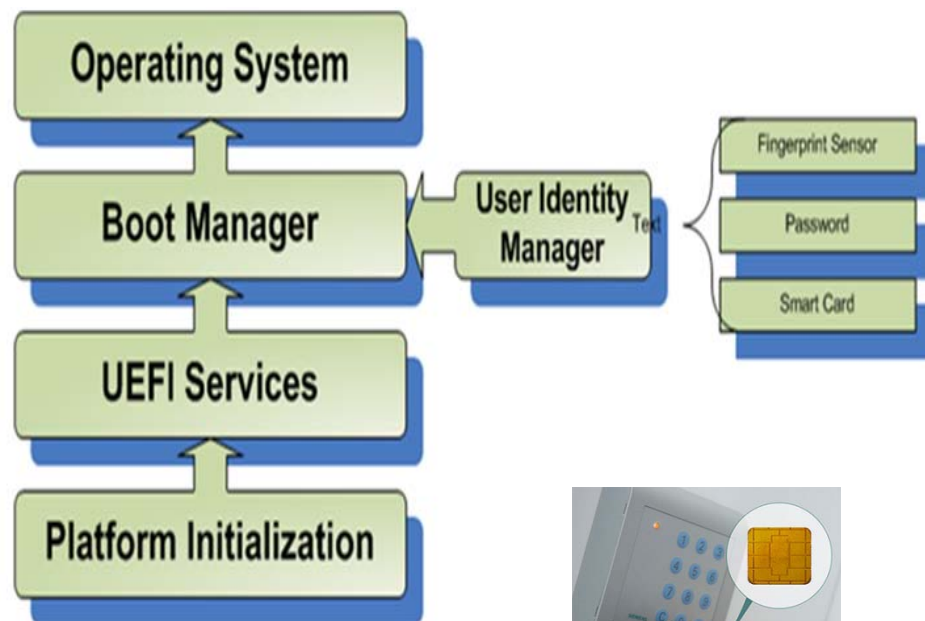
Support for various pre-boot authenticators

IDF2010
INTEL DEVELOPER FORUM

Intel® UDK2010 Putting it All together

Intel UDK2010 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

Silicon Packages

- Platform, chipset & CPU

Platform ROM Image

- Build system

Advanced Development Environment
Modular. Flexible. Extensible.

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

Intel® UDK2010 Available on tianocore.org

tianocore.org

Intel® UDK2010 *Open Source* UEFI Development Kit

Develop. Contribute. Advance.

http://www.tianocore.Sourceforge.net

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

IDF2010
INTEL DEVELOPER FORUM

Agenda

- **Latest UEFI specs releases**
- **Intel® UEFI Development Kit 2010 (Intel® UDK 2010) Key features**
- **IBM Experience**
- **HP Experience**
- **Summary**
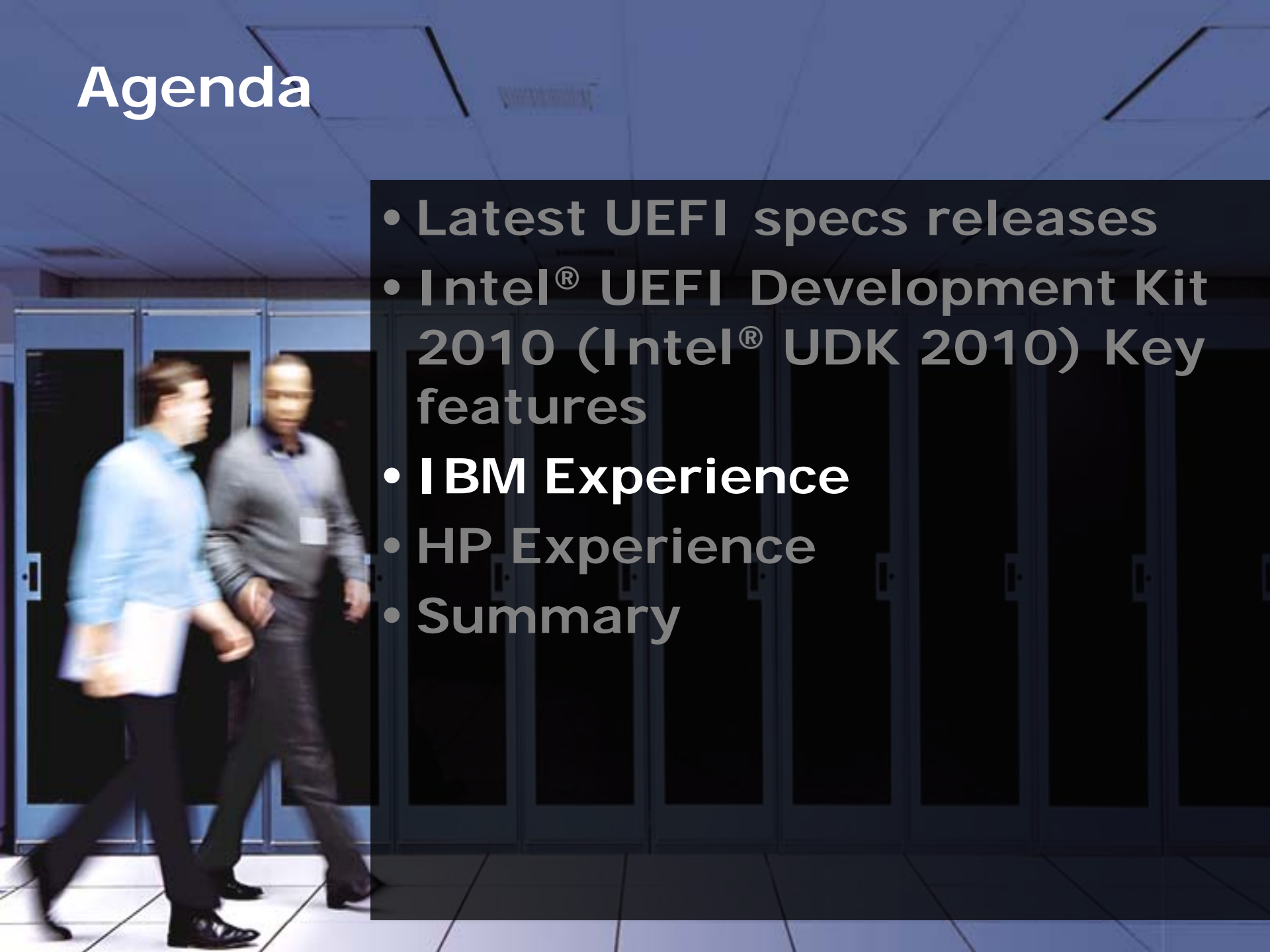
IBM Experience
"Smarter Firmware for a Smarter Planet"

Nathan C. Skalsky
Advisory Firmware Engineer, IBM
September 13th, 2010

Agenda

- Summary of IBM's commitment to UEFI, key milestones and business results

- UEFI vs. BIOS; Why UEFI brings value to IBM's Customers

- What IBM looks for in a next-generation UEFI development kit (UDK2010)

- UDK2010 Key benefits for UEFI development

- System x firmware development model

- Examples of IBM UDK2010 Value Add Packages

- EDKI Pain Points vs. UDK2010 Benefits

- UDK2010 Key Conceptual Improvements

- Summary

IBM's Major UEFI Milestones

- **Mid-2007**
  - UEFI Pilot Project and EDKI-based Core development Kickoff
  - IBM actively participates in UEFI and PI industry workgroups
- **Early 2009**
  - First UEFI-compliant IBM x86 product family launches (Xeon* 5500 blade, modular, and tower systems)
    - UEFI 2.1 and PI 1.1 Compliance
  - EDKII transition begins
- **Early 2010**
  - Second major UEFI-compliant product family launches (Xeon 6500/7500) based on EDKII UEFI Core
- **Sept 2010**
  - ⭐ **Over 1 Million Class 2 UEFI-compliant IBM x86 Servers Shipped**
- **Future UDK 2010**
  - Migration of IBM value-add/differentiation into EDKII native packages/library-class
    - UEFI 2.3 and PI1.2 Compliance (UDK2010)

IBM

IDF2010
INTEL DEVELOPER FORUM

IBM UEFI Key Features and Benefits

Key Feature	Customer Benefits
Easier configuration and management	• Ability to configure machines remotely with the Advance Settings Utility • In-band and out-of-band firmware update • Remote configuration which lowers TCO by reducing upgrade downtime and making platforms easier to manage and deploy
Simplified error handling	• No more cryptic event logs and reduction of out date errors in BIOS • Beep codes now covered completely by light path diagnostics
Abilities beyond legacy BIOS	• No limits on number of adapter cards (no more 1801 resource errors*) • Ability to manage adapter configuration out of "F1 Setup" • Ability to run pre-boot env. in 64-bit mode • Ability to boot storage partitions larger than 2.2TB

IBM's UEFI Success Factors

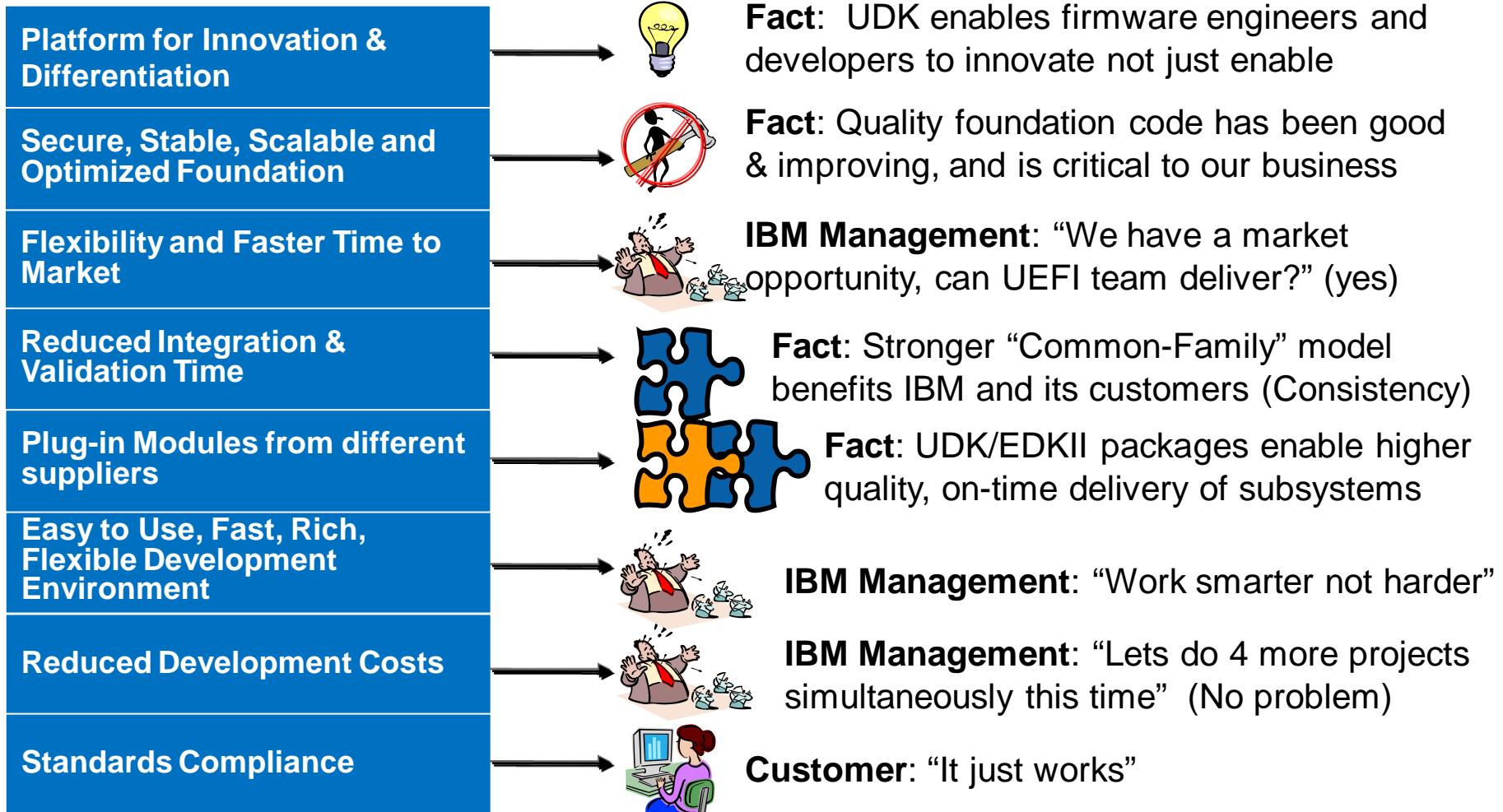- UEFI supported the most extensive IBM enterprise-class x86 portfolio launch in System x history (eX5)

  > "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

- Over 1million UEFI-compliant IBM System x Servers and Blades shipped to customers

  - 14 Product offerings ranging from entry-level towers, mid-range modular, HPC Cluster, and enterprise-class leadership 4-socket scalable systems
  - Transition occurred within normal product refresh cycle without adverse impact to product launch schedules

What We Look for in a Next Generation UEFI Development Ecosystem

Platform for Innovation & Differentiation	**Fact**: UDK enables firmware engineers and developers to innovate not just enable
Secure, Stable, Scalable and Optimized Foundation	**Fact**: Quality foundation code has been good & improving, and is critical to our business
Flexibility and Faster Time to Market	**IBM Management**: "We have a market opportunity, can UEFI team deliver?" (yes)
Reduced Integration & Validation Time	**Fact**: Stronger "Common-Family" model benefits IBM and its customers (Consistency)
Plug-in Modules from different suppliers	**Fact**: UDK/EDKII packages enable higher quality, on-time delivery of subsystems
Easy to Use, Fast, Rich, Flexible Development Environment	**IBM Management**: "Work smarter not harder"
Reduced Development Costs	**IBM Management**: "Lets do 4 more projects simultaneously this time" (No problem)
Standards Compliance	**Customer**: "It just works"

UDK Development Benefits

Packages	Integration effort	Developer efficiency
■ Package(s) can come from different providers, such as TianoCore, IHV, etc. ■ Ability to self-contain functionality and better manage dependencies	■ Reduce integration effort with package based release – Dramatically lower integration time for merging updates – More able to "divide and conquer"	■ Improve developer efficiency – Improved build time – Better code documentation – Strong/Explicit package structure to support isolation and clean Core/Platform model – New features such as PCD, Library class to allow common function to be extended safely/efficiently

IBM

IDF2010
INTEL DEVELOPER FORUM

UDK2010 Customers & OEM Benefits

Improved standardization, feature set and consistency
- EDKII core code follows the UEFI and PI standards closely.
- New features, delivered in UDK2010 packages, can reach customers sooner due to better code containment and ease of integration
- More consistent user experience and operation since more code is shared (between platforms and generations)
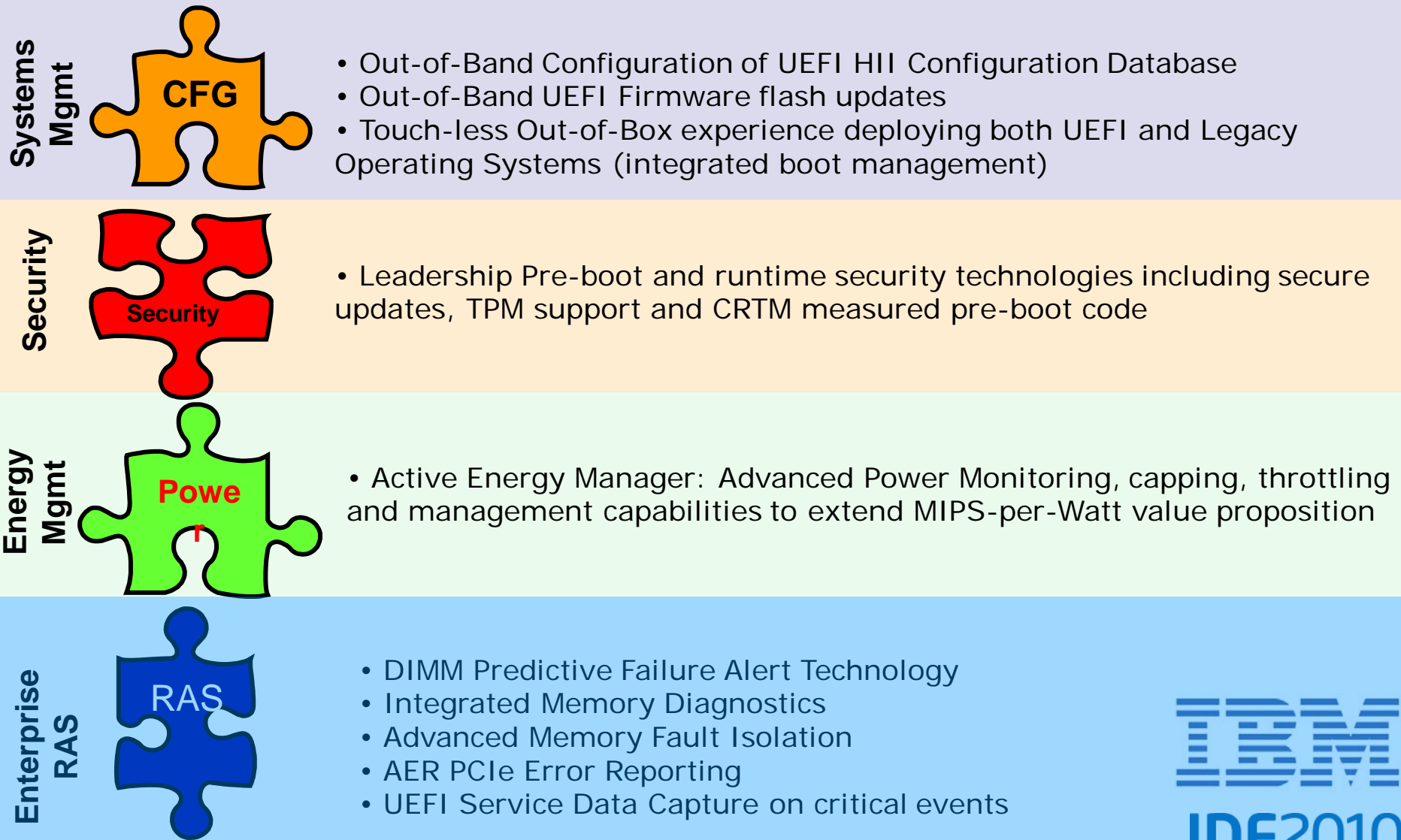
Easy for OEM vendor to personalize, brand and extend
- OEM vendors can set a look and feel through PCD and IBMs OEM firmware volume toolkit
- OEM vendors can extend functionality through adding signed drivers to the OEM firmware volume

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

IBM UDK-based Common Core 'Hexagon' Development Model

Platform Uniqueness

Chipset Family

IBM Innovation / Value Features

Secure · Power · RAS · CFG · UI · BOFM

UDK2010 Foundation

UEFI 2.3 Framework

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

IDF2010
INTEL DEVELOPER FORUM

IBM UDK2010 Value-Add in action

Systems Mgmt

CFG

- Out-of-Band Configuration of UEFI HII Configuration Database
- Out-of-Band UEFI Firmware flash updates
- Touch-less Out-of-Box experience deploying both UEFI and Legacy Operating Systems (integrated boot management)

Security

Security

- Leadership Pre-boot and runtime security technologies including secure updates, TPM support and CRTM measured pre-boot code

Energy Mgmt

Power

- Active Energy Manager: Advanced Power Monitoring, capping, throttling and management capabilities to extend MIPS-per-Watt value proposition

Enterprise RAS

RAS

- DIMM Predictive Failure Alert Technology
- Integrated Memory Diagnostics
- Advanced Memory Fault Isolation
- AER PCIe Error Reporting
- UEFI Service Data Capture on critical events

IBM

IDF2010
INTEL DEVELOPER FORUM

28

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

IBM UDK2010 Value-Add in action (cont.)

Legacy Support

CSM

- IBM Surepath™ CSM (Legacy x86 BIOS support for legacy OS support)
  - Touch-less CSM invocation - auto detection of boot target
  - Full support of legacy Option ROMs

Virtualization

SRIOV,VT

- SRIOV – Ability to share adapter physical functions across multiple guest OS instances.
- Intel Virtualization Technology Support (VT)

Enterprise Scalability

eX5
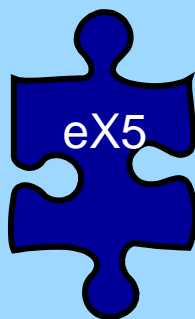
- Intel® Xeon® 7500 Support
- Intel® QPI Scalability
- IBM EXA Scalability
- MAX5 Memory Expansion Support
- FlexNode Technology

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

IDF2010
INTEL DEVELOPER FORUM

EDKI vs. UDK2010 Features

- **EDKI Challenge**: Large amount of source code (compared to typical BIOS implementations), longer and more involved build process, extended code review time needed
- **UDK2010 Solution**: UDK2010 Packages allow IBM to manage code at the feature/technology level making division of labor cleaner and more efficient
- **UDK2010 Solution**: UDK2010 doxygen-style commenting makes code review, API reference, and education far easier to accomplish

- **EDKI Challenge**: Overriding/extending core features requires platform team to take ownership and manually merge updates
- **UDK2010 Solution**: Library Class/Instance concept allows platform teams to define custom implementations for standard interfaces

- **EDKI Challenge**:   BIOS developers need 'context shift' and time to become proficient UEFI developers
- **UDK2010 Solution**: Improved in-code documentation and logical code-resource grouping (packages) have improved bring-up time of new talent

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

IBM

IDF2010
INTEL DEVELOPER FORUM

IBM Experience Conclusion

Parity+: EDKI enabled IBM to efficiently transition its entire range of x86 offerings from BIOS to UEFI 2.1 on-time and without disruption in the pre-boot feature set

Parity++: EDKII enabled IBM to reach beyond functional parity and innovate with our eX5 enterprise-class systems

Innovation+: UDK2010 is enabling IBM to further extend its x86 pre-boot technology leadership by providing a robust UEFI 2.3/PI 1.2 development environment from which to deliver, package, and distribute advanced pre-boot technology

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

Agenda

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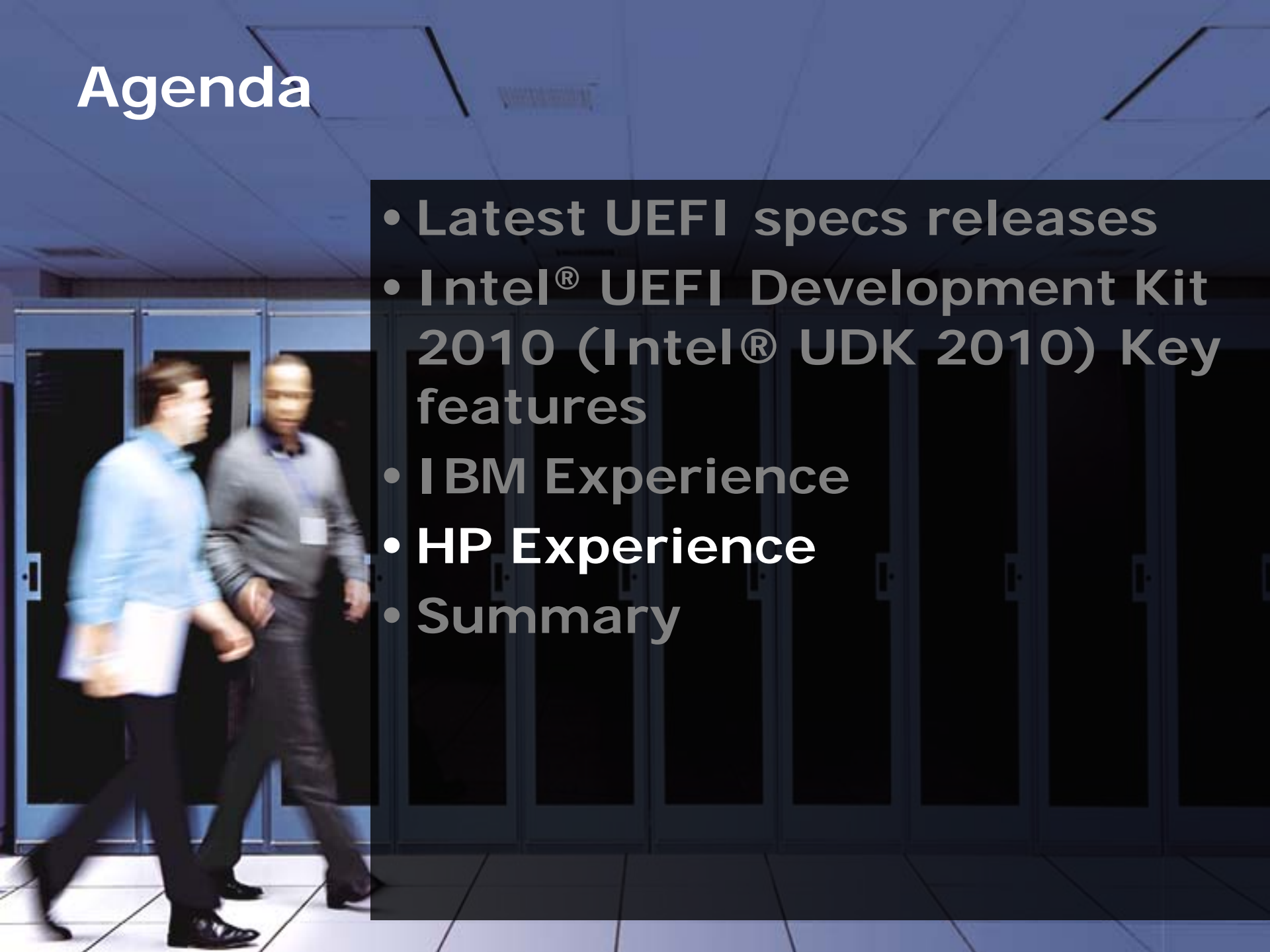
WITNESS

The Next Era of Mission-Critical Computing

EDK II Transition on the First Mission-Critical Converged Infrastructure

Dong Wei – Distinguished Technologist/Strategist

Sept 13, 2010

intel Itanium inside™

Powerful. Intelligent.

hp

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

The First Mission-Critical Converged Infrastructure

New Integrity systems optimized for the converged infrastructure

Storage

Servers

HP Converged Infrastructure

Power & cooling

Network

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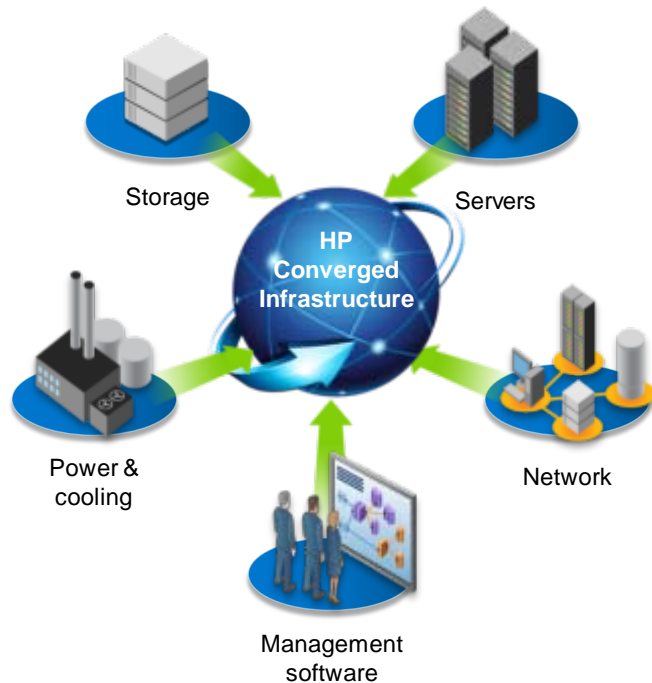
A common, modular architecture that simplifies, consolidates, and automates everything

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

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

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
c3000   c7000

**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

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

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

Summary

- Intel® UDK2010 meets the OEMs advanced requirements for platform development and enables common firmware foundation across the compute continuum

- Intel UDK2010 enables IBM to develop consistent cross-platform 'core' code stack with advanced configuration, reliability, and boot management features

- EDK II/Intel UDK2010 enables HP Platform Innovations and Excellent Execution

- Intel UDK2010 is available on tianocore.org

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

IDF2010
INTEL DEVELOPER FORUM

Additional sources of information on this topic:

- Other Sessions – See Next Slide
- Demos in the showcase – #160
- Additional info in the SSG community – EFI Booth
- More web based info:
  - *UDK 2010 -* *http://www.tianocore.Sourceforge.net*
  - *UEFI Specifications - http://www.uefi.org*
- Books on topic:
  - Beyond BIOS 2nd edition - Intel Press
  - IBM's "Introducing UEFI on IBM System x and BladeCenter Servers" Whitepaper
    - http://www-947.ibm.com/support/entry/portal/docdisplay?brand=5000008&lndocid=MIGR-5083207
  - http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01717787/c01717787.pdf?jumpid=reg_R1002_USEN
  - http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA2-2423ENW.pdf

Intel® UDK2010 Available on tianocore.org

tianocore.org

Intel® UDK2010
Open Source
UEFI Development Kit

Develop. Contribute. Advance.

http://www.tianocore.Sourceforge.net

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

Beyond BIOS 2nd edition promotion

Beyond BIOS:
Developing with the Unified
Extensible Firmware Interface

2nd Edition

Vincent Zimmer, Michael Rothman and Suresh Marisetty

Intel PRESS — Books by Engineers, for Engineers — (intel)

2nd Edition - _Beyond BIOS_ available Q4 2010

To receive a complementary copy of the book
Register at
http://www.intel.com/intelpress/register.htm

Enter "Beyond BIOS Offer" plus the serial
number on the back of this voucher in the
Book Title field. Your book will be shipped to you.

Offer not valid for Intel employees. Limited time offer.

Vouchers available in session room and
UEFI Technology showcase booth #160

IDF2010
INTEL DEVELOPER FORUM

UEFI PLUGFEST in Taiwan Oct 12-15, 2010

FALL 2010   OCTOBER 12-15   TAIPEI

UEFI PLUGFEST

Save the date!

Visit www.uefi.org/events for Event Info and Registration

IDF2010
INTEL DEVELOPER FORUM

IDF 2010 UEFI Fall Sessions
Sept. 13, 2010 Moscone Room 2006

EFI#	Company	Description	Time
✓ S001	Intel, IBM, HP	Introducing the New Intel® UEFI Development Kit: Industry Foundation for Platform Innovation	11:00 AM
S002	Intel, LSI, Dell, Phoenix	UEFI Advancements for Independent Hardware Vendors	1:05 PM
S003	Intel, WindRiver	Boot Loader Solutions for Intel® Atom™ Processor Based Embedded Devices	2:10 PM
S004	Intel, Dell, AMI	Zero-Touch Platform Manageability with UEFI	3:15 PM
S005	Intel, IBM, Insyde	Beyond DOS: The UEFI Shell – a Modern Pre-boot Application Environment	4:20 PM
Q001	All	UEFI Q & A session with all Speakers	5:25 PM

✓ DONE

Please Fill out the Session Evaluation Form

Give the completed form to the room monitors as you exit!

Thank You for your input, we use it to improve future Intel Developer Forum events

IDF2010
INTEL DEVELOPER FORUM

Q&A

Tweet your questions and comments to @intel_uefi

IDF2010
INTEL DEVELOPER FORUM

Session Presentations - PDFs

The PDF for this Session presentation is available from our IDF Content Catalog at the end of the day at:

intel.com/go/idfsessions

URL is on top of Session Agenda Pages in Pocket Guide

IDF2010
INTEL DEVELOPER FORUM

Legal Disclaimer

IDF2010
INTEL DEVELOPER FORUM

Risk Factors

The above statements and any others in this document that refer to plans and expectations for the second quarter, the year and the future are forward-looking statements that involve a number of risks and uncertainties. Many factors could affect Intel's actual results, and variances from Intel's current expectations regarding such factors could cause actual results to differ materially from those expressed in these forward-looking statements. Intel presently considers the following to be the important factors that could cause actual results to differ materially from the corporation's expectations. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions; customer acceptance of Intel's and competitors' products; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Intel operates in intensely competitive industries that are characterized by a high percentage of costs that are fixed or difficult to reduce in the short term and product demand that is highly variable and difficult to forecast. Additionally, Intel is in the process of transitioning to its next generation of products on 32nm process technology, and there could be execution issues associated with these changes, including product defects and errata along with lower than anticipated manufacturing yields. Revenue and the gross margin percentage are affected by the timing of new Intel product introductions and the demand for and market acceptance of Intel's products; actions taken by Intel's competitors, including product offerings and introductions, marketing programs and pricing pressures and Intel's response to such actions; defects or disruptions in the supply of materials or resources; and Intel's ability to respond quickly to technological developments and to incorporate new features into its products. The gross margin percentage could vary significantly from expectations based on changes in revenue levels; product mix and pricing; start-up costs, including costs associated with the new 32nm process technology; variations in inventory valuation, including variations related to the timing of qualifying products for sale; excess or obsolete inventory; manufacturing yields; changes in unit costs; impairments of long-lived assets, including manufacturing, assembly/test and intangible assets; the timing and execution of the manufacturing ramp and associated costs; and capacity utilization. Expenses, particularly certain marketing and compensation expenses, as well as restructuring and asset impairment charges, vary depending on the level of demand for Intel's products and the level of revenue and profits. The majority of our non-marketable equity investment portfolio balance is concentrated in the flash memory market segment, and declines in this market segment or changes in management's plans with respect to our investment in this market segment could result in significant impairment charges, impacting restructuring charges as well as gains/losses on equity investments and interest and other. Intel's results could be impacted by adverse economic, social, political and physical/infrastructure conditions in countries where Intel, its customers or its suppliers operate, including military conflict and other security risks, natural disasters, infrastructure disruptions, health concerns and fluctuations in currency exchange rates. Intel's results could be affected by the timing of closing of acquisitions and divestitures. Intel's results could be affected by adverse effects associated with product defects and errata (deviations from published specifications), and by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust and other issues, such as the litigation and regulatory matters described in Intel's SEC reports. An unfavorable ruling could include monetary damages or an injunction prohibiting us from manufacturing or selling one or more products, precluding particular business practices, impacting our ability to design our products, or requiring other remedies such as compulsory licensing of intellectual property. A detailed discussion of these and other factors that could affect Intel's results is included in Intel's SEC filings, including the report on Form 10-Q for the quarter ended March 27, 2010.

Rev. 5/7/10

IDF2010
INTEL DEVELOPER FORUM