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

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

**2000**
tianocore.org, open source EFI community launched

**2004**
Unified EFI (UEFI)
Industry forum, with 11 members, was formed to standardize EFI

**2005**
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

Full system stack (user -> hardware)
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

- Smartphones
- TVs
- Notebooks
- Desktop PCs
- Netbooks
- Data Center / Servers
- Gadgets
- Networks
- Embedded: Auto, Signage, Printers, etc.
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

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

**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

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

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

**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
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

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 autonomies 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

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

- 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*

![Extensible integrity architecture](image-url)
**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

- UEFI 2.2, 2.3, PI 1.1, 1.2
- UEFI 2.3 and PI 1.2 definitions
- UEFI 2.3/PI 1.2 Tool updates
- Backward compatible solution for PI 1.1 SMM/S3/SMBIOS
- IP4 stack update for IP6-readiness
- IP6 stack, ISCSI, PXE, Ipsec, VLAN
- Configuration Tools
- Compatibility package
- UEFI Shell 2.0

Silicon Packages

- Platform, chipset & CPU

Advanced Development Environment

*Modular. Flexible. Extensible.*
UDK2010: Available at tianocore.org

http://www.tianocore.Sourceforge.net

UDK2010
Open Source
UEFI Development Kit

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
**INTEGRITY† LEADS HP EDK II TRANSITION**

EDK II Enables HP Platform Innovation and Execution Excellence

<table>
<thead>
<tr>
<th>Single Source Tree</th>
<th>Superior Packages</th>
<th>ECP Works Well</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Superdome 2, Blades and Rack Servers</td>
<td>Ability to reuse Single module/solution owner Global visibility for bug fix</td>
<td>Reuse existing silicon modules, applications</td>
</tr>
</tbody>
</table>

**Superdome 2**
The ultimate mission-critical consolidation platform

**BladeSystem Matrix with HP-UX**
First Converged Infrastructure platform for shared services, now mission-critical

**Integrity Server Blades**

**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
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

- **Customizable information**
- **Calendar**
- **To-do List**

**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†**

**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.

---

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