

IDF2012
INTEL DEVELOPER FORUM

Microsoft* Windows* 8 Firmware Developments and Intel® Platforms

Mark Doran, Senior Principal Engineer, Intel
Tony Mangefeste, Senior Program Manager, Microsoft

EFIS004

Sponsors of Tomorrow: 

Microsoft®

Please Fill Out The Online Session Evaluation Form

**Enter to win fabulous prizes including
Ultrabooks™, SSDs and more!**

**You will receive an email with a link to the online
session evaluation prior to the end of this session.
Please submit the evaluation by 10am tomorrow
to be entered to win.**

Winners will be announced by email

**Sweepstakes rules are available at the Help Desk on Level 2
All sessions evaluations must be submitted by Friday Sept 14 at 5pm**

Agenda

- UEFI 2.3.1c Specification Update and Intel Support
- Microsoft* Windows* 8 & UEFI
- Features for Modern PC Experiences
- Platform Recommendations
- Summary and Call to Action

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

intel.com/go/idfsessions

URL is on top of Session Agenda Pages in Pocket Guide

Agenda

- **UEFI 2.3.1c Specification Update and Intel Support**
- Microsoft* Windows* 8 & UEFI
- Features for Modern PC Experiences
- Platform Recommendations
- Summary and Call to Action

UEFI 2.3.1c Specification Update and Intel Support

- State of the Industry
- What's New?
 - UEFI 2.3.1c
 - Platform Initialization (PI)1.2.1
 - Intel® UDK2010.SR1.UP1
- Useful Development Tools
 - Intel UEFI Community
 - Web-based UEFI Training
 - Driver Writer's Guide
 - UEFI Driver Wizard
 - Intel® UDK Debugger Tool



State of the Industry



State of the Industry

- UEFI is at a tipping point...
 - Logo requirement for Microsoft* Windows* 8
 - Supported by major Linux* distributions
- Still room for improvement in UEFI
 - Developer education, improving the number of peripherals with UEFI Drivers
 - User education, based on common mistakes in coverage on topics like UEFI Secure Boot

What's New?
UEFI 2.3.1c
Intel® UDK2010.SR1.UP1



What's New?

- UEFI 2.3.1c
 - Update to the UEFI 2.3.1 Specification
 - Adds important firmware considerations
 - Addresses numerous ECRs
- UEFI Self Certification Test (SCT)
 - Updates for the UEFI 2.3.1c Specification
 - Soon to be released <http://uefi.org>
- Intel® UDK2010.SR1.UP1
 - Incorporates items deferred from Intel UDK2010.SR1
 - Posted to tianocore.org on June 25th
 - Updates to EDK II specs (v1.22 Errata B)
 - Available at <http://tianocore.org>

What's New in UEFI 2.3.1c?

- Add: OS Indications Variable
 - OS/FW feature & capability communication
 - End-users can request to enter BIOS setup menu after next reboot from the OS
- Add: Retain factory default keys in Setup Mode
 - Related to UEFI Secure Boot for Open Source OS or “OS agnostic” end-user configurations
- Remove: Runtime driver requirement for UNDI
 - Allows Network UNDI drivers in EFI Byte Code (EBC)
- Other Engineering Change Requests (ECR) in MANTIS
 - See the Specification for Details



Useful Development Tools

- **Intel UEFI Community**
- **Web-based UEFI Training**
- **Driver Writer's Guide**
- **UEFI Driver Wizard**
- **Intel® UDK Debugger Tool**

Intel UEFI Community

<http://intel.com/udk>

Intel UEFI Community Resource Center

Support Feedback Contact Us

Home Learn Communicate Share Develop Find Solutions

Welcome to Intel UEFI Community Resource Center

Your gateway for developing UEFI firmware, drivers, and applications for use on Intel® architecture platforms.

[Learn more about UEFI >](#)

Learn.
Training courses and Intel® Developer Forum presentation library »



Communicate.
Forum for discussions with Intel engineers and other developers »



Share.
Upload and download files for sharing with the community »



Develop.
Intel UEFI technology, software and tools, specs, and docs »

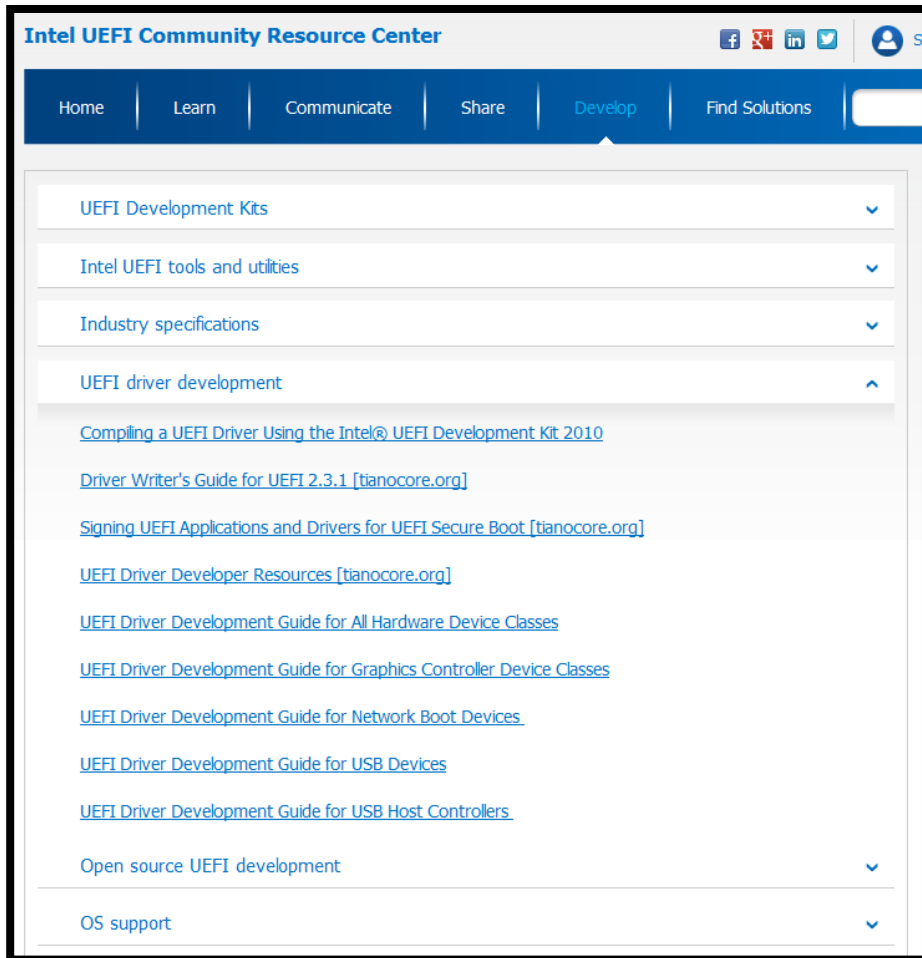


Find solutions.
Get conforming devices, BIOS, and drivers from participating vendors »



Launched June 2012

Intel UEFI Community



<http://intel.com/udk>

Example content from the 'Develop' page...

Pointers to content from Intel, TianoCore.org, uefi.org, OS vendor websites and more

UEFI Self-paced Web-based Training

- UEFI and Platform Initialization Specification Training
 - From Power on through PEI, DXE, BDS and Booting the OS
 - 6 lessons with key point questions



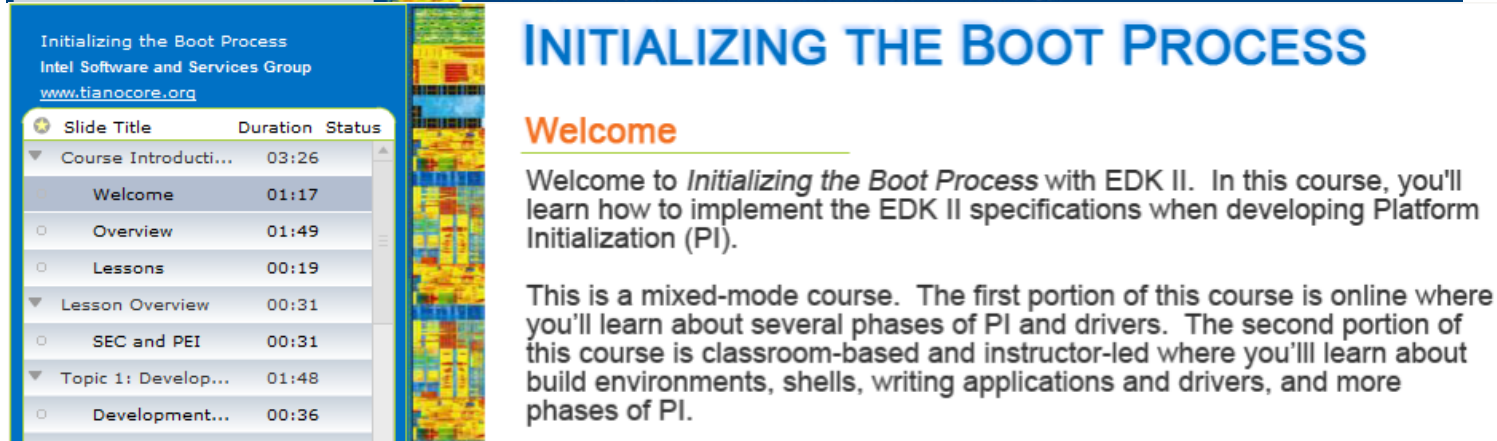
Defining Specifications' Role in Firmware
Intel Software and Services Group
www.tianocore.org

Slide Title	Duration
Introduction	01:24
Course Overview	00:39
▶ Topic 1: Legacy BIOS a...	06:57
▶ Topic 2: Intel Framework	04:30
▶ Topic 3: EDK	01:49
▶ Course Summary	01:09

DEFINING SPECIFICATIONS' ROLE IN FIRMWARE

Welcome

Welcome to *Defining Specifications' Role in Firmware*. This course will help you understand the background of firmware specifications and their purposes. While you will not become an expert in firmware specifications by taking this course, you will have a basic understanding of Legacy BIOS, UEFI, PI, and EDK (all explained and defined in this training).



Initializing the Boot Process
Intel Software and Services Group
www.tianocore.org

Slide Title	Duration	Status
▼ Course Introducti...	03:26	
Welcome	01:17	
Overview	01:49	
Lessons	00:19	
▼ Lesson Overview	00:31	
SEC and PEI	00:31	
▼ Topic 1: Develop...	01:48	
Development...	00:36	

INITIALIZING THE BOOT PROCESS

Welcome

Welcome to *Initializing the Boot Process* with EDK II. In this course, you'll learn how to implement the EDK II specifications when developing Platform Initialization (PI).

This is a mixed-mode course. The first portion of this course is online where you'll learn about several phases of PI and drivers. The second portion of this course is classroom-based and instructor-led where you'll learn about build environments, shells, writing applications and drivers, and more phases of PI.

Driver Writer's Guide for UEFI 2.3.1

- Expanded to cover UEFI 2.3.1 topics
- Designed as a developer reference
 - Organized & indexed by driver function
 - Not a “cover to cover read”
- See '[Enabling Resources for UEFI Driver Developers Using EDK II](#)' at tianocore.org



Driver Writer's Guide for UEFI 2.3.1

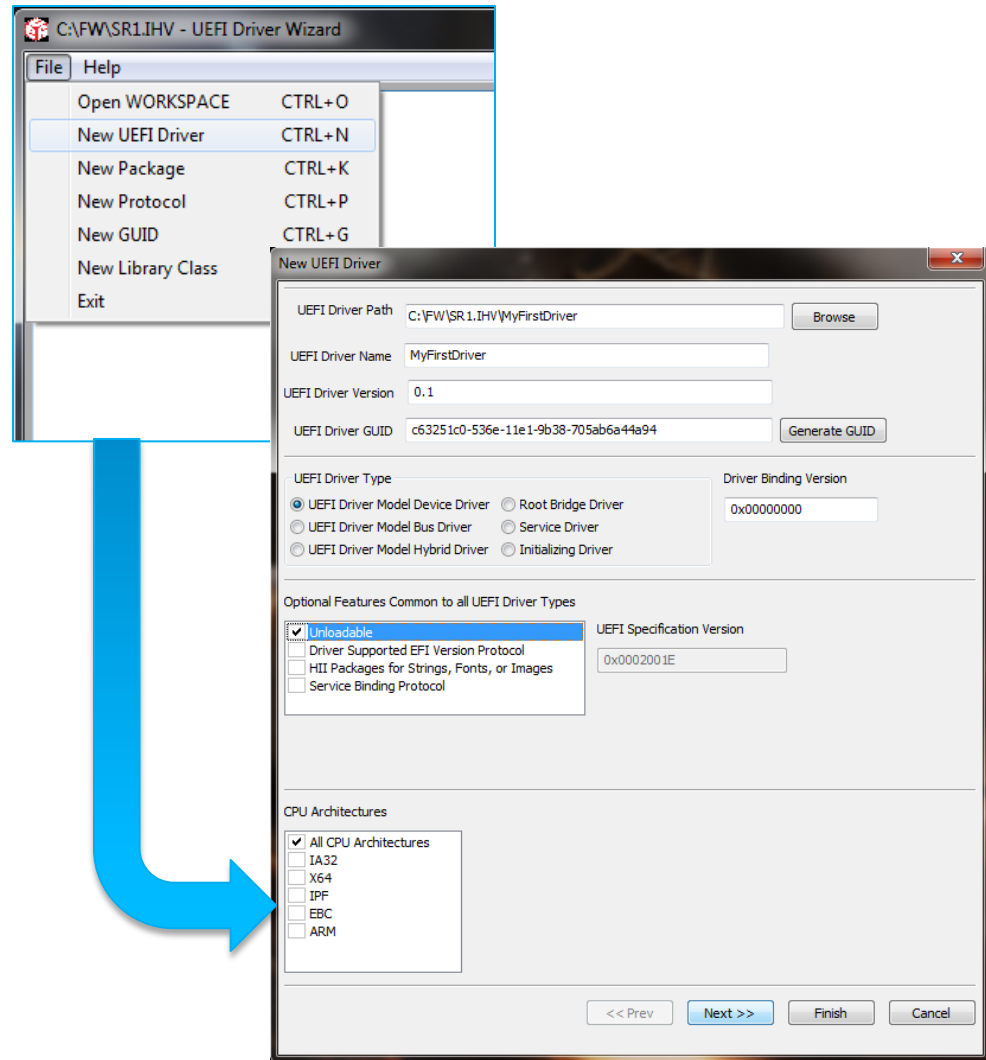
03/08/2012

Version 1.01

IDF2012
INTEL DEVELOPER FORUM

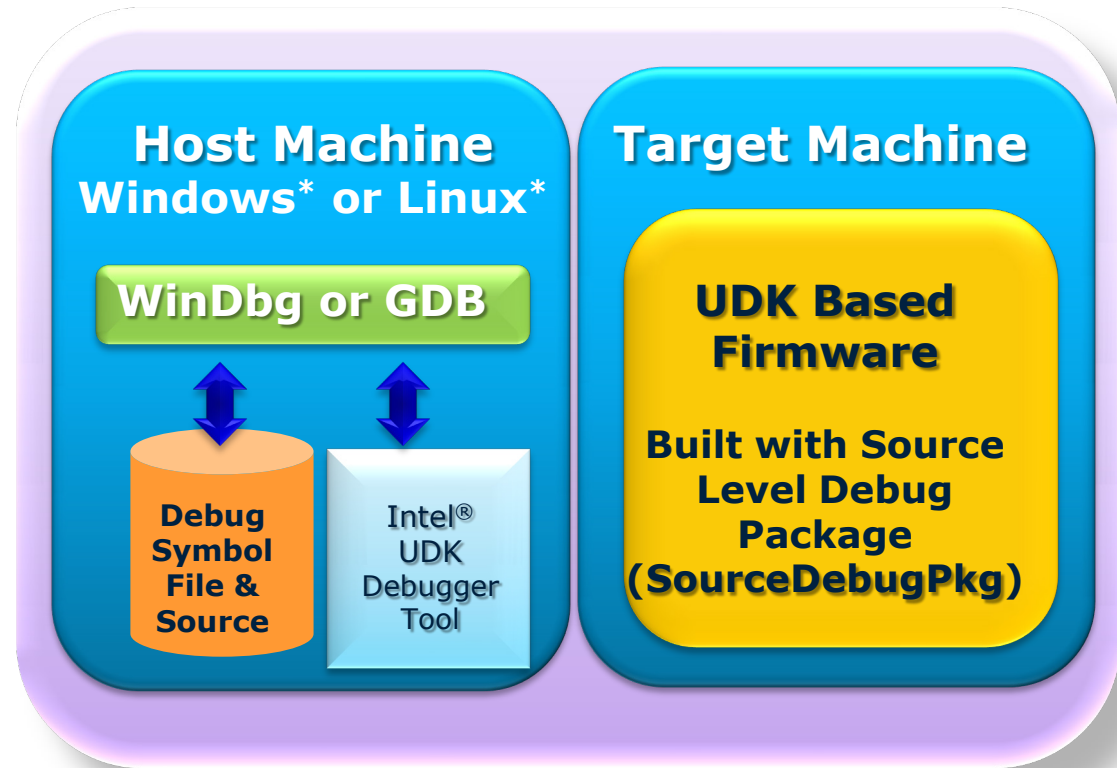
UEFI Driver Wizard

- Menu-based GUI to simplify UEFI Driver development
 - Uses EDK II or “IHV” subset of UDK2010
 - Wizard-based template generation
- Open source project contributed to tianocore.org by Intel SSG
 - Python* interface, designed for extensibility
 - Intel encourages contribution by developers
- Download Link: [UEFI Driver Wizard \(MSI\)](#) on Sourceforge.net



Intel® UDK Debugger Tool

- Source level debugger for UEFI firmware & drivers
 - Debug the boot phases – SEC, PEI, DXE, BDS, SMM
 - Set breakpoints, step into, and step over routines
 - View and edit local & global variables, and general purpose registers
- Low-cost alternative to a hardware ITP/JTAG debug



<http://intel.com/udk>

Many Tools and Resources are Available for UEFI Developers ...

Agenda

- UEFI 2.3.1c Specification Update and Intel Support
- **Microsoft* Windows* 8 & UEFI**
- Features for Modern PC Experiences
- Platform Recommendations
- Summary and Call to Action

Why UEFI?

- User Experience value prop from day one: Fast Boot, OEM Certification, smooth transitions, etc.
- Secure Boot
- eDrive support for BitLocker
- SOC support
- WDS Multicast
- Boot Next support
- Seamless Boot
- Network unlock support for BitLocker
- Support for > 2.2 TB system disks

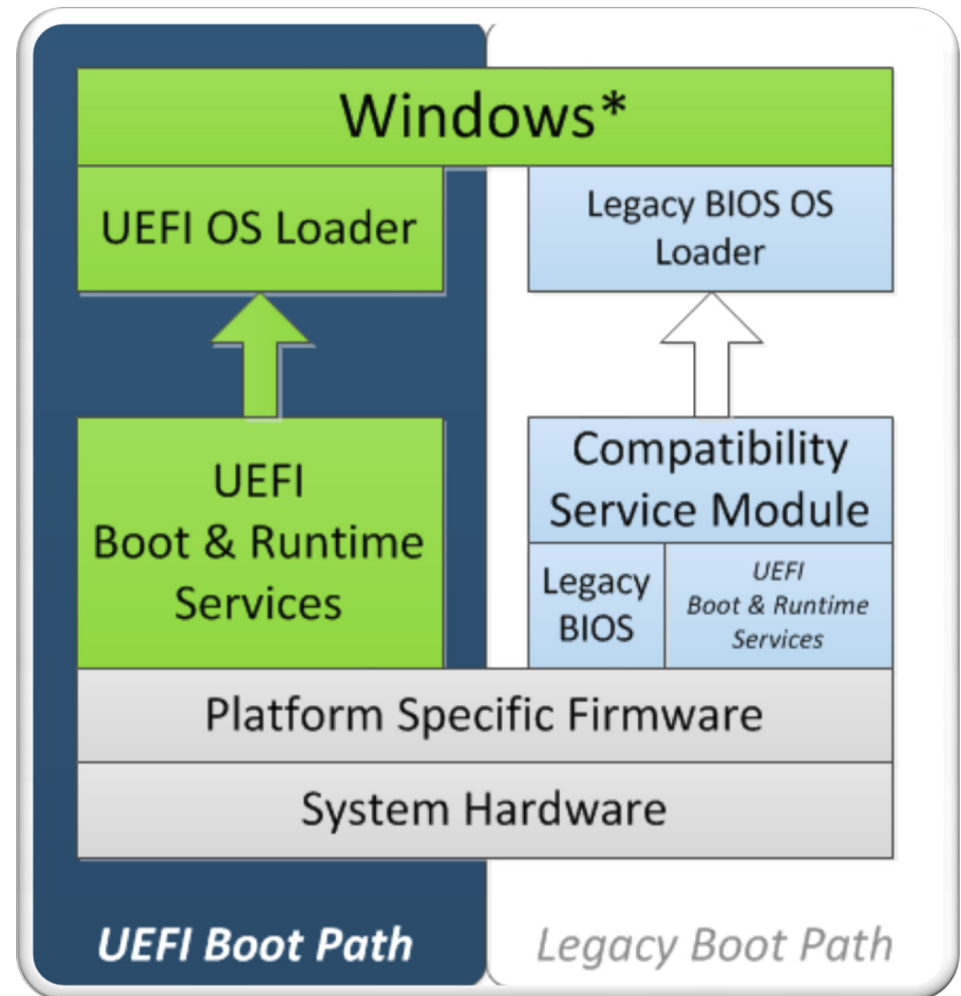


Windows* 8 Certification– UEFI

- Requirements:
 - All Windows* 8 Client systems must ship in native UEFI mode
 - Class 2 – CSM Disabled
 - Class 3
 - Secure Boot¹
 - New graphics requirements
 - POST time maximums
 - OEM Certification display guidance
- If implemented:
 - BitLocker network key protector¹
 - BitLocker Encrypted Hard Drive (eDrive) support¹

Windows* 8 Boot Flow

- Windows 8 installs UEFI OS Loader if UEFI is detected
- Many PCs today boot through CSM path
- For compatibility the CSM boot path available



Windows 8 with UEFI is preferred

Windows* Deployment Paths

Original OS UEFI or BIOS mode	Upgrade to Windows* 8 UEFI Native ² Mode	Clean Install Windows 8 UEFI Native ² Mode
Windows XP (BIOS Only)	No support	No Support
Windows Vista/7 (BIOS mode)	No support	No Support
Windows Vista/7 (UEFI mode)	Yes	Yes
Windows 8 (BIOS mode)¹	No support	No support

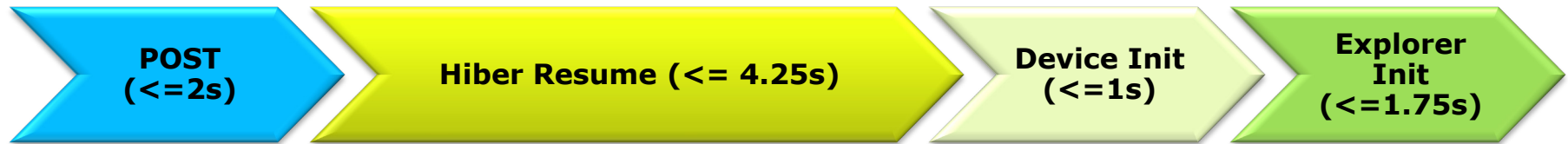
¹ Windows 8 supports install in BIOS mode systems (Legacy), but not feature parity between UEFI and BIOS systems

² UEFI Native Mode – UEFI BIOS without CSM

Agenda

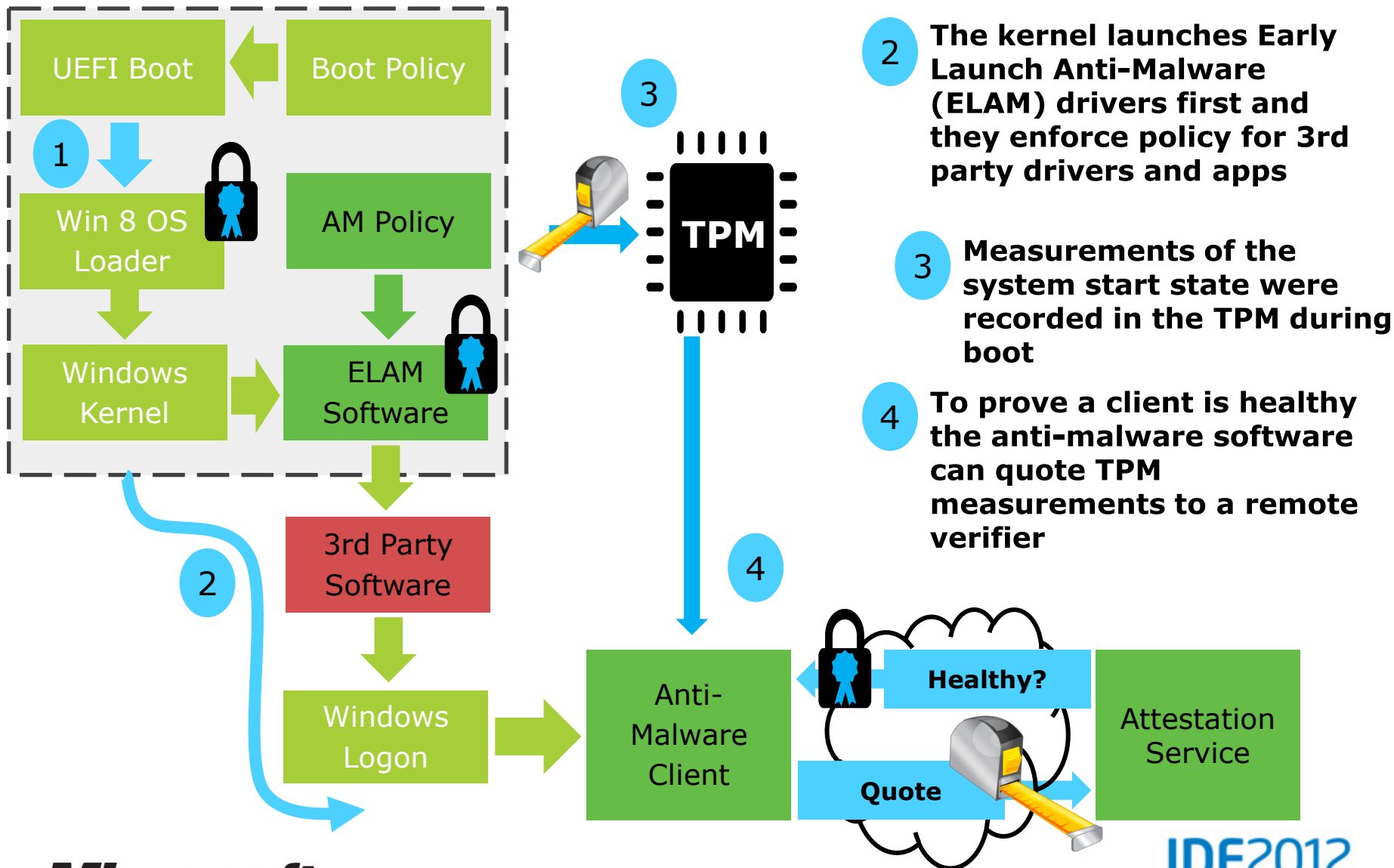
- UEFI 2.3.1c Specification Update and Intel Support
- Microsoft* Windows* 8 & UEFI
- Features for Modern PC Experiences
- Platform Recommendations
- Summary and Call to Action

Windows* 8 Certification Requirements – UEFI Boot Boot Performance Requirements



- Windows* 8 aims to support fast boot, on SSD systems
 - POST: <2s (without TPM; SSD) **requirement**
 - Boot to OS: <4s **best practice, varies by apps**
 - Device Init: <2s **best practice, varies by drivers**
- New WHQL Requirements for hardware design
 - TPM: <300ms init
 - Applies mostly to PCs with integrated displays (laptops, tablets, notebooks)
 - Read the Windows 8 System Certification Requirements for more details

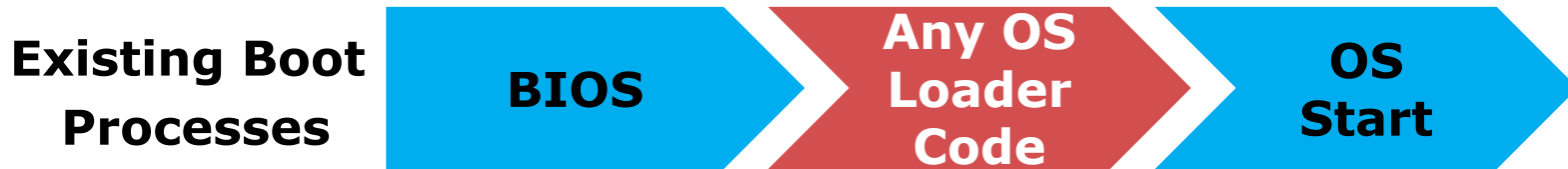
Trusted Boot Architecture



Trusted Boot: Improving Malware Resistance

- **Secure Boot**: Firmware policy prevents launch of an untrusted OS by verifying the publisher of the OS Loader
- **Anti-Malware Starts First**: Reduce the likelihood of a compromised operating system through early launch of approved AM software during the boot process
- **Measured Boot**: Remotely determine if the operating system has been compromised by malware during the boot process via a comprehensive chain of measurements recorded during the boot process and stored in a Trusted Platform Module (TPM)

Secure Boot



- The BIOS starts any OS loader, even malware
- Now firmware enforces policy, only starting trusted OS loaders
- OS loader enforces signature verification of later components



- UEFI will only launch a verified OS loader – such as in Windows 8
- Malware cannot switch the boot loader

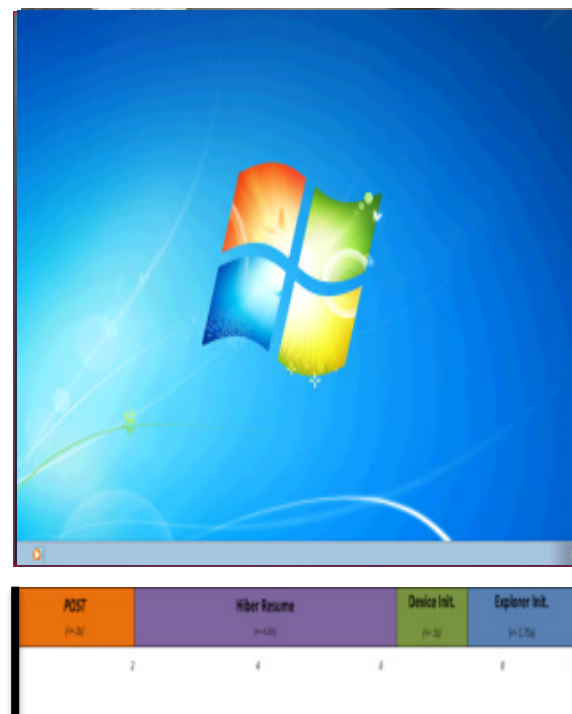
Secure Boot & Windows* 8

- Challenges
 - Growing class of pervasive malware that targets the boot path
 - Should Windows* be compromised by this type of attack, often the only plausible method to fix the problem is to reinstall the operating system
- Windows 8 Solution
 - Secure boot and remediation hardens the boot process against malware from the moment of power on through the initialization of anti-malware software
 - All firmware and software in the boot process must be signed by a trusted CA
- Required for all Windows 8 x64 client and SOC systems

A Seamless Boot Experience

...the modern PC experience

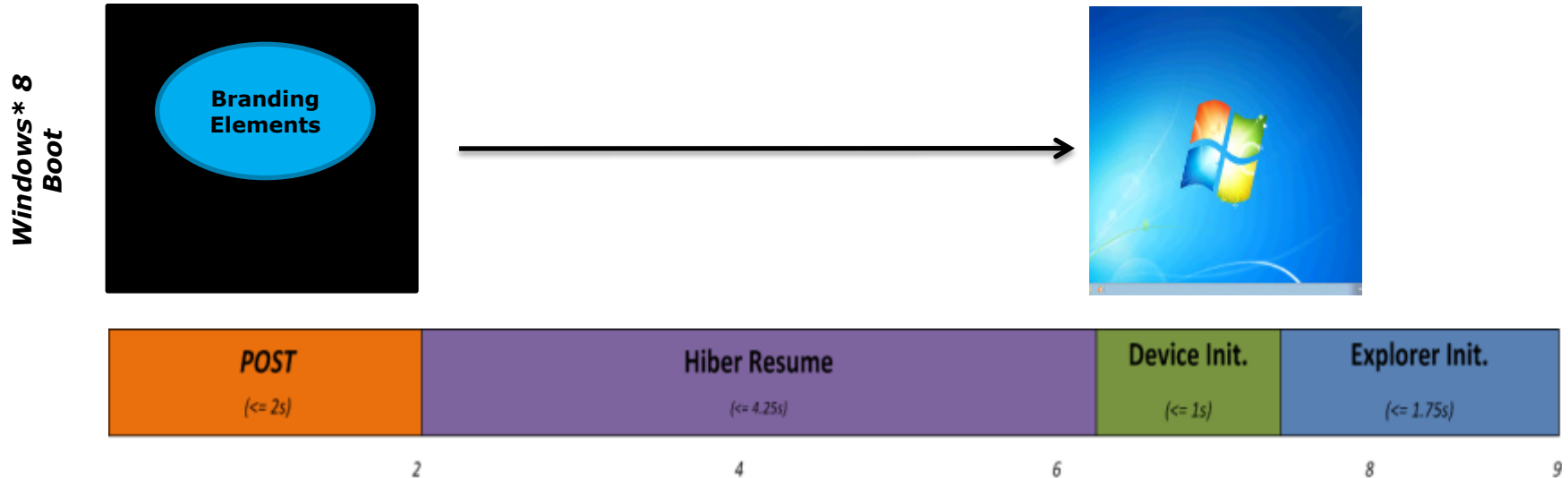
- Consistent requests for consumer electronics-like experience
- Current boot process is:
 - Disjointed, inconsistent
 - Displays varying levels of fidelity
 - When errors occur, displays scary text without actionable information
 - Making boot faster doesn't resolve the problem



**Boot Visual Experience
with Hybrid Boot**

Seamless to the Desktop

...sleek and seamless



- Two visual experiences, seamless transition between them
- Clean up the look and feel of POST—proposed enhancements:
 - Render clean, high-resolution branding elements on black background
 - Remove “Text Mode” items / displays
 - Standardize input methods (e.g., F12 is always boot options across all systems)
- Fix / remove graphics mode switches
 - Several mode switches today—goal to reduce down to one when high-res driver is initialized
 - Systems should post with highest supported native display resolution

Pre-OS Firmware Setup

...Adding Firmware boot options to Boot Menu & how to access it

- F8 No longer available at Boot
- Windows Key preferred method for accessing PC Firmware settings
- Alternative method found in PC Settings to Reboot the system into settings
 - Tailored for environments without keyboard
 - Very fast POST times
- Preferred Key: Windows Key

Introduction to eDrives

What is an eDrive?

- A regular HDD that comes with hardware offload to accelerate crypto processing

How is it different from SEDs?

- **S**elf-**E**ncrypting **D**rive
 - TCG standards
- **E**ncrypted **D**rive
 - TCG OPAL + IEEE 1667

Why should the ecosystem care?

- Initial hardware-based encryption is near line
- Faster than software-based during standard operation
- Removes initial and on-going performance hit caused by software-based encryption be it BitLocker or other 3rd party
- Standardize in-box support can enable broad adoption

Agenda

- UEFI 2.3.1c Specification Update and Intel Support
- Microsoft* Windows* 8 & UEFI
- Features for Modern PC Experiences
- Platform Recommendations
- Summary and Call to Action

Windows* 8 Platform Recommendations

- Improve platform security by ensuring that all assets are trusted on the platform
- Leverage UEFI drivers instead of option ROMs
- Design for adequate flash storage to store keys, certificates
- Consider impact of improved security
- Validate firmware components prior to execution
- Warn the customer if platform is not secure

Agenda

- UEFI 2.3.1c Specification Update and Intel Support
- Microsoft* Windows* 8 & UEFI
- Features for Modern PC Experiences
- Platform Recommendations
- Summary and Call to Action

Summary

- All Windows* 8 Client systems must ship in native UEFI mode
- Microsoft will continue to invest in UEFI
- Windows 8 & UEFI are foundation of the modern computing experience

Microsoft Call to Action

- Assess your UEFI readiness
 - Are you ready?
 - Are your processes ready?
 - Are your customers ready?
- Invest in platform firmware
 - Current investment, future potential
- Review Windows* 8 Certification Documentation
<http://msdn.microsoft.com/en-us/library/windows/hardware/hh748200.aspx>
- Review //BUILD 2011 Presentations on hardware, UEFI and security
<http://channel9.msdn.com/Events/BUILD/BUILD2011>
- Participate in UEFI plugfests
 - Bring your hardware, plug it in, test
- Join the UEFI Forum!
 - Contribute to the success of UEFI

Get More Information

- For more information on the Unified EFI Forum and UEFI Specifications, visit <http://www.uefi.org>
- UEFI Forum Learning Center
http://www.uefi.org/learning_center/
- Intel UEFI Community - <http://intel.com/udk>
- Use the TianoCore [*edk2-devel mailing list*](#) for support from other UEFI developers

- Go see UEFI Booth #946 in the showcase

Other UEFI Sessions @ IDF

Session	Title	RM	Day	Date	Time
✓ EFIS001	Developing UEFI Support for Linux*	2008	Tue	11-Sep	10:30
✓ EFIS002	Using Wind River Simics* Virtual Platforms to Accelerate Firmware Development	2008	Tue	11-Sep	12:45
✓ EFIS003	Intel and McAfee: Hardening and Harnessing the Secure Platform	2008	Tue	11-Sep	3:30
✓ EFIS004	Microsoft* Windows* 8 Firmware Developments and Intel® Platforms	2008	Wed	12-Sep	10:30
SECS004	Security Innovations in Intel® Platforms and Microsoft Windows 8	2008	Wed	12-Sep	2:00
EFIC001	Poster: Intel® UEFI Development Kit Debugger Tool	Poster	Thur	13-Sep	11:15
EFIC002	Poster: UEFI Driver Development Tools	Poster	Thur	13-Sep	11:15

✓ = DONE

USB Thumb Drive Contents



➤ Driver Development

- Driver Writer's Guide for UEFI 2.3.1 (PDF)
- UEFI Drivers Wizard Install (MSI)
- UDK2010.SR1.UP1.IHV (ZIP)

➤ UEFI Summer Summit – 8 (PDF)

➤ EDK II Specs – Build specifications V 1.22 B (PDF)

➤ The Intel Technology Journal V15 #1 (PDF)

➤ Security – Signing UEFI Images (PDF)

➤ UDK2010.SR1.UP1 Release – (ZIP)

➤ UEFI and EDK II Training - (Self-paced Web)

Resources

- <http://intel.com/go/idfsessionSF>
- <http://intel.com/udk>
- <http://uefi.org>
- <http://tianocore.org>



Please Fill Out The Online Session Evaluation Form

**Enter to win fabulous prizes including
Ultrabooks™, SSDs and more!**

**You will receive an email with a link to the online
session evaluation prior to the end of this session.
Please submit the evaluation by 10am tomorrow
to be entered to win.**

Winners will be announced by email

**Sweepstakes rules are available at the Help Desk on Level 2
All sessions evaluations must be submitted by Friday Sept 14 at 5pm**

Q&A

Legal Disclaimer

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

- A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.
- Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.
- The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.
- Intel product plans in this presentation do not constitute Intel plan of record product roadmaps. Please contact your Intel representative to obtain Intel's current plan of record product roadmaps.
- Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. Go to: http://www.intel.com/products/processor_number.
- Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.
- Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: <http://www.intel.com/design/literature.htm>
- Intel, Ultrabook, Sponsors of Tomorrow and the Intel logo are trademarks of Intel Corporation in the United States and other countries.
- *Other names and brands may be claimed as the property of others.
- Copyright ©2012 Intel Corporation.

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. Words such as “anticipates,” “expects,” “intends,” “plans,” “believes,” “seeks,” “estimates,” “may,” “will,” “should” and their variations identify forward-looking statements. Statements that refer to or are based on projections, uncertain events or assumptions also identify forward-looking statements. 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 company’s expectations. Demand could be different from Intel’s expectations due to factors including changes in business and economic conditions, including supply constraints and other disruptions affecting customers; 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. Uncertainty in global economic and financial conditions poses a risk that consumers and businesses may defer purchases in response to negative financial events, which could negatively affect product demand and other related matters. 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. Revenue and the gross margin percentage are affected by the timing of 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; and Intel’s ability to respond quickly to technological developments and to incorporate new features into its products. Intel is in the process of transitioning to its next generation of products on 22nm process technology, and there could be execution and timing issues associated with these changes, including products defects and errata and lower than anticipated manufacturing yields. The gross margin percentage could vary significantly from expectations based on capacity utilization; variations in inventory valuation, including variations related to the timing of qualifying products for sale; changes in revenue levels; segment product mix; the timing and execution of the manufacturing ramp and associated costs; start-up costs; excess or obsolete inventory; changes in unit costs; defects or disruptions in the supply of materials or resources; product manufacturing quality/yields; and impairments of long-lived assets, including manufacturing, assembly/test and intangible assets. The majority of Intel’s non-marketable equity investment portfolio balance is concentrated in companies in the flash memory market segment, and declines in this market segment or changes in management’s plans with respect to Intel’s investments 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 affected 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. 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. 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, disclosure 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 Intel from manufacturing or selling one or more products, precluding particular business practices, impacting Intel’s ability to design its 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 company’s most recent Form 10-Q, Form 10-K and earnings release.

Rev. 5/4/12

Backup

What's New in UEFI 2.3.1c?

- Address Engineering Change Requests (ECR) in MANTIS
 - 831 PXE Boot CSA Type definition cleanup
 - 874 Provide a mechanism for providing keys in setup mode
 - 882 Indications Variable - OS/FW feature & capability communication
 - 907 iSCSI Device Path error
 - 909 Update to return codes for AllocatePool / AllocatePages
 - 912 UEFI 2.3.1 Type
 - 913 Enum definition does not match what our current compilers implement
 - 914 Error Descriptor Reset Flag clarification
 - 915 For x64, Change Floating Point Default Configuration to Double-Extended Precision
 - 917 UNDI drive does not need to be initialized as runtime driver
 - 921 Length of IPv6 Device Path is incorrect

See the spec for details!