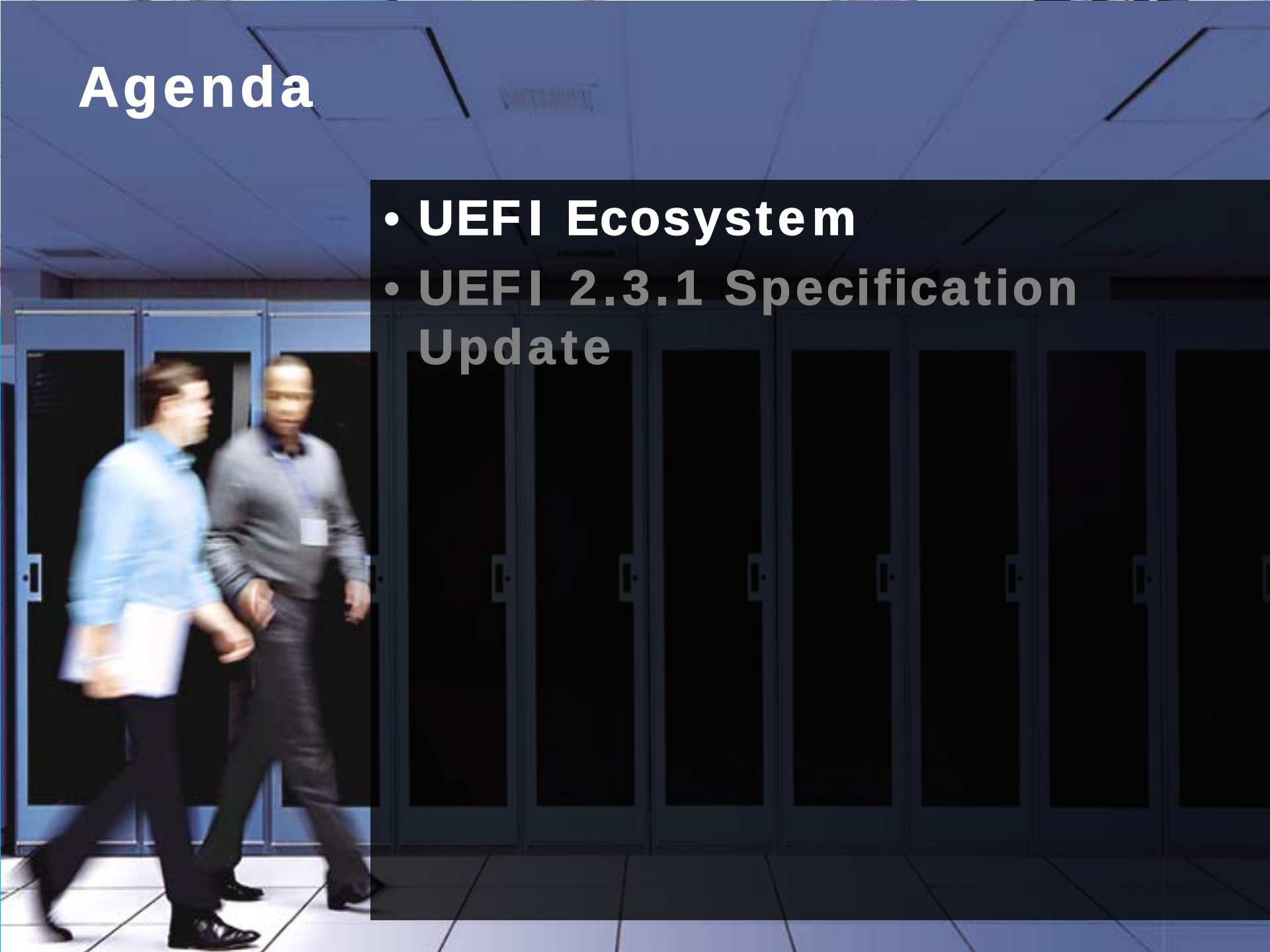
UEFI Ecosystem Update --- Microsoft* Windows* Platform Evolution and UEFI

Du Xiong
BIOS Engineer, Intel Corporation
Tony Mangefeste
Senior Program Manager, Microsoft Corporation

EFIS001

Sponsors of Tomorrow.™ intel

Agenda



- UEFI Ecosystem
- UEFI 2.3.1 Specification Update

Industry BIOS Transition

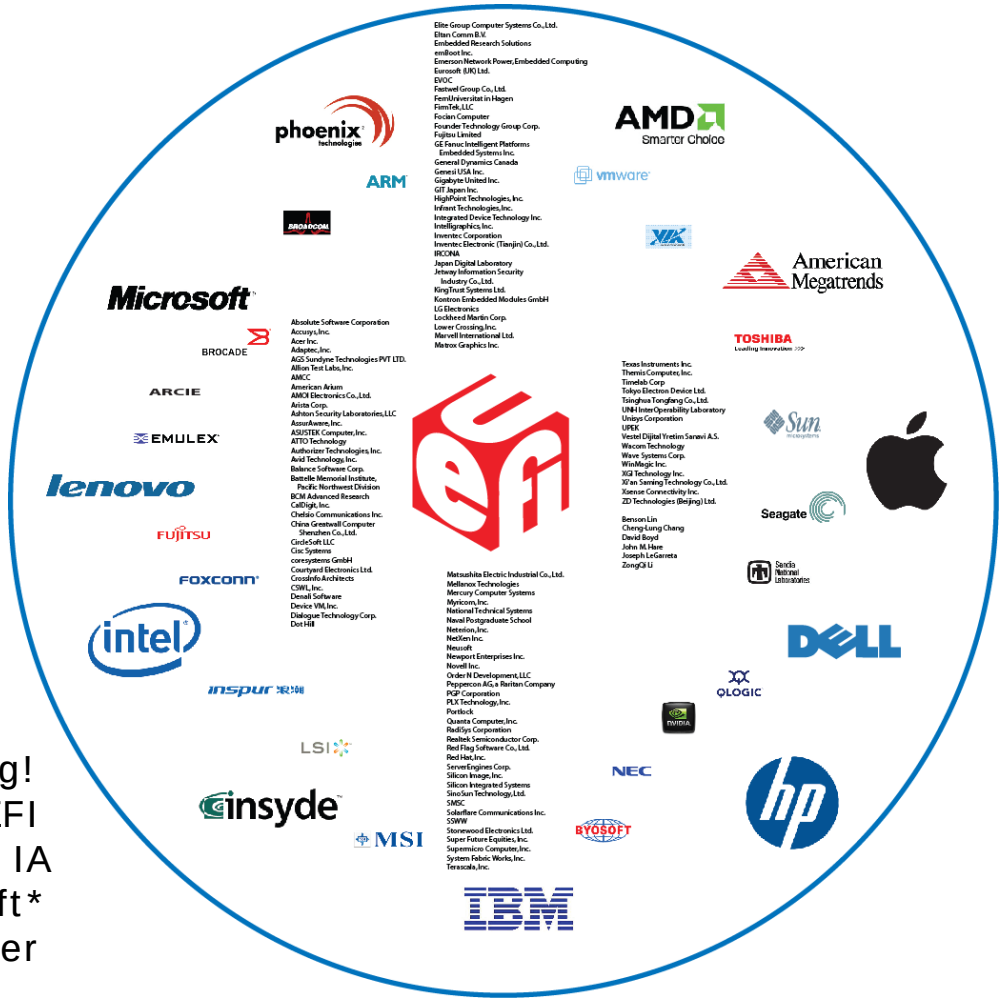
Pre-2000
All Platforms BIOS were proprietary

2000
Intel invented the Extensible Firmware Interface (EFI) and provided sample implementation under free BSD terms

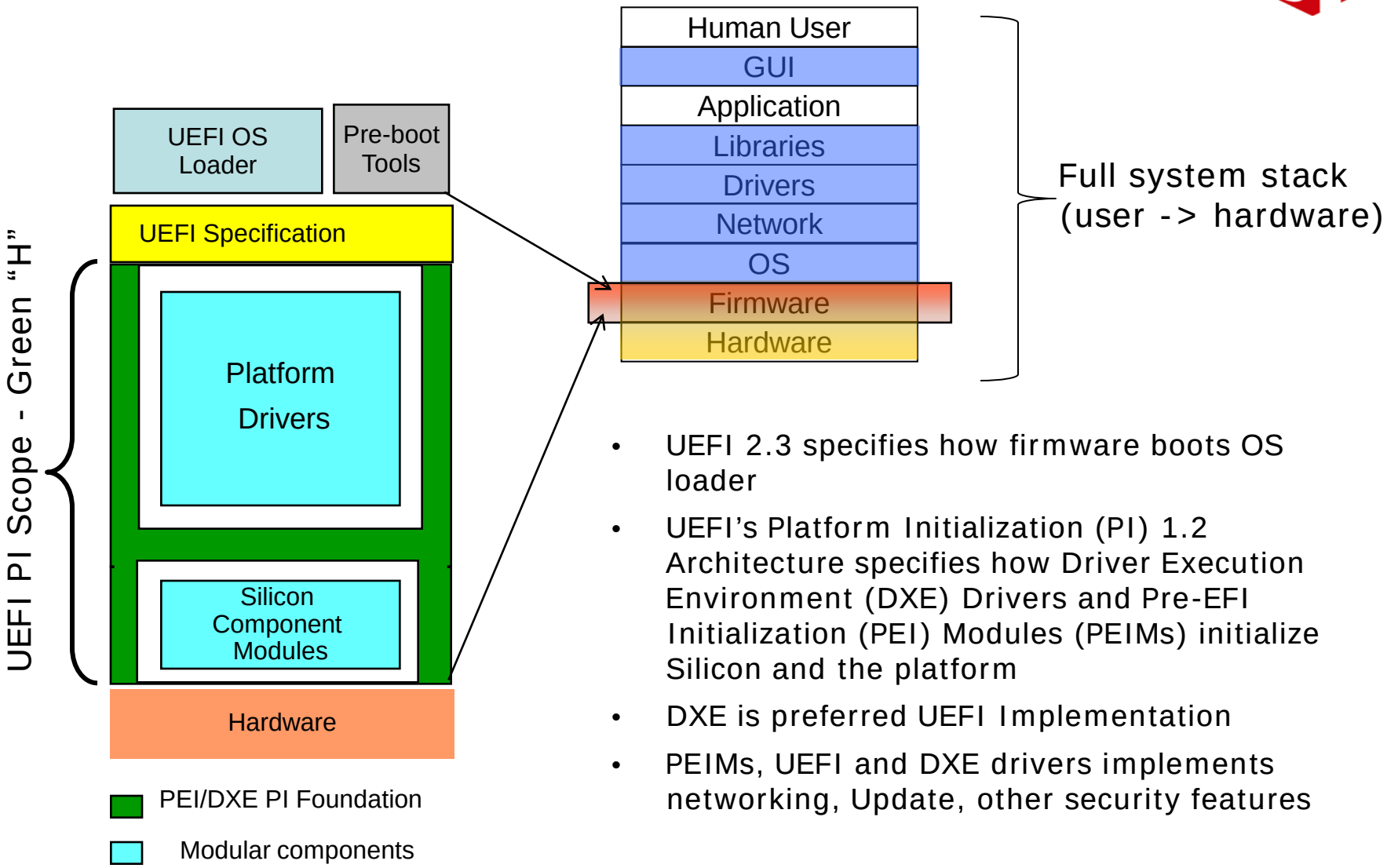
2004
tianocore.org, open source EFI community launched

2005
Unified EFI (UEFI) Industry forum, with 11 members, was formed to standardize EFI

2011
170 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

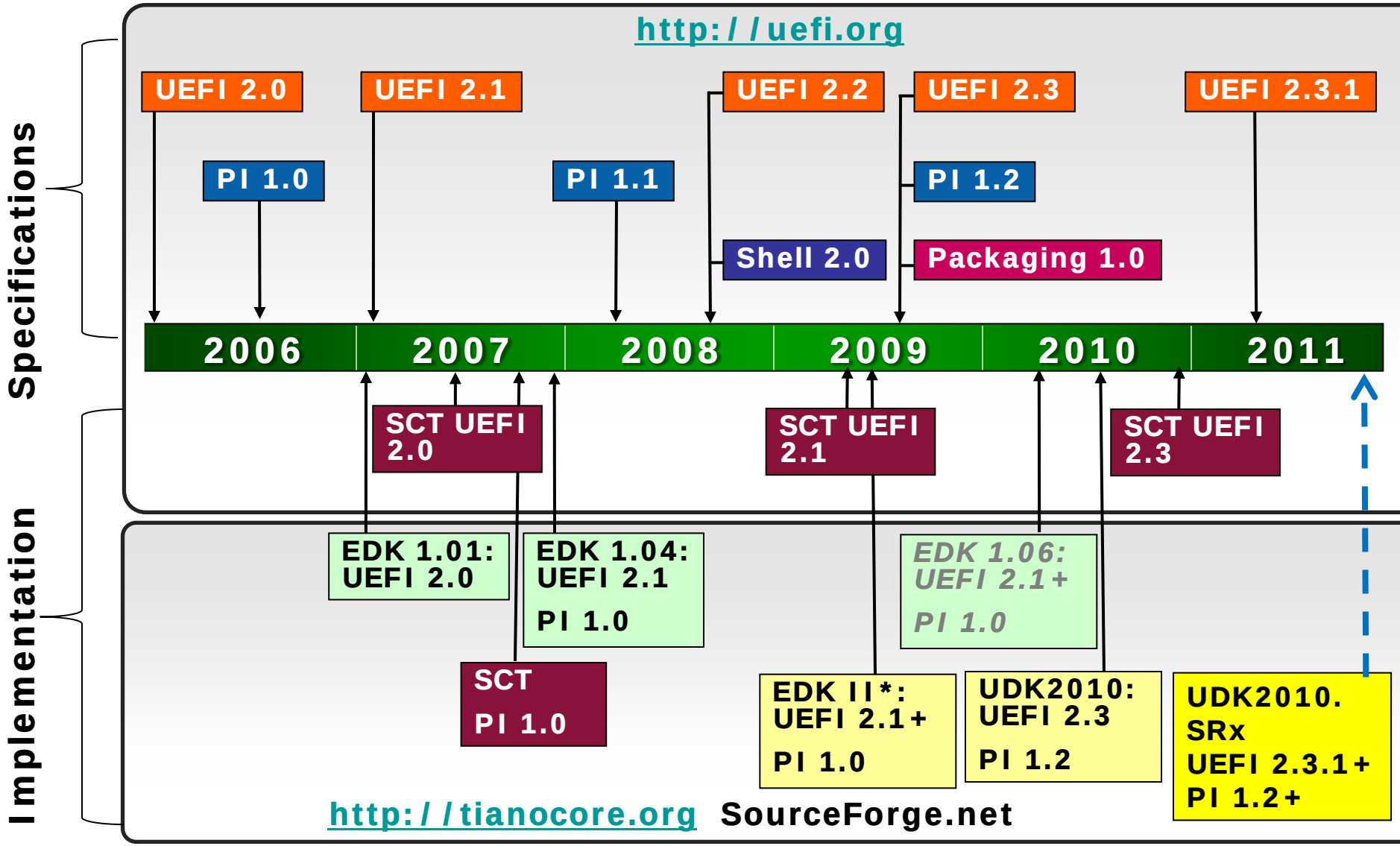


UEFI Platform Initialization Overview



- 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 Silicon and the platform
- DXE is preferred UEFI Implementation
- PEIMs, UEFI and DXE drivers implements networking, Update, other security features

Specification & Tianocore.org Timeline



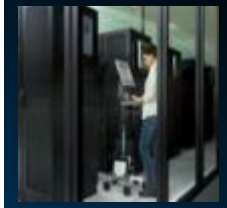
All products, dates, and programs are based on current expectations and subject to change without notice.

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

Areas of Industry UEFI-based Value-add & Innovation

Pre-OS Security & Rich Networking

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



Manageability

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

Power Management

- Power metering, power capping, power saving

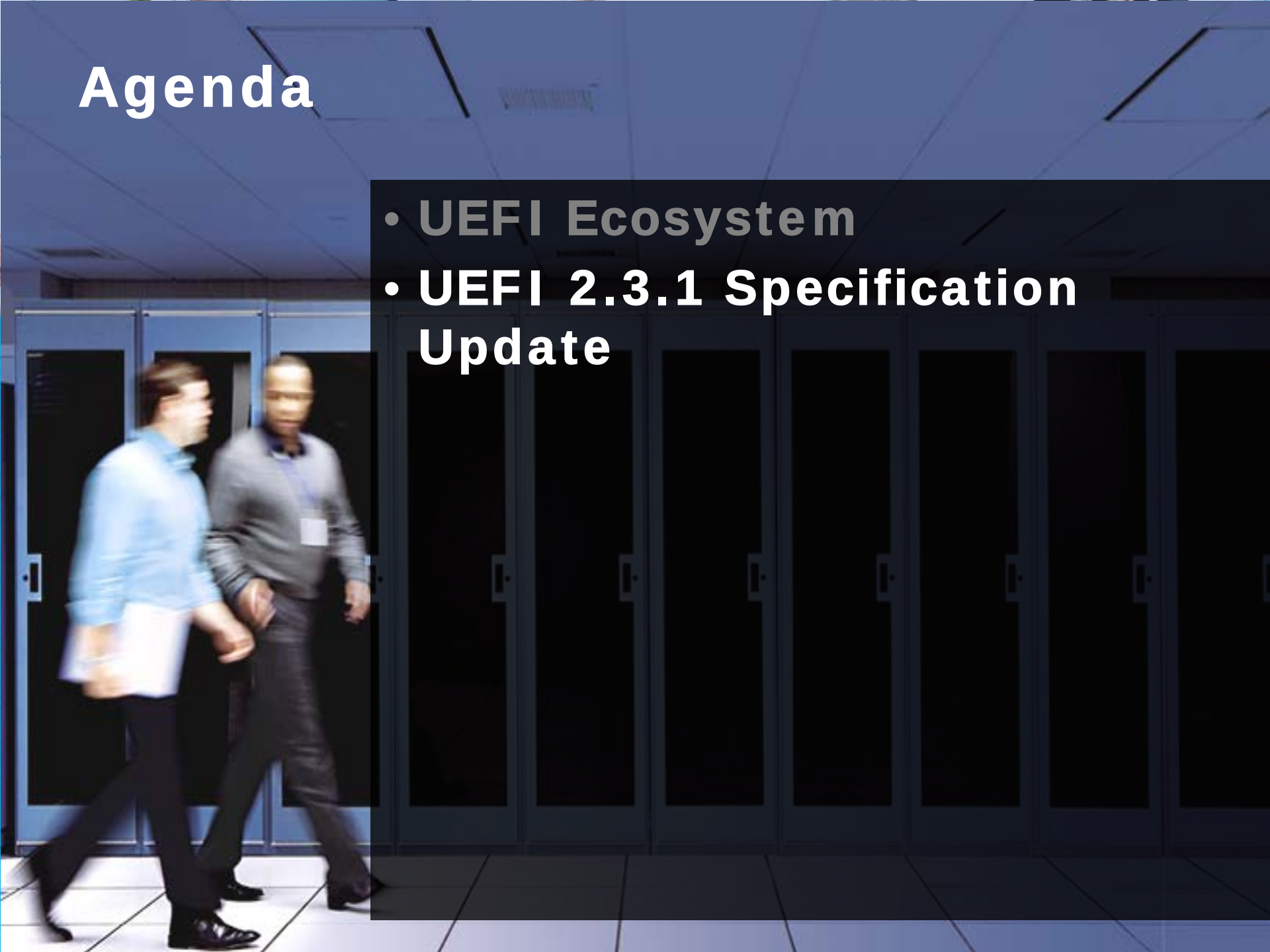
Optimized Boot & Modern Look

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

New Usages – UEFI Applications

- Access Outlook* data in seconds when notebook is off; Pre-boot video advertisement

Agenda



- UEFI Ecosystem
- UEFI 2.3.1 Specification Update

UEFI 2.3.1 Specification Update

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

Network
- Netboot6 client use DUID-UUID to report platform identifier

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

Performance
- Non-blocking interface for BLOCK oriented devices

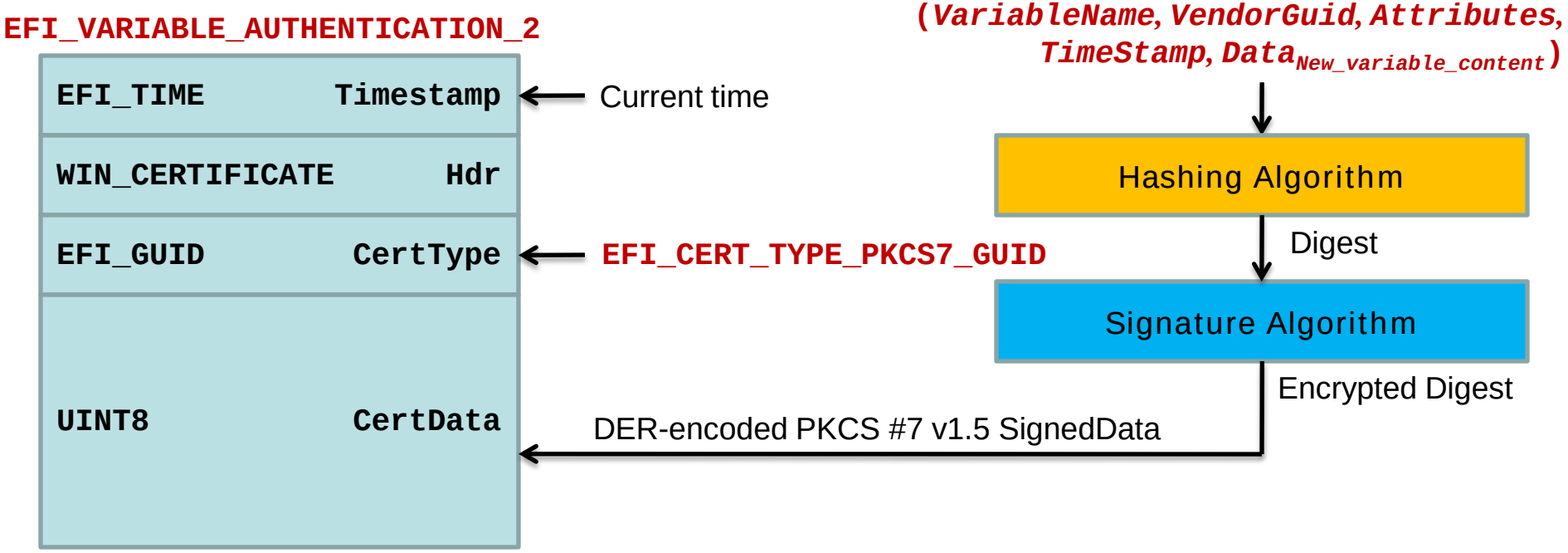
Technology
- USB 3.0

Maintenance
- User Identifier, etc.

UEFI 2.3.1 Enabling More Security Support

UEFI 2.3.1 Security Spec. Update

- Time-based authenticated Variable
  - Certificate chaining infrastructure
  - Absolute time for rollback protection
  - Append operation for Signature Databases



Better support servicing of UEFI Secure Boot in a large ecosystem with many actors

UEFI 2.3.1 Security Spec. Update

- Key Management Service (KMS)
  - Services to generate, store, retrieve, and manage cryptographic keys
  - Based on remote key server, or local Hardware Security Module (HSM), or software
- Storage Security Command Protocol
  - Send/receive security protocol defined data to/from mass storage devices
  - Supported command set
    - **TRUSTED SEND/RECEIVE** (ATA8-ACS)
    - **SECURITY PROTOCOL IN/OUT** (SPC-4)

Microsoft* Windows* Platform Evolution and UEFI

Tony Mangefeste
Senior Program Manager, Microsoft Corporation

Microsoft®

Sponsors of Tomorrow.™ intel

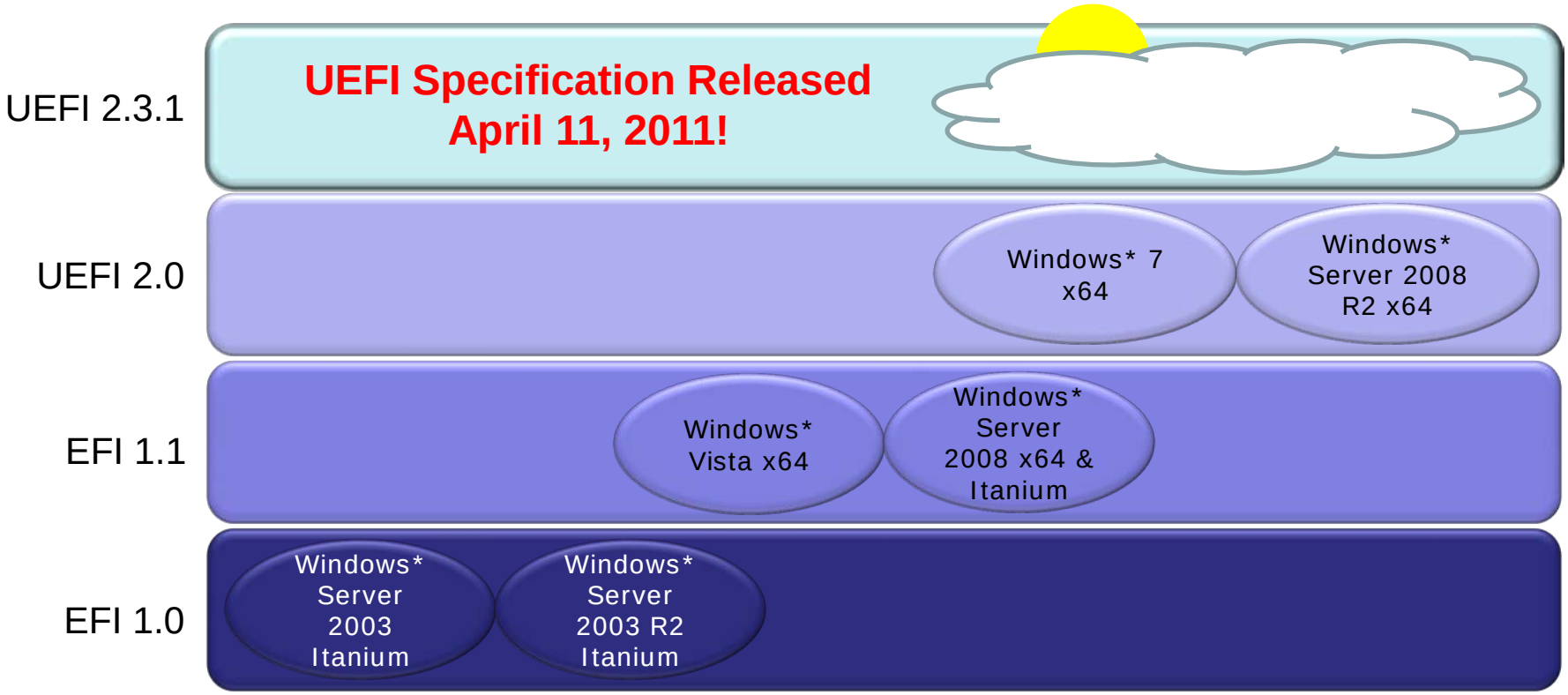
Agenda

- Microsoft Platform Evolution
- Microsoft Platform & UEFI
- Call to Action

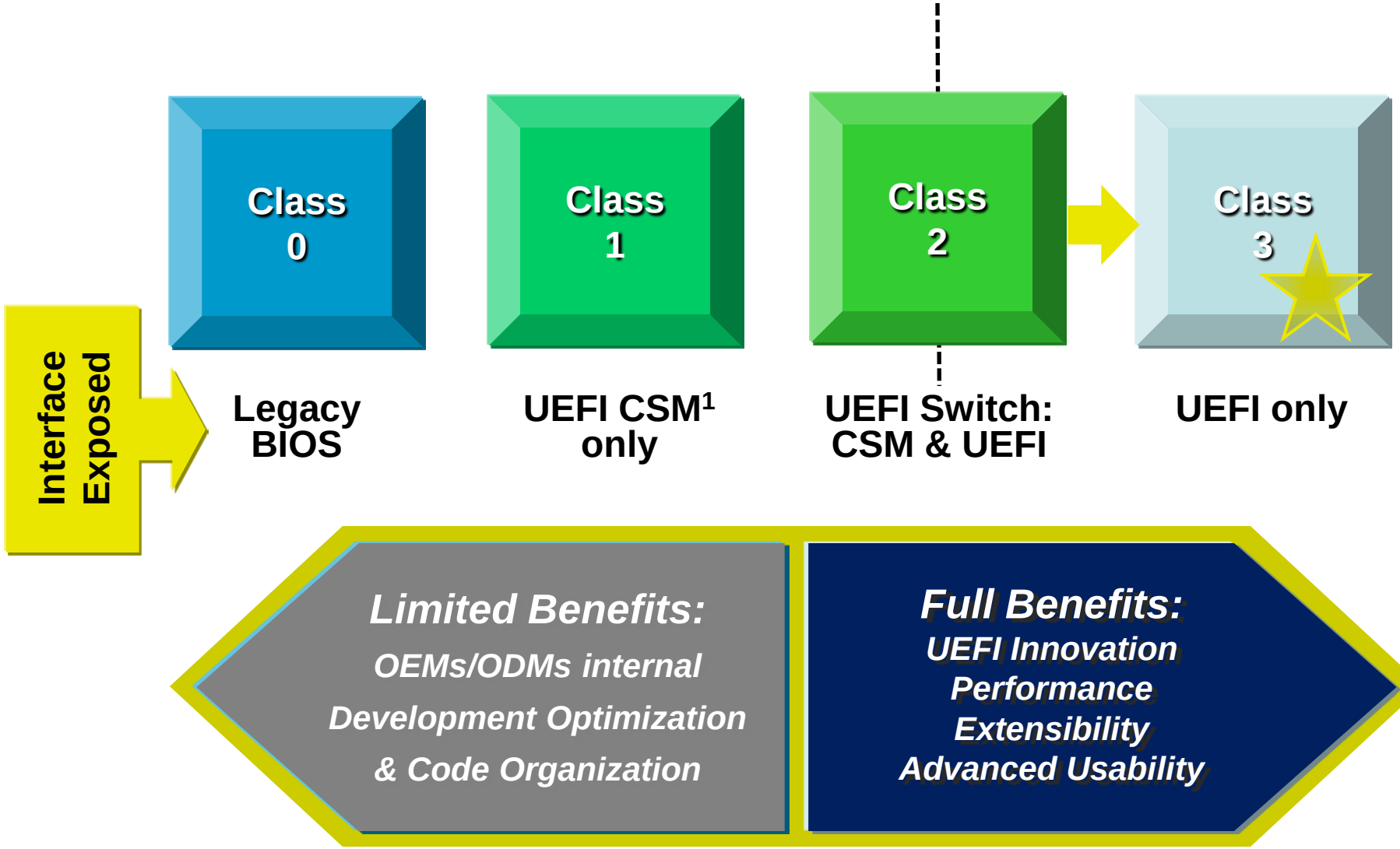
Microsoft®

Microsoft* Platform Evolution

- Microsoft* is committed to supporting UEFI, with a track record of innovation with each release



UEFI System Classes Based on Firmware I/F

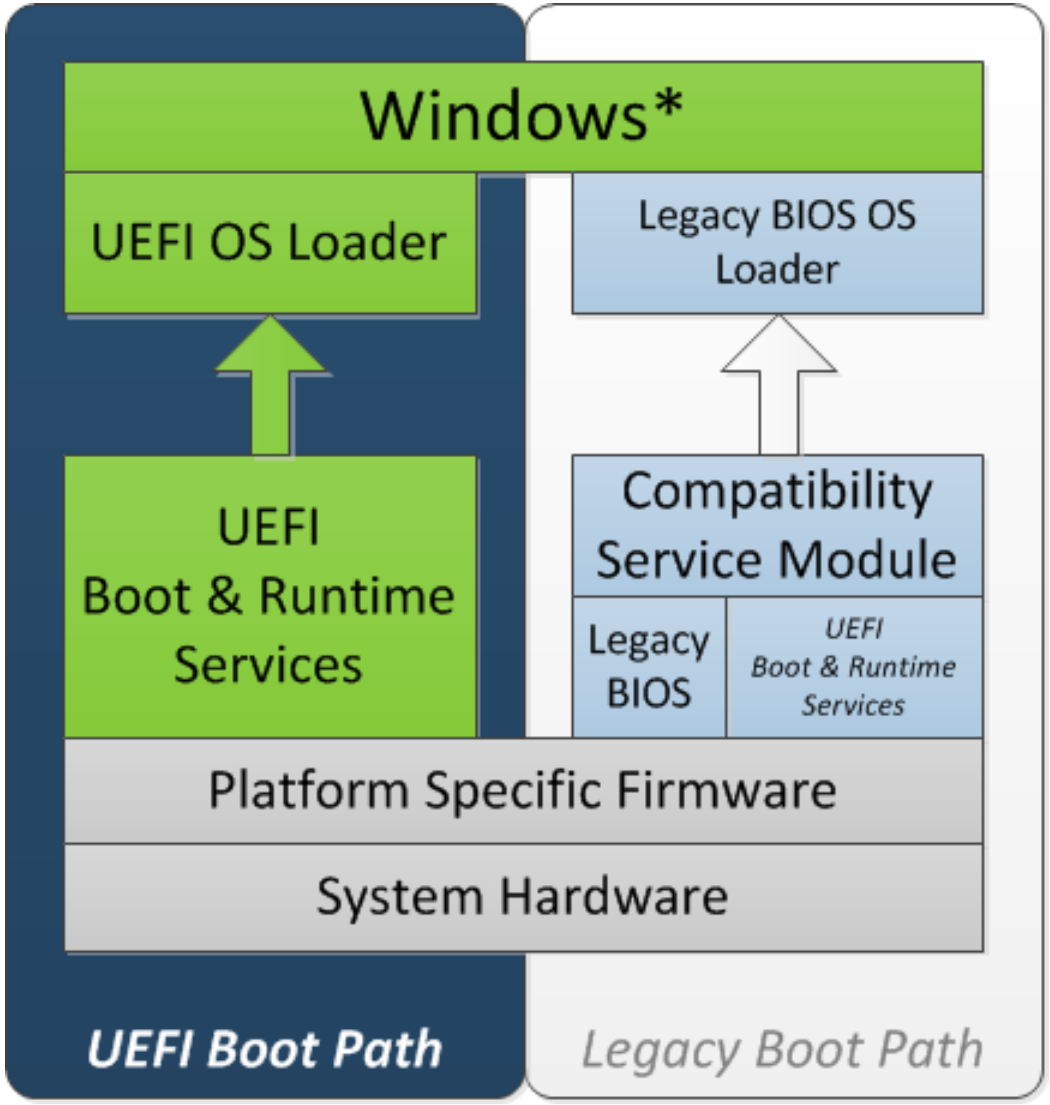


UEFI & Windows* Evolution

- Most PCs today are Class 2 UEFI and boot BIOS mode with CSM
- UEFI provides faster boot and resume times because of block I/O disk access instead of Int13h
- GPT (GUID Partition Table) partitioned disks allows disks greater than 2.2TB for system disks
- As of Windows* 7 SP1 Windows Hardware Logo no longer supports “Hybrid MBR”
- UEFI supports Authenticode verification of firmware images in the pre-OS environment

Windows* Boot Flow

- Most PCs boot through CSM (Class 1 & 2)
- Windows* 7 x64 & Windows* Server 2008 R2 x64 support UEFI OS loader if UEFI is detected
- Legacy Boot Path sustained
- **UEFI Boot Path preferred**



Microsoft

IDF2011 INTEL DEVELOPER FORUM

Optimizing for UEFI

- Redesign legacy Option ROMs into UEFI Option ROMs

- **IHVs** – deploy UEFI option ROM support, manufacturing tools and device drivers with UEFI support
- **ODMs** – provide service with updated toolsets, 64-bit environments, native factory tools with UEFI
- **OEMs** – secure your firmware, optimize for speed
- **Consumer** – look for newer UEFI based platform firmware

Microsoft* & UEFI Forum

- Microsoft* is an active member of the Forum
- UEFI 2.3.1 specification ready for download!
- Microsoft* Contributions to the UEFI Specification:

Requirement	UEFI Version	Chapter[1]
Storage	2.3.1	12.11
Secure Boot	2.3.1	7.2, 27

[1] May have dependencies on other UEFI protocols & services

Agenda

- UEFI & Windows* Overview
- Microsoft* Platform & UEFI
- Call to Action

Microsoft®

Large Disk Support with UEFI

- Disk drives >2.2TB already in the market
  - UEFI Platforms support GUID Partition Table (GPT)
  - BIOS Platforms support MBR partitioning
  - “Hybrid MBR” or enabling BIOS systems to boot GPT disks are not supported by Windows*
- Windows* 7 SP1 supports large system disks through Windows Hardware Logo
- Customer benefits
  - Support for large disks
  - Disk utilities supported for disk management

Microsoft

UEFI Secure Boot - Introduction

- UEFI provides a root of trust to verify platform firmware
  - Class 2/3 systems must boot into UEFI mode to protect against tampering
- Secure Variables store keys necessary to validate signatures of firmware
- Firmware must be signed by a certificate authority
- Update process must be secure
- UEFI Runtime Services GetVariable() & SetVariable() used to update signature databases

UEFI Secure Boot – Key Management

- Secure Boot Keys Rooted in ROM & NV-RAM
  - A minimum of 64KB of variable storage for secure boot
- UEFI PI Scope must be signed with a ROM key
- UEFI Keys (e.g. PK, KEK, etc…) stored in NV-RAM to facilitate field updates
- Verify Signed Firmware (Option ROMs) and OS Loader (BootMgr)
- Use 2048 bit RSA Keys with SHA-256 hashes
- Embed approved CA in Key Enrollment Key (KEK) and Signature Database
- **Attend the IDF HP*/Insyde* Session on Security for more details**

Microsoft

UEFI Secure Boot – Validating Firmware Images

- Key Enrollment Key Database (KEK) can also be updated with an authenticated variable signed by the PK
  - PK to be owned by the OEM
- Variable updates should be uncommon
- Images must be checked against Signature DB before loading
  - Failed images do not load and are noted in the Image Execution Table
- Image verification consumes on average 3.6-15.6ms[1] per image
  - 3.6ms for root
  - 15.6ms for 3-deep chained

[1] *Source: UEFI-USWG Reflector*

Signature Database Updates

- UEFI Runtime Services GetVariable() and SetVariable() used to update the Signature Databases
  - EFI_IMAGE_SECURITY_DATABASE_GUID
    - EFI_IMAGE_SECURITY_DATABASE contains permitted signers
    - EFI_IMAGE_SECURITY_DATABASE1 contains forbidden signers
- **Authenticated variable – must be signed with a KEK already trusted**
- **For more details see Chapters 7 & 27 of UEFI 2.3.1 Specification**

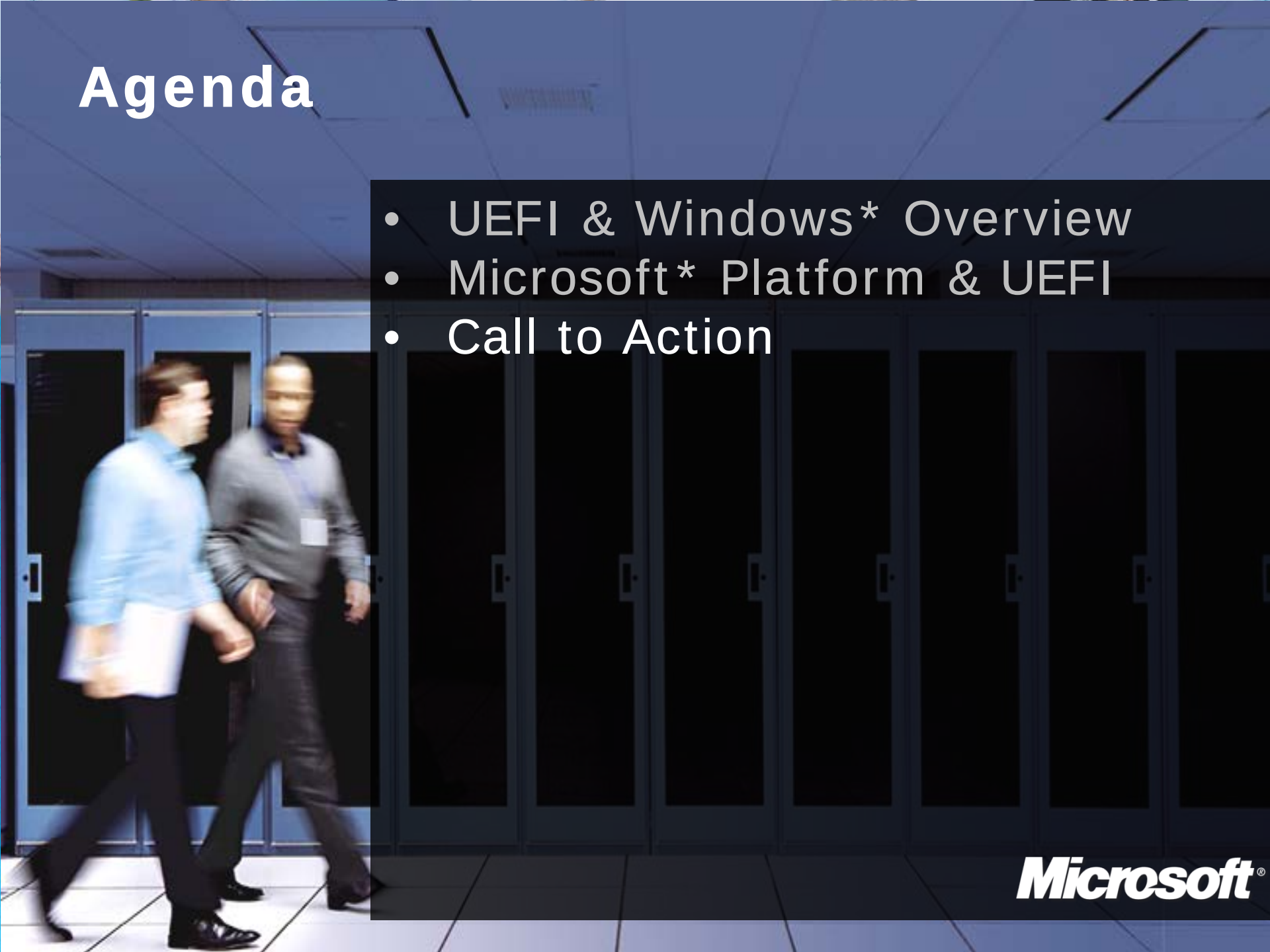
Hard Disk Encryption and Performance

- Standards based
  - OPAL v2.x+
  - IEEE 1667 TCG Storage Silo
- Benefits
  - Automatic Drive Configuration
  - Customizable encryption bands
  - Offloading data encryption from software to hardware
- Non-Blocking I/O
  - Overlap computation and disk access
  - Block I/O results in improved performance for data access
- **See Chapter 12 of UEFI 2.3.1 Specification**

Windows* 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
- Update UEFI storage stack
  - Support EFI_STORAGE_SECURITY_COMMAND_PROTOCOL
  - Support EFI_BLOCK_IO2_PROTOCOL

Agenda



- UEFI & Windows* Overview
- Microsoft* Platform & UEFI
- Call to Action

Microsoft®

Microsoft Call to Action

- Evaluate your UEFI readiness
  - Are you ready?
  - Are your processes ready?
  - Are your customers ready?
- Invest in platform firmware
  - Current investment, future potential
- Participate in UEFI plugfests
  - Bring your hardware, plug it in, test
- Join the UEFI Forum!
  - Contribute to the success of UEFI

Microsoft

Recognition

- Thanks to Intel Corporation for their ongoing efforts in UEFI development!
- Thanks to Insyde* Software and HP* for their support in secure boot presentation at IDF!
  - Attend Insyde* Software presentation about secure boot, for more details
- **Thanks to the UEFI forum for collaborating on UEFI 2.3.1 specification!**

Microsoft

EFI Track Sessions

Session ID	Title	Day/ Time	Room
EFIS001 ✓	Microsoft* Windows* Platform Evolution and UEFI	Tuesday 11:10	306A
EFIS002	UEFI Development and Innovations for System-On-Chip (SoC)	Tuesday 14:05	306A
EFIS003	UEFI and Transparent Computing Technology	Tuesday 15:10	306A
EFIS004	Intel® UEFI Development Kit 2010 and Intel® Boot Loader Development Kit: Foundations for Advanced Embedded Development	Tuesday 16:10	306A
SPCQ001	Hot Topic Q&A: Intel® Boot Loader Development Kit (Intel® BLDK)	Tuesday 17:00	306A
EFIS005	Security and Networking Advancements Today's UEFI and Intel® UEFI Development Kit 2010 (Intel® UDK2010)	Wednesday 11:10	306A

✓ = DONE

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/idfsessionsBJ

URL is on top of Session Agenda Pages in Pocket Guide

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

IDF2011
INTEL DEVELOPER FORUM

Q&A

Microsoft Legal Disclaimer

- INFORMATION IN THIS DOCUMENT IS PROVIDED AS-IS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPETY RIGHTS IS GRANTED BY THIS DOCUMENT. MICROSOFT ASSUMES NO LIABILITY WHATSOEVER, AND MICROSOFT DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF MICROSOFT PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.
- Microsoft may make changes to specifications and product descriptions at any time, without notice.
- All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.
- Nothing in this presentation modifies any of the terms and conditions of Microsoft's written and signed agreements. This is not an offer and applicable terms and the information provided is subject to revision and may be changed at any time by Microsoft.
- The information contained in this presentation represents the current view of Microsoft on the issues discussed as of the date of presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of presentation.
- Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this presentation may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Intel 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 PROPETY 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.
- Intel may make changes to specifications and product descriptions at any time, without notice.
- All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.
- Intel, processors, chipsets, and desktop boards 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.
- Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.
- Intel, 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.
-

Risk Factors

The above statements and any others in this document that refer to plans and expectations for the first 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. 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. 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; product mix and pricing; 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. 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 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 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 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 report on Form 10-Q for the quarter ended September 25, 2010.

Rev. 1/13/11