微软* Windows*平台演进与UEFI规范

杜雄 – BIOS工程师，英特尔
Tony Mangefeste – 高级项目经理，微软

EFIS001

英特尔®与你共创明天™ intel

议程

- UEFI生态系统
- UEFI 2.3.1规范的更新

业界BIOS演进

之前

所有平台的BIOS都是私有的

2000

英特尔推出可扩展固件接口(EFI)规范并提供遵照free BSD条款的示例实现

2004

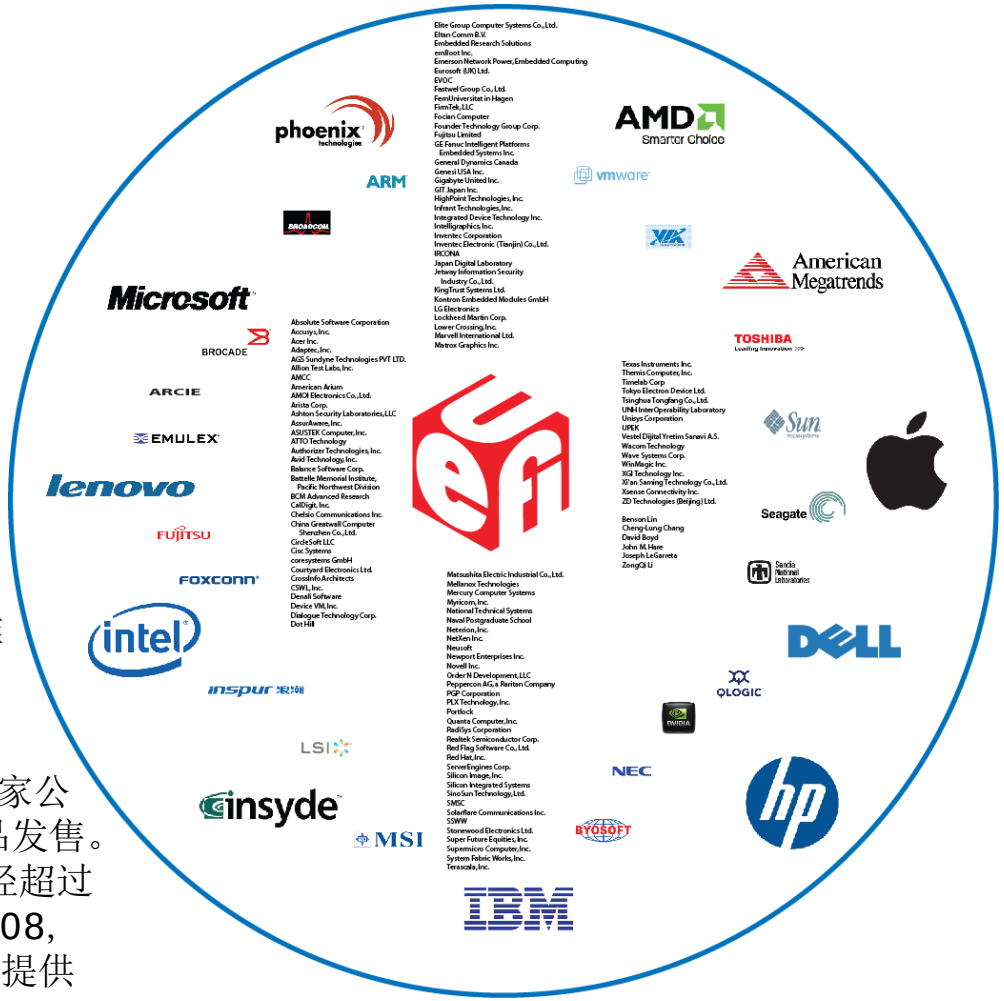
tianocore.org，EFI开源社区启动

2005

11家公司联合创办**统一可扩展固件接口(UEFI)**论坛以推进EFI规范的标准化

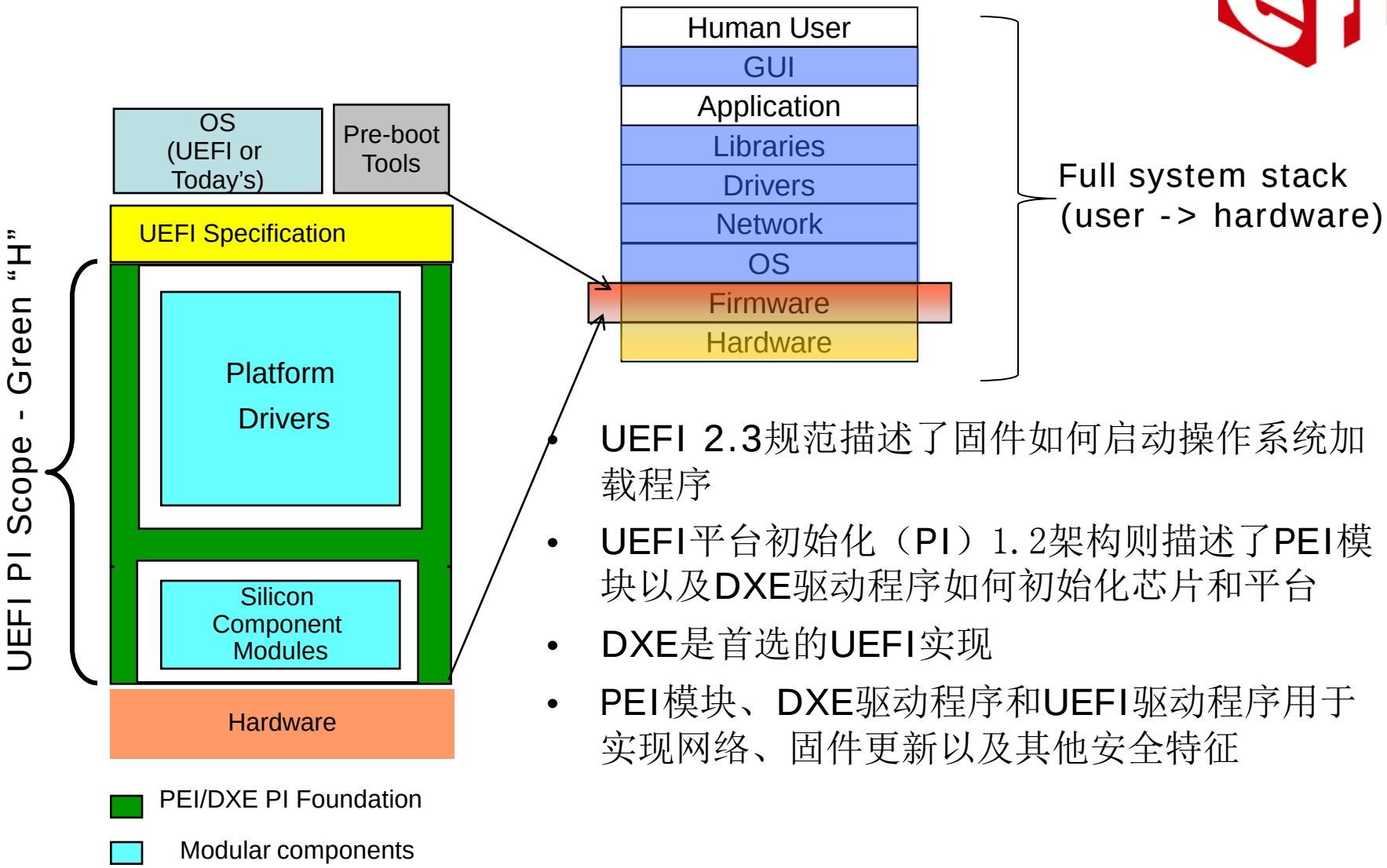
2011

UEFI论坛茁壮成长，已有170家公司加入！主要的MNC均有产品发售。IA架构中使用UEFI的平台已经超过50%，Microsoft* Server 2008, Vista* 和Win7* 操作系统均提供64位UEFI的支持，Redhat*和Novell* OS也提供对UEFI的支持



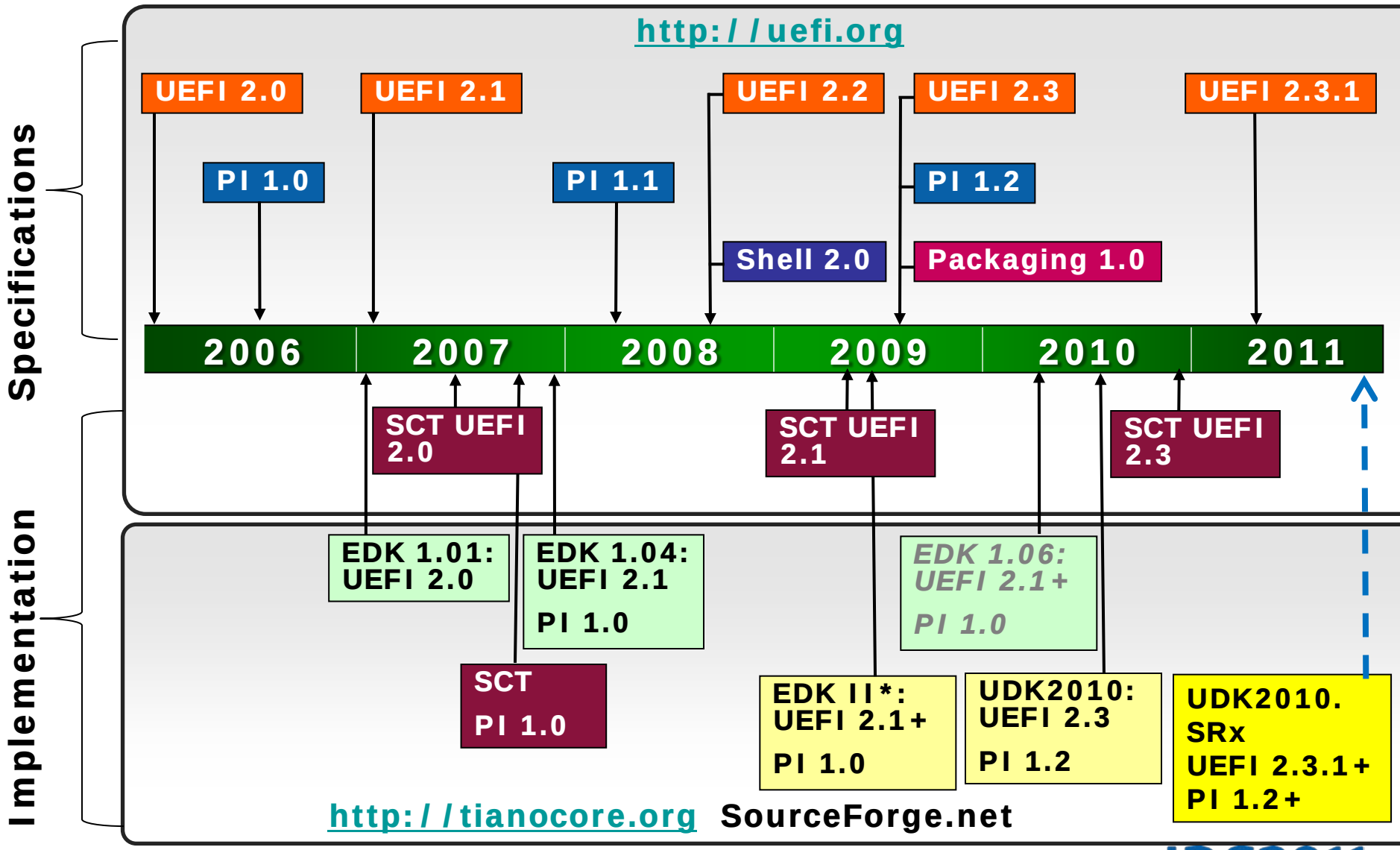
IDF2011
英特尔信息技术峰会

UEFI平台初始化概述



- UEFI 2.3规范描述了固件如何启动操作系统加载程序
- UEFI平台初始化（PI）1.2架构则描述了PEI模块以及DXE驱动程序如何初始化芯片和平台
- DXE是首选的UEFI实现
- PEI模块、DXE驱动程序和UEFI驱动程序用于实现网络、固件更新以及其他安全特征

UEFI规范和Tianocore.org时间表

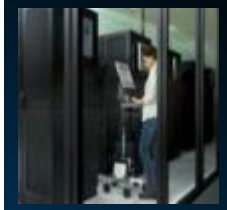


* EDK II与UDK2010是相同的代码库

业界基于UEFI的增值服务及创新领域

Pre-OS安全性以及丰富的网络功能

- IPV6/IPSec；固件模块数字签名；受保护的固件升级；TPM & S-RTM



可管理性

- 增强型诊断；智能高效的平台升级；灵活的操作系统部署；一致的界面及用户感受；改进的UI可用性以及OOB管理功能

电源管理

- 计量，限电，省电

启动优化及现代的视图

- 快速启动和恢复响应；高图形分辨率；支持从>2.2 TB的硬盘启动

新应用—UEFI应用程序

- 笔记本关机状态下在数秒内访问Outlook*数据；开机启动时播放视频广告

议程

- UEFI生态系统
- UEFI 2.3.1规范的更新

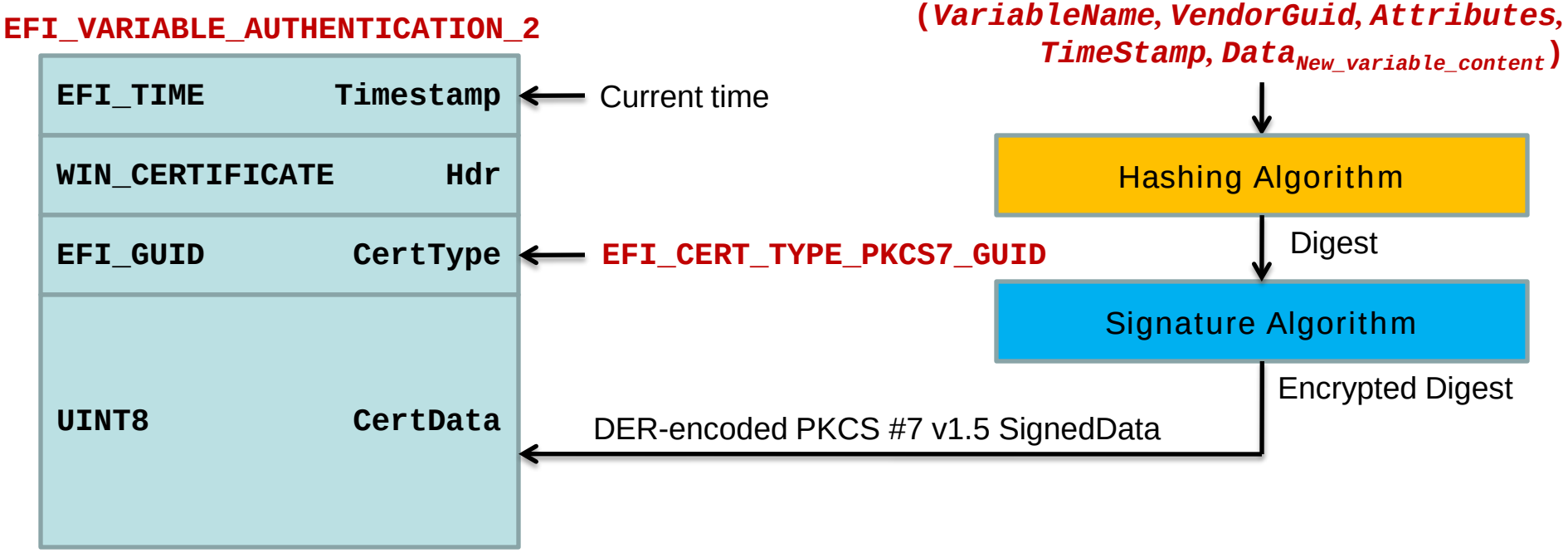
UEFI 2.3.1规范的更新

安全	• 认证变量及签名数据库 • 密钥管理服务（KMS） • 为自加密硬盘定义的存储安全命令协议
网络	支持DUID-UUID选项报告平台标识
互通	• 新定义FC和SAS设备路径 • FAT32数据区域对齐 • HII相关更新 • 新增HII对话框形式的窗体
性能	操作块设备的非阻塞接口
技术	与USB 3.0相关的更新
维护	用户身份鉴别以及其他

UEFI 2.3.1 使更多安全相关的支持成为可能

UEFI 2.3.1规范中安全相关的更新

- 基于时间戳的认证变量
  - 对证书链架构的支持
  - 利用绝对时间来防止rollback攻击
  - 签名数据库支持添加操作



在复杂环境中更好的提供UEFI安全启动支持

UEFI 2.3.1规范中安全相关的更新

- 密钥管理服务(KMS)
  - 包括提供生成、存储、获取以及管理密钥的相关服务
  - 基于远端密钥服务器、本地的硬件安全模块(HSM)、或者软件提供服务
- 存储安全命令协议
  - 发送和读取安全协议数据
  - 支持的命令集包括：
    - 可信赖的发送/接收(ATA8-ACS)
    - 安全输入/输出协议(SPC-4)

微软* Windows*平台演进与UEFI规范

Tony Mangefeste
高级计划经理，Microsoft Corporation

Microsoft

Sponsors of Tomorrow.™ intel

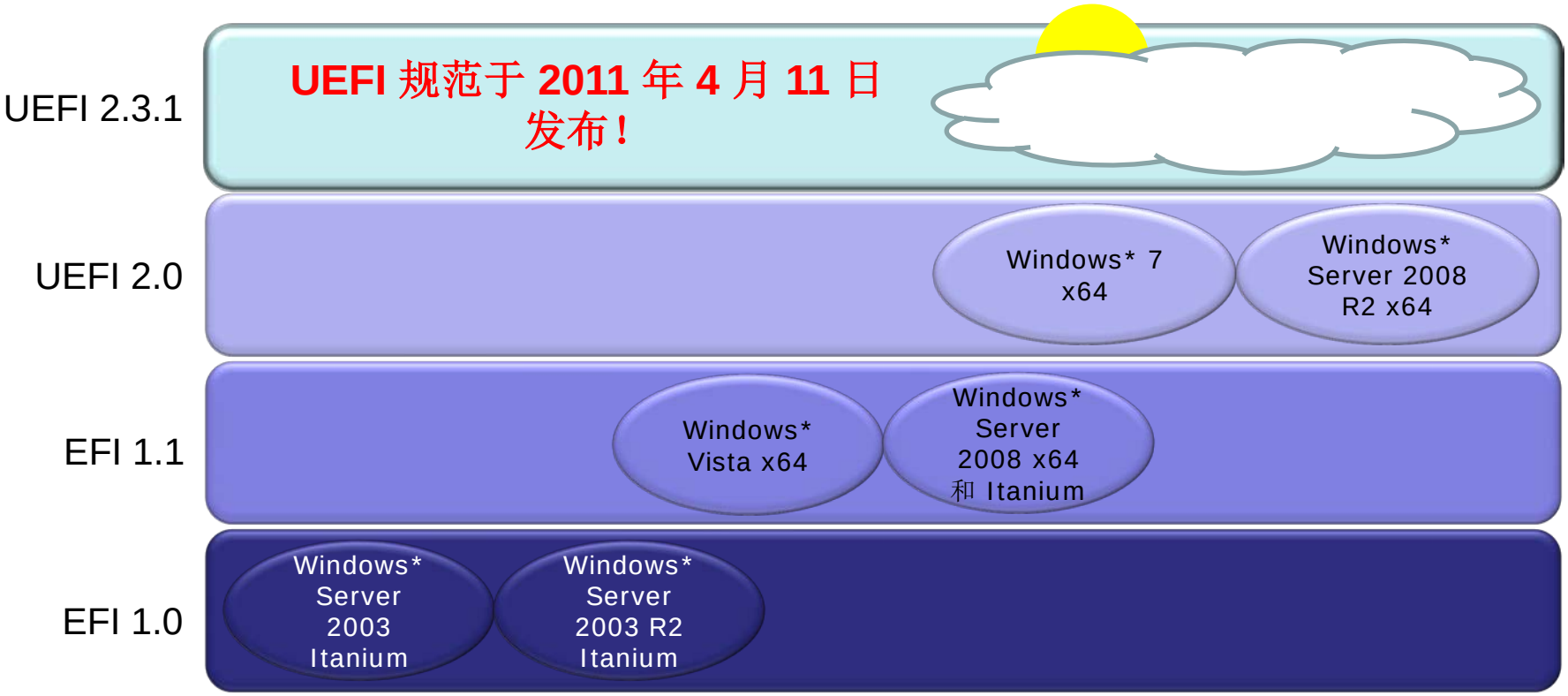
议程

- Microsoft 平台发展
- Microsoft 平台与 UEFI
- 行动呼吁

Microsoft

Microsoft* 平台发展

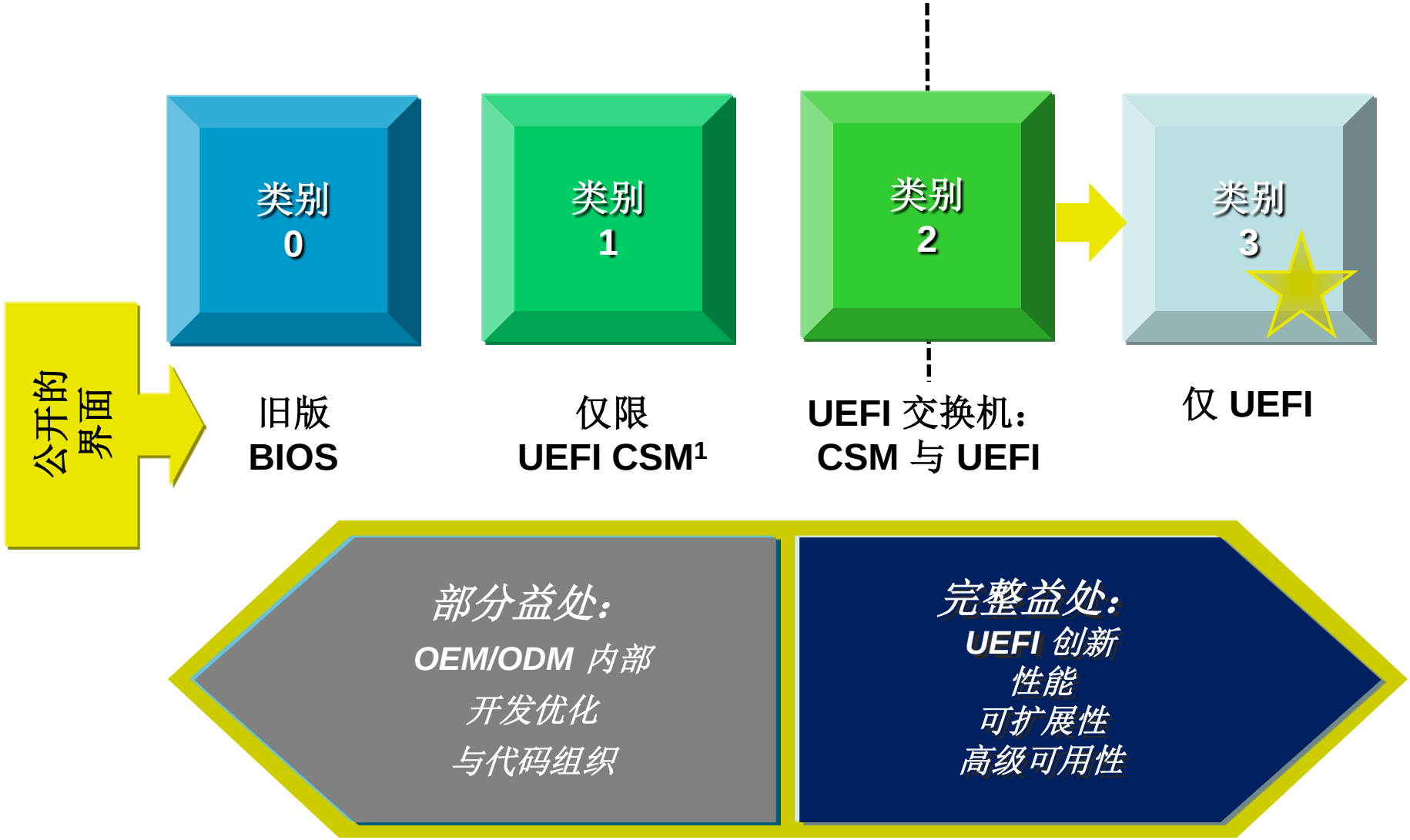
- Microsoft* 致力于支持 UEFI，每次发行新版本时都有所创新



Microsoft

IDF2011 英特尔信息技术峰会

UEFI 系统类别（基于固件 I/F）



Microsoft

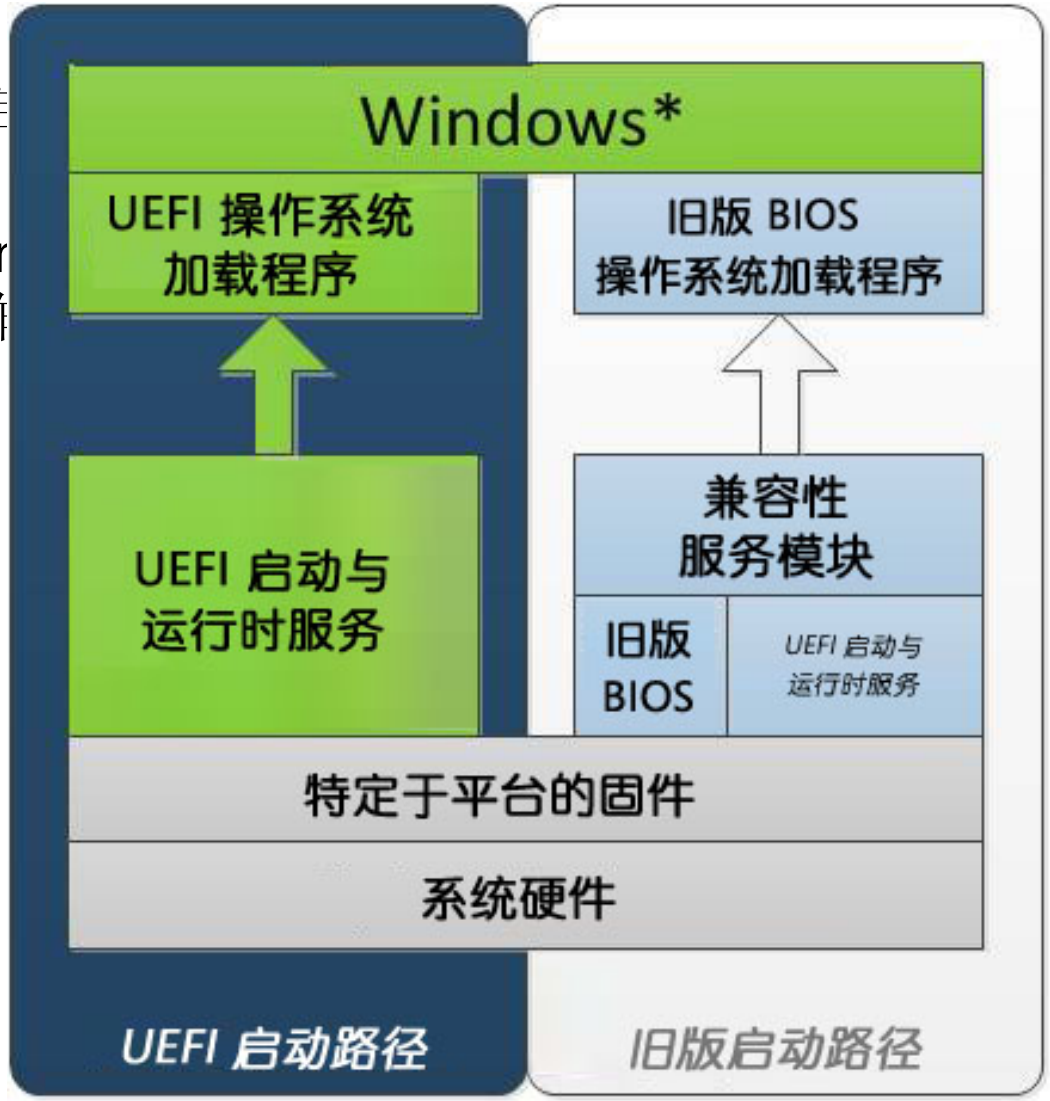
IDF2011
英特尔信息技术峰会

UEFI 与 Windows* 发展

- 目前的大多数 PC 为第 2 类 UEFI，通过 CSM 启动 BIOS 模式
- 由于采用数据块 I/O 磁盘访问而非 Int13h，UEFI 提供更快的启动与恢复时间
- GPT（GUID 分区表）分区磁盘允许系统磁盘超过 2.2TB
- 自 Windows* 7 SP1 起，Windows 硬盘徽标不再支持“混合 MBR”
- UEFI 支持在预操作系统环境中对固件映像进行 Authenticode 验证

Windows* 启动流程

- 大多数 PC 通过 CSM 启
  和第 2 类）
- 如检测到 UEFI，则 Wir
  R2 x64 支持 UEFI 操作
  程序
- 保留旧版启动路径
- **首选 UEFI 启动路径**



Microsoft

IDF2011
英特尔信息技术峰会

针对 UEFI 进行优化

- 将旧版可选 ROM 重新设计为 UEFI 可选 ROM
- **IHV** – 利用 UEFI 支持来部署 UEFI 可选 ROM 支持、制造工具和设备驱动程序
- **ODM** – 通过更新的工具集、64 位环境和带 UEFI 的本机出厂工具提供服务
- **OEM** – 保护固件安全，针对速度进行优化
- **使用者** – 寻求基于 UEFI 的更高版本平台固件

Microsoft* 与 UEFI 论坛

- Microsoft* 是本论坛的活跃成员
- UEFI 2.3.1 规范随时可供下载！
- Microsoft* 对 UEFI 规范的贡献：

要求	UEFI 版本	章节[1]
Storage	2.3.1	12.11
安全启动	2.3.1	7.2, 27

[1] 可能取决于其他 UEFI 协议和服务

Microsoft

议程

- UEFI 与 Windows* 概述
- Microsoft* 平台与 UEFI
- 行动呼吁

Microsoft®

通过 UEFI 支持大磁盘

- 容量 >2.2 TB 的磁盘驱动器已经上市
  - UEFI 平台可支持 GUID 分区表 (GPT)
  - BIOS 平台可支持 MBR 分区
  - Windows* 不支持通过“混合 MBR”或启用 BIOS 系统来启动 GPT 磁盘
- Windows* 7 SP1 通过 Windows 硬件徽标支持大系统磁盘
- 对客户的益处
  - 支持大磁盘
  - 支持磁盘实用工具以用于磁盘管理

UEFI 安全启动 – 简介

- UEFI 提供一个信任根，用于验证平台固件
  - 第 2/3 类系统在启动后必须进入 UEFI 模式，防止篡改
- 保护在验证固件签名时所需的变量存储密钥
- 固件必须具有证书颁发机构的签名
- 更新流程必须安全
- UEFI 运行时服务 GetVariable() 和 SetVariable() 用于更新签名数据库

UEFI 安全启动 – 密钥管理

- 安全启动密钥基于 ROM 和 NV-RAM
  - 至少 64KB 的变量存储以实现安全启动
- UEFI PI 范围必须使用 ROM 密钥签名
- UEFI 密钥（如：PK、KEK 等）存储于 NV-RAM 以加快字段更新
- 验证带有签名的固件（可选 ROM）和操作系统加载程序 (BootMgr)
- 使用 2048 位 RSA 密钥和 SHA-256 哈希算法
- 在密钥注册密钥 (KEK) 和签名数据库中嵌入已批准的 CA
- **有关详细信息，请参加 IDF HP* / Insyde* 关于安全主题的演讲**

UEFI 安全启动 – 验证固件映像

- 密钥注册密钥 (KEK) 数据库还可以通过已获身份验证、由 PK 签名的变量进行更新
  - PK 由 OEM 拥有
- 变量不应经常更新
- 在加载映像前必须参照签名数据库对其进行检查
  - 有故障的映像不会加载，将在映像执行表中予以注明
- 每个映像的平均验证时间为 3.6–15.6 毫秒[1]
  - 根目录验证为 3.6 毫秒
  - 3 层深度链路结构验证为 15.6 毫秒

[1] *资料来源：UEFI-USWG Reflector*

签名数据库更新

- UEFI 运行时服务 GetVariable() 和 SetVariable() 用于更新签名数据库
  - EFI_IMAGE_SECURITY_DATABASE_GUID
    - EFI_IMAGE_SECURITY_DATABASE 包含已获准的签名者
    - EFI_IMAGE_SECURITY_DATABASE1 包含被禁止的签名者
- **已获身份验证的变量 – 必须通过已获信任的 KEK 签名**
- **有关详细信息，请参见 UEFI 2.3.1 规范的第 7 章和第 27 章**

硬盘加密和性能

- 依据的标准
  - OPAL v2.x+
  - IEEE 1667 TCG 存储单元
- 益处
  - 自动驱动器配置
  - 自定义加密带
  - 将数据加密从软件转移至硬件
- 非数据块 I/O
  - 重叠计算和磁盘访问
  - 数据块 I/O 可提高数据访问的性能
- **请参见 UEFI 2.3.1 规范的第 12 章**

Windows* 平台建议

- 确保所有资产都在平台上受到信赖以提高平台安全性
- 利用 UEFI 驱动程序而不是可选 ROM
- 设计提供足够的闪存存储以存储密钥和证书
- 考虑提高安全性的影响
- 在执行之前验证固件组件
- 当平台不安全时向客户发出警告
- 更新 UEFI 存储堆栈
  - 支持 EFI_STORAGE_SECURITY_COMMAND_PROTOCOL
  - 支持 EFI_BLOCK_IO2_PROTOCOL

议程

- UEFI 与 Windows* 概述
- Microsoft* 平台与 UEFI
- 行动呼吁

Microsoft®

Microsoft 行动呼吁

- 评估 UEFI 就绪性
  - 您准备就绪了吗？
  - 您的流程准备就绪了吗？
  - 您的客户准备就绪了吗？
- 投资平台固件
  - 现在进行投资，未来收获潜力
- 参加 UEFI 互通性测试
  - 将硬件带来，插入，然后测试
- 加入 UEFI 论坛！
  - 为 UEFI 的成功作出贡献

Microsoft

鸣谢

- 感谢 Intel Corporation 长久以来对于 UEFI 开发工作的支持！
- 感谢 Insyde* Software 和 HP* 对 IDF 上有关安全启动的演讲的支持！
  - 有关详细信息，请参加 Insyde* Software 关于安全启动主题的演讲
- **感谢 UEFI 论坛在 UEFI 2.3.1 规范上给予的协作！**

EFI 专题讲座课程

课程编号	课程标题	日期/时间	教室
✓ EFIS001	微软* Windows*平台演进与UEFI规范	周二 11:10	306A
EFIS002	片上系统（SoC）的 UEFI 开发与创新特性	周二 14:05	306A
EFIS003	UEFI 和透明计算技术	周二 15:10	306A
EFIS004	英特尔® UEFI 开发套件 2010 和英特尔® Boot Loader 开发套件： 高级嵌入式开发基础	周二 16:10	306A
SPCQ001	热点问题问答:英特尔® Boot Loader 开发套件（英特尔® BLDK）	周二 17:00	306A
EFIS005	当前 UEFI 和英特尔® UEFI 开发套件 2010（英特尔® UDK2010）在安全性和网络连接方面的进展	周三 11:10	306A

✓ =完毕

本课程演示文稿 - PDFs

本课程演示文稿（PDF）发布在技术课程目录网站：

intel.com/go/idfsessionsBJ

该网址同时打印于会议指南中专题讲座日程页的上方

请 填 写 课 程 评 估 表

请将您填写完的课程评估表
交予大会工作人员

非常感谢您的反馈，我们将据此改进未来的
英特尔信息技术峰会

问答

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.

Microsoft

IDF2011
英特尔信息技术峰会

Legal Disclaimer

DO not translate

- 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.
- Copyright ©2011 Intel Corporation.

Risk Factors

DO not translate

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