IDF2013
英特尔信息技术峰会

UEFI 固件增强 Linux* 安全性并带来全新优势

龙勤, 软件架构师，英特尔
Jeff Bobzin, 副总裁，系微股份有限公司
胡立聖, BIOS工程师，科能软件股份有限公司

PTAS001

英特尔®与你共创明天™ intel®

议程

- 针对 Linux* 的 UEFI 注意事项
- 针对企业系统的安全启动 – Insyde*
- Ubuntu* UEFI/安全启动的实现与工具
- 总结

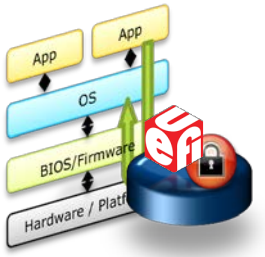
本课程演示文稿（PDF）发布在技术课程目录网站:
intel.com/go/idfsessionsBJ

该网址同时打印于会议指南中专题讲座日程页的上方

针对 Linux* 的 UEFI 注意事项

- UEFI 安全启动概述
- Linux* 下安全启动面临的挑战
- Linux 发行版安全启动支持的最新进展

UEFI 安全启动技术概述



- **系统启动面临的问题**
  - 越来越多的恶意软件开始以启动路径为攻击目标
  - 通常情况下，唯一的解决办法是重新安装操作系统
- **UEFI 安全启动使启动过程更安全**
  - 启动过程中，所有的固件和软件必须由可信的证书权威(CA)进行签名
  - 利用固件策略对OS加载程序、Option Cards等进行验证
  - 为用户提供一种阻止外部入侵的系统保护方式
  - 减少 rootkits, bootkits 和其它恶意软件的可能性

Linux* 支持安全启动所面临的挑战

- 双操作系统部署挑战
  - 用户可以通过禁用 UEFI 安全启动进行 Linux* 的安装，但这并非最佳部署方案
  - 当其它操作系统已经启用 UEFI 安全启动时，用户必须有一个其它方案继续安装 Linux
- 如果满足以下条件，Linux 亦可受益于 UEFI 安全启动技术
  - 客户能够在无需禁用该功能情况下安装 Linux
  - 平台所有者能够设置安全策略并定制系统
- 对于UEFI，Linux 发行版还存在其它注意事项
  - 内核如何处理已签名和未签名的代码
  - 驱动程序从传统的 BIOS 调用（ INT中断处理）迁移到 UEFI

Linux 发行版必须确定如何实现安全启动技术

来自 Linux* 发行版的进展信息

- Ubuntu* 12.10 – 已发布的64位 Ubuntu 12.10 利用Shim方案支持UEFI安全启动
- Fedora* 18 – 已包含支持 MOK(Machine Owned Key) 功能的 Shim 解决方案
- Red Hat* 和 SUSE* 都将在各自的发布版本中加入对第三方签名的支持
- OpenSuse* 12.3 发布版支持 MOK 管理器和多签名的Shim 加载器
- Linux Foundation 安全启动系统已发布
- Linux 社区采用 UEFI 技术†

结合 MOK 提供第三方签名支持的 Linux 发行版已经实现

† http://www.businesswire.com/news/home/20130319006268/en/UEFI-Technology-Adopted-Linux-Community

UEFI，安全启动和企业版系统

Jeff Bobzin
副总裁，系微股份有限公司

insyde™

IDF2013
英特尔信息技术峰会

议程

- 保护企业系统的启动过程
- 为什么企业用户需要安全启动
- 安全启动功能的技术解析
- Linux*系统上的安全系统软件更新
- 我的平台为Linux的安全启动做好准备了吗？

2012的进展

Windows 8 和 Windows Server 2012 的推出*

“我想补充的是，安全机制的改进，可能成为许多企业用户购买的理由。 [...] 例如 Windows 8 和 Windows Server 2012 已取代了传统的ROM-BIOS，运用的就是新的、改进的被称为UEFI安全强化的 2.3.1 版本的业界启动标准”

Roger Grimes, infoworld.com

UEFI 版本的 Fedora 和 Ubuntu* 的推出*

“UEFI将为所有的软件层提供一个基础的信任链，它可以阻止企图在**[Linux*]**电脑上安装非法、有害的软件”

Joab Jackson, pcworld.com

insyde™

IDF2013
英特尔信息技术峰会

企业已经准备好安全启动技术

系统固件
OpRom 固件

系统主板
外插卡

恢复软件
操作系统

insyde™

议程

- 保护企业系统的启动过程
- 为什么企业用户需要安全启动
- 安全启动功能的技术解析
- Linux*系统上的安全系统软件更新
- 我的平台为Linux的安全启动做好准备了吗？

安全启动为企业用户带来的好处

- UEFI 启动针对企业用户，具有诸多优势
  - 支持大容量磁盘
  - 支持复杂的分区结构
  - 包括IPv6在内的丰富的网络支持
  - 更好地支持 PXE 预装和 iSCSI 启动
  - 更好的错误报告与管理工具

- 但是，UEFI 启动需要安全启动机制去保护对关键启动文件的访问

项目规划很关键

- 强化系统启动的好处是明显的，但是，
- 要记住，一个具有足够安全性保护，可信赖的企业用户产品，从固件开始一直延续到 Linux*的启动过程中，都需要选择优先考虑安全性的合作伙伴

合作伙伴可以协助您达到您的安全性目标!

insyde™

议程

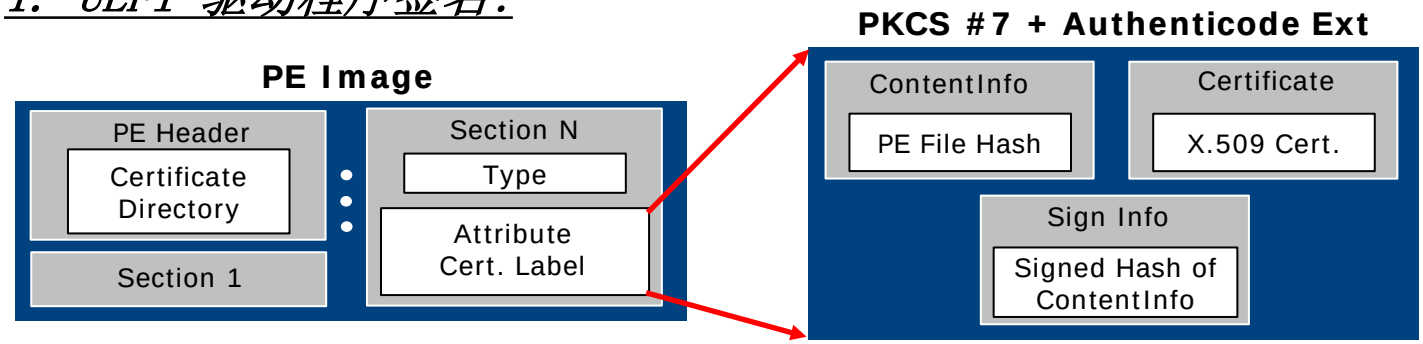
- 保护企业系统的启动过程
- 为什么企业用户需要安全启动
- 安全启动功能的技术解析
- Linux*系统上的安全系统软件更新
- 我的平台为Linux的安全启动做好准备了吗？

快速回顾 – 何谓安全启动?

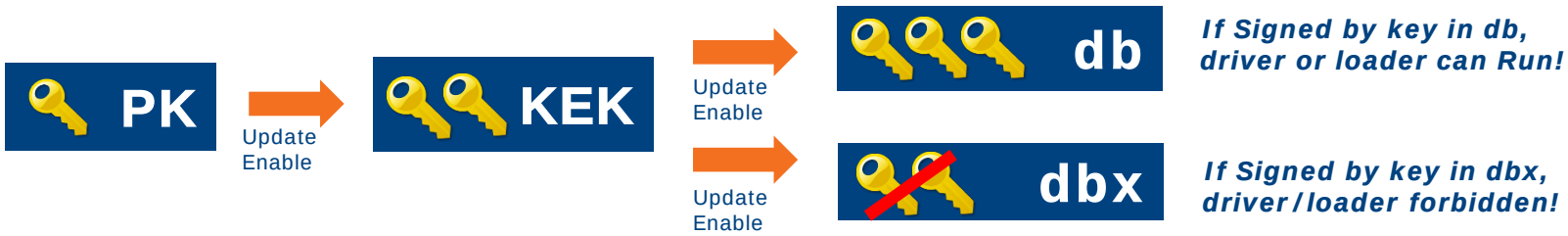
- 所谓 UEFI 安全启动，是消除从 UEFI 固件执行到 UEFI 操作系统过程中重大安全漏洞的一项技术
- Option ROMs 和 OS bootloaders 需要由私钥进行签名，而其对应的证书，则存放于系统安全数据库中
- 数据库由电脑制造商在生产时提供。需要撤销时，则由OS端来负责维护

安全启动 – 逐步解析

1. UEFI 驱动程序签名:

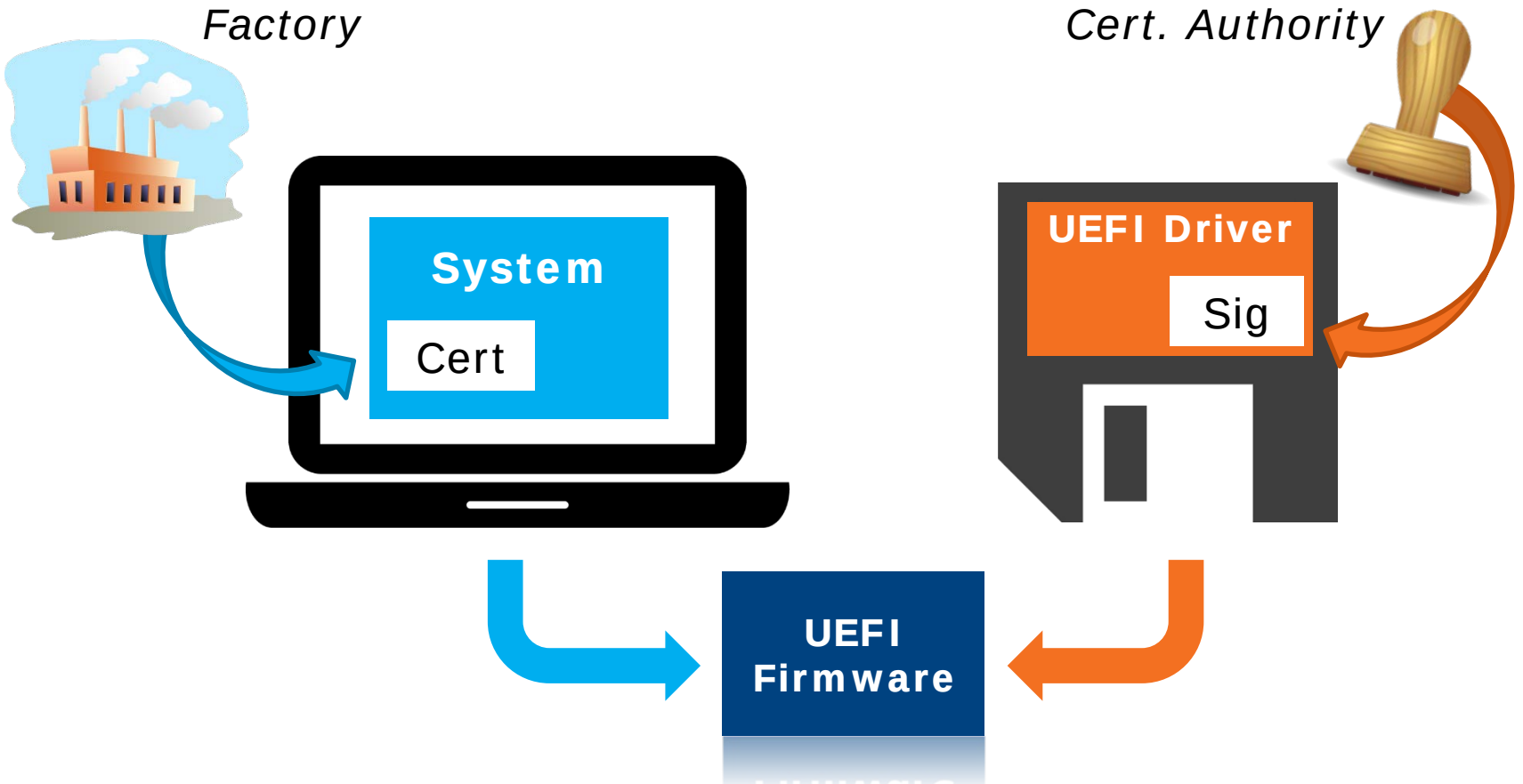


2. UEFI 安全启动数据库:



安全启动 – 逐步解析

3. 平台负责 UEFI 驱动程序检查:



固件负责校验数字签名以及数据库中的签名者信息，当满足所有要求时，驱动程序将被获准执行

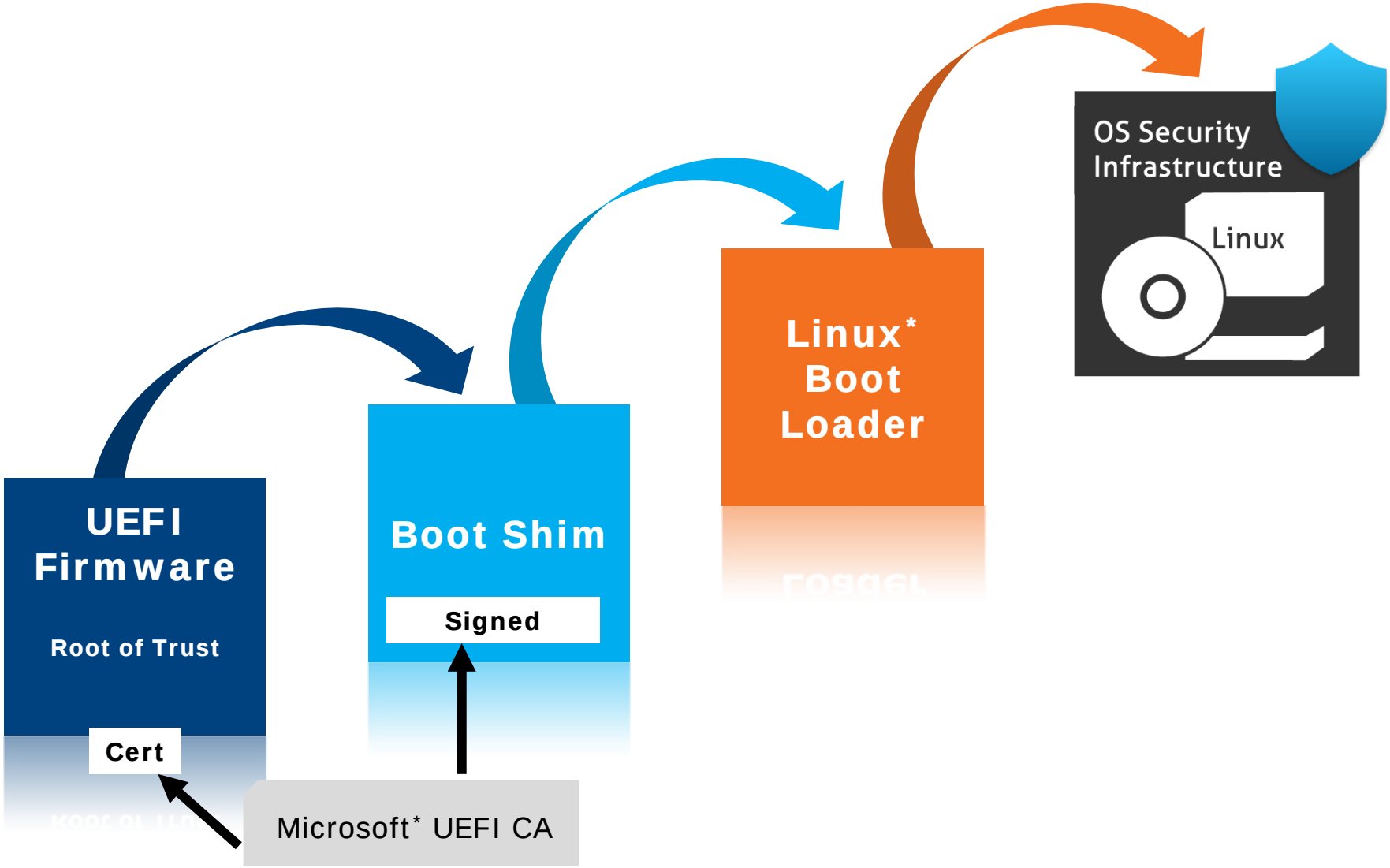
insyde™

IDF2013
英特尔信息技术峰会

微软* 为 UEFI 提供 CA 支持

- UEFI Option ROMs 需要被广泛信任的 CA 所签名
- 微软* 具有CA运营经验，并志愿提供首个面向整个工业界的 UEFI CA
- 鼓励制造商将 MS CA 证书导入“Allowed”数据库
- 微软的政策是非歧视性的，例如，微软的 CA 已签发了 Linux* ‘Shim’启动驱动程序
- 是否可能出现另一个可信 CA?
  - 有可能，足够的数据库空间
  - 需要说服OEM厂商预先导入

安全启动，Linux* 和信任链



insyde™

议程

- 保护企业系统的启动过程
- 为什么企业用户需要安全启动
- 安全启动功能的技术解析
- Linux* 系统上的安全系统软件更新
- 我的平台为Linux的安全启动做好准备了吗？

insyde™

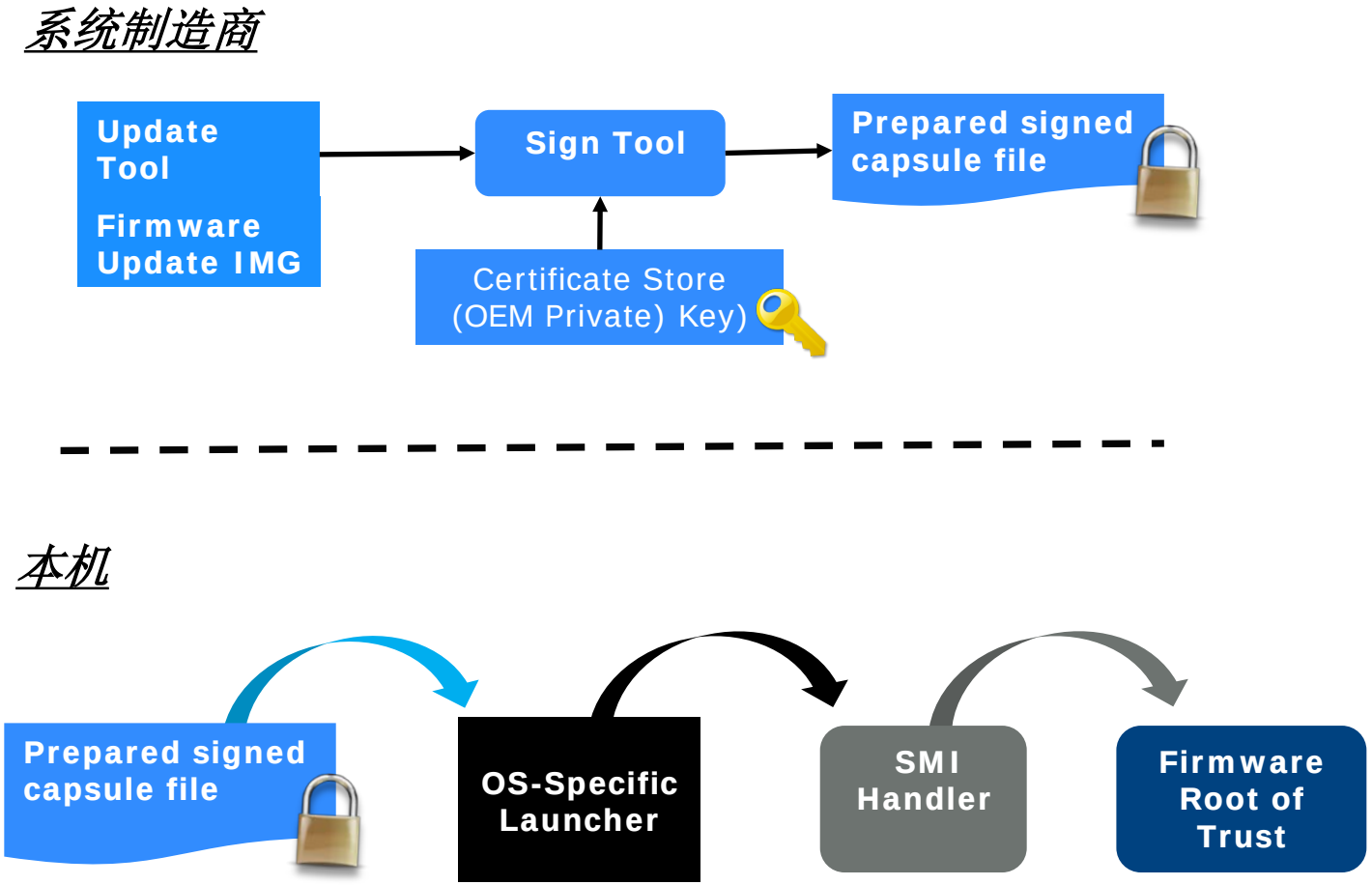
IDF2013
英特尔信息技术峰会

固件是信任根

- 安全启动的有效性取决于：是否能够保护固件代码和数据的存储免受攻击
- 目前的硬件保护机制:
  - 所有的Flash更改需被保护在 SMI 的特权代码等级之下
  - 针对代码存储或安全系统数据库的修改，必须由 SMI 下的代码来测试其签名的有效性
- 操作系统需定制专用的固件更新工具
- 系微为 OEM 提供 Windows* 和 Linux* 操作系统下的安全固件更新工具

insyde™

当前的安全固件更新机制



Linux* 系统上安全固件更新的准备步骤

OEM 步骤

1. 生成已签名的包含更新的Capsule文件 (与Windows*相同)
2. 生成适用于目标 OS 的 Linux* Flash* 更新工具

   注: 系微提供驱动程序的源代码
3. 对于非常见发行版的用户，需要生成驱动程序

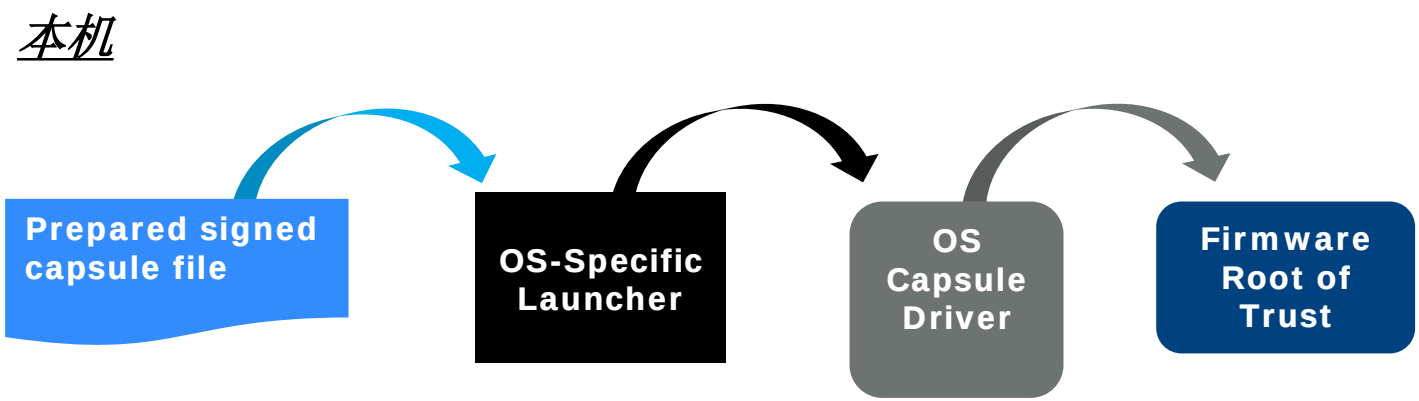
用户步骤

1. 下载包含固件更新工具的软件包，解压缩并设定权限
2. 复制已签名的 “isFlash.bin”到 InsydeFlash 文件夹
3. 固件更新程序需要管理员（root）权限才能执行
4. 执行 Linux Flash工具, 应用程序会检查是否存在正确的安全 BIOS 映像
5. 是 -> 执行 SMI 去启动安全刷新模式
6. 重启平台，在固件启动过程中应用固件更新

insyde™

工业界正致力于确保安全更新更简单、更可靠

- UEFI 提供一个针对固件更新的 UpdateCapsule 接口.期待OS厂商在2013年增加这一重要功能
  - 内嵌于Linux*，用户不必自行编译!
- 也期待针对 UEFI 扩展卡进行固件更新的工具

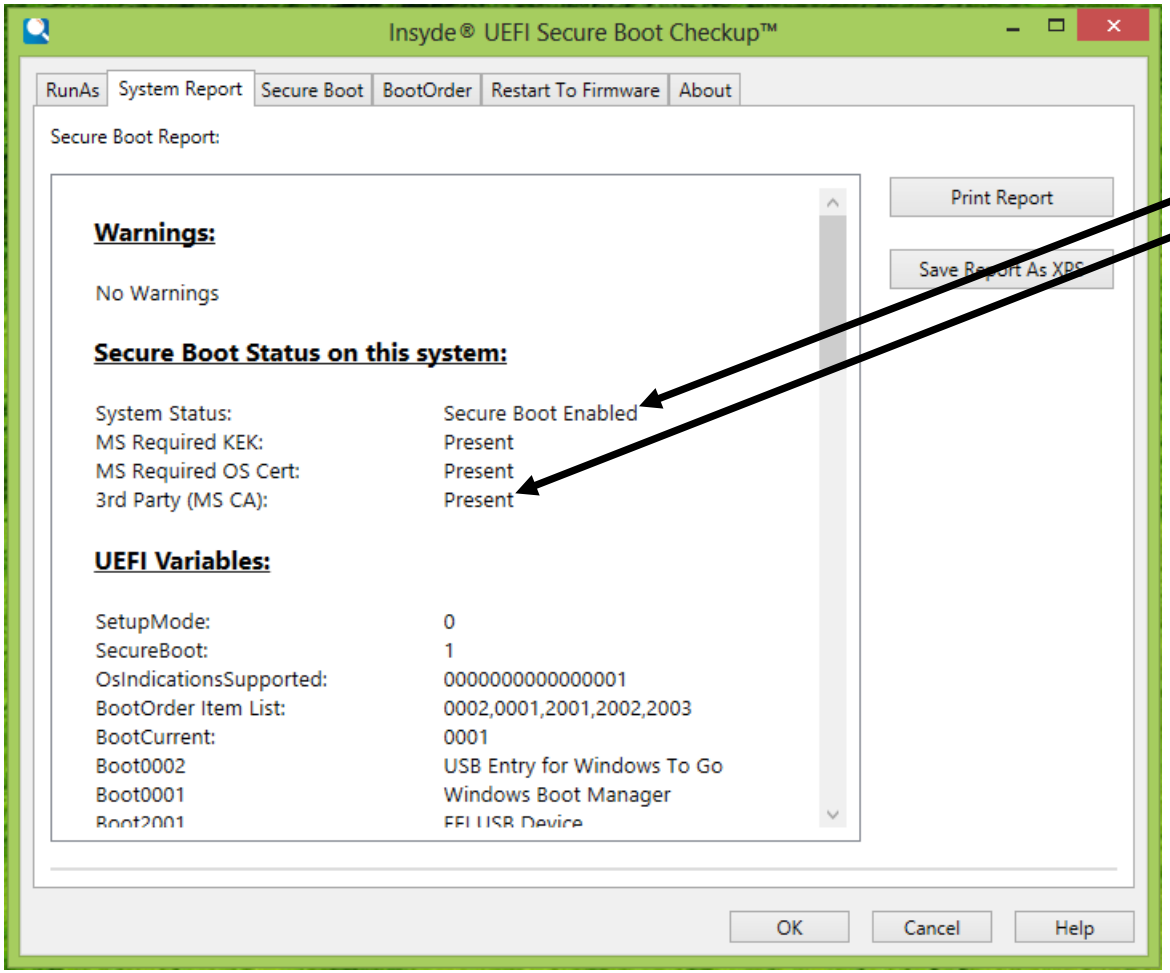


insyde™

IDF2013
英特尔信息技术峰会

议程

- 保护企业系统的启动过程
- 为什么企业用户需要安全启动
- 安全启动功能的技术解析
- Linux*系统上的安全系统软件更新
- 我的平台为Linux的安全启动做好准备了吗？



1. 安全启动已启用
2. MS CA 证书已部署

下载 Checkup Tool： http://apps.insyde.com

2013年UEFI论坛针对企业用户的目标

- 企业用户的广泛采用是个非常重要的目标!
- 对 UEFI 安全固件更新提供更流畅的用户体验

- 为达到此目标，UEFI 社区承诺:
  - 关注生态系统的所有环节 – 系统厂商、扩展卡厂商和企业级操作系统
  - 宣传其优势
  - 响应用户需求

Ubuntu* UEFI/安全启动 实现与工具

胡立聖
BIOS工程师，肯诺软件股份有限公司

CANONICAL

IDF2013
英特尔信息技术峰会

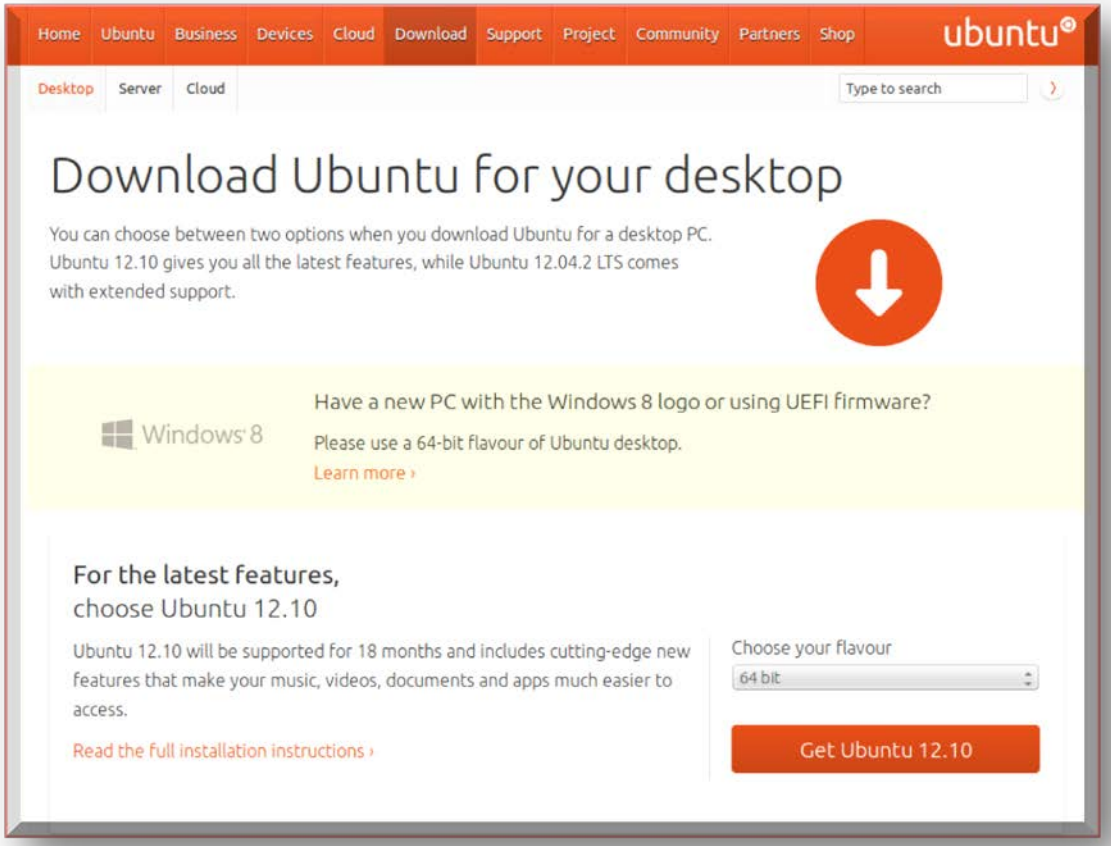
议程

- UEFI/安全启动实现
- 固件测试套件 / 固件测试套件 – Live
- 演示

UEFI/安全启动实现

UEFI/安全启动

- Ubuntu* 12.10 实现了 UEFI 安全启动
- 下载：http://www.ubuntu.com/download/desktop



CANONICAL

UEFI/安全启动实现

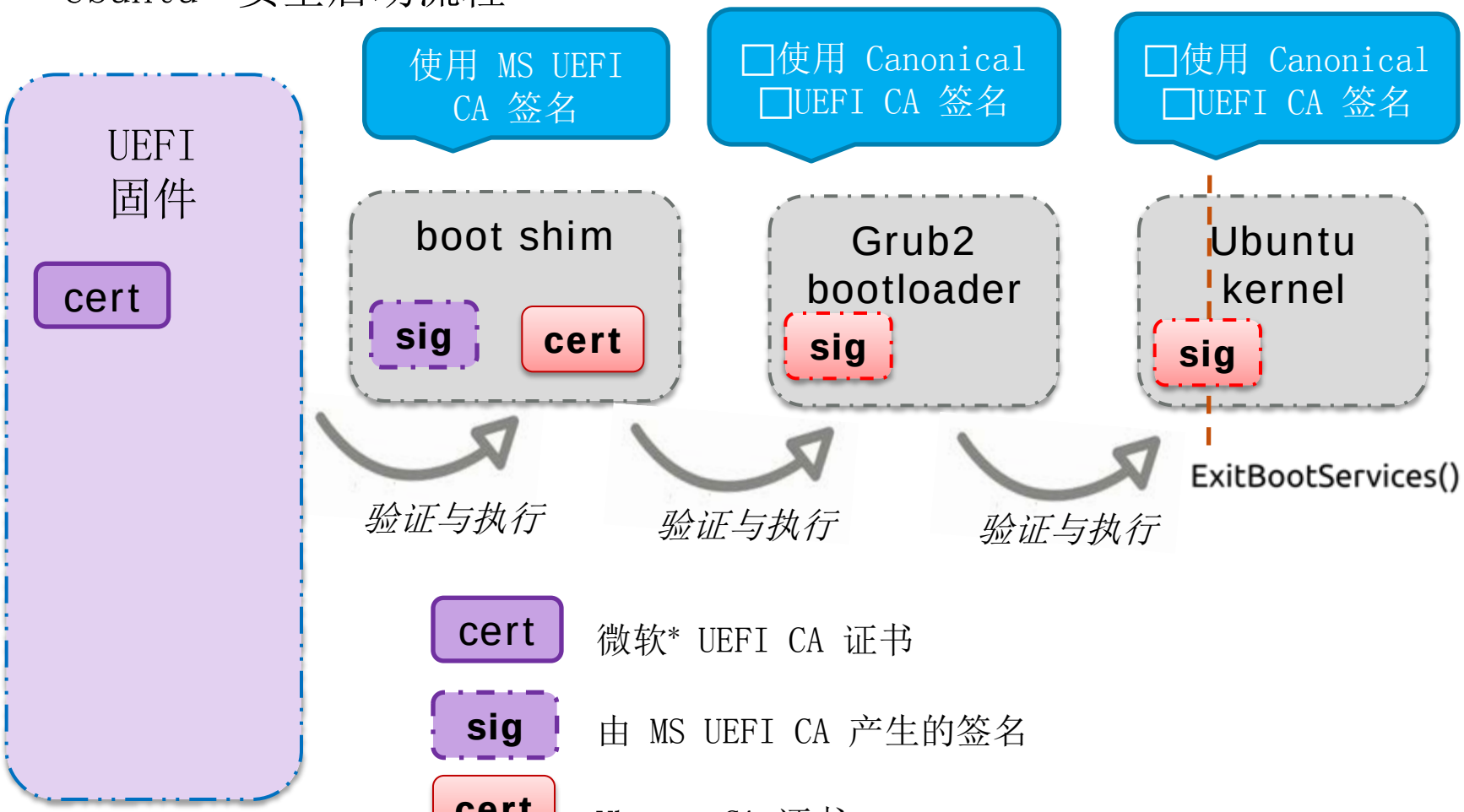
BIOS/UEFI 要求

- 兼容 UEFI 2.3.1 规范
- UEFI 启动时/运行时服务
- UEFI 启动管理器
  - 变量 Boot#### 及 BootOrder
  - BIOS 缺省状态重置

UEFI/安全启动实现

UEFI/安全启动

- Ubuntu* 安全启动流程

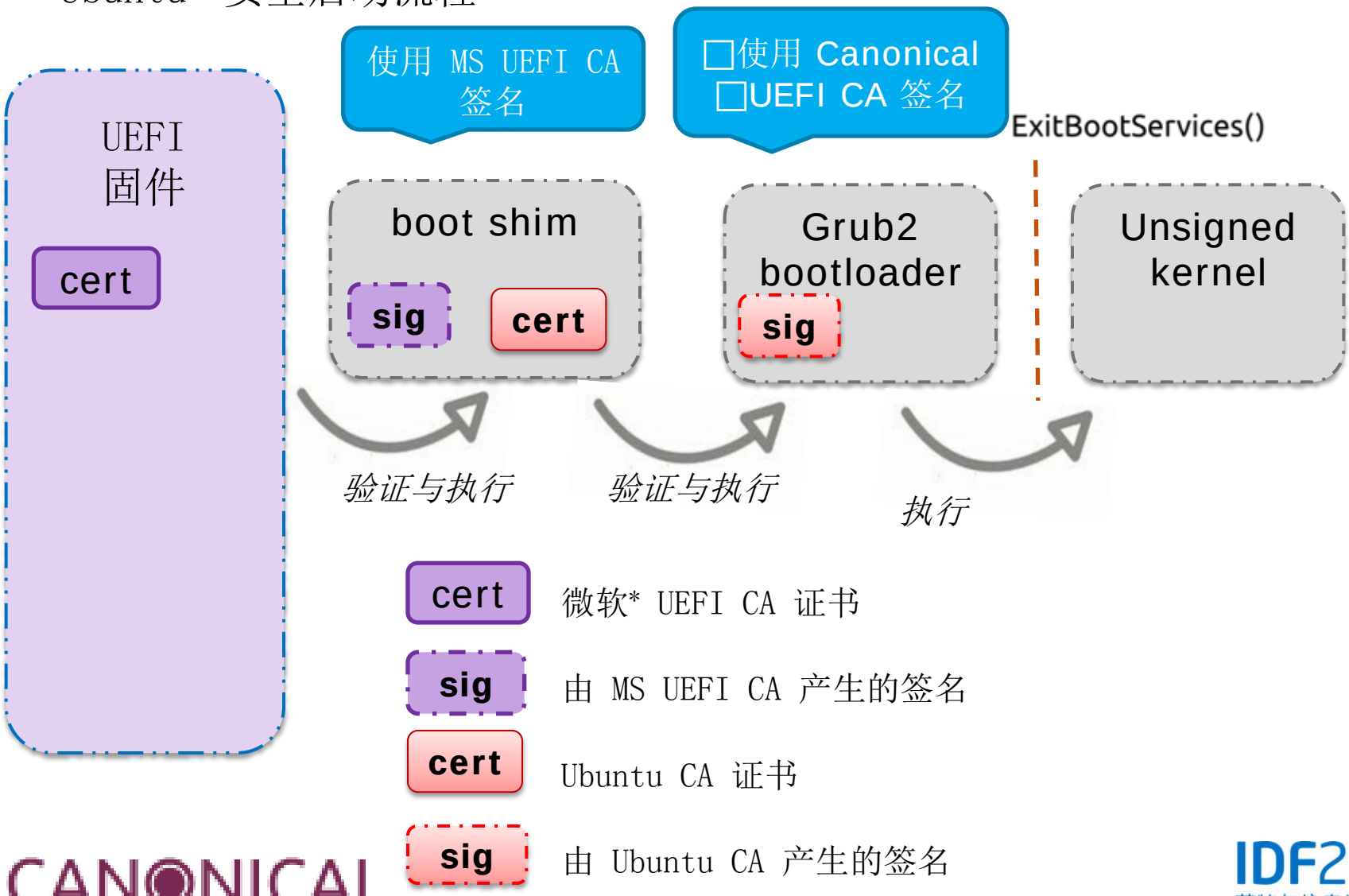


CANONICAL

UEFI/安全启动实现

UEFI/安全启动

- Ubuntu* 安全启动流程



CANONICAL

UEFI/安全启动实现

Ubuntu* 安全启动的实现

- Ubuntu 12.10 版本对安全启动的实现
  - 由微软* UEFI CA 签名的启动加载程序 shim
  - Ubuntu 签名的启动加载程序
  - Ubuntu 签名的Kernel
  - 支持未签名的 Kernel
  - 不强制模块签名
- Ubuntu 认证规范
  - 初始密钥数据库配置
  - 用户密钥重配置功能
  - 启用/禁用安全启动的设置功能
- 支持运行时的密钥重配置
  - 使用 efivars 接口对 PK, KEK, db, dbx进行更新
  - 安全启动签名工具“sbsingtool”

CANONICAL

固件测试套件（fwts）

什么是 fwts?

- Fwts是一套 Linux* 自动化固件测试工具，致力于 Bug 检测及固件修复
- 基于英特尔2007年10月发布的Linux可用的固件开发包衍生而来

- 自动检测错误
- 核心功能的正确性检测
- 确保 Linux 和固件之间的交互性
- 捕获 Linux Kernel 产生的警告
- 提供可用的解决方案建议
- 为调试收集固件数据

CANONICAL

固件测试套件（fwts）

关键功能（1/2）

- 命令行
  - 设计可供其它测试工具使用
  - 亦可单独运行
  - 并为开发者收集相关数据
- 批量测试
  - 自动化运行
- 交互性测试
  - Hot-key, lid, AC Power
- 完整的测试日志
  - 每个测试项目都有 PASS/FAIL结果
  - 解释可能失败的原因（ADVICE lines）
  - 严重性分类（CRITICAL, HIGH, LOW…）
- 结果总结
  - 提供结果日志格式设定

固件测试套件（fwts）

关键功能（2/2）

- 稳定性测试
  - 挂起/唤醒，休眠/唤醒
- 工具
  - ACPI，UEFI 变量导出…
- UEFI 运行时服务测试
  - Variable，time，其它服务
- 安全启动测试
  - 安全启动变量和证书测试

固件测试套件（fwts）

Fwts 针对安全启动的测试项目

- UEFI 安全启动的变量测试
  - SetupMode, SecureBoot 变量
- 针对微软* UEFI CA 签名数据库（“db”）的检测
- Ubuntu* 主 CA 证书是否存在于 KEK 中的检测

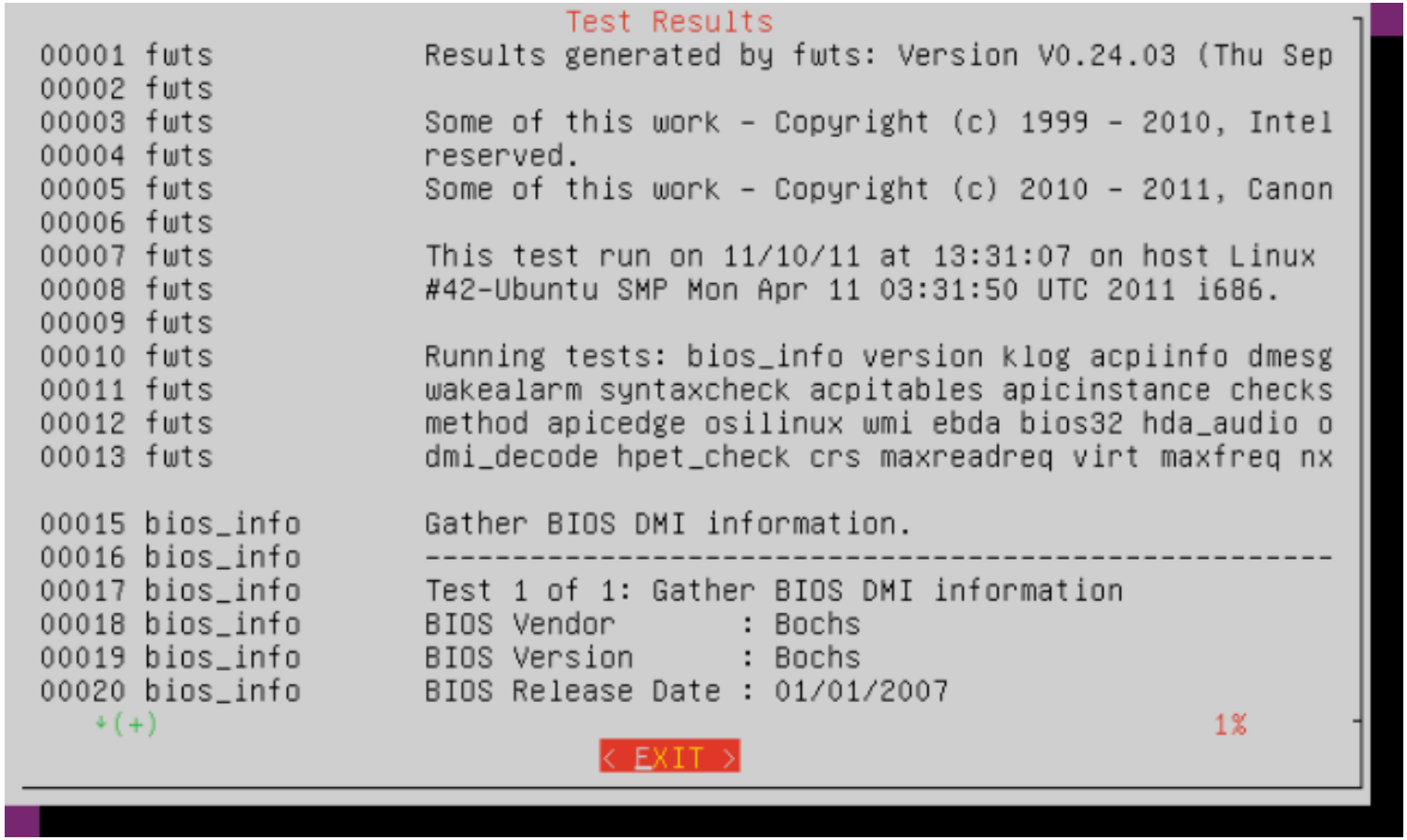
固件测试套件 Live 版 (fwts-live)

什么是 fwts-live?

- fwts-live 是一个可启动的 USB 映像，能够在未安装 Linux*/Ubuntu* 的情况下，完成启动并运行固件测试套件。结果日志直接存储在 USB 磁盘中，供日后分析使用。

- 无需安装
- 易于使用
- 随最新 Ubuntu 发布

固件测试套件 Live 版 (fwts-live)



CANONICAL

IDF2013
英特尔信息技术峰会

演示：固件测试套件（fwts）

信息

寻求更多信息

- Ubuntu* ODM 网址 - http://odm.ubuntu.com/
- 安全启动签名工具 - git://kernel.ubuntu.com/jk/sbsigntool
- Fwts
  - https://wiki.ubuntu.com/Kernel/Reference/fwts
- Fwts-live
  - https://wiki.ubuntu.com/HardwareEnablementTeam/Documentation/FirmwareTestSuiteLive

报告 fwts 错误?

- Fwts
  - https://bugs.launchpad.net/ubuntu/+source/fwts

Ubuntu* 的 UEFI 实现

- Ubuntu* 12.10 是第一个支持安全启动的版本
- Ubuntu 的安全启动在保持灵活性的同时，也保障了固件免被恶意代码攻击
- Ubuntu认证要求系统提供用户可控的安全策略
- 固件测试套件（FWTS）能够自动检测固件 - 包括对 UEFI 和安全启动的检测

CANONICAL

总结

- UEFI 安全启动使启动过程更安全
- 针对 UEFI 安全启动，生态系统已然就绪
- 基于已有的不同方案，Linux* 发行版必须确定如何实现安全启动
- Ubuntu* 支持 UEFI 安全启动，同时还提供支持自动化固件测试的FWTS套件

立即行动

- 使用已有的丰富资源，学习 UEFI 安全启动相关技术
- 为部署 UEFI 安全启动，请评估您的平台是否就绪
- 下载并测试支持 UEFI 及安全启动技术的最新 Linux* 发行版
  - Ubuntu* 安全启动相关资源：
    https://wiki.ubuntu.com/UEFI/SecureBoot
  - SUSE* 安全启动细节信息：
    https://www.suse.com/blogs/uefi-secure-boot-details/

关于这一主题的其它信息，请参照：

- Intel UEFI 社区 - http://intel.com/udk
- UEFI 论坛学习中心
  - http://www.uefi.org/learning_center/
- 使用 TianoCore edk2-devel mailing list，寻求来自其他 UEFI 开发者的支持
- 从 tianocore.org 获取白皮书 “A Tour Beyond BIOS into UEFI Secure Boot”
- 关于 Ubuntu* 的更多信息…
  - Ubuntu ODM 网址 - http://odm.ubuntu.com/
  - 安全启动工具 - git://kernel.ubuntu.com/jk/sbsigntool
- 关于 Fedora* 的更多信息…
  - http://fedoraproject.org/
- SUSE* UEFI安全启动支持计划: https://www.suse.com/blogs/tag/secure-boot/

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, 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.
-

Legal Disclaimer

- Software Source Code Disclaimer: Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license.
  Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
  THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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. 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; customer acceptance of Intel’s and competitors’ products; supply constraints and other disruptions affecting customers; 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. 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. 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 current chief executive officer plans to retire in May 2013 and the Board of Directors is working to choose a successor. The succession and transition process may have a direct and/or indirect effect on the business and operations of the company. In connection with the appointment of the new CEO, the company will seek to retain our executive management team (some of whom are being considered for the CEO position), and keep employees focused on achieving the company’s strategic goals and objectives. 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, report on Form 10-K and earnings release.

Rev. 1/17/13