IDF2012
INTEL DEVELOPER FORUM

Developing UEFI Support for Linux*

Brian Richardson, Senior Technical Marketing Engineer, Intel
Jeremy Kerr, Technical Architect, Canonical Ltd.
Matthew Garrett, Sr. Software Engineer, RedHat Inc.

EFIS001

Sponsors of Tomorrow. intel

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

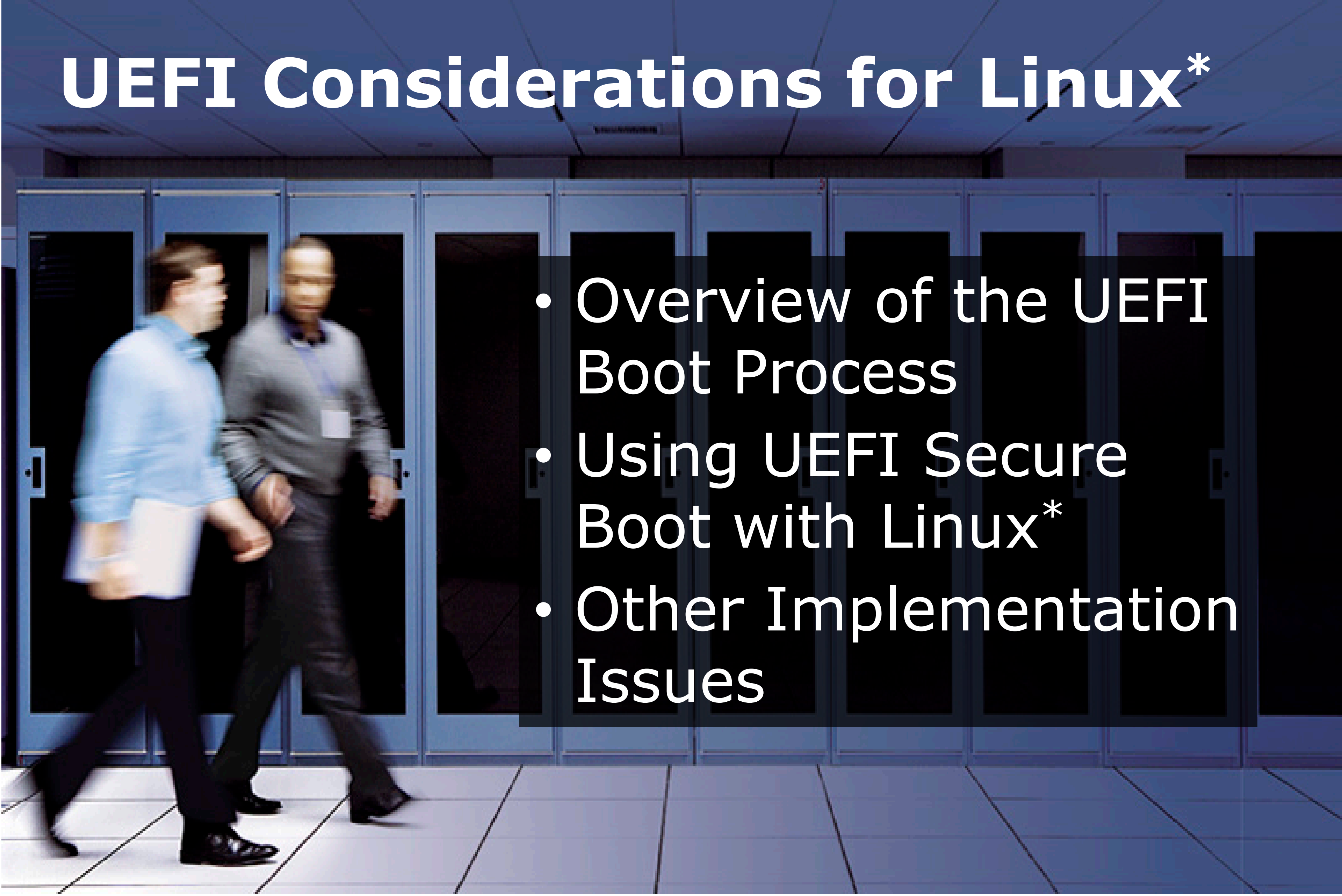
- UEFI Considerations for Linux*
  - Overview of the UEFI Boot Process
  - Using UEFI Secure Boot with Linux
  - Other Implementation Issues
- Implementing UEFI in Ubuntu* 12.10
- Implementing UEFI in Fedora* 18
- Latest Updates to SUSE* Secure Boot Plans
- Summary / Next Steps / Q&A

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

intel.com/go/idfsessions

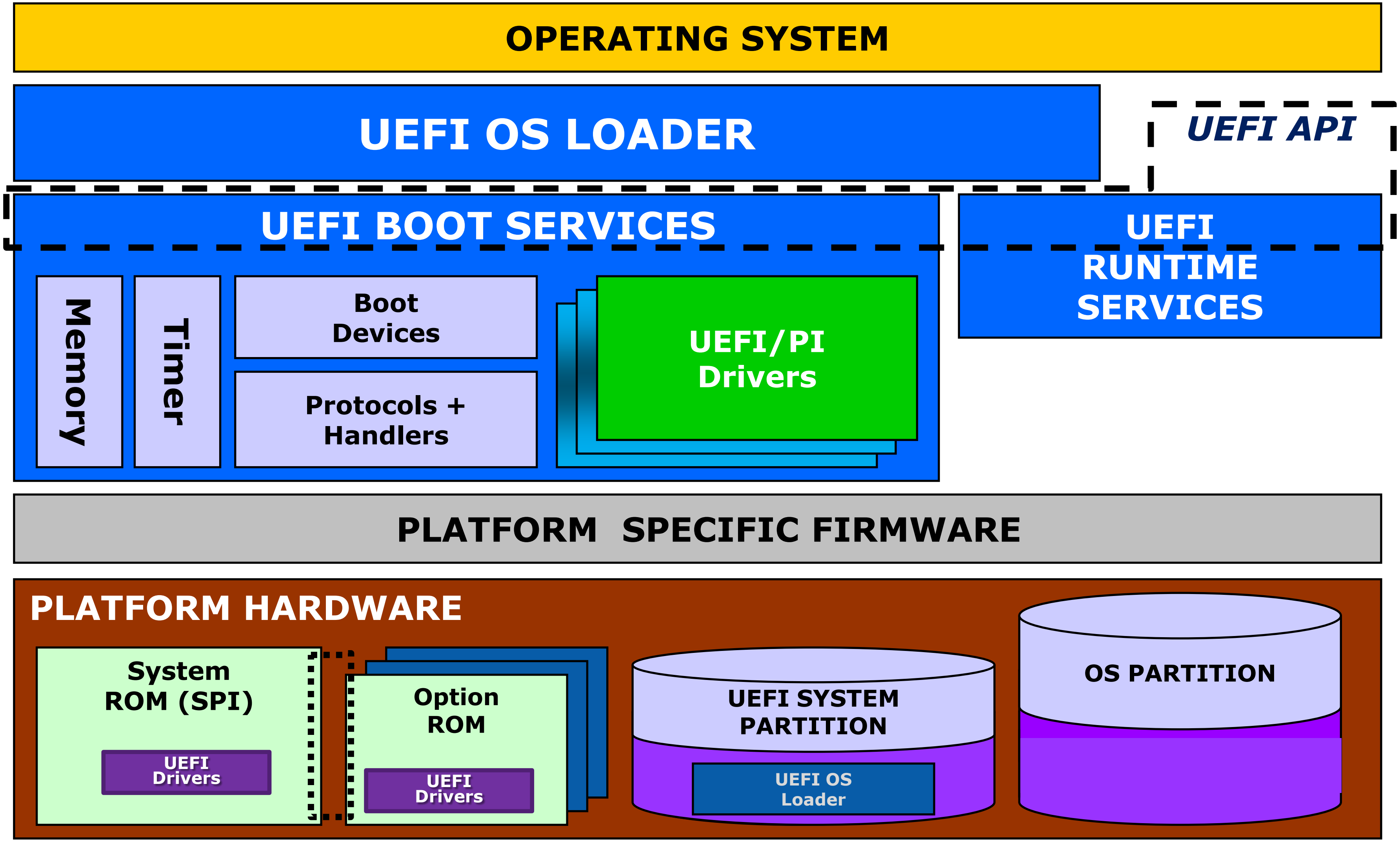
URL is on top of Session Agenda Pages in Pocket Guide

UEFI Considerations for Linux*



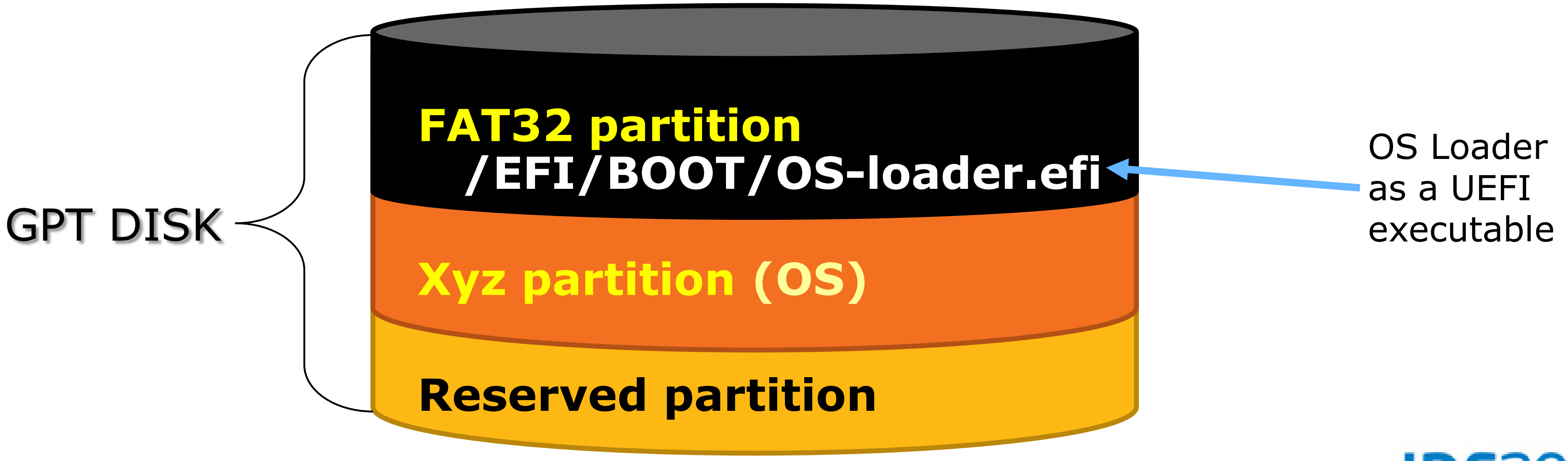
- Overview of the UEFI Boot Process
- Using UEFI Secure Boot with Linux*
- Other Implementation Issues

Overview of the UEFI Boot Process



Typical OS Loader Scenario for UEFI

- One GPT disk partition is FAT32 (service partition)
- OS installer puts the loader on the service partition
  - Under `/EFI/BOOT` or `/EFI/osname` directory
  - Ex: `/efi/boot/bootx64.efi`, `/efi/ubuntu/grubx64.efi`
- NVRAM `(Bootxxxx)` has a device path to OS loader
  - Maps to specific device, GUID partition & filename



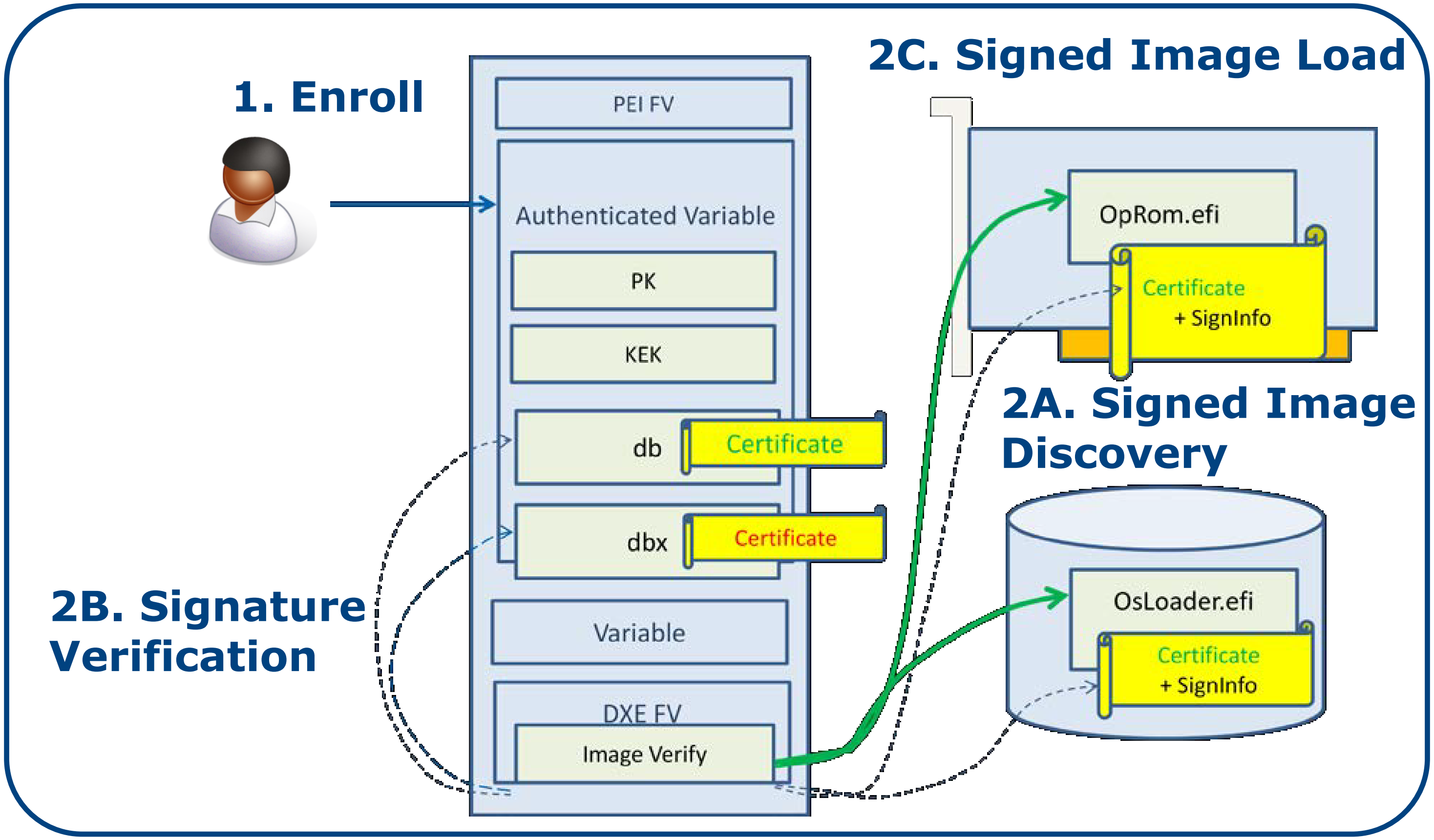
IDF2012 INTEL DEVELOPER FORUM

Advantages of UEFI Boot Process

- Extensible across multiple boot devices
  - SATA, SAS, USB, PXE/iSCSI (IPv4/IPv6), …
- Supports multi-boot operations
  - Multi-boot loaders w/o MBR chain-loading
  - UEFI Forum reserves directories to avoid collisions
  - Use `/efi/boot` directory for removable media
- Device path stored in boot options (NVRAM)
  - Pointer to specific boot device
- Boot image can be validated when loaded
  - Allows firmware loader to perform security checks

Using UEFI Secure Boot with Linux

The key is in the keys …
Signed images for the OS loader, UEFI Drivers & Option ROMs must reference some key in the db (and not be in the dbx)



Reference: Figure 11 from the "A Tour Beyond BIOS into UEFI Secure Boot" whitepaper at tianocore.org

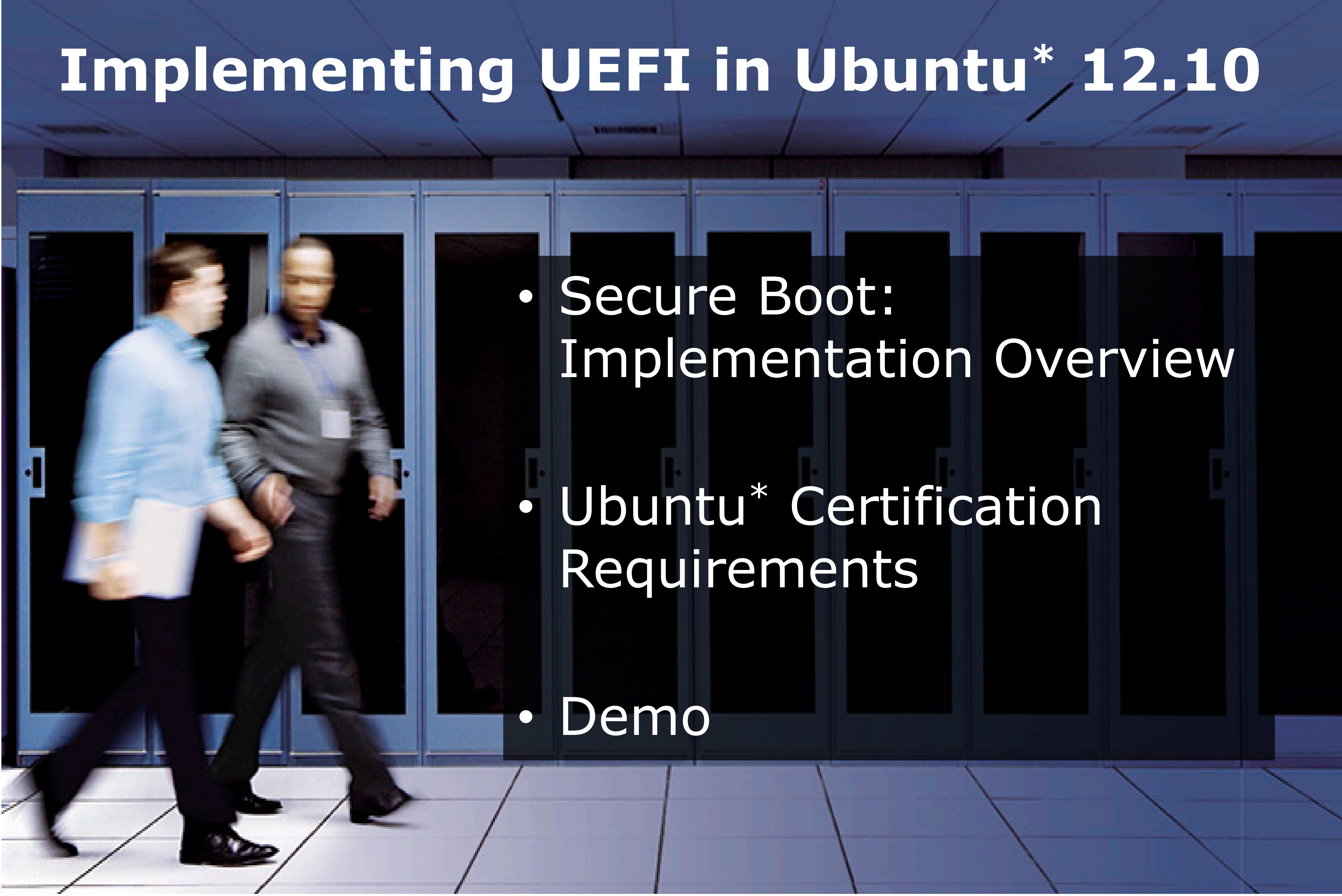
Secure Boot Challenges for Linux*

- Users can disable UEFI Secure Boot to install Linux*… but this isn’t the best deployment plan

- Users must have an option to install Linux alongside an OS, even when UEFI Secure Boot is enabled
- Linux can benefit from UEFI Secure Boot, if…
  - Customers can install Linux without disabling the feature
  - Platform owner can set security policy & customize system
- Distributions have other considerations for UEFI
  - How the kernel handles signed & unsigned code
  - Migrating drivers from legacy BIOS calls (INTxx) to UEFI

Linux distributions must determine how to implement secure boot

Implementing UEFI in Ubuntu* 12.10



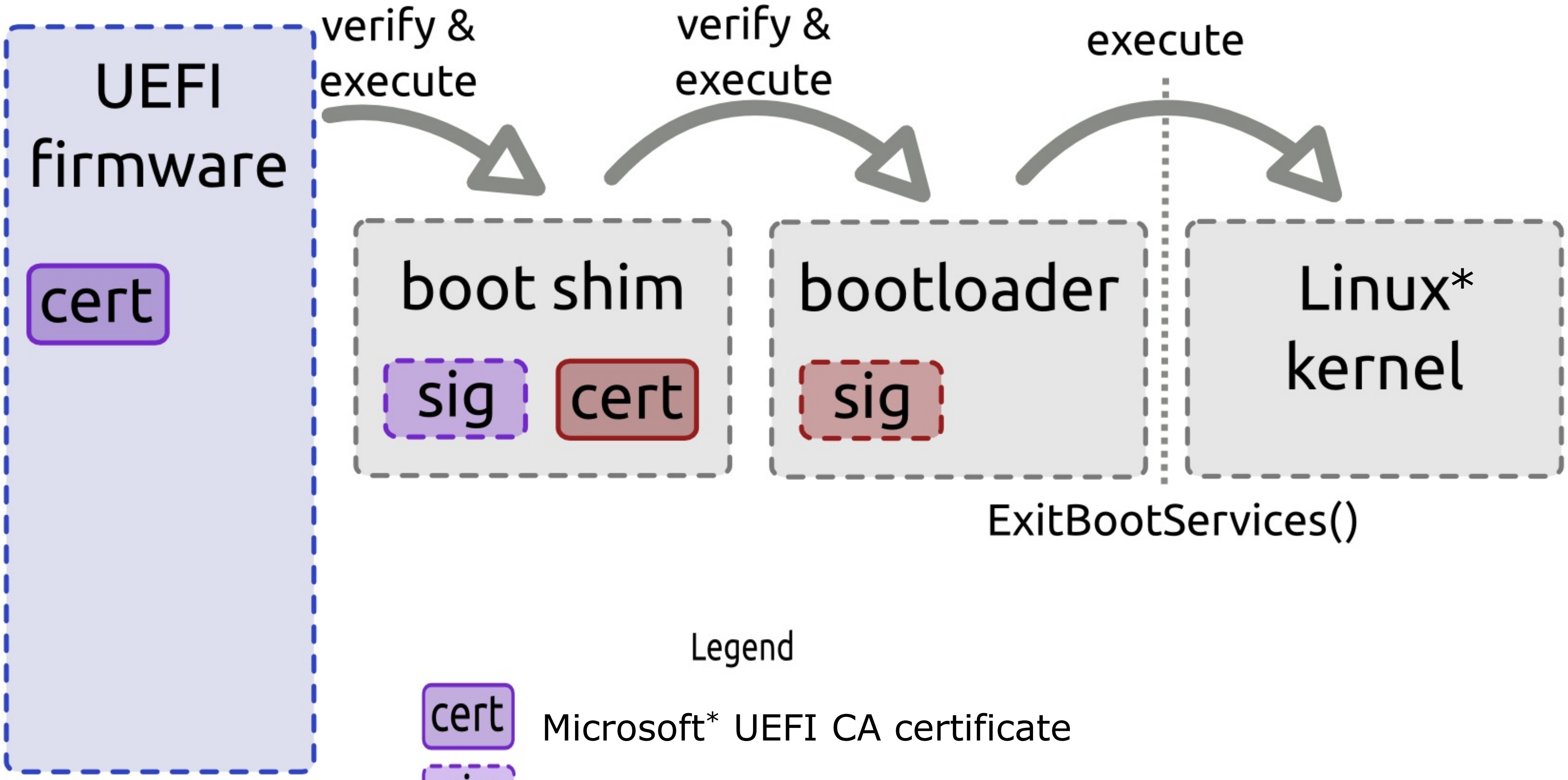
- Secure Boot: Implementation Overview
- Ubuntu* Certification Requirements
- Demo

Secure Boot: Implementation Overview

UEFI Secure Boot can’t interfere with Ubuntu’s* value…

- Must allow user modification
  - Allow user-defined trust verification
- Must work on generic hardware
  - Without reconfiguration!
- Must work with Ubuntu infrastructure

Ubuntu* Implementation



UEFI firmware

cert

verify & execute

boot shim

sig

cert

verify & execute

bootloader

sig

execute

Linux* kernel

ExitBootServices()

Legend

cert Microsoft* UEFI CA certificate

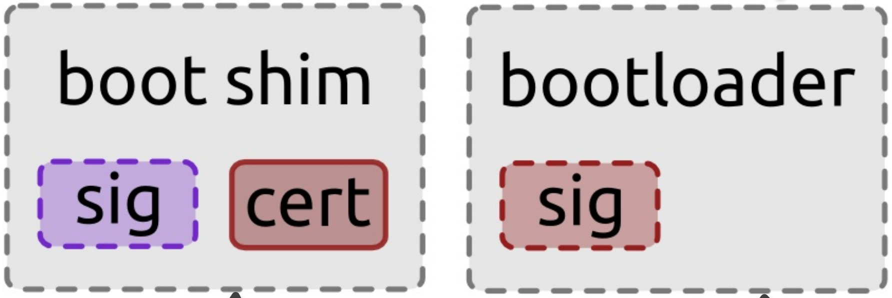
sig Signature generated from Microsoft UEFI CA

cert Ubuntu* CA certificate

sig Signature generated from Ubuntu CA

Ubuntu* Implementation

Code up to ExitBootServices() is signed



boot shim

sig

cert

bootloader

sig

Bootloader shim allows compatibility with Microsoft* UEFI CA

Bootloader images will be signed during build. No requirements for driver signing.

Ubuntu* Certification

System requirements for Ubuntu* preinstalls

UEFI requirements include:

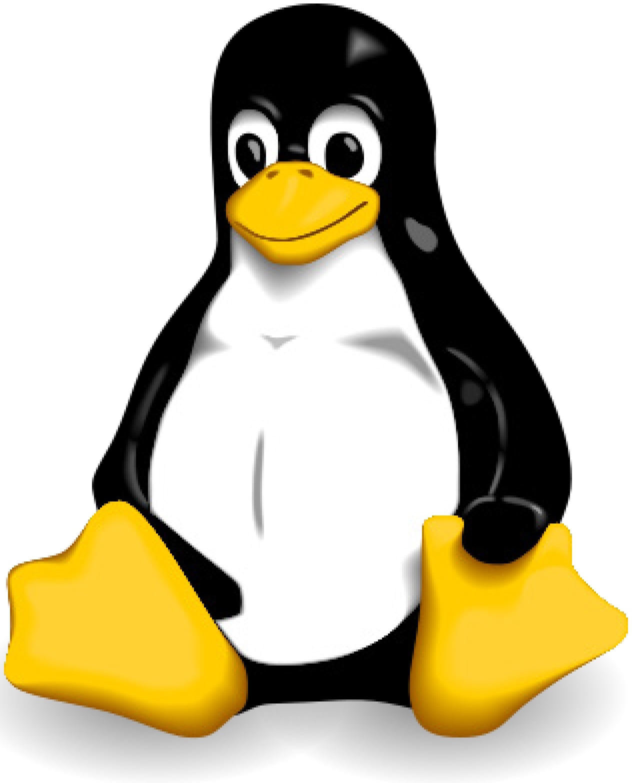
- Initial key database configuration
- User key reconfiguration functionality
- Facility to enable/disable secure boot

For more information …

- Ubuntu ODM Portal - http://odm.ubuntu.com/
- Secure Boot Signing Tools - git://kernel.ubuntu.com/jk/sbsigntool

Ubuntu* Demo with UEFI

- Key reconfiguration through standard firmware interfaces
- Ubuntu* images verified by firmware
- Key reconfiguration at OS level (with appropriate KEK installed)



Ubuntu* Implementation for UEFI

Ubuntu* 12.10 implements UEFI Secure Boot

- Boot loader shim signed by Microsoft* UEFI CA
- Ubuntu signed boot loader

Supports runtime key reconfiguration

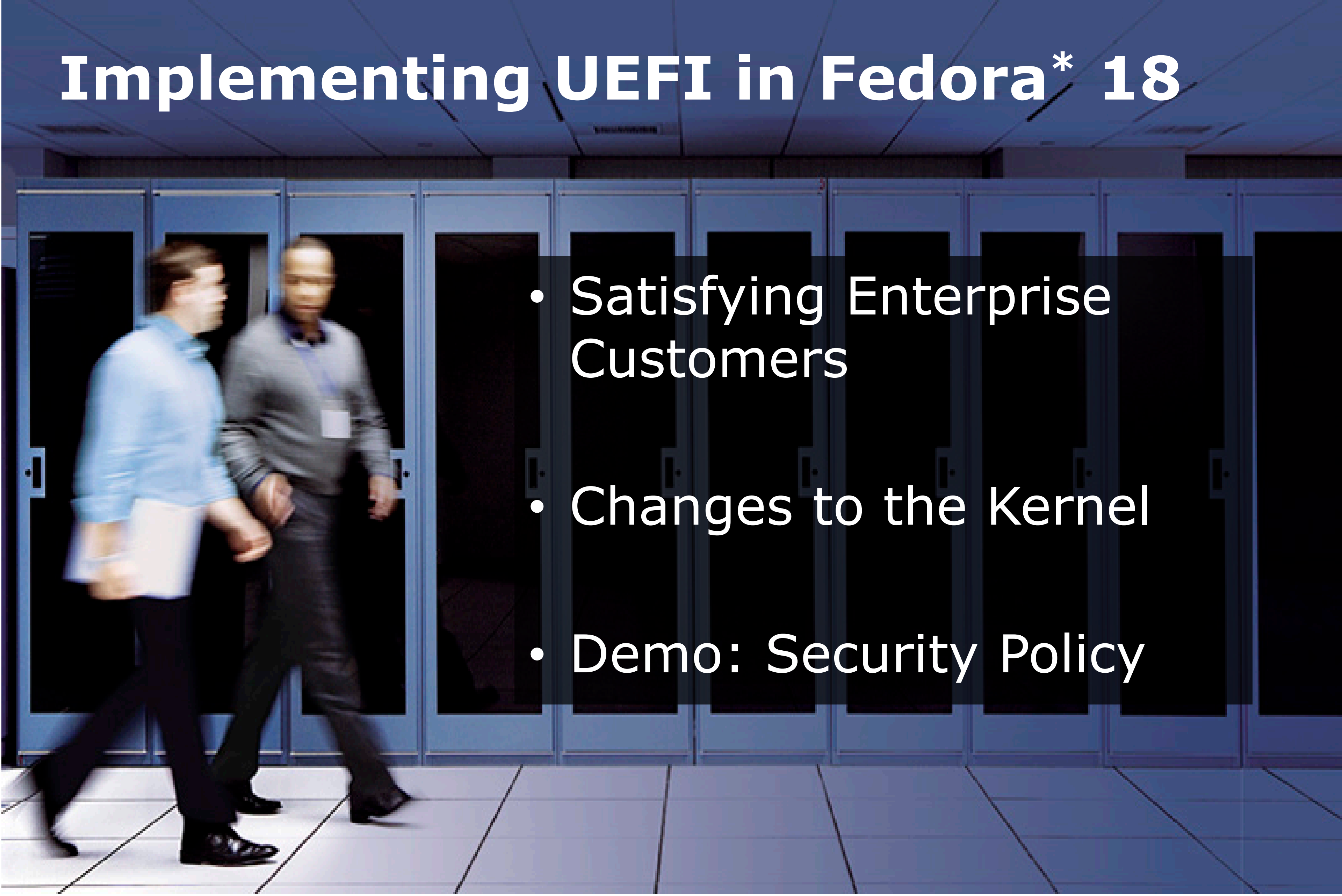
- Using efivars interface to update PK, KEK, db, dbx

Certification requires user-modifiable keys

- User control of security policy

Ubuntu uses existing Linux* infrastructure to support UEFI with Secure Boot

Implementing UEFI in Fedora* 18



- Satisfying Enterprise Customers
- Changes to the Kernel
- Demo: Security Policy

Implementing UEFI in Fedora* 18

- Fedora* 18 implements full UEFI Secure Boot support
  - Due for release early November 2012

- Uses UEFI for new enterprise-level features
  - Use UEFI for new functionality, not the bare minimum

- Implementing UEFI requires a surprisingly large set of functional changes

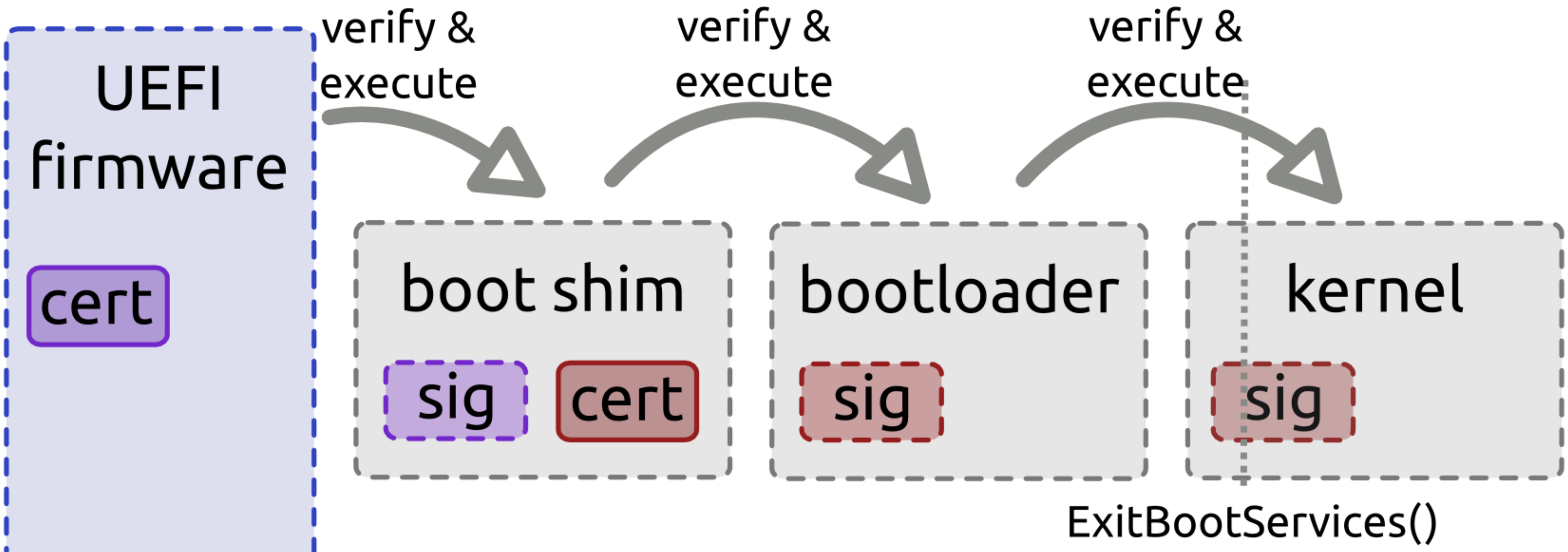
Satisfying Enterprise Customers

- UEFI Secure Boot can bring value to servers
  - However, customer configuration & integration is vital
  - Vital that trust be determined by the customer
  - Functionality for self-signing is hugely important
  - Integration into update system is also a key factor
- IPv6 support in the firmware permits net installs
  - Next generation network infrastructure support
- UEFI offers persistent NVRAM storage
  - Perfect for crash dumps and back-traces

Increased Kernel Security

- Signed drivers
  - Kernel refuses to load drivers unless signed with trusted key
  - Support for key installation
- Controlled hardware access
  - No direct user space access to hardware resources
  - All access mediated via the kernel
  - Graphics processor command streams validated to prevent DMA attacks
- Some debugging features disabled
  - Must be impossible for users to programmatically override security policy
  - Debug support must involve physically-present end user enablement

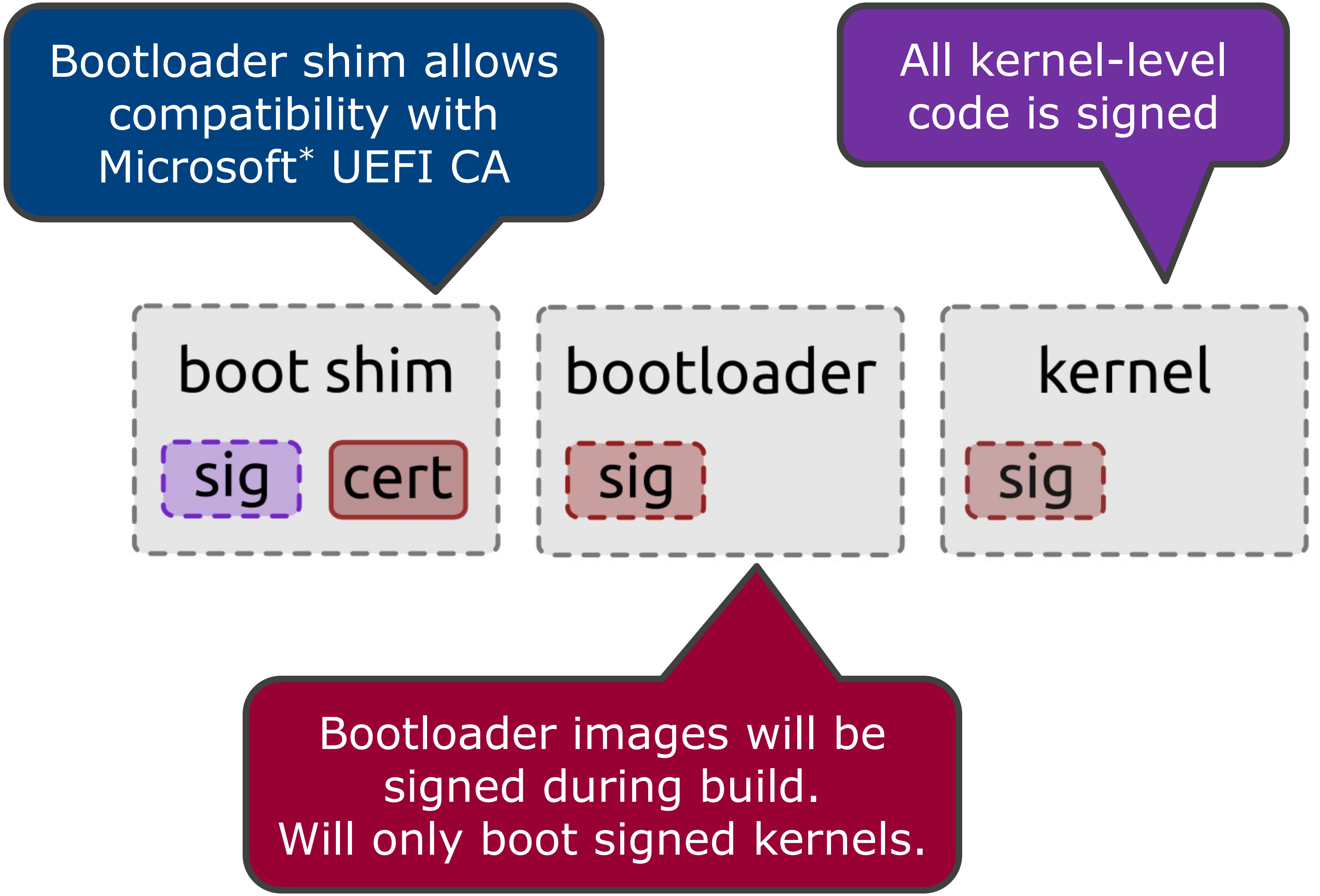
Fedora* Implementation



Legend

cert	Microsoft* UEFI CA certificate
sig	Signature generated from Microsoft UEFI CA
cert	Fedora* CA certificate
sig	Signature generated from Fedora CA

Fedora* Implementation



Bootloader shim allows compatibility with Microsoft* UEFI CA

All kernel-level code is signed

boot shim

sig

cert

bootloader

sig

kernel

sig

Bootloader images will be signed during build.
Will only boot signed kernels.

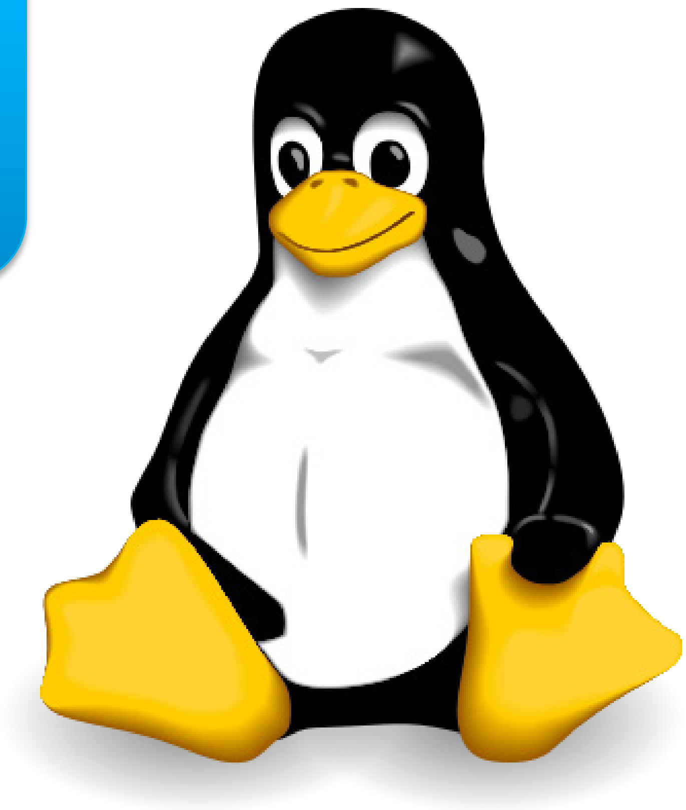
Hardware Enablement

- Kernel-mediated hardware access involves some new driver support
  - Added new kernel support for obsolescent graphics chipsets
  - Additional benefits in the form of power management
  - Server hardware environment very different to client
  - Still vital to provide full support

- The impact of UEFI & Secure Boot on the wider ecosystem will take time to determine

Demo: Security Policy in Fedora* 18

Use UEFI Secure Boot to enforce boot policy …
Fedora* 18 boot using only signed binaries and drivers



UEFI Support in Fedora* 18

Full system security

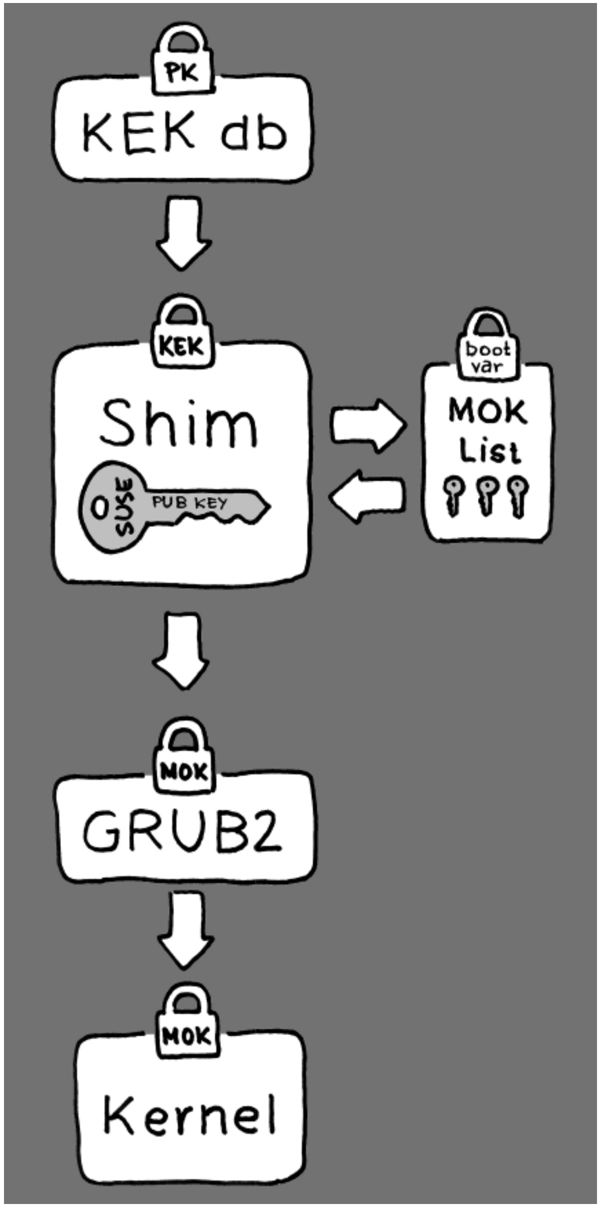
Designed to minimize impact on users

Available later this year

Fedora* uses UEFI Secure Boot as part of value-add for enterprise customers

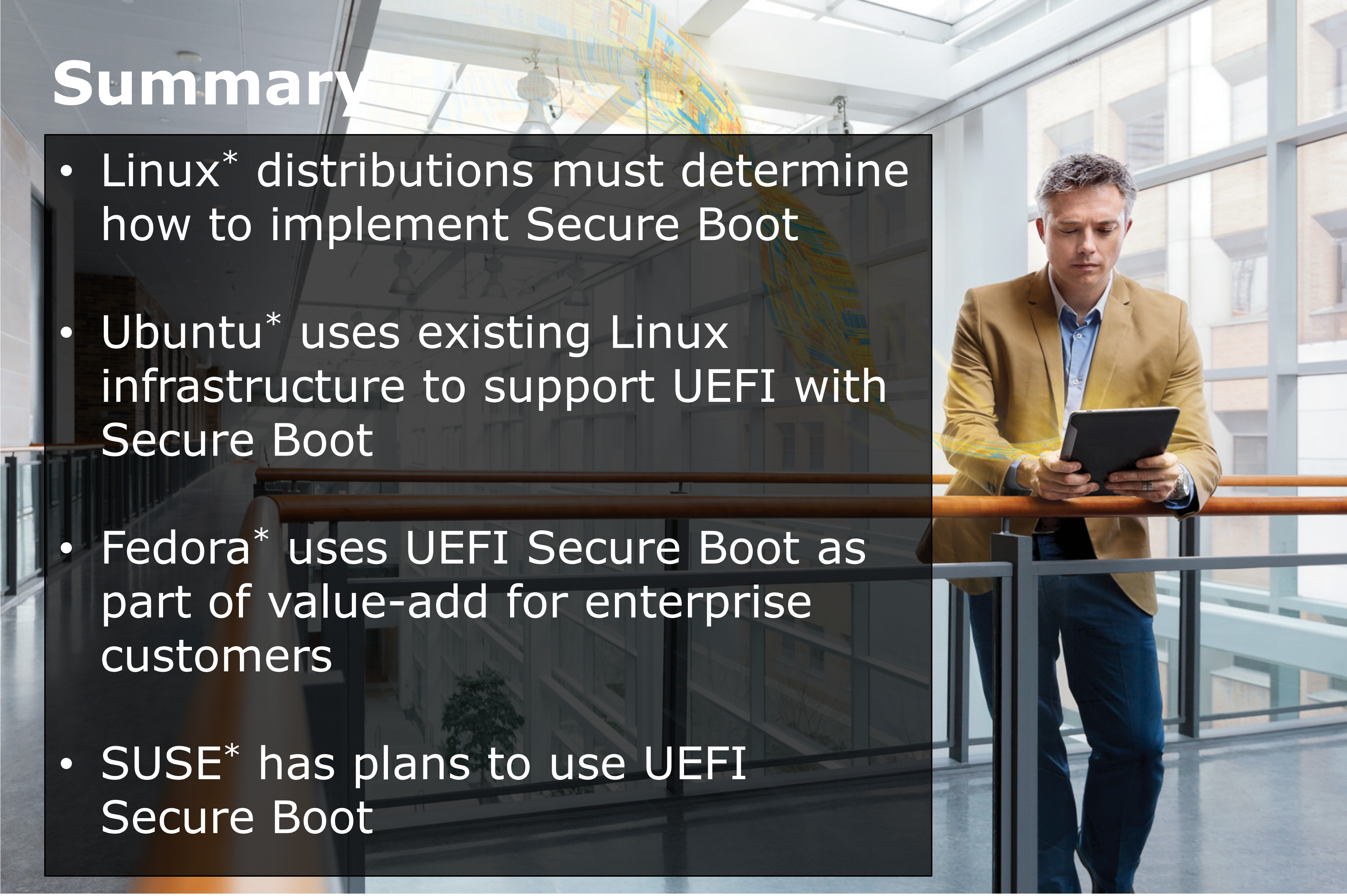
Latest updates to SUSE* UEFI secure boot plans

SUSE* Approach to UEFI Secure Boot



- SUSE has to balance two goals
  - Improving enterprise security by adopting UEFI Secure Boot
  - Reconcile UEFI Secure Boot with Linux developer's need to run a custom boot loader & kernel
- Aiming to support Secure Boot in SLE11 SP3* and openSUSE*
- Working with Linux* community and other vendors
  - Building on the shim loader created by Matthew Garrett
  - Extending it to allow machine owner to securely boot other kernels

Summary



- Linux* distributions must determine how to implement Secure Boot
- Ubuntu* uses existing Linux infrastructure to support UEFI with Secure Boot
- Fedora* uses UEFI Secure Boot as part of value-add for enterprise customers
- SUSE* has plans to use UEFI Secure Boot

Call to action

- Evaluate platform support for UEFI
- Become familiar with UEFI Secure Boot and how it effects your platform
- Download and test the latest Linux* distributions with support for UEFI & Secure Boot
  - The link for Ubuntu* Secure boot resources is at: https://wiki.ubuntu.com/UEFI/SecureBoot
  - Versions of Fedora https://fedoraproject.org/wiki/Secure_Boot_Testing

Get More Information

- Intel UEFI Community - http://intel.com/udk
- UEFI Forum Learning Center
  - http://www.uefi.org/learning_center/
- Use the TianoCore edk2-devel mailing list for support from other UEFI developers
- Read the "A Tour Beyond BIOS into UEFI Secure Boot" whitepaper at tianocore.org
- For more information on Ubuntu* …
  - Ubuntu ODM Portal - http://odm.ubuntu.com/
  - Secure Boot Tools - git://kernel.ubuntu.com/jk/sbsigntool
- For more information on Fedora* …
  - http://fedoraproject.org/
- Latest updates to SUSE* UEFI secure boot plans: https://www.suse.com/blogs/tag/secure-boot/

- Technical Showcase Booth #946

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
MSTS002	Shift Left! Leverage Full System Simulation to Reduce Your Time to Market	2003	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

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

IDF2012
INTEL DEVELOPER FORUM

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, Ultrabook, 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

- Other Software Code Disclaimer

  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 above copyright notice and this permission notice (including the next paragraph) shall be included in all copies or substantial portions of the Software.

  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 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

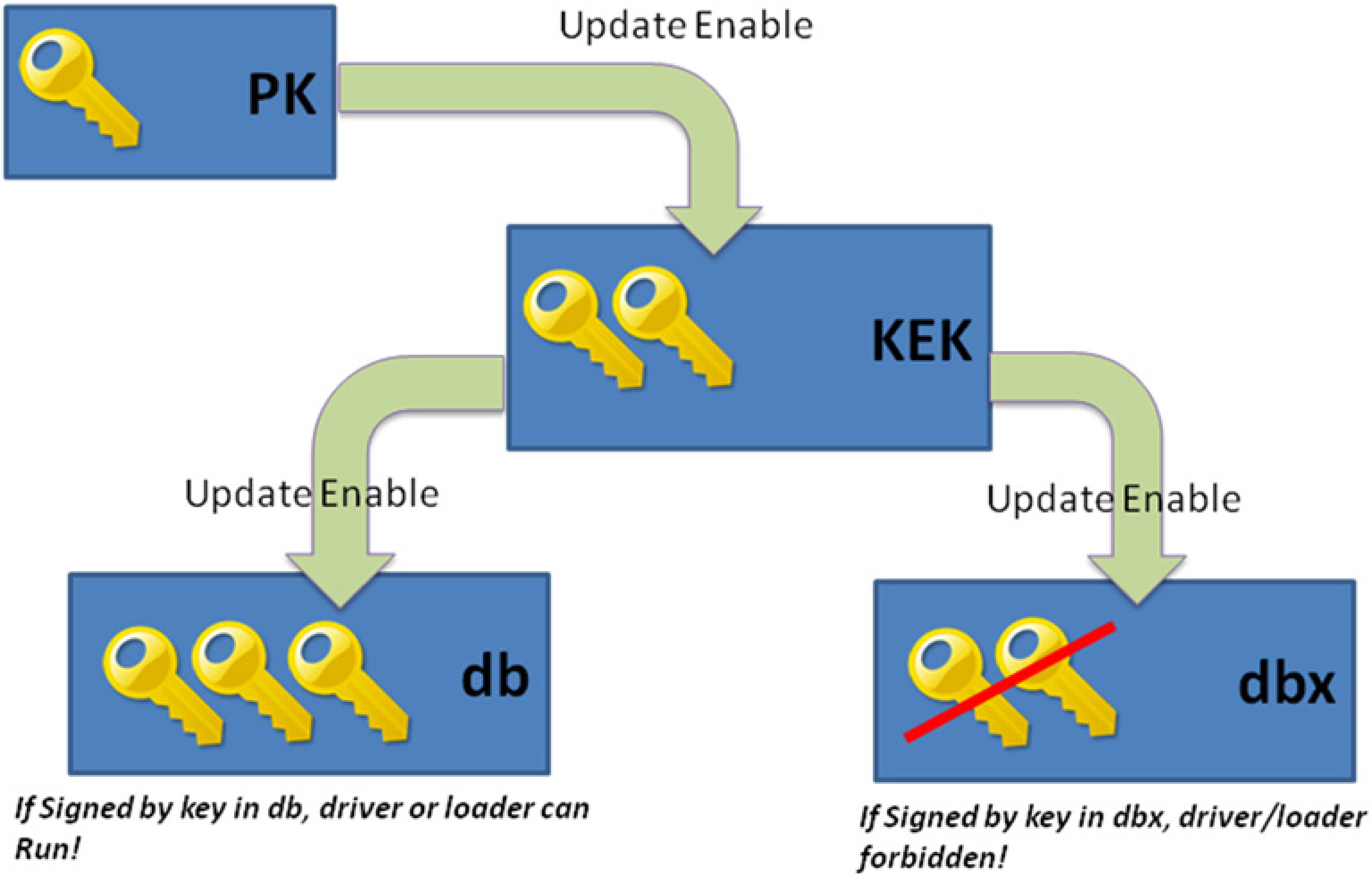

Update Enable
PK
KEK
Update Enable
Update Enable
db
dbx
If Signed by key in db, driver or loader can Run!
If Signed by key in dbx, driver/loader forbidden!

Figure 11 from the "A Tour Beyond BIOS into UEFI Secure Boot" whitepaper at tianocore.org