IDF13

UEFI Secure Boot in Linux*

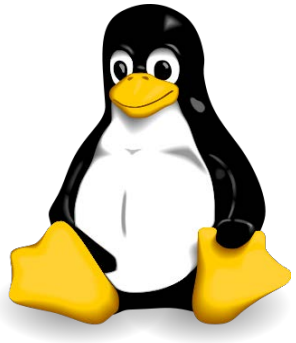
Vincent Zimmer – Principal Engineer, Intel Corporation
Philip Oswald – Project Manager, SUSE
Gary Lin – Software Engineer, SUSE

STTS002

intel Look Inside.

Agenda

- Problem Statement
- What is UEFI Secure Boot
- Introduction to Machine Owner Key
- Secure Boot in SUSE Linux
- Demo

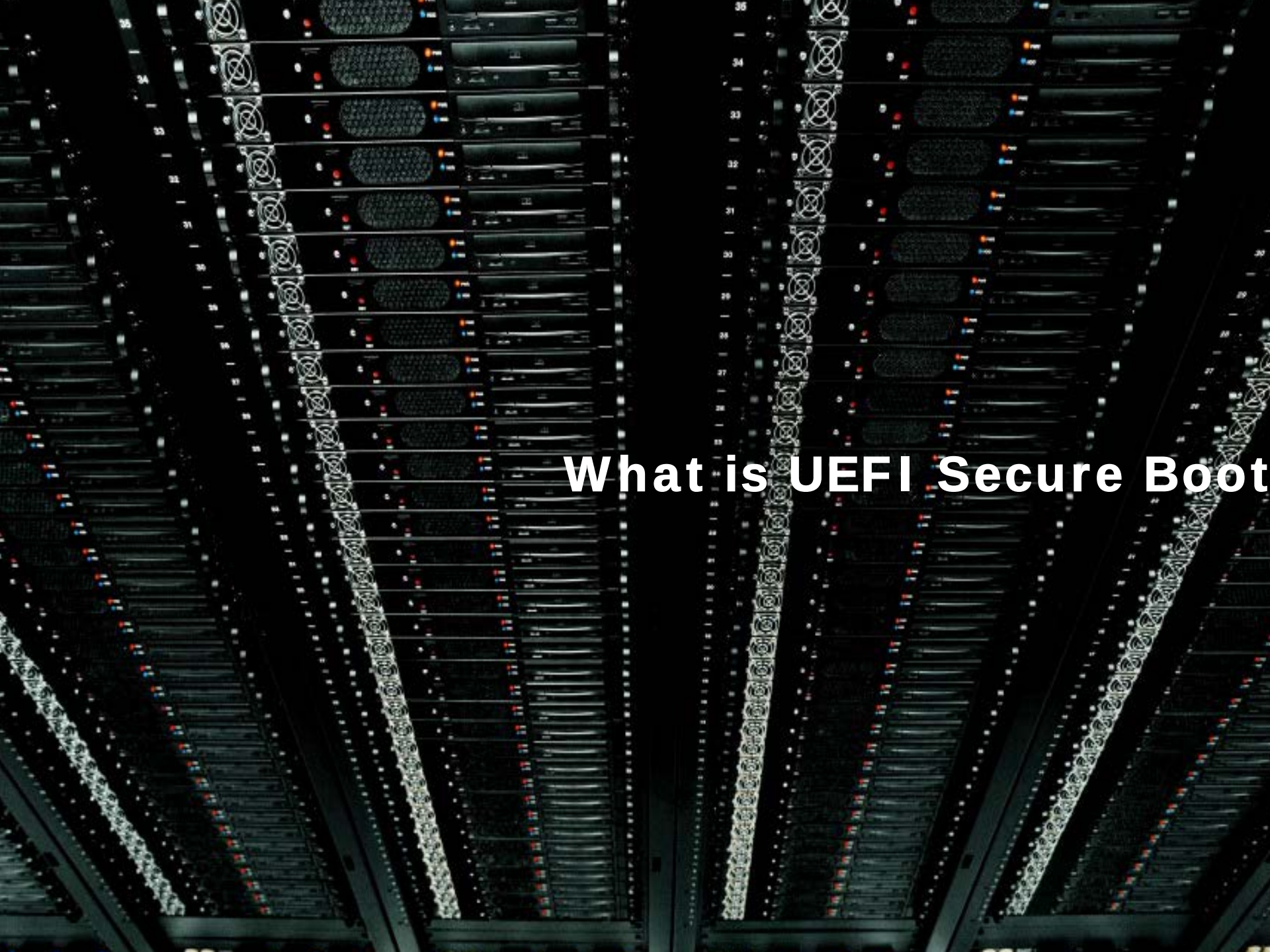


IDF13

Problem Statement

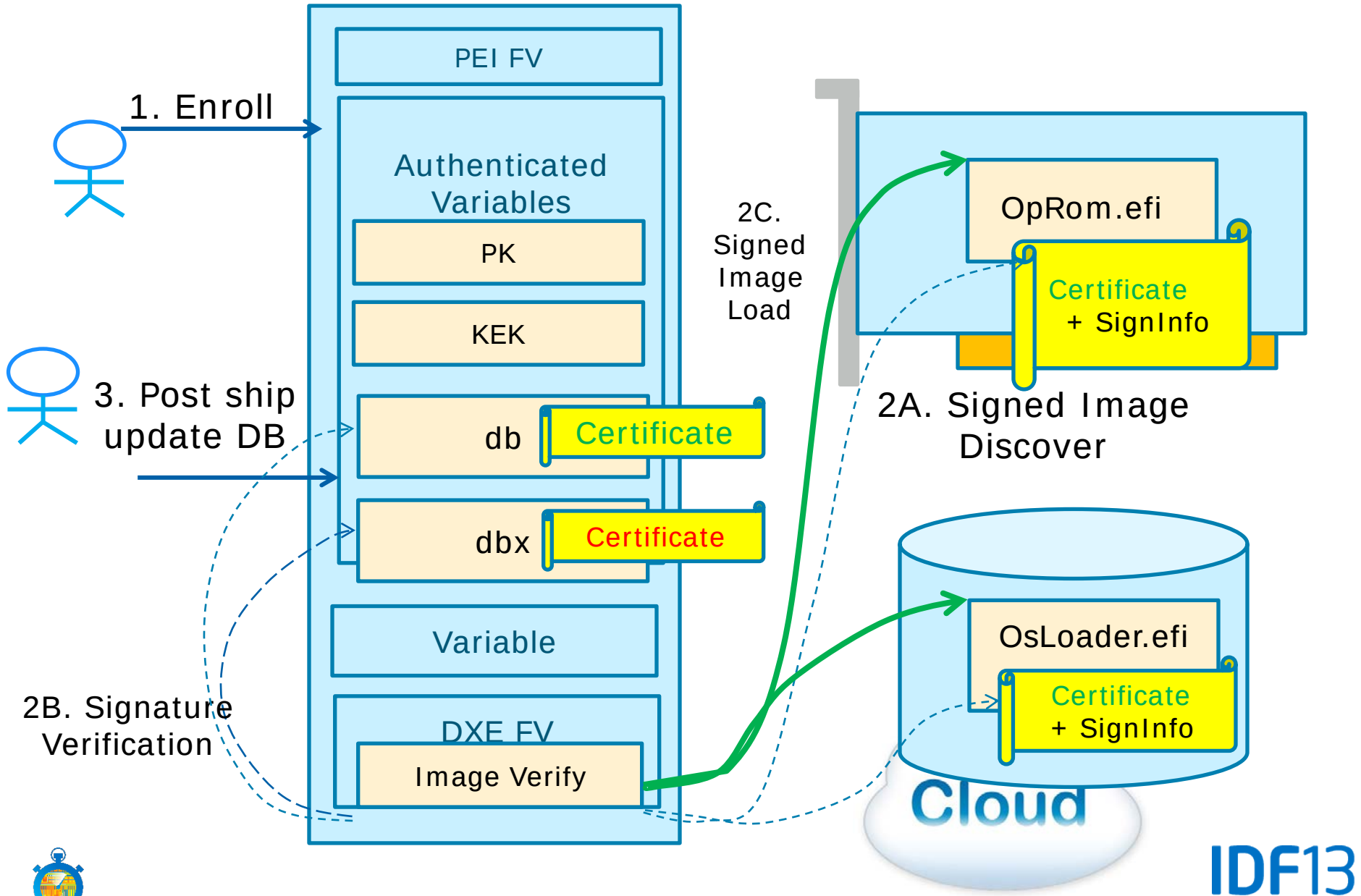
Secure Boot Problem

- Malware moving more into the platform
- UEFI extensibility can be exploited by unauthorized parties
- Attacks increasingly targeting the platform firmware
  - Black Hat 2007, 2009, 2013, CanSecWest 2013…
- Need to balance UEFI code loading controls and maintain platform owner and user choice
- For platform integrity and user flexibility:
  - Maintain ability to have several operating systems on the platform
  - Provide platform owner a choice for software



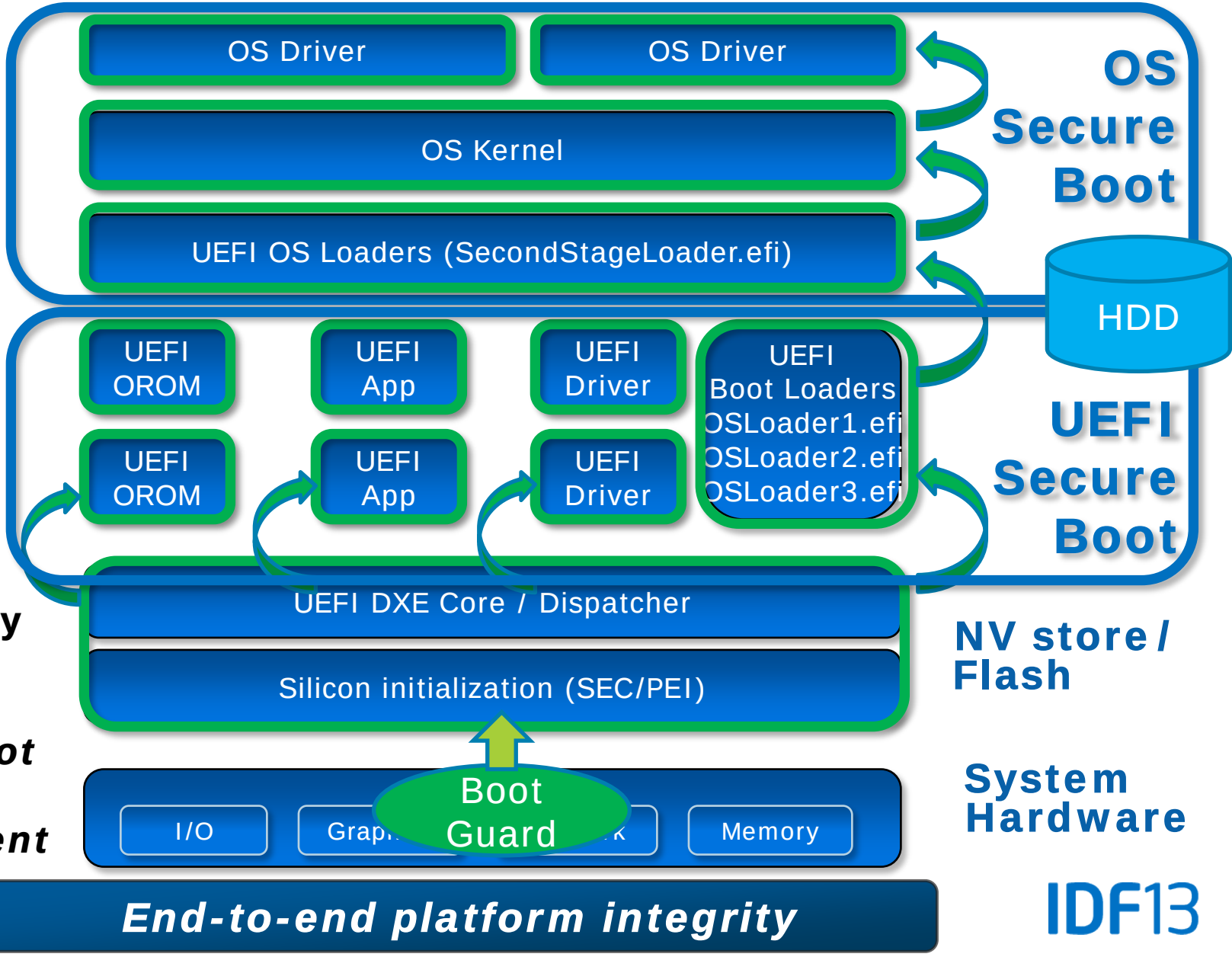
What is UEFI Secure Boot

UEFI Secure Boot



IDF13

The Full Solution

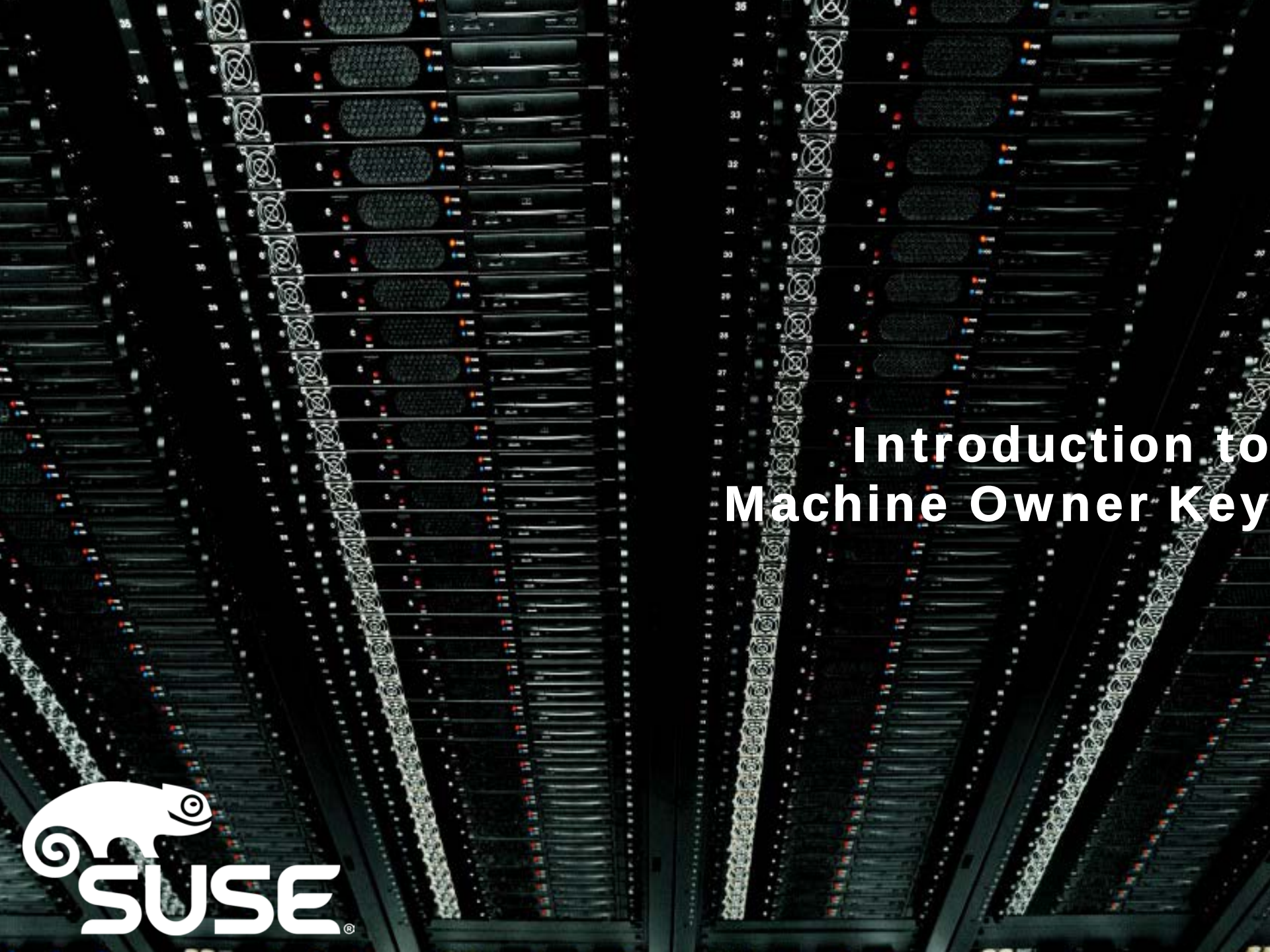


Intel® Device Protection Technology with Boot Guard – Secure *Boot Policy Enforcement*

Secure Boot Challenges for Linux*

- Dual OS deployment challenge
  - 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 and customize system
- Different roles interact with UEFI Secure Boot
  - Kernel hacker – disable or enroll own keys w/firmware screens
  - Consumer – just want it to work, seamless boot of live images
  - Managed IT machine – IT is the 'owner.' Control end user actions.

Linux distributions have several options to implement secure boot


Introduction to
Machine Owner Key
SUSE

Machine Owner Key (MOK)

- To support UEFI Secure Boot in Linux*, there are two challenges to overcome
  - Coexist with other operating systems
  - Avoid the potential General Public License (GPL) copyright issues caused by the UEFI image signature
- MOK gives back the key management control to users or security admin

SUSE Solution

MOK comprised of 4 parts

shim

grub2, kernel, and kernel drivers

- A BSD licensed preloader of the OS loader(grub2) signed with the db key
- All involved components are signed

MOKList

MOK database - The key database implemented in a UEFI nvram variable, MOKList

MokManager

The UEFI program to manipulate the MOK database

mokutil

The Linux* utility program to issue requests to MokManager

IDF13

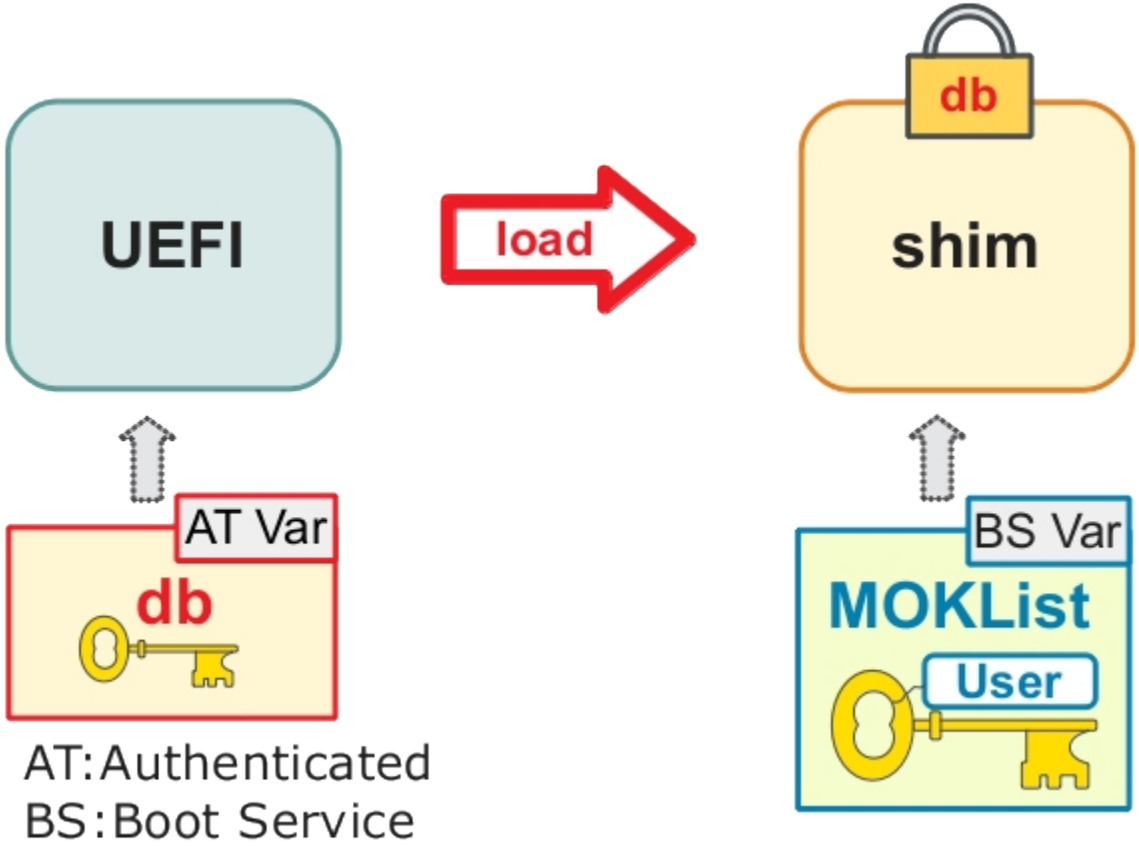
MOK Database

- The MOK database is used as a boot service non-volatile variable
- UEFI Boot Service non-volatile variables are immune from threats from OS
- MOKList is not the db and does not need to be controlled by KEK

	Boot Service	Runtime Service	Authenticated
UEFI - Read	Yes	Yes	Yes
UEFI - Write	Yes	Yes	Restricted
OS - Read	**No**	Yes	Yes
OS - Write	**No**	Yes	Restricted
	BS Var	RT Var	AT Var

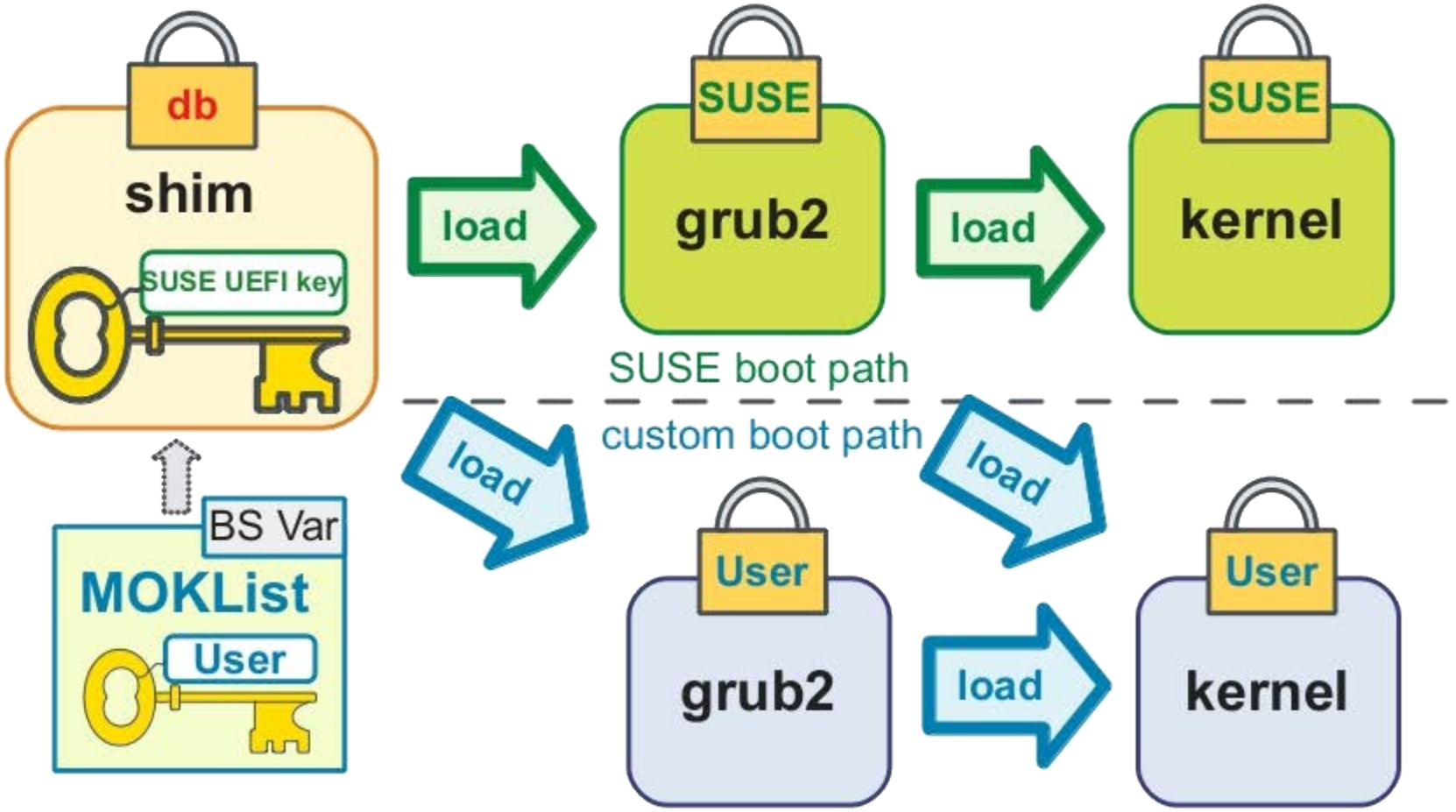
MOKList is not accessible at OS runtime

UEFI Secure Boot With MOK



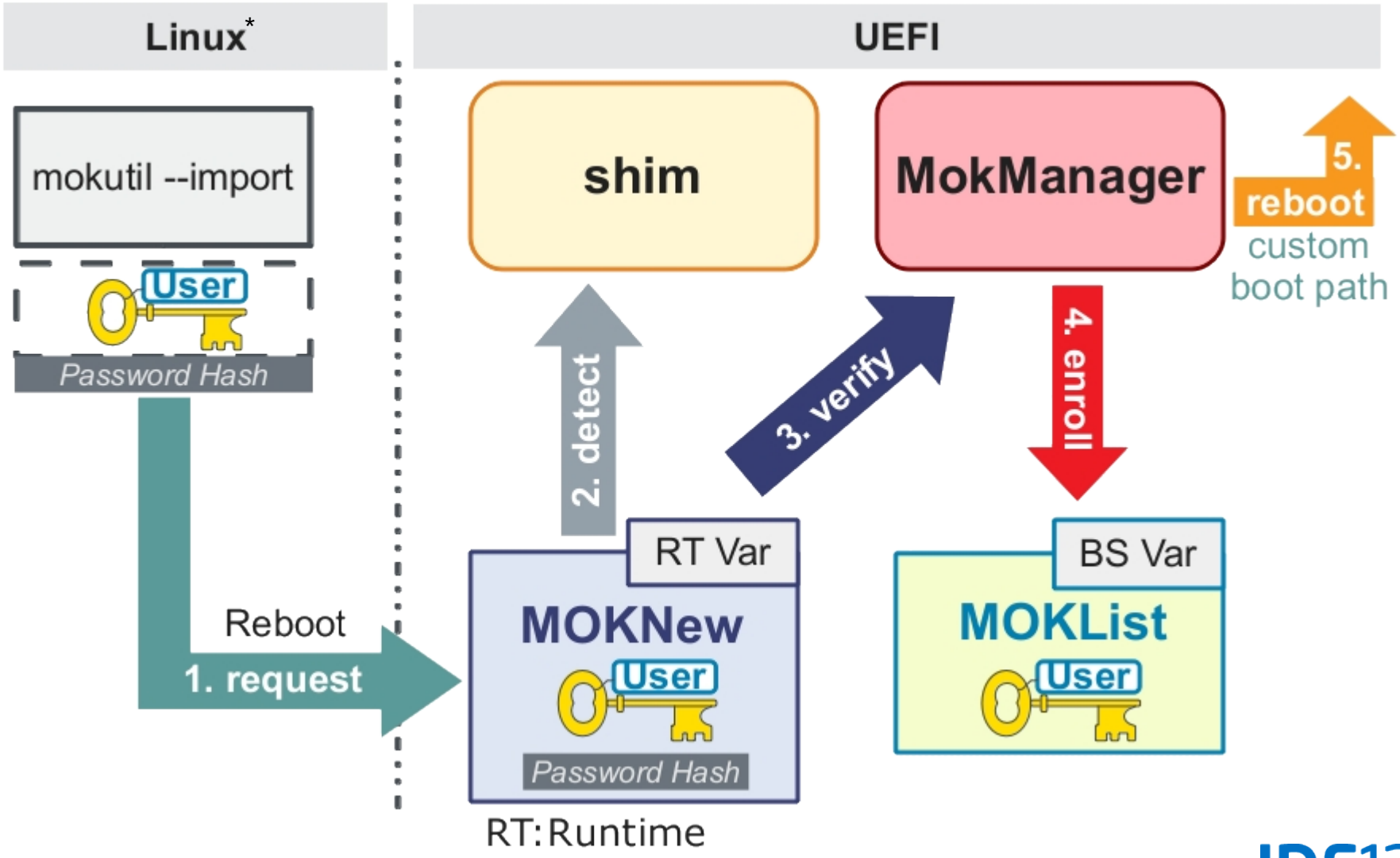
shim is loaded before other UEFI images

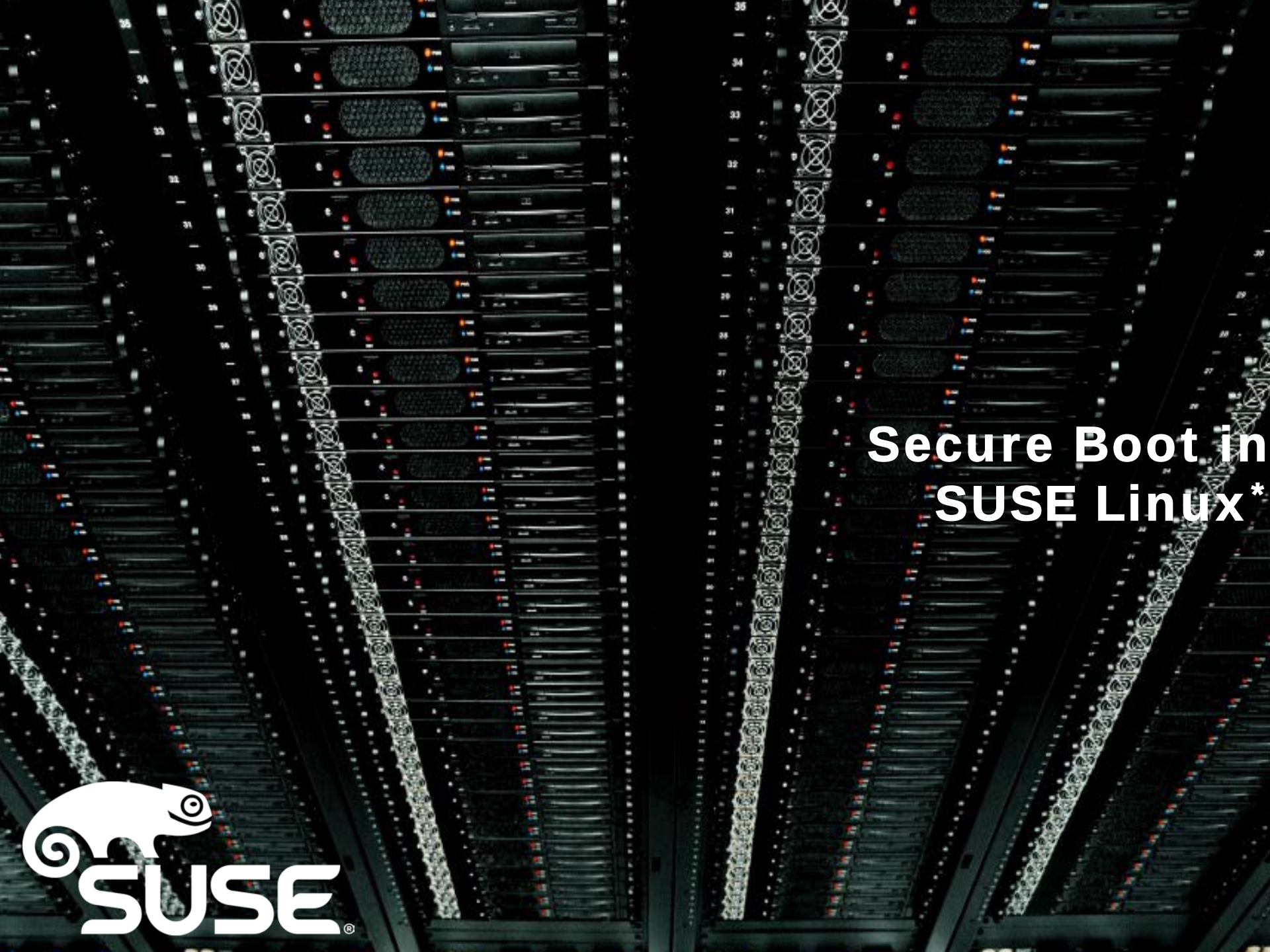
Multi-boot with MOK



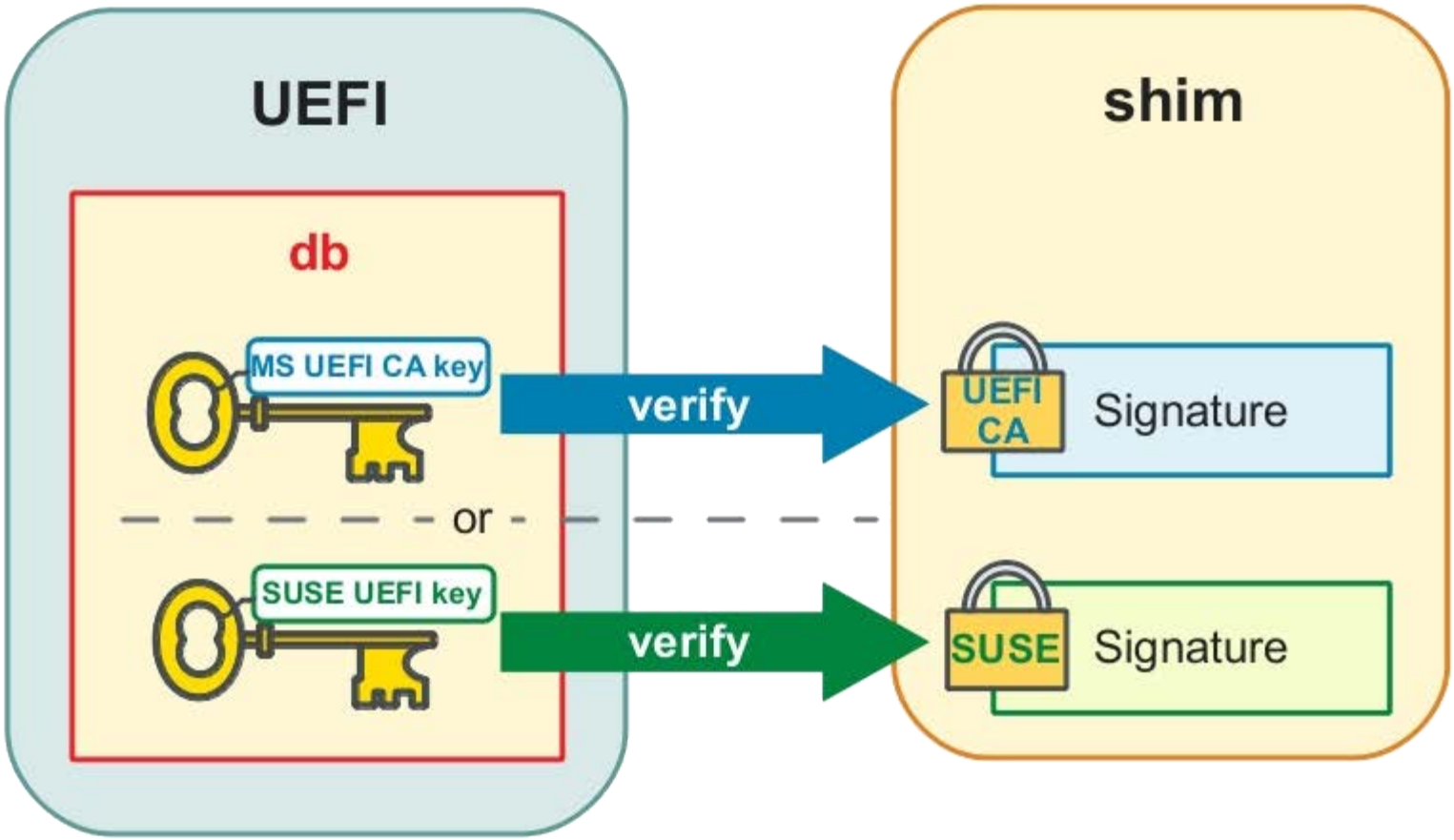
Load the UEFI image as long as it is trusted

Enroll A New MOK Key




Secure Boot in
SUSE Linux*
SUSE

Multisigned shim



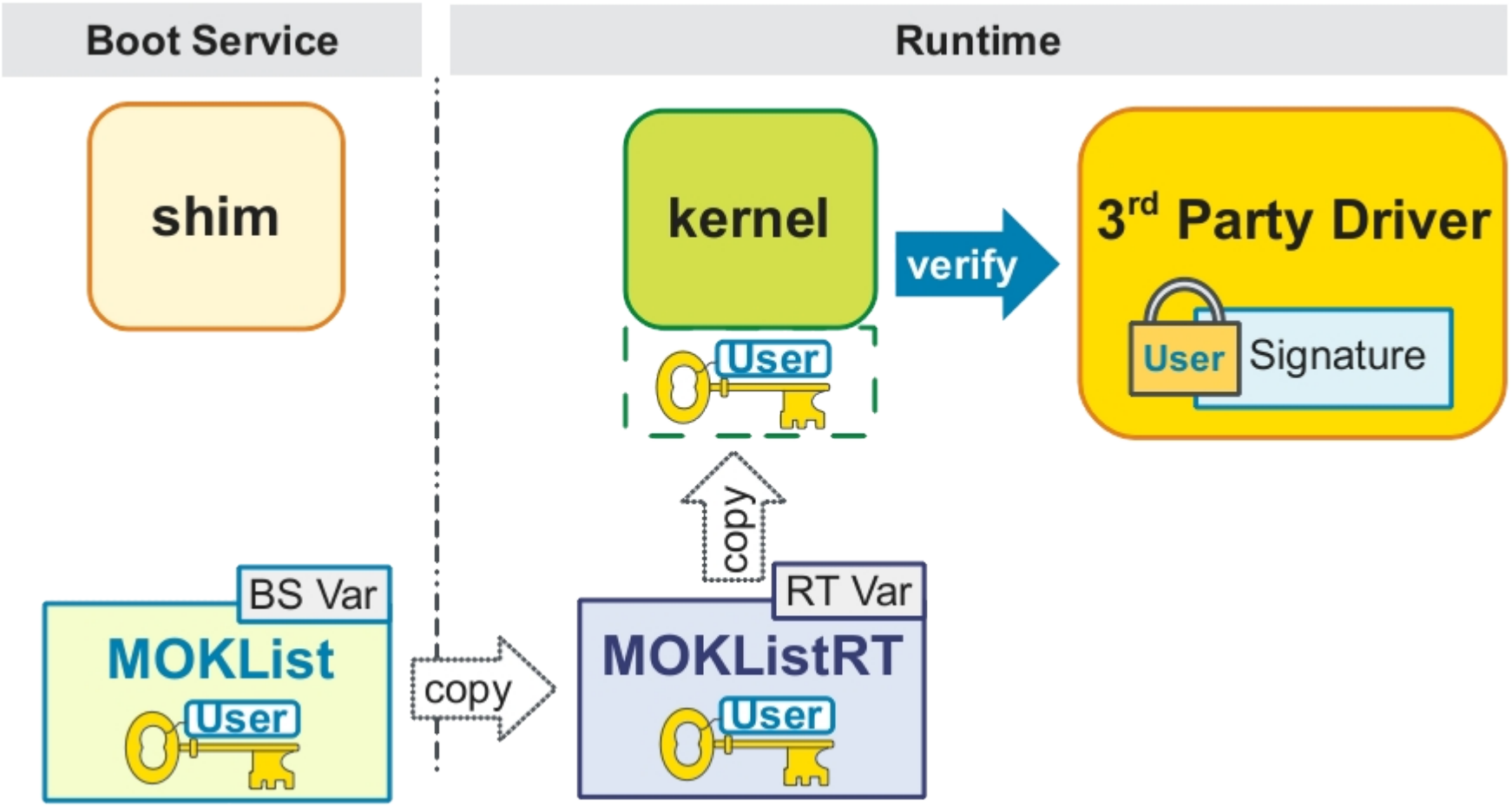
Either the UEFI CA key or SUSE key will let the shim boot with UEFI secure boot

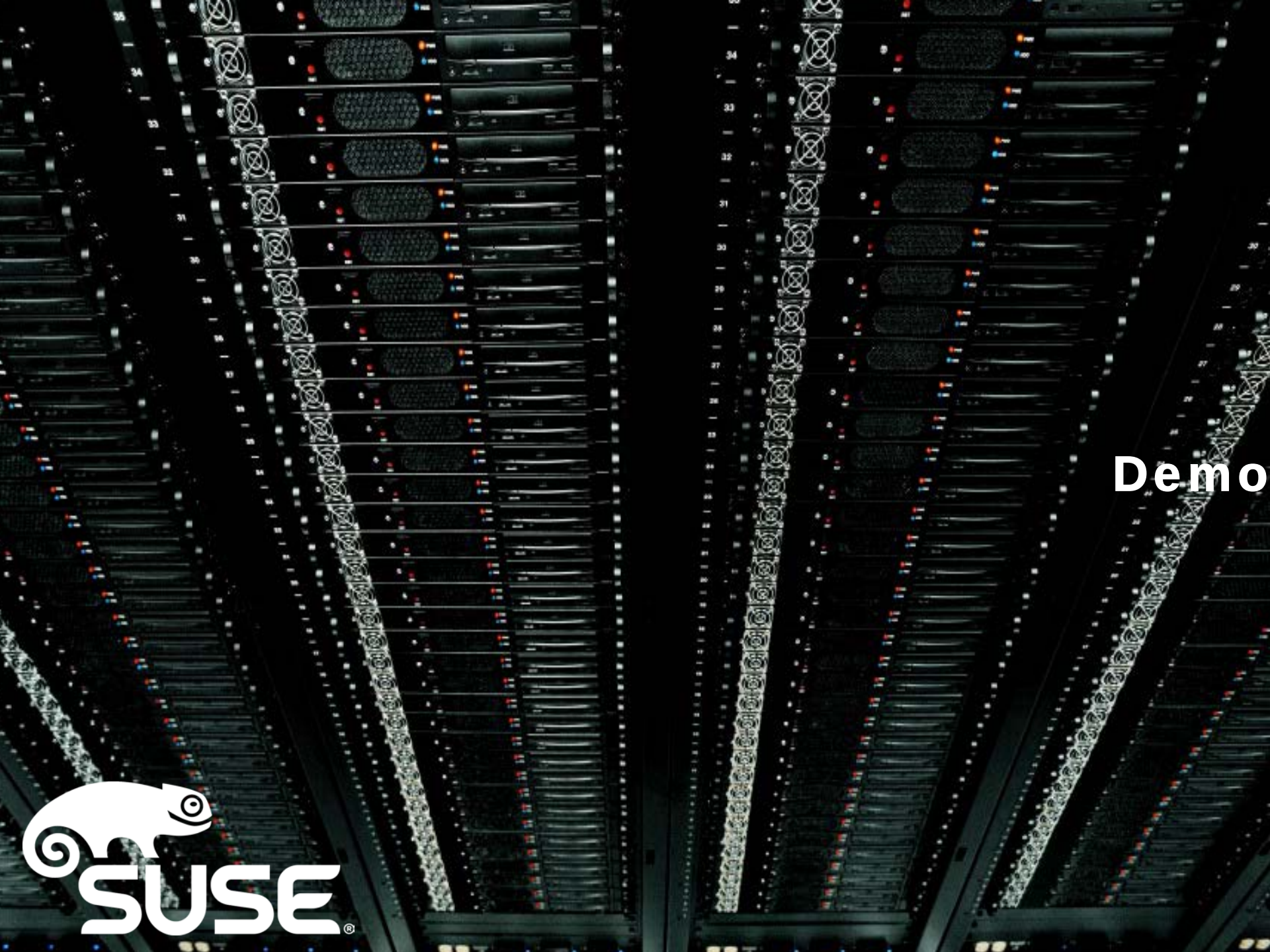
Linux* Driver Verification

- All kernel drivers have to be signed with the SUSE key
- Linux* kernel verifies drivers with the built-in SUSE key or MOK keys
- SUSE will NOT sign any binary driver that is incompatible with GPLv2
- The user is free to enroll the key for the third party binary driver
- SUSE's Partner Linux Driver Program (PLDP) - simplifies MOK implementation

Users can get their 3rd party drivers included in the secure boot with MOK

Third Party Driver Verification




Demo
SUSE

SUSE Summary and Call to Action

- UEFI Secure Boot no longer an issue to the Linux* World
- With MOK, users select the keys they trust
- Linux systems benefit from MOK to ensure the integrity of the drivers

Call to action:

- Use MOK in your Linux deployments
- Put SUSE key in UEFI database to test multi-signed shim
- Utilize SUSE's Partner Linux Driver Program for delivering kernel drivers compatible with SUSE Linux Enterprise and Secure Boot
  - https://www.suse.com/partners/linux-driver-program/

Summary

- Attacks against the platform will most likely continue
- Deploy UEFI Secure Boot to address pre-OS malware
- Design a robust platform implementation
- Avoid ‘restricted boot’ & continue to enable platform owner choice of UEFI Secure Booted code
- Emergent tools for choice include multi-signed images, the Shim Loader, and Machine Owner Key
- Machine Owner Key provides practical solution for implementing key management

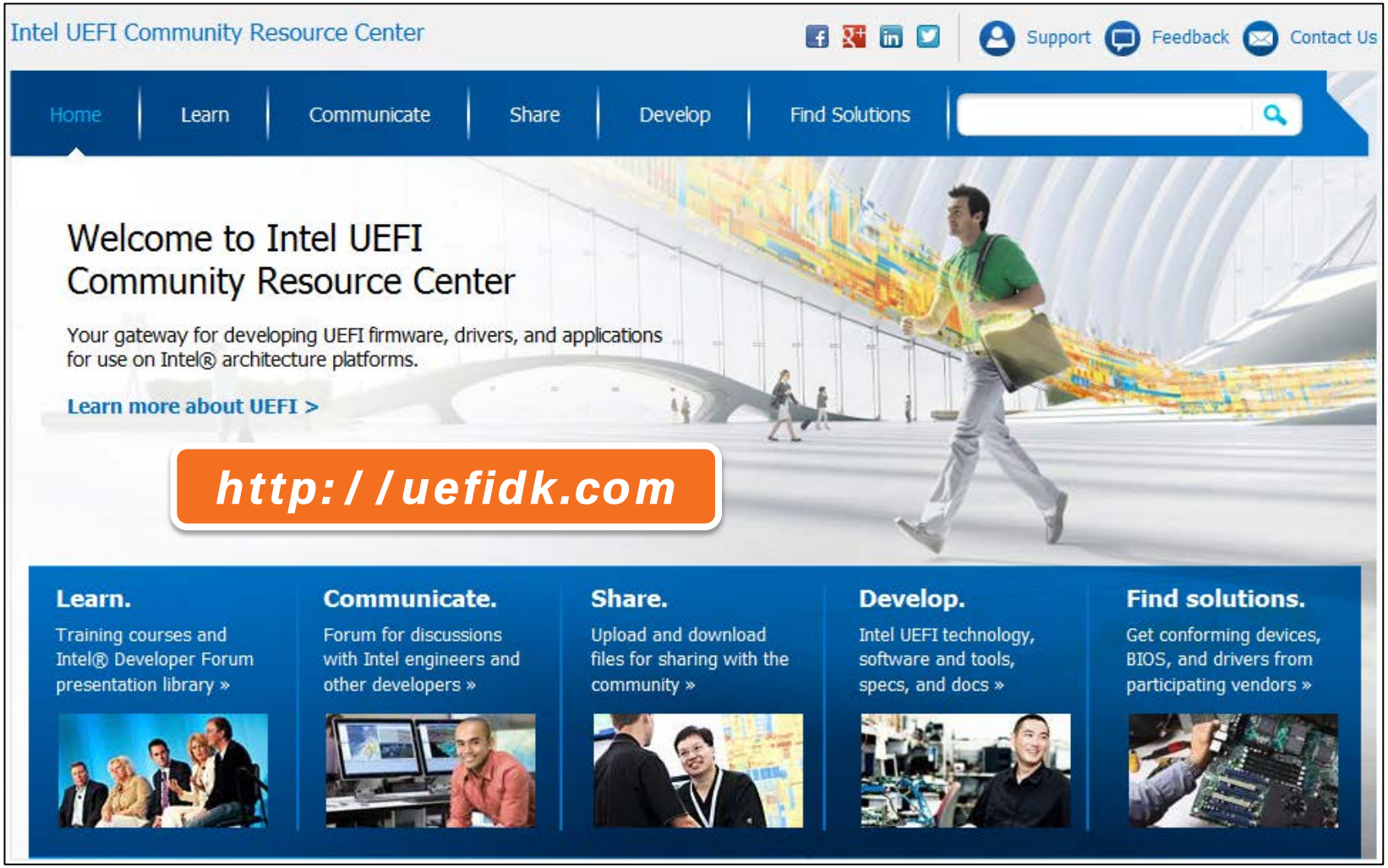
Updates from Linux* Distributions

- **Ubuntu* 12.10** – 64-bit version of Ubuntu 12.10 shipped with Shim to support secure boot
- **Fedora* 19** – included Shim with MOK (Machine Owned Key) functionality
- **OpenSUSE* 12.3** release supports MOK manager and multisigned Shim loader
- **SUSE SLES 11 SP3*** - included multisigned Shim with MOK functionality and runtime Mokutil
- **Linux* Foundation** Secure Boot System Released
- UEFI Technology Adopted by Linux Community†

Linux distro implementation with MOK 3rd party manager signing list implemented already

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

Intel UEFI Community Resource Center



Central resource for UEFI on Intel® Architecture

IDF13

Additional Sources of Information

PDF of this presentation is available is available from our Technical Session Catalog: www.intel.com/idfsessionsSF.
The URL is on top of Session Agenda Pages in Pocket Guide.

Visit the Unified EFI Forum for the latest specifications.

The EDK II project is hosted at http://tianocore.org.

Latest updates to SUSE* UEFI secure boot:

OpenSUSE tools UEFI:

http://download.opensuse.org/repositories/home:/jejb1:/UEFI/
http://build.opensuse.org/project/show/home:jejb1:UEFI

Related Articles/Whitepapers at tianocore.org:

- "A Tour Beyond BIOS into UEFI Secure Boot"
- Images with Multiple Signatures

Other Sessions at IDF
Wednesday, Sept 11, Moscone Room 2008

ID	Title	Time
✓ STTS001	Creating UEFI Solutions Optimized for Mobile Devices	11:00
✓ STTS002	UEFI Secure Boot in Linux*	13:00
STTS003	Using UEFI for Secure Firmware Update of Expansion Cards	14:15
STTS004	Predicting Performance of Hadoop* and Data Center Clusters with Intel® CoFluent™ Studio	15:45
STTS005	Accelerating Software Development on Next Generation Intel® Architecture Microservers and Tablets with Wind River Simics*	17:00

See also

Technical Showcase Booths 408, 409, 410

"Intel® Device Protection Technology with Boot Guard - Secure *Boot Policy Enforcement*, booth #318"

✓ = DONE

Software Developers: *Network & Have Fun!*

Don't miss out on some great IDF networking and social activities hosted by Intel Software & Services Group (SSG):

- Day 1, Tuesday, Sept 10th, 7pm-10:30pm
  - **Software Developer Networking Party**
    - **Pick up your Software VIP lanyard at the Software and Services Pavilion Info Counter to get party access!**
- Day 2, Wednesday, Sept 11
  - **SSG Inspiration Through Innovation Hour**
    - Location: Showcase Networking Plaza, 11am-12pm & 5pm-6pm
    - SSG/guests discuss how innovation has inspired their products
  - **Doug Fisher (Intel VP, GM SSG) Meet & Greet**
    - Software & Services Pavilion, 5-7pm

- Watch out for SSG Mobile lunch food and dessert carts outside Moscone throughout the conference
- Visit SSG Pavilion Showcase for great demos and games!

Additional Linux Resources

IDF 2012 – Developing UEFI Support for Linux*

https://intel.activeevents.com/sf12/scheduler/catalog/catalog.jsp?sy=42

For more information on Ubuntu* …

Ubuntu ODM Portal - http://odm.ubuntu.com/

Secure Boot Tools - git://kernel.ubuntu.com/jk/sbsigntool
https://github.com/vathpela/pesign

Summary of secure bootloaders

http://www.rodsbooks.com/efi-bootloaders/secureboot.html

Matthew Garrett http://mjg59.dreamwidth.org/

Shim https://github.com/mjg59/

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.

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, Look Inside 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 third 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 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 reports on Form 10-Q, Form 10-K and earnings release.

Rev. 7/17/13

IDF13

Backup

Authenticated Variables

Authenticated Variables (AT):
Small signed named data containers
- Managed, protected by the system BIOS
- Read by BIOS, OS.
- Modified by BIOS, OS only if signature verifies (or local user on Intel® Architecture platforms)

Signed PE/COFF executables
- Op ROMs
- Boot loaders
- Applications

Authenticode signing format

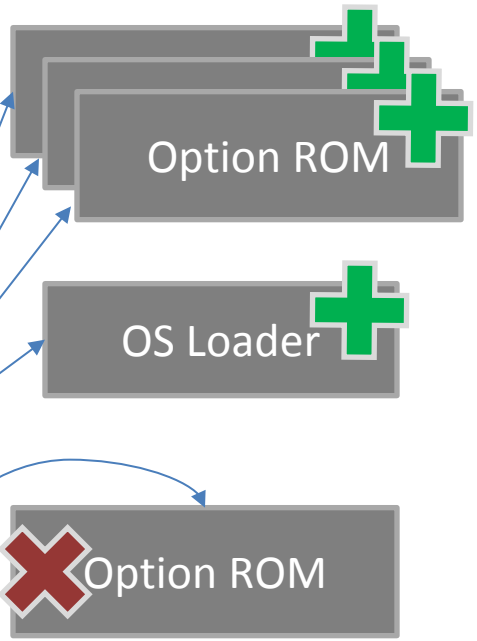
Relationships

PK: Platform Key: AT containing OEM's keys.
Party who can edit the KEK via s/w

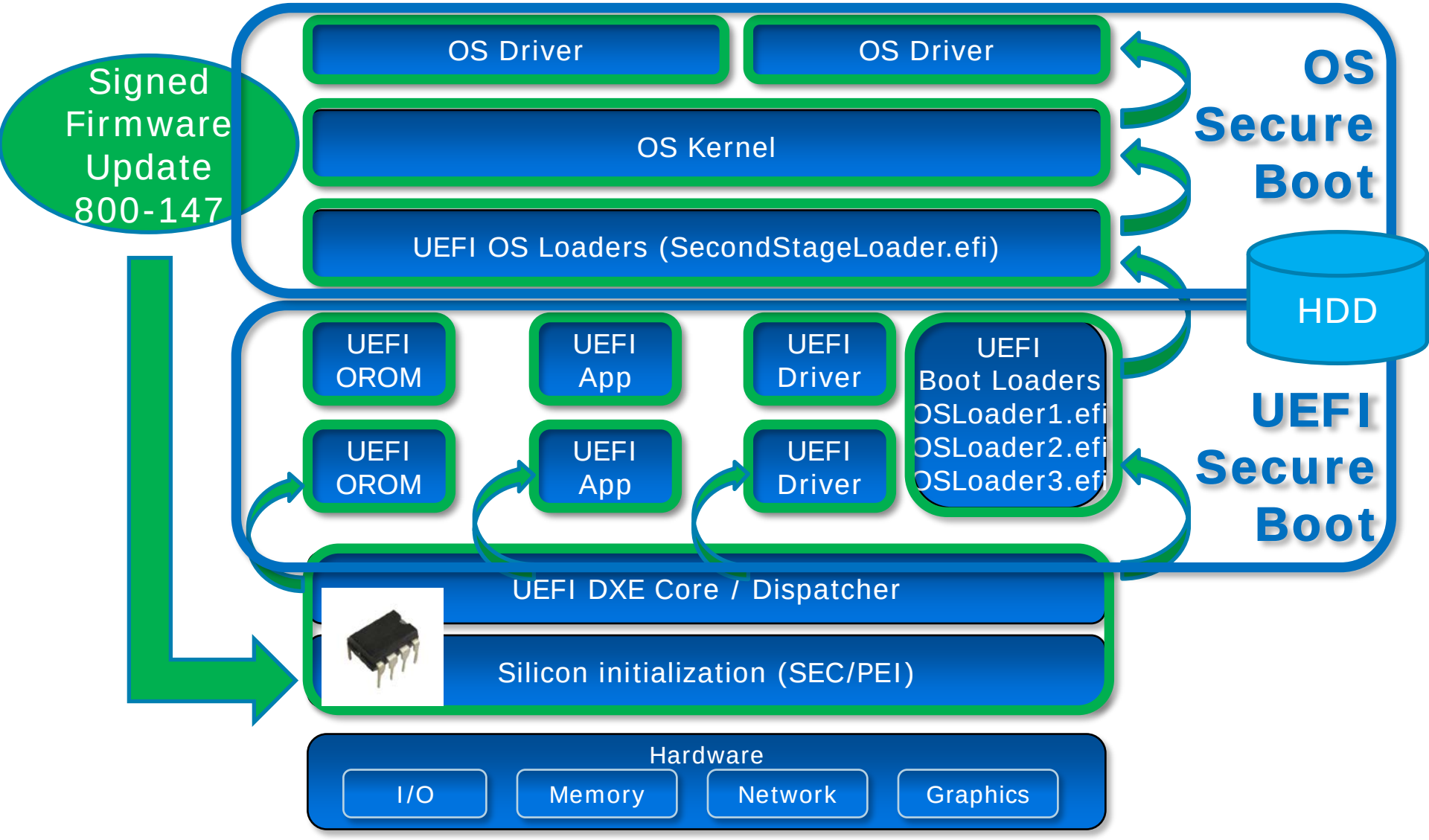
KEK: Key Exchange Key: List of certificates of owners allowed to update white list (db), black list (dbx)

db: Authorization Database: AT containing authorized certs / hashes

dbx: Exclusion Database: AT containing excluded certs / hashes



The Full Solution



End to end platform integrity