IDF2012
INTEL DEVELOPER FORUM

Implementing Platform Security with UEFI

Dong Wei, VP, UEFI Forum, Distinguished Technologist, HP
Jiewen Yao, UEFI BIOS Architect, Intel
Jeff Bobzin, Secretary UEFI Forum, VP, Insyde Software

PTAS004

Sponsors of Tomorrow.™ intel

Please Fill out the Online Session Evaluation Form

Be entered to win fabulous prizes everyday!

Winners will be announced at 8pm today

You will receive an email prior to the end of this session
Fill out the evaluation by 7pm today to be entered for the prizes

Sweepstakes rules available at Information desk

IDF2012
INTEL DEVELOPER FORUM

Agenda

- UEFI Updates
- Security Feature of Intel® UDK2010 SR1 Release
- Secure Boot Factory Tools
- Secure Firmware Updates
- Summary

The PDF for this Session presentation is available from our Technical Session Catalog at the end of the day at: intel.com/go/idfsessionsBJ

URL is on top of Session Agenda Pages in Pocket Guide

Agenda

- UEFI Updates
- Security Feature of Intel® UDK2010 SR1 Release
- Secure Boot Factory Tools
- Secure Firmware Updates
- Summary

UEFI Updates

- UEFI Specification
  - Version 2.3.1, Errata A published on Sept. 7, 2011
  - Clarifications from version 2.3.1
  - Additional ECRs are work in progress
- UEFI SCT
  - Published a UEFI Winter 2012 Plugfest Release in Feb, 2012
    - Version 2.3.1 compliance test preview
  - Investigating coverage for 2.3.1 Errata A
- Be Ready for Windows* 8
  - UEFI 2.3.1 support
  - UEFI drivers and applications
  - Secure boot (sign the executables)
  - Seamless boot, hybrid boot, fast boot
  - IPv6 and IPv4 network stack
  - UEFI Spring 2012 Plugfest in Taipei (May 8-10)
- PI Specification
  - Version 1.2 Errata C published in October 2011

2012 marks the ubiquitous adoption of UEFI on PCs

Intel® UDK2010 SR1 Key features

- UEFI 2.3.1 Secure Boot
- TCG Physical Presence v1.2 rev 1.0 support
- User Identification(UID) per UEFI 2.3.1a
- iSCSI over IPv6
- Networking Improvements - DHCP4/DHCP6 API & IPV6 identification
- Opal/eDrive SATA devices support per UEFI 2.3.1a
- USB 3.0 Controller support (XHCI)
- UEFI 2.3.1 Internal Forms Representation (IFR) support
- Modular and Faster Build Process
- Fast Boot support (asynchronous Block I/O)

HP Experience on Intel® UDK2010 SR1

- Advantages
  - Support for many of the new UEFI and Windows* 8 features
    - UEFI 2.3.1 support
    - Support for Windows 8 features
      - Secure Boot
      - Seamless Boot
    - Support for IPv6 and IPv4 network stacks
      - IPSec is implemented
  - Most of the code is ready-to-go and doesn't require changes

Intel® UDK2010 SR1 provides a valuable reference implementation for the industry

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

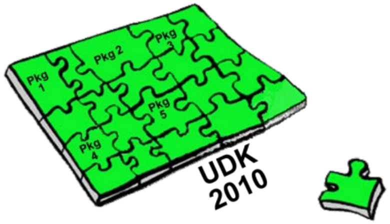
Hewlett-Packard Company makes no warranty as to the accuracy or completeness of the foregoing material and hereby disclaims any responsibility therefor.

Agenda

- UEFI Updates
- Security Feature of Intel® UDK2010 SR1 Release
- Secure Boot Factory Tools
- Secure Firmware Updates
- Summary

Intel® UDK2010 SR1 Security Features

- UEFI Secure Boot
  - UEFI variable support for UEFI Secure Boot as defined by UEFI 2.3.1a (EFI_VARIABLE_TIME_BASED_AUTHENTICATED_WRITE_ACCESS attribute with EFI_VARIABLE_AUTHENTICATION_2 and EFI_VARIABLE_AUTHENTICATION support)
  - DXE Image Verification library to support UEFI Secure Boot (UEFI 2.3.1a)
  - PK x509 Certificate Support
  - Support EFI_VARIABLE_AUTHENTICATION_2 for PK variable format (UEFI 2.3.1a)
  - Add enable/disable mechanism for UEFI Secure Boot
- TCG Trusted Boot
  - TCG EFI Platform Specification



Intel® UDK2010 SR1 Other Features

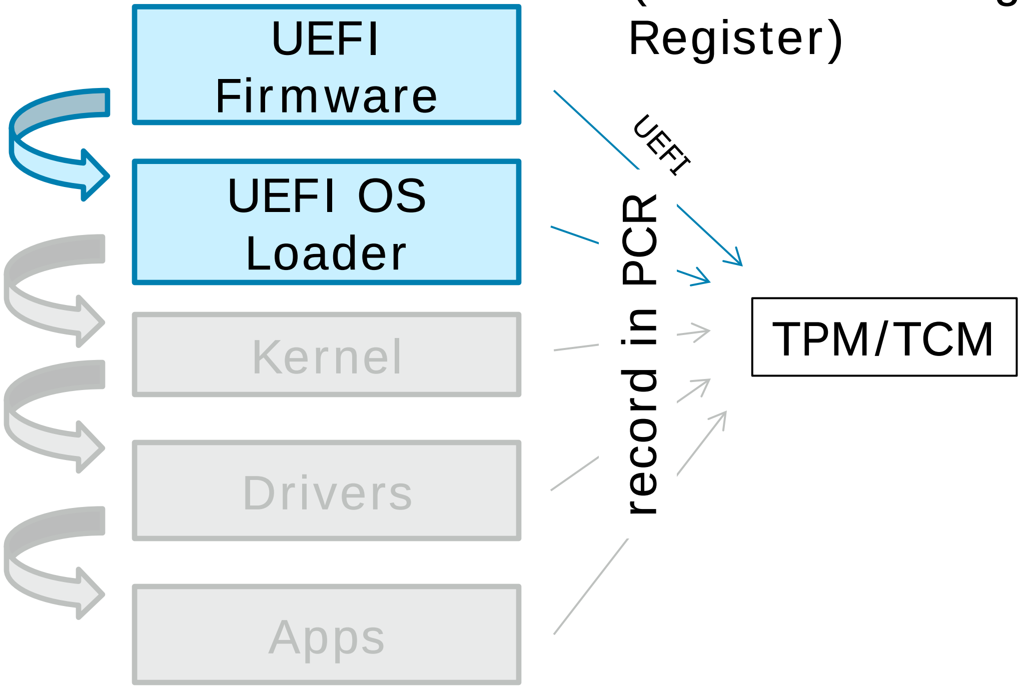
- User Identity (UID) Support (UEFI 2.3.1a)
- Secure Storage Protocol
  - Enable Opal/eDrive SATA devices using the EFI_STORAGE_SECURITY_COMMAND_PROTOCOL, ATA-8 Trusted Send/Receive and IEEE1667 Silo (UEFI 2.3.1a)
- Networking Improvements
  - Errata related to Netboot6-DUID
  - Provide more DHCP4 & DHCP6 API support
  - iSCSI (ip6) open source implementation for IPv6
- TCG Physical Presence (PP). Based on the Physical Presence Interface Specification Version 1.20, Revision 1.0.
- Support ATA Asynchronous Block Io (UEFI 2.3.1a)
- USB 3.0 Controller Support (XHCI)
- Update Internal Forms Representation (IFR) implementation to match UEFI 2.3.1 Specification

UEFI Secure Boot VS TCG Trusted Boot

UEFI authenticate
OS loader
(pub key and policy)

Check signature of
before loading

TPM/TCM will measure
OS loader into PCR
(Platform Configuration
Register)



UEFI Firmware

UEFI OS Loader

Kernel

Drivers

Apps

UEFI

record in PCR

TPM/TCM

- UEFI Secure boot will stop platform boot if signature not valid (OEM to provide remediation capability)
- UEFI will require remediation mechanisms if boot fails

- TCG Trusted boot will never fail
- Up to other SW to make security decision using attestation

UEFI Secure Boot Component:

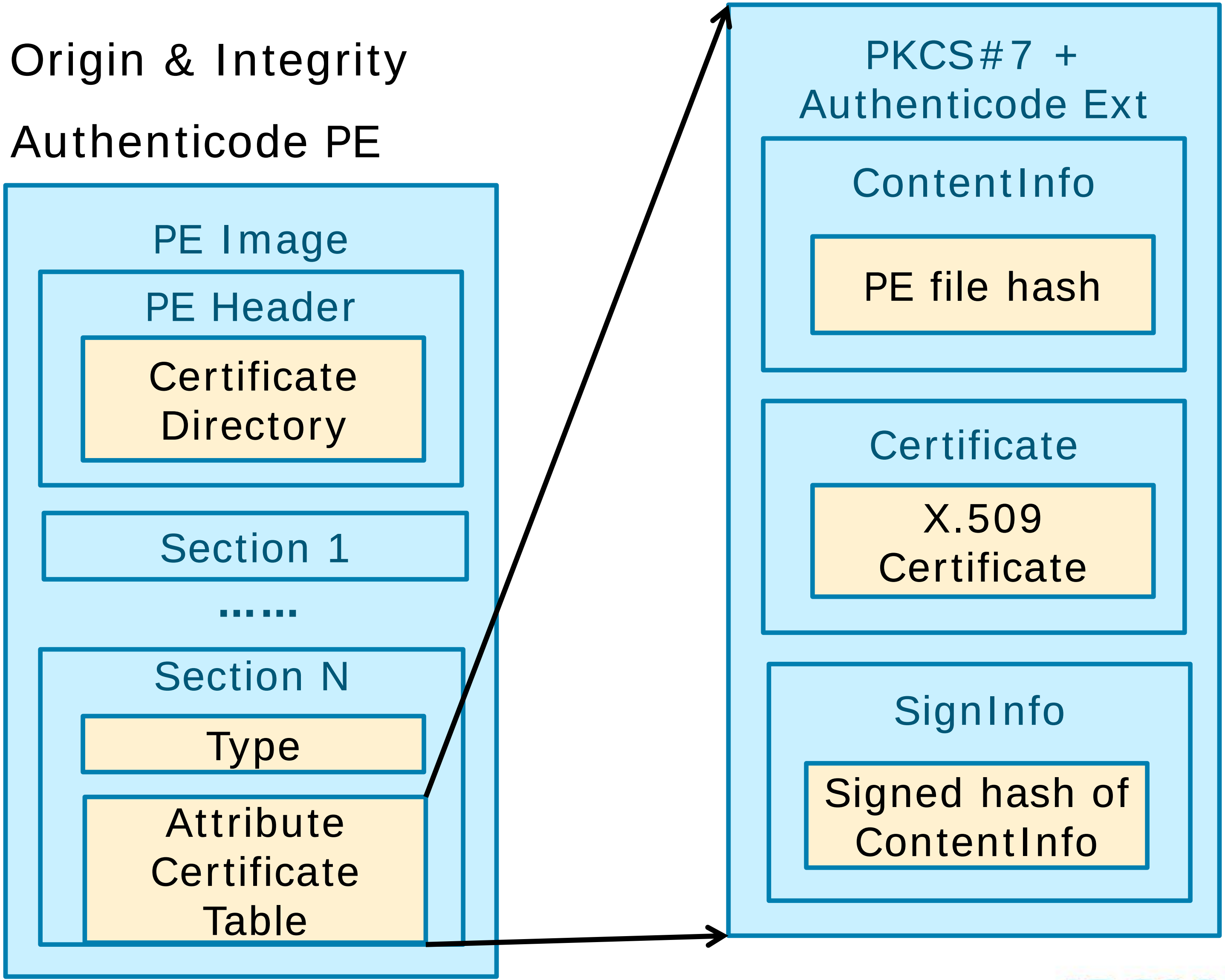
UEFI Driver **Signing** → The system provider may decide to authenticate either the origin of the executable or its integrity

Authenticated UEFI Variable → It provides a way to protect the critical variable being modified by malicious software.

Firmware/OS **Key** → We can create a trust relationship between the platform owner, the platform firmware, and an operating system.

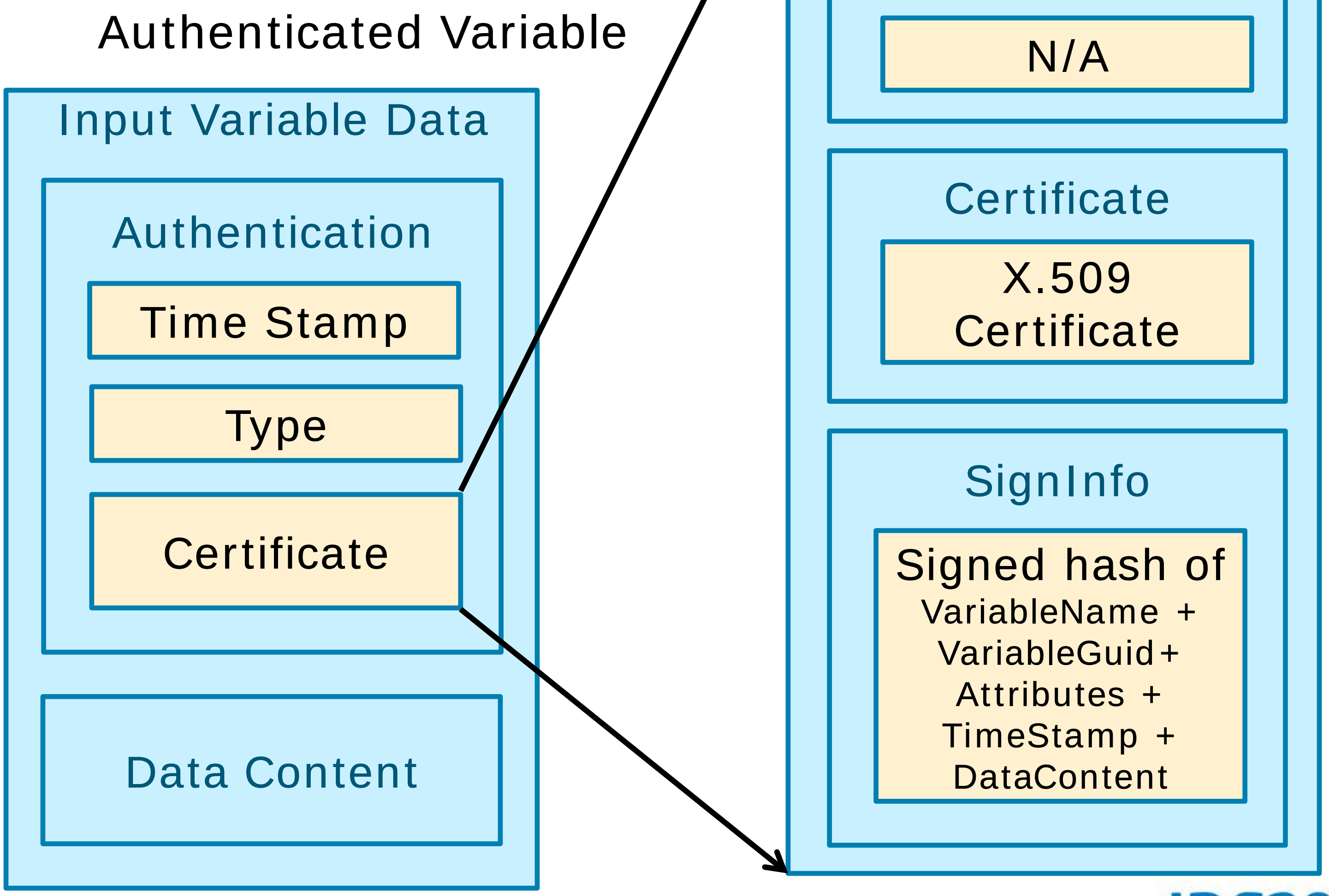
UEFI Driver Signing

- **Why**? – Origin & Integrity
- **How**? – Authenticode PE



UEFI Authenticated Variable

- **Why**? – Integrity (no confidentiality)
- **How**? – Time Based



Authenticated Variable

Input Variable Data

Authentication

Time Stamp

Type

Certificate

Data Content

PKCS#7

ContentInfo

N/A

Certificate

X.509 Certificate

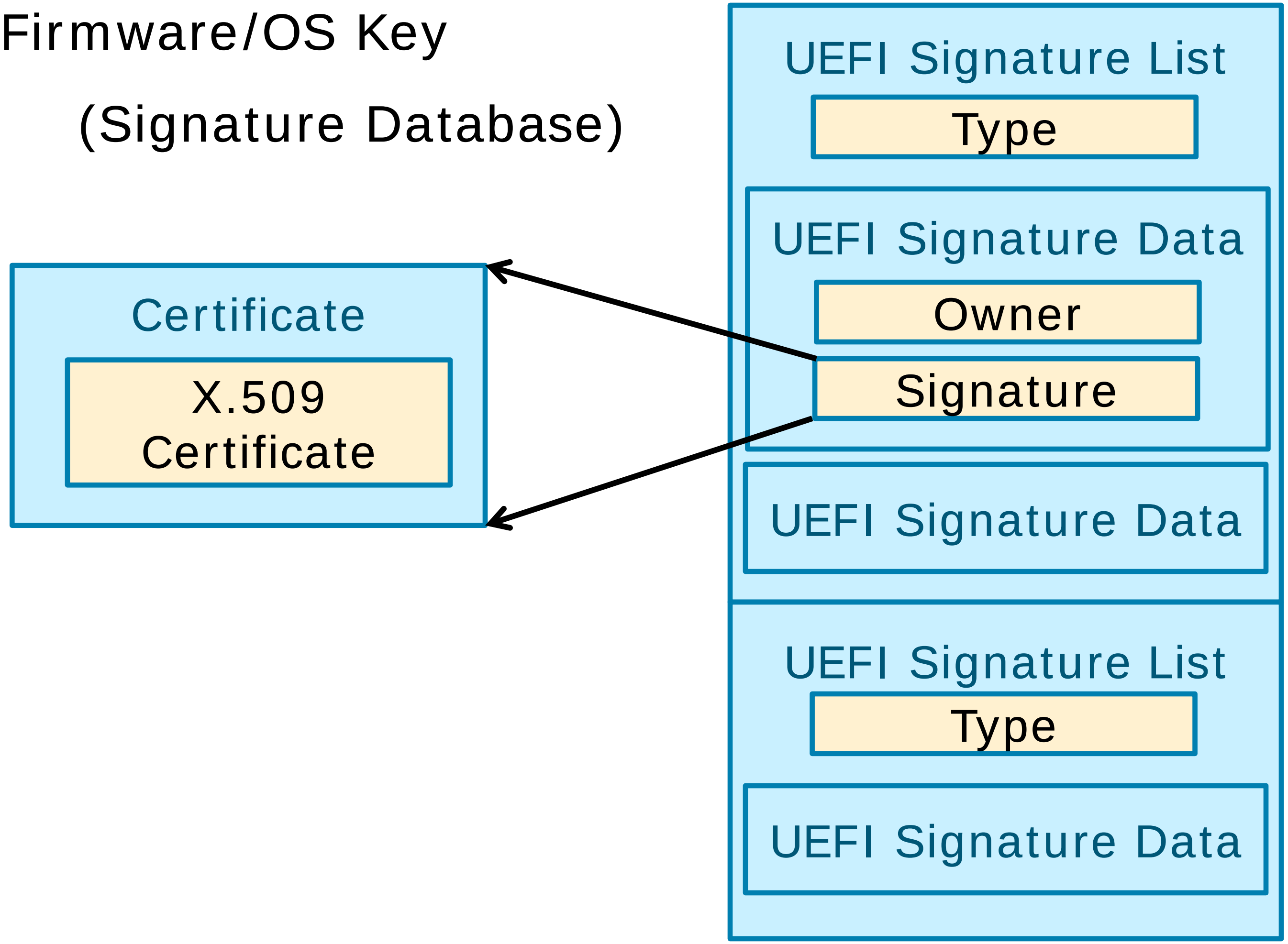
SignInfo

Signed hash of VariableName + VariableGuid+ Attributes + TimeStamp + DataContent

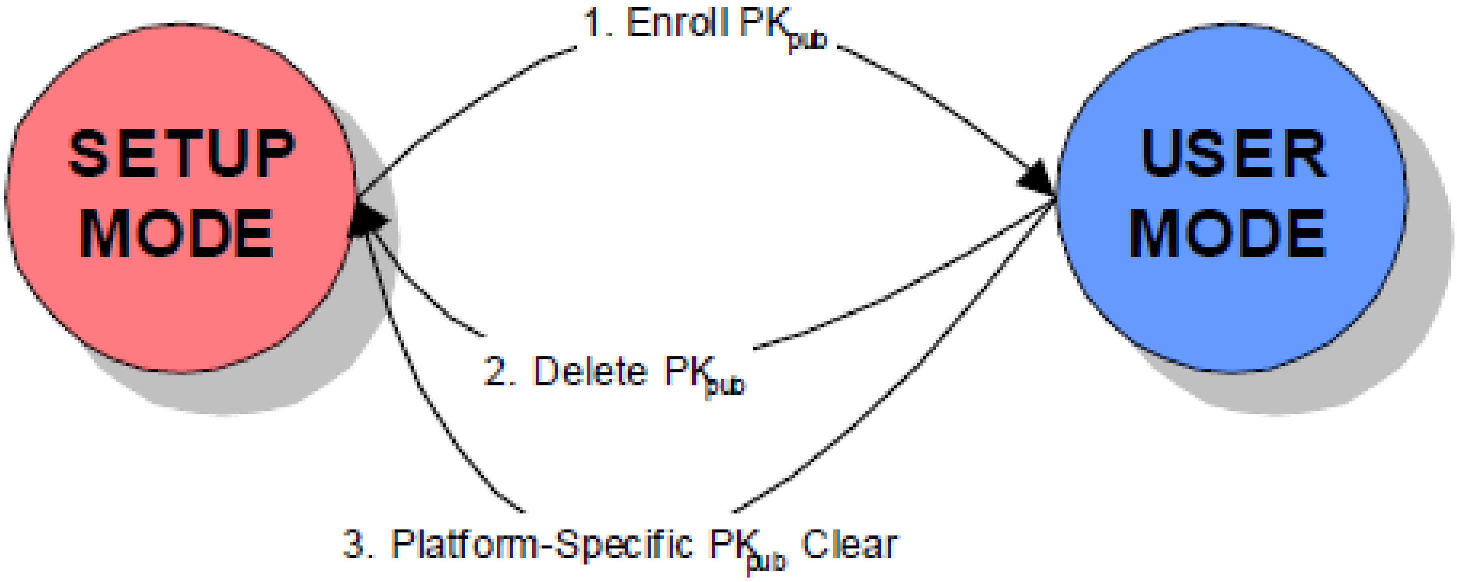
Firmware/OS Key

- **Why**? – How can firmware know if certificate is valid?
- **How**? – Firmware/OS Key

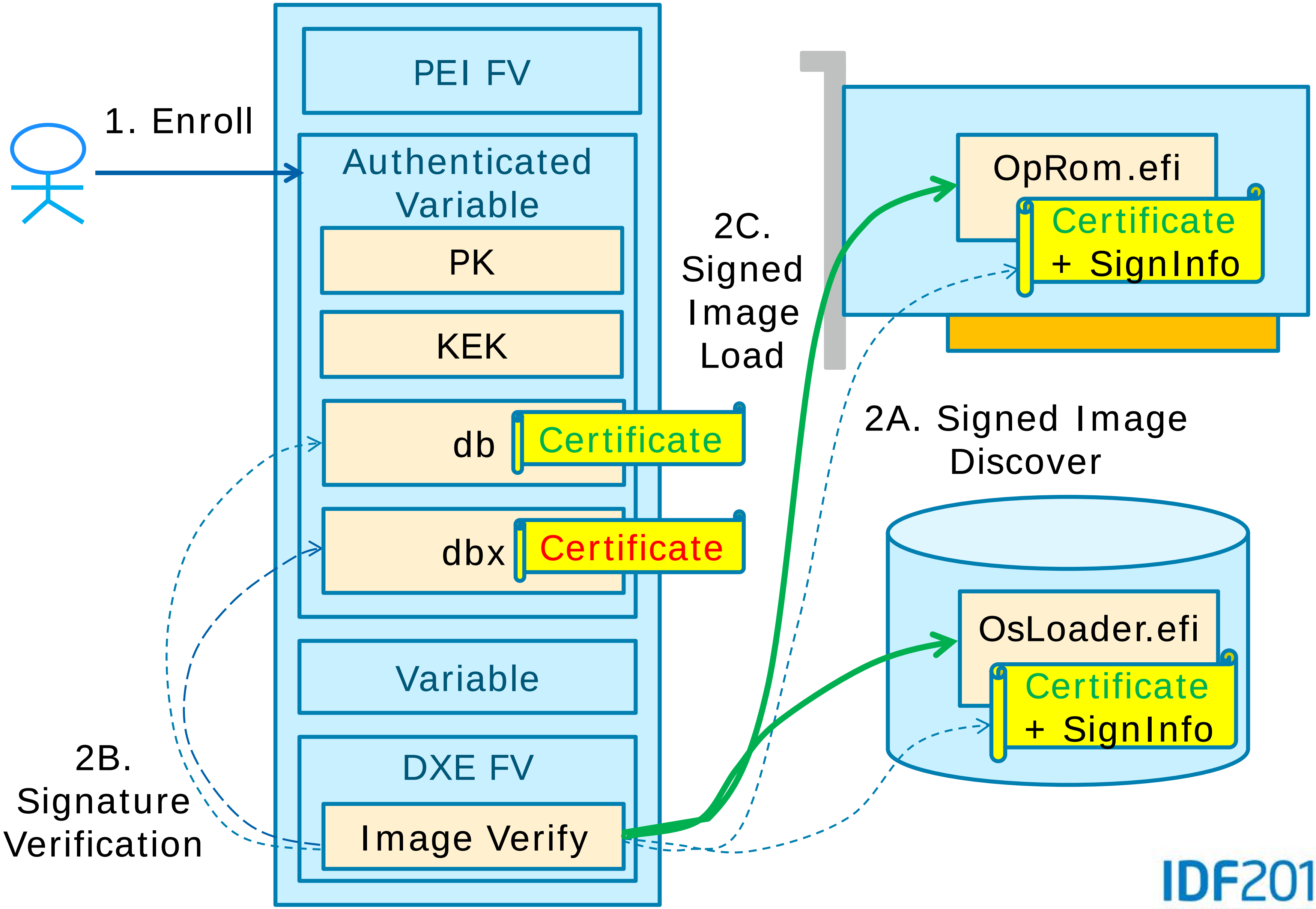
(Signature Database)



Put Them Altogether: UEFI Secure Boot



Put Them Altogether: UEFI Secure Boot

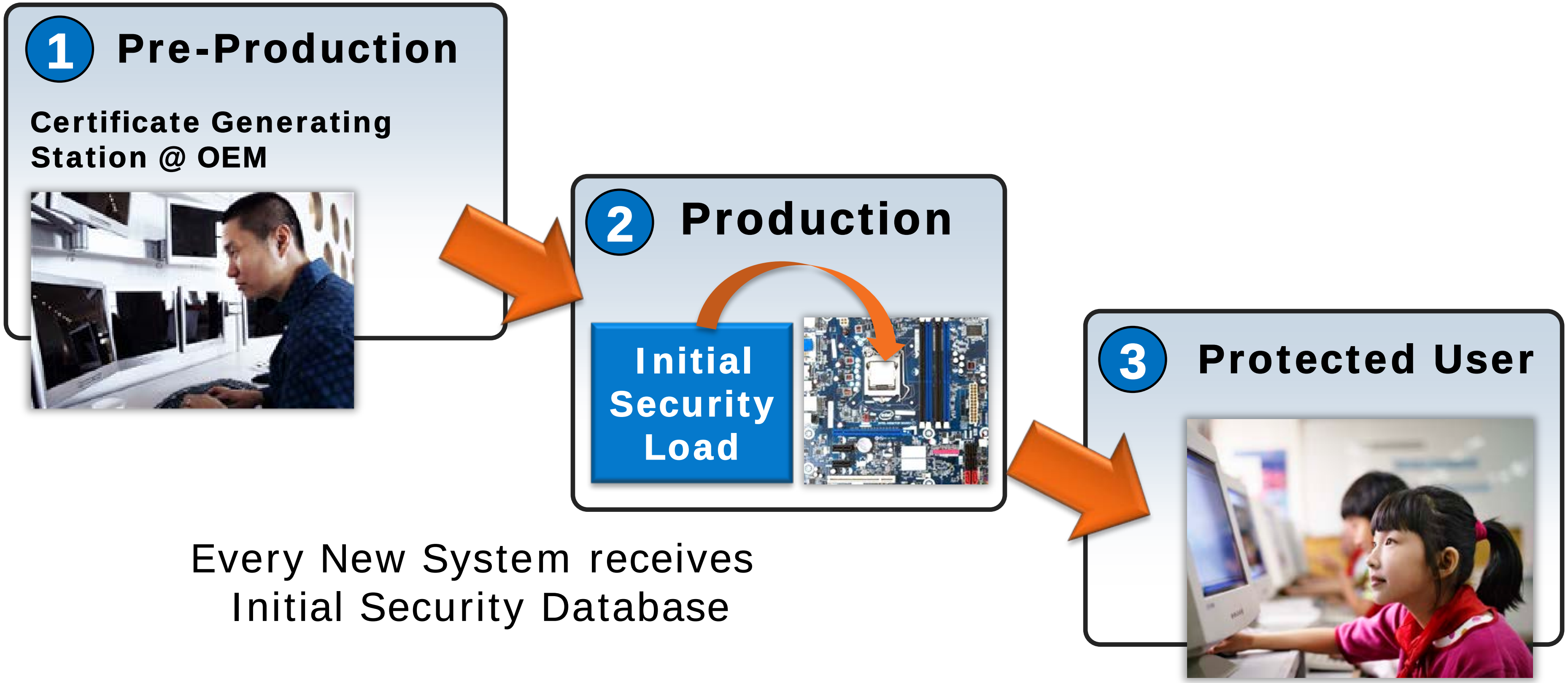


IDF2012 INTEL DEVELOPER FORUM

Agenda

- UEFI Updates
- Security Feature of Intel® UDK2010 SR1 Release
- Secure Boot Factory Tools
- Secure Firmware Updates
- Summary

UEFI 2.3.1 Secure Boot Begins at the Factory



1 Pre-Production

Certificate Generating Station @ OEM

2 Production

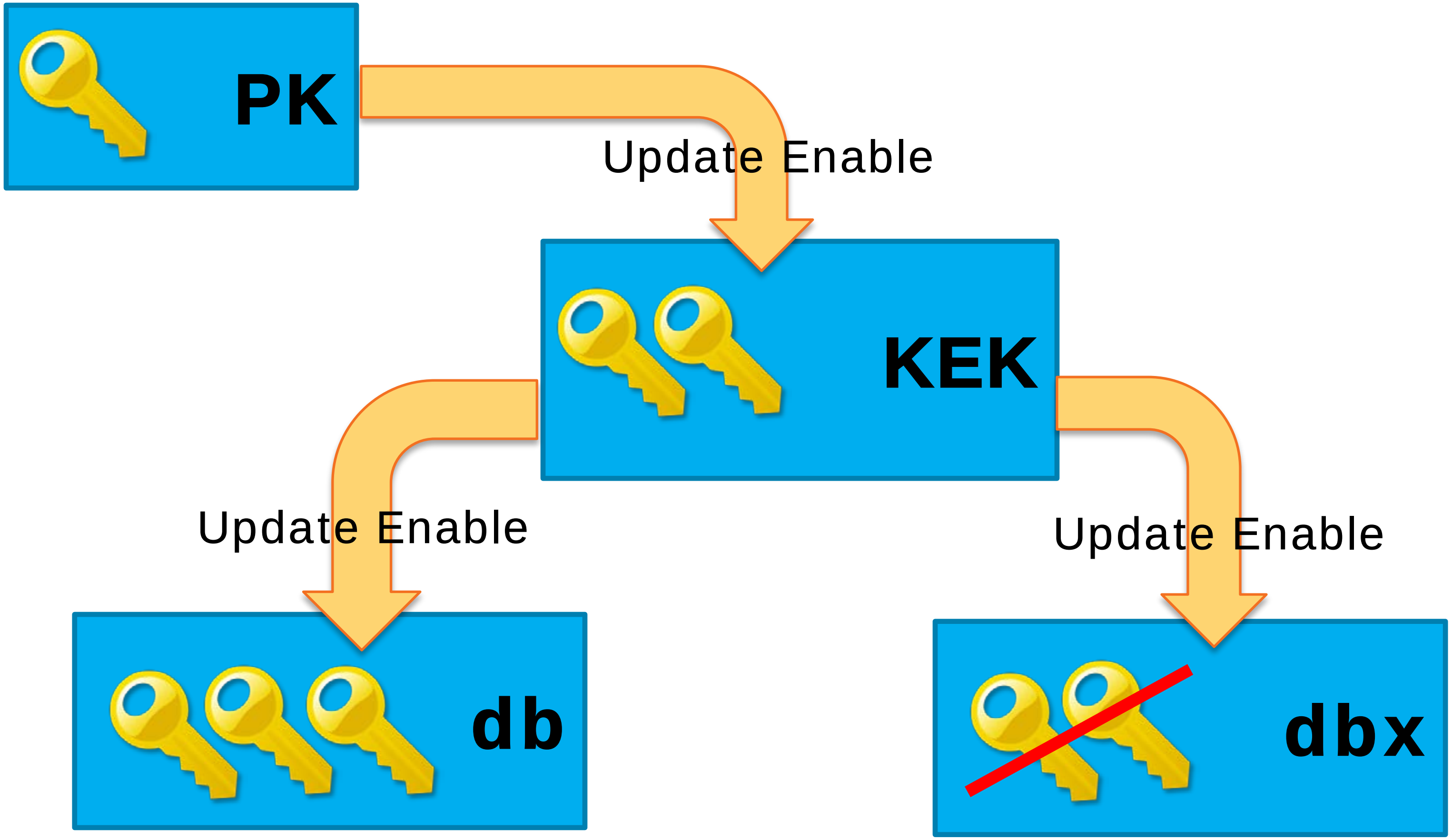
Initial Security Load

3 Protected User

Every New System receives
Initial Security Database

OEM is Responsible for Initializing Secure Boot

UEFI Secure Boot Database Review



If Signed by key in db, driver or loader can Run!

If Signed by key in dbx, driver/loader forbidden!

Public vs. Private Keys

- A pair of keys, one public, one private, are created
- Private keys stay secure at Partner or in the OEM’s Security Office
- Private keys are used to ‘sign’ objects
- Only Public keys loaded into the Platform
- Public keys are used to check signatures

Public
Private

Private Keys Must be Stored Securely!

Who "Owns" The System Security Keys?

- PK – Key pair is created by Platform Manufacturer

  Typically one PK pair used for a model or model Line

- KEK – Key supplied by OS Partner,

  Optional: Include 2nd key created by OEM

- db – OS Partner supplies Key,

  CA Partner supplies Key,

  Optional: OEM App Signing Key

Signature Tests using db Keys Block Rogue S/W!

OEM Administration

- Keys are installed for testing with target OS
- Keys are installed in the factory before shipping

- **Preparation Tasks**

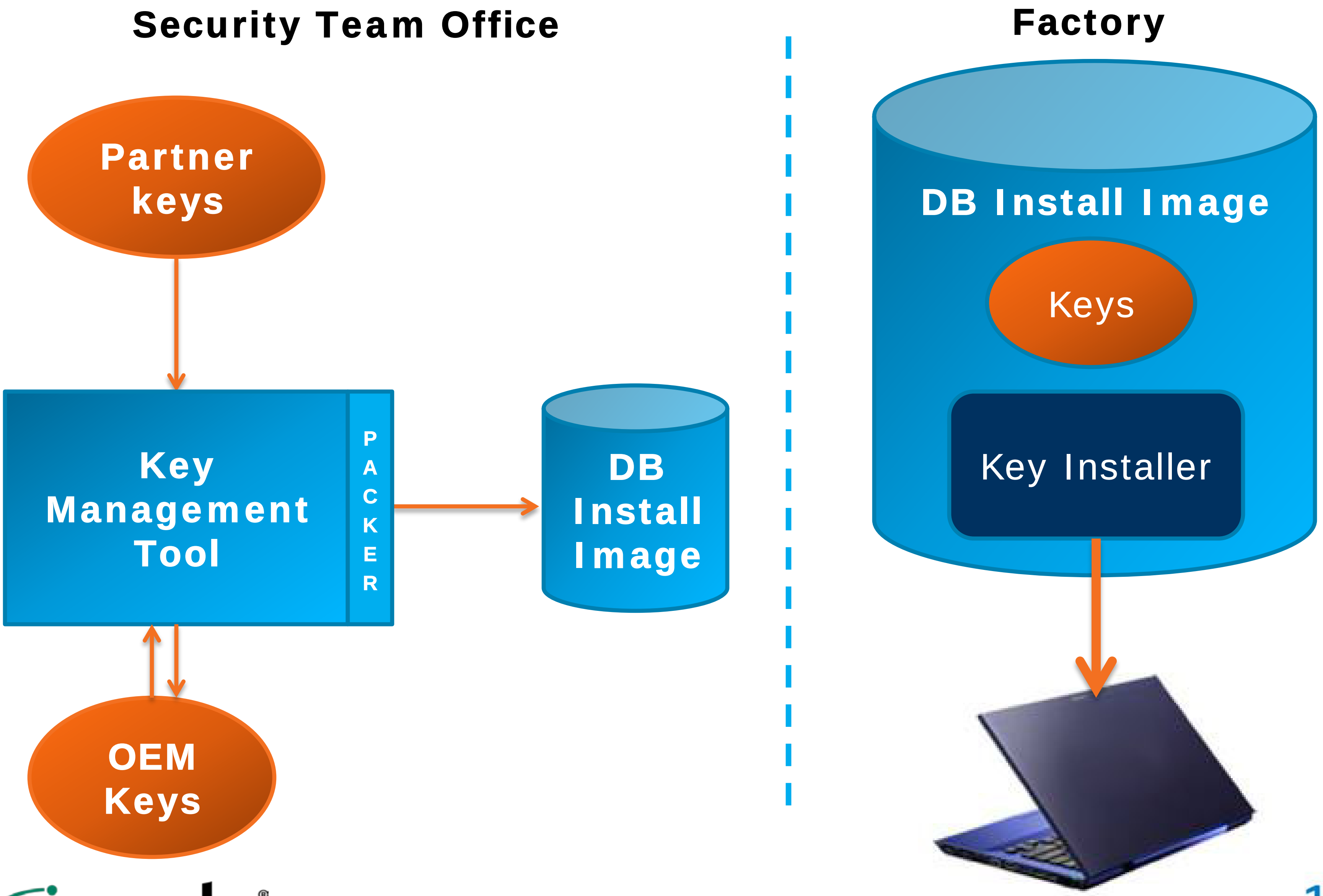
1. Gather public keys from partners
2. Generate PK for model
3. Make a package of initial key load
4. Occasional maintenance of forbidden list

- **Repetitive Tasks**

1. Factory will boot and install the initial key load

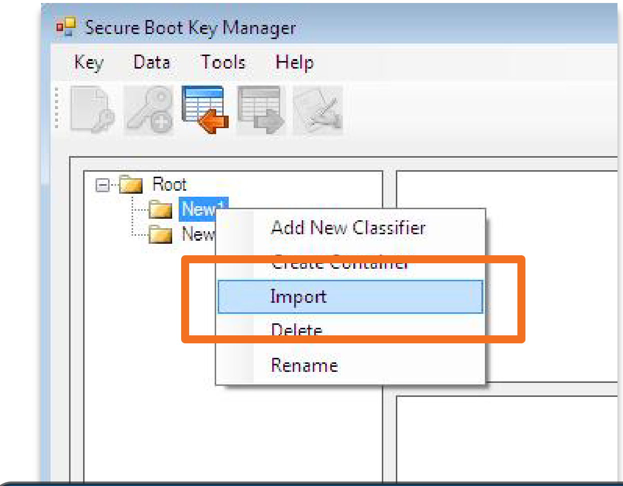
Careful Preparation Delivers Successful Launch

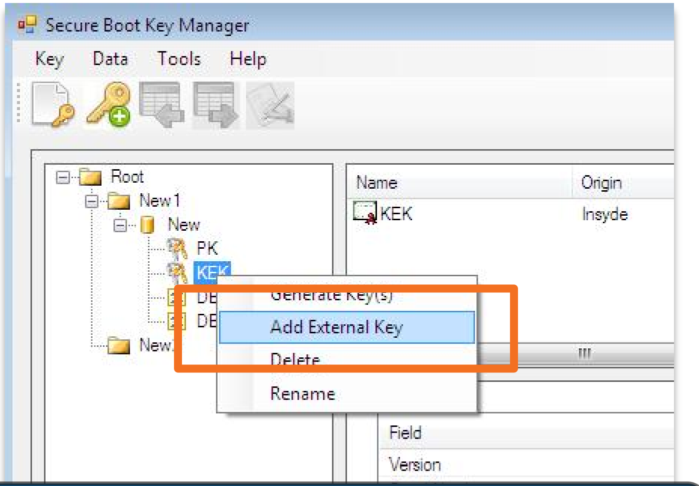
Major Components of the Tool Set



Key Generator and Management Tool

- InsydeH2O* Key Manager imports:
  - Partner's KEKpub
  - Public signing keys for db (example Microsoft Signing Authority, Windows Signing key, OEM signing authority)
  - Current Revoked keys or hash list for dbx

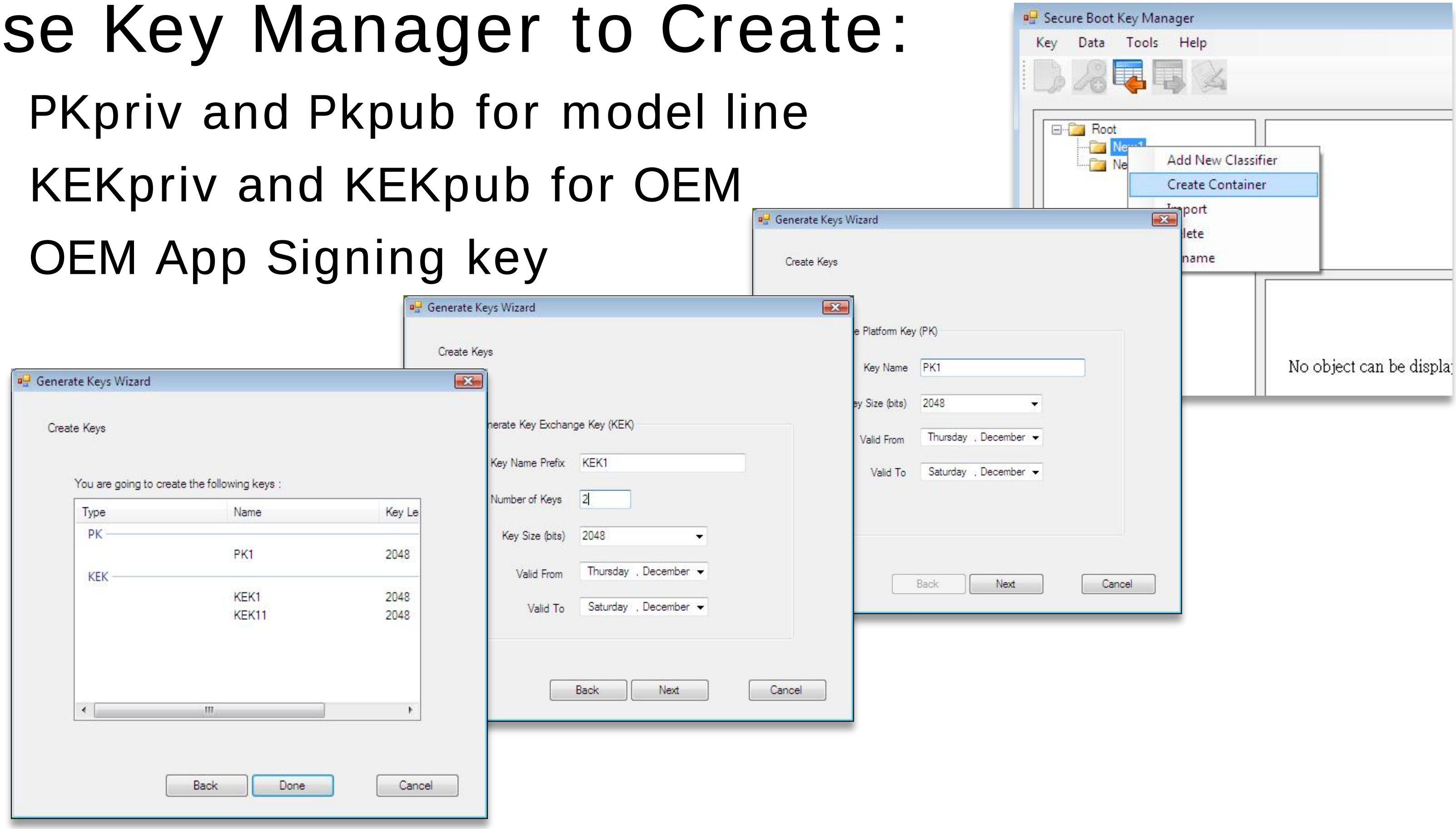




Key Manager Organizes Database Prep

Key Generator and Management Tool

- Use Key Manager to Create:
  - PKpriv and Pkpub for model line
  - KEKpriv and KEKpub for OEM
  - OEM App Signing key



No object can be displa

Create Keys

Platform Key (PK)

Key Name: PK1
Key Size (bits): 2048
Valid From: Thursday , December
Valid To: Saturday , December

Create Keys

erate Key Exchange Key (KEK)

Key Name Prefix: KEK1
Number of Keys: 2
Key Size (bits): 2048
Valid From: Thursday , December
Valid To: Saturday , December

Create Keys

You are going to create the following keys :

Type	Name	Key Le
PK		
	PK1	2048
KEK		
	KEK1	2048
	KEK11	2048

Key Manager Creates OEM Required Keys

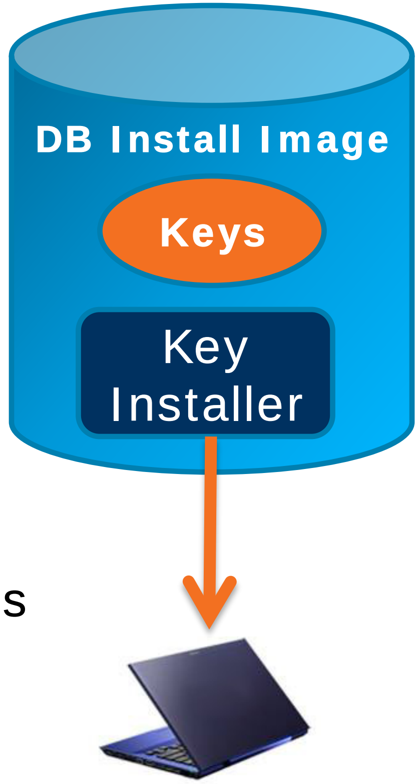
Insyde Factory Install Image File

(1) Key Installer

- Runs in WIN8 or WINPE
- Checks it's own integrity
- Installs the Secure Keys

(2) Initial Database Image

- PK – System Master Key
- KEK – OEM and Partner Management Keys
- db – Industry Recognized Driver/app signing Keys
- dbx – Revoked signing keys



DB Install Image

Keys

Key Installer

Single Signed Installer File Prevents Factory Tampering

Agenda

- UEFI Updates
- Security Feature of Intel® UDK2010 SR1 Release
- Secure Boot Factory Tools
- Secure Firmware Updates
- Summary

Secure Field Update to Firmware Store

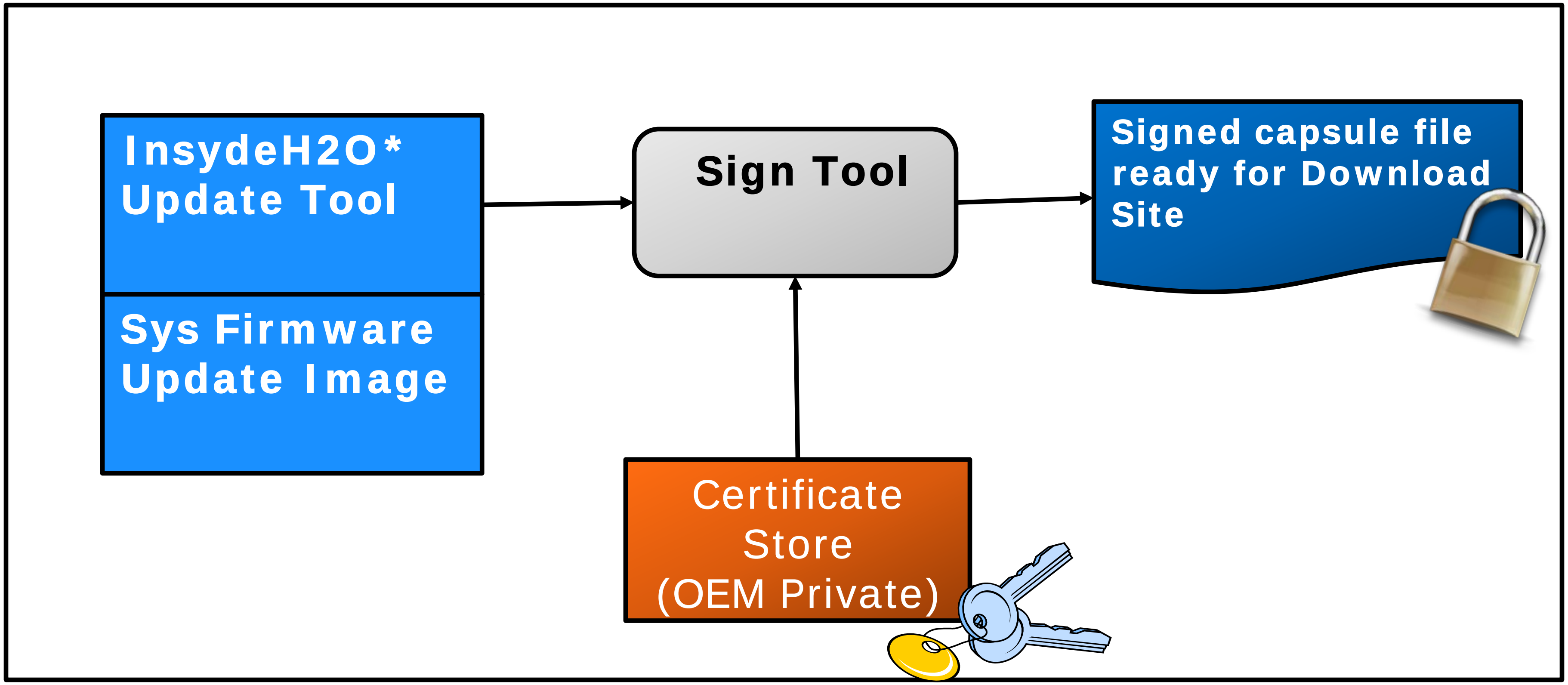
- Field Firmware Update must support all elements of NIST 800-147 & Windows* 8 client recommendations
  - Any update to the firmware flash store but be signed by creator
  - Firmware must check signature of the update
  - Firmware updates are signed by another key – not PK
  - Policy must remain in effect even if Secure Boot Database is cleared by user

All Firmware Updates Must be Signed at Factory

insyde®

IDF2012 INTEL DEVELOPER FORUM

Signing Firmware Update Files:



InsydeH2O* Update Tool

Sys Firmware Update Image

Sign Tool

Signed capsule file ready for Download Site

Certificate Store (OEM Private)

InsydeH2O* Secure Update Meets Industry Requirements

insyde®

IDF2012 INTEL DEVELOPER FORUM

DEMO!

Agenda

- UEFI Updates
- Security Feature of Intel® UDK2010 SR1 Release
- Secure Boot Factory Tools
- Secure Firmware Updates
- Summary

Summary

- 2012 is the year for ubiquitous UEFI adoption
- With UEFI 2.3.1, the boot experience is fast, secure and beautiful leading to higher customer satisfaction and opportunity for product differentiation.
- Intel® UDK2010 SR1 is a good reference, especially for security features
- With the benefits of secure boot come new responsibilities for OEMs in management of security database.
- Modern standards require secure firmware updates

Call To Action

System OEMs and their partners need to plan the switch to UEFI 2.3.1 Secure Boot:

1. Use learning resources including Intel® UDK2010 SR1
2. Develop procedures and assign clear responsibilities for security tasks
3. Work with IBV for firmware implementation and new factory tools

Related Sessions

Session ID	Title	Day	Time	Room
GVCS001 ✓	Leveraging the Full Processing Power of Next Generation Intel® core Microarchitecture, Code Name Ivy Bridge	Wed	11:00	306B
GVCQ001 ✓	Hot Topic Q&A: Graphics and Visual Computing	Wed	17:15	306B
GVCC001 ✓	Poster Chat: Tools for Tuning Graphics and Heterogeneous Computing Applications for the Next Generation Intel® Processor Graphics	Wed	14:00	Poster Station 6
	Platform Technologies and Analysis Sessions			
PTAC001 ✓	Poster Chat: UEFI Application Development using Standard Libraries and Python*	Wed	14:00 16:25	Station 7
PTAC002 ✓	Poster Chat: Power and Thermal Analysis using Intel® Platform Profiling Tool	Wed	14:00 16:26	Station 8
PTAS001 ✓	System Behavior and Performance Prediction using System Modeling and Simulation Tools	Wed	14:15	310
PTAS002 ✓	Shift Left! Leverage Full System Simulation to Reduce Your Time To Market	Wed	15:20	310
PTAS003 ✓	Advanced UEFI Development Environment for Embedded Platforms	Wed	16:25	310
PTAQ001 ✓	Platform Technologies and Analysis Q&A	Wed	17:15	310
PTAS004 ✓	Implementing Platform Security with UEFI	Thurs	13:10	306B
PTAS005	Platform Optimization Using Open Computing Language (OpenCL*) Tool	Thurs	14:15	306B
	Software and Services Group Pavilion - Platform Technologies: UEFI, Analysis Tools, and Simulation Booth Number 16	Wed - Thurs		Show Case

✓ = DONE

Please Fill out the Online Session Evaluation Form

Be entered to win fabulous prizes everyday!

Winners will be announced at 8pm today

You will receive an email prior to the end of this session
Fill out the evaluation by 7pm today to be entered for the prizes

Sweepstakes rules available at Information desk

IDF2012
INTEL DEVELOPER FORUM

Q&A

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 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.
-

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, 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; 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. 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 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 Oct. 1, 2011.

Rev. 1/19/12