IDF2011
INTEL DEVELOPER FORUM

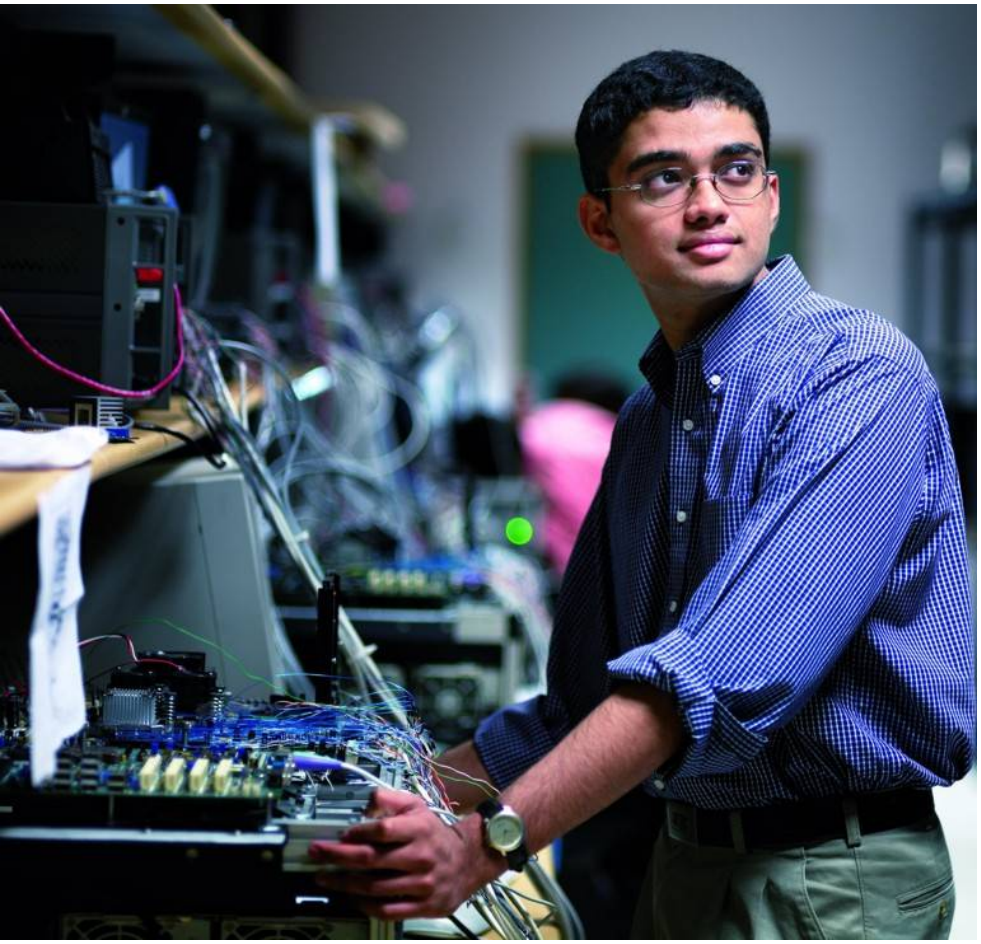
UEFI Security and Networking Advancements

Mark Doran, Senior Principal Engineer, Intel Corporation
Jeff Bobzin, Senior Director Software Architecture, Insyde* Software

EFIS001

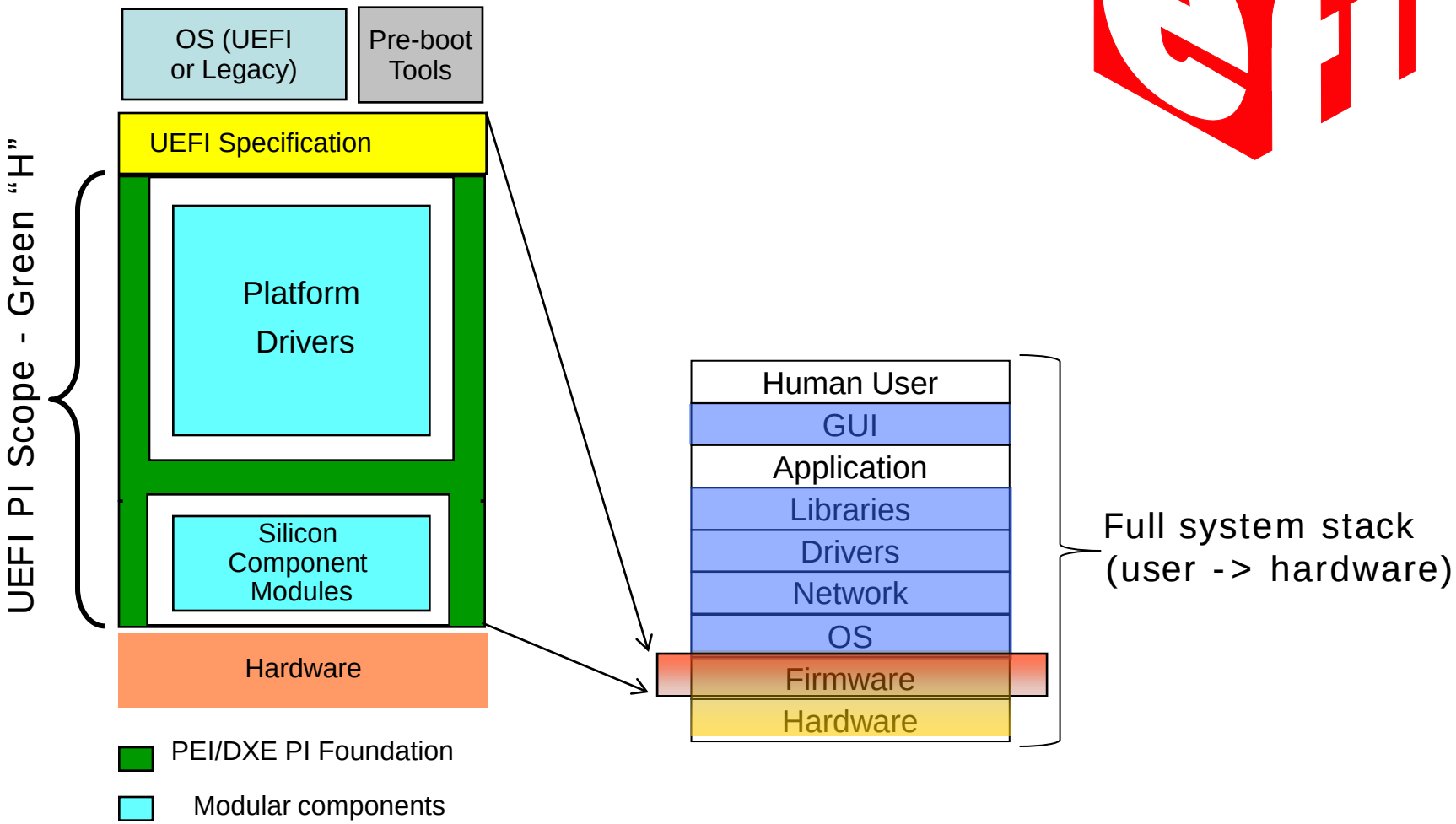
Sponsors of Tomorrow.™ intel

Agenda



- UEFI Specification Updates
- Intel® UEFI Development Kit 2010 (Intel® UDK 2010) Key Features
- Drill Down: Secure Boot in UEFI 2.3.1
- Implementing a Secure Boot Path with UEFI 2.3.1

UEFI Platform Initialization Overview



Key Updates in UEFI 2.3.1

Security

- Authenticated Variable & Signature Data Base
- Key Management Service (KMS)
- Storage Security Command Protocol for encrypted HDD

Interoperability

- New FC and SAS Device Path
- FAT32 data region alignment
- HII Updates

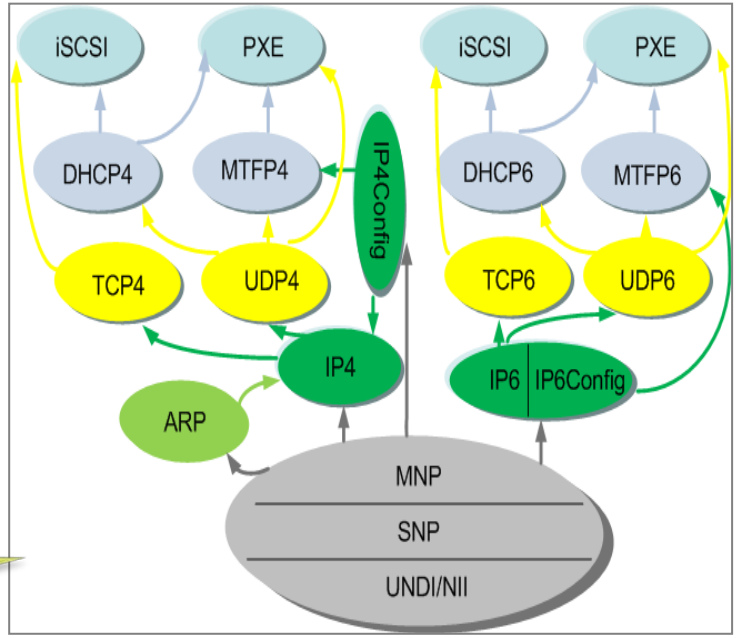
Technology & Performance Updates

- USB 3.0
- Netboot6 client (report platform ID using DUID-UUID)
- Non-blocking interface for BLOCK-oriented devices

Focus: IPv6 Networking

- **IPv6 protocol compliance**
  - **"IPv6 ready" logo approved**
  - **Requirements for IPv6 transition (PDF)**
- **UEFI IPv6 Features**
  - **IP4/6, UDP4/6, TCP4/6**
  - **DHCP4/6, MTFP4/6**
  - **iSCSI, PXE, IPsec**
  - **Allows for concurrent network applications Dual stack (IPv4 and/or IPv6)**
  - **DUID-UUID support**
    - **New in UEFI 2.3.1**
    - **Use SMBIOS system GUID as UUID**

2.3.1



OS Support for Netboot6[1]

- SUSE* Linux Enterprise Server 11 Service Pack 2 x86_64 Beta 4* (SLES 11 SP2 x86_64 Beta 4)
  - Supports UEFI 2.3.1 PXE Netboot6
  - Can support at the same time requests for booting PXE to both IPV4 and IPV6 UEFI 2.3.1 clients
- Next version of Windows Server 2008* will support UEFI 2.3.1 PXE Netboot6 in Windows Deployment Services (WDS)
- Please come to the next UEFI Plugfest in Taiwan to test Netboot6
  - Visit: www.UEFI.org for Event Info
  - Windows and SUSE servers with IPV6 will be provided
- Download the newer version of Windows Server* and SLES 11 SP2 x86_64* and test Netboot6 on your IPV6 network

Next UEFI Plugfest in Taiwan to test Netboot6

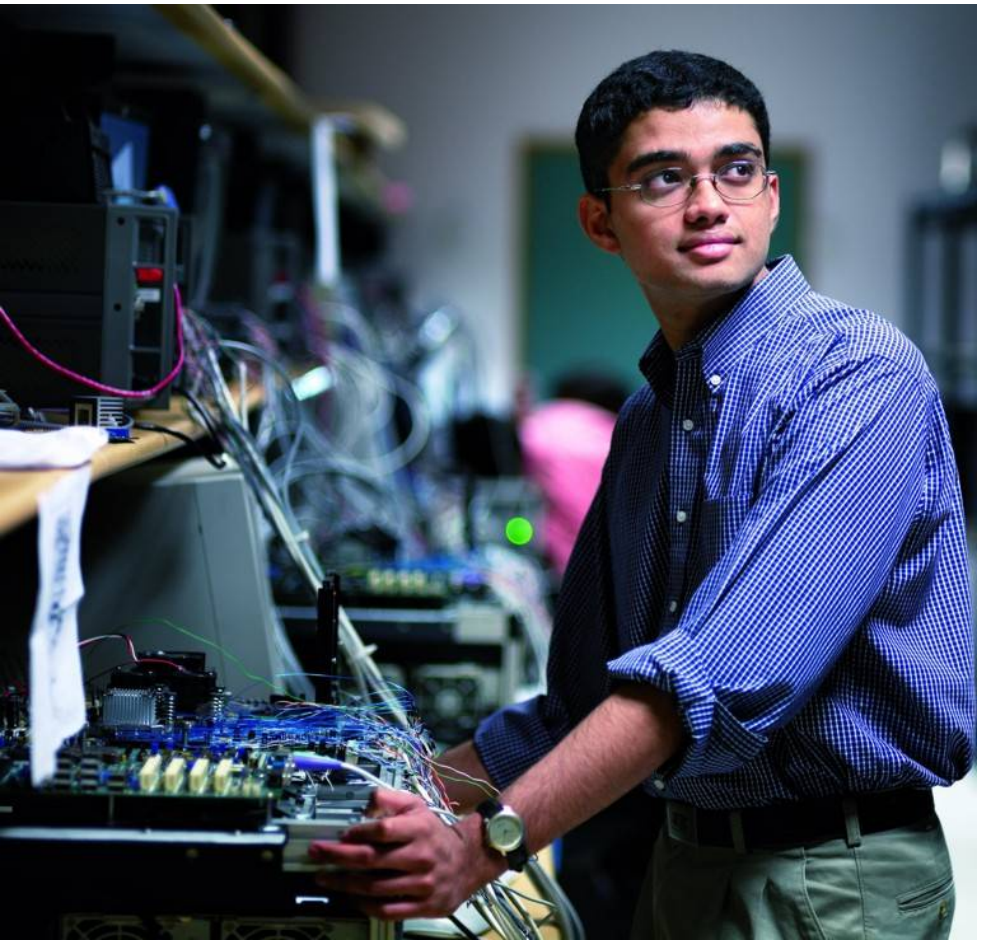
[1] Details on Netbvoot6 can be found in the UEFI2.3.1 Specification

Focus: UEFI Security Features

- **Platform security starts at the lowest level of the software stack … firmware & OS loader**
- **Industry concern over security reflected in new NIST BIOS Protection Guidelines (PDF)**
  - **For details on NIST, refer to the Session EFIS002**
- **UEFI 2.3 & 2.3.1 address these threats with multiple security items**
  - **Closing "Legacy Holes" to achieve Secure Boot (covered in detail later in this session)**
  - **Authenticated Variables & UEFI Driver Signing**
  - ***Started by UEFI 2.3 … enhanced by UEFI 2.3.1***

UEFI 2.3.1 enables key networking and security technologies

Agenda



- UEFI Specification Updates
- **Intel® UEFI Development Kit 2010 (Intel® UDK 2010) Key Features**
- Drill Down: Secure Boot in UEFI 2.3.1
- Implementing a Secure Boot Path with UEFI 2.3.1

Intel® UDK 2010 Enables a Common Firmware Development Foundation Across the Compute Continuum

IDF2011
INTEL DEVELOPER FORUM

Intel® UDK2010 Key Features

Industry Standards Compliance

- UEFI 2.0, UEFI 2.1, UEFI 2.2, UEFI 2.3
- PI 1.0, PI 1.1, PI 1.2
- IPv6, ACPI, SMBIOS, …

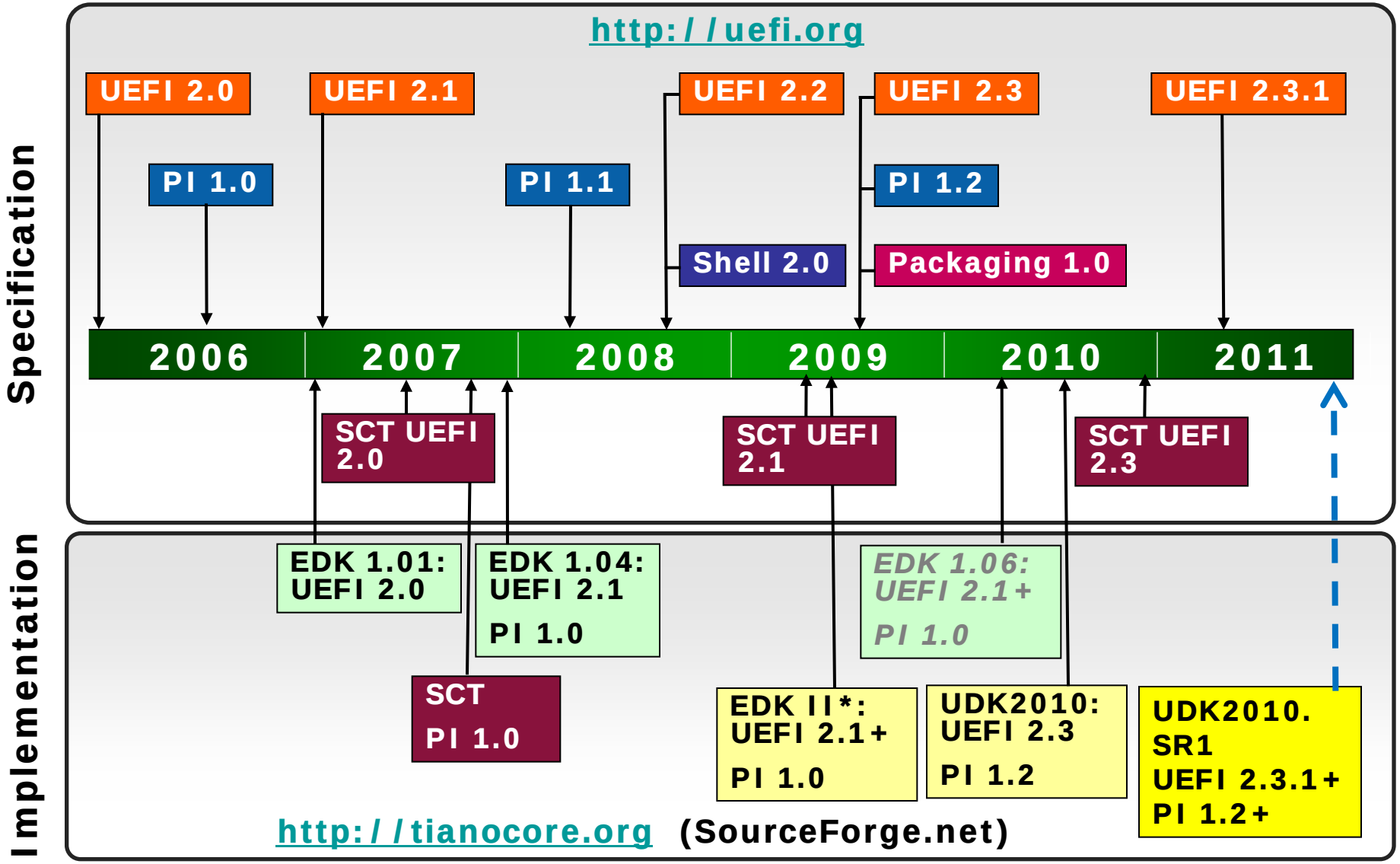
Foundation for Advanced Capabilities

- Pre-OS Security
- Rich Networking
- Manageability

Powerful Firmware Development

- Maximize Code Reuse with Modular Coding
- Use ECP for reuse of EDK1117 (EDK I) modules
- Development under Microsoft Windows, Linux & OSX

Specification & Tianocore.org Timeline



All products, dates, and programs are based on current expectations and subject to change without notice.

* EDK II is the code base used by Intel® UDK 2010

IDF2011 INTEL DEVELOPER FORUM

Intel UDK 2010 SR1 (Q4 2011)

Updated for UEFI 2.3.1+ and PI 1.2+

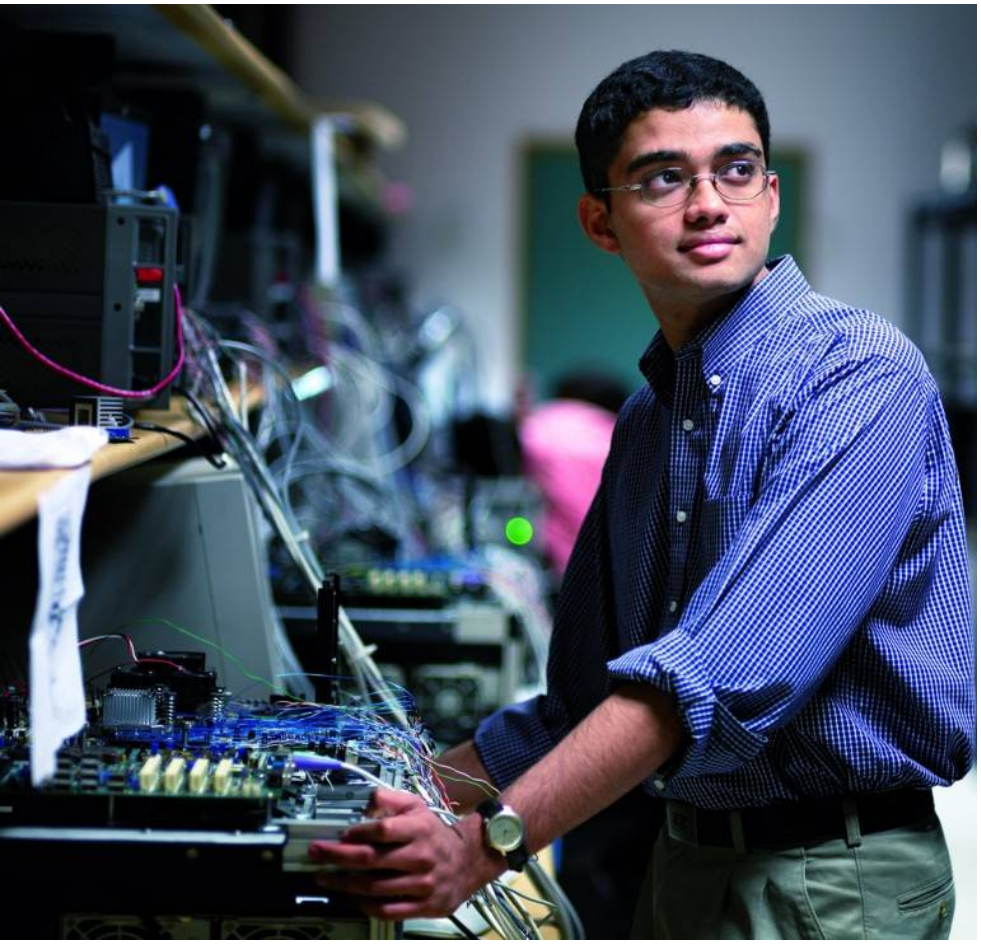
Enabling key OS partners for UEFI 2.3.1

Enable UEFI 2.3+ Security Features

Intel UDK 2010 enables key UEFI features for the industry

IDF2011
INTEL DEVELOPER FORUM

Agenda



- UEFI Specification Updates
- Intel® UEFI Development Kit 2010 (Intel® UDK 2010) Key Features
- **Drill Down: Secure Boot in UEFI 2.3.1**
- Implementing a Secure Boot Path with UEFI 2.3.1

Why Implement UEFI Secure Boot?

- **As OS becomes more resistant to attack the threat targets the weakest element in the chain**
- **And 16-bit Legacy Boot is not secure!**

> ***It should be no surprise that a TDL Gang botnet climbed into the number one position in the Damballa Threat Report – Top 10 Botnets of 2010. "RudeWarlockMob" … applied effective behaviors of old viruses and kits. It combined techniques that have been effective since the days of 16-bit operating systems, like Master Boot Record (MBR) infection … with newer malware techniques.***
> ***(from http://blog.damballa.com)***

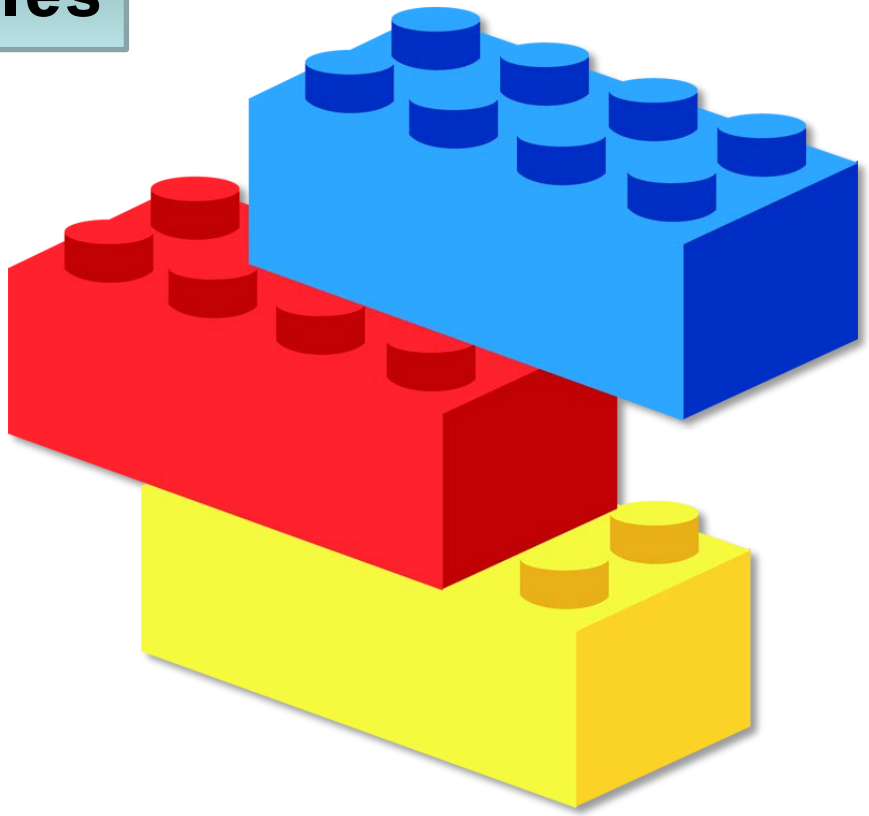
- **Secure Boot based on UEFI 2.3.1 removes the Legacy Threat and provides software identity checking at every step of boot – Platform Firmware, Option Cards, and OS Bootloader**

Secure Boot – Three Components

1. Authenticated Variables

2. Driver Signing

3. System-Defined Variables

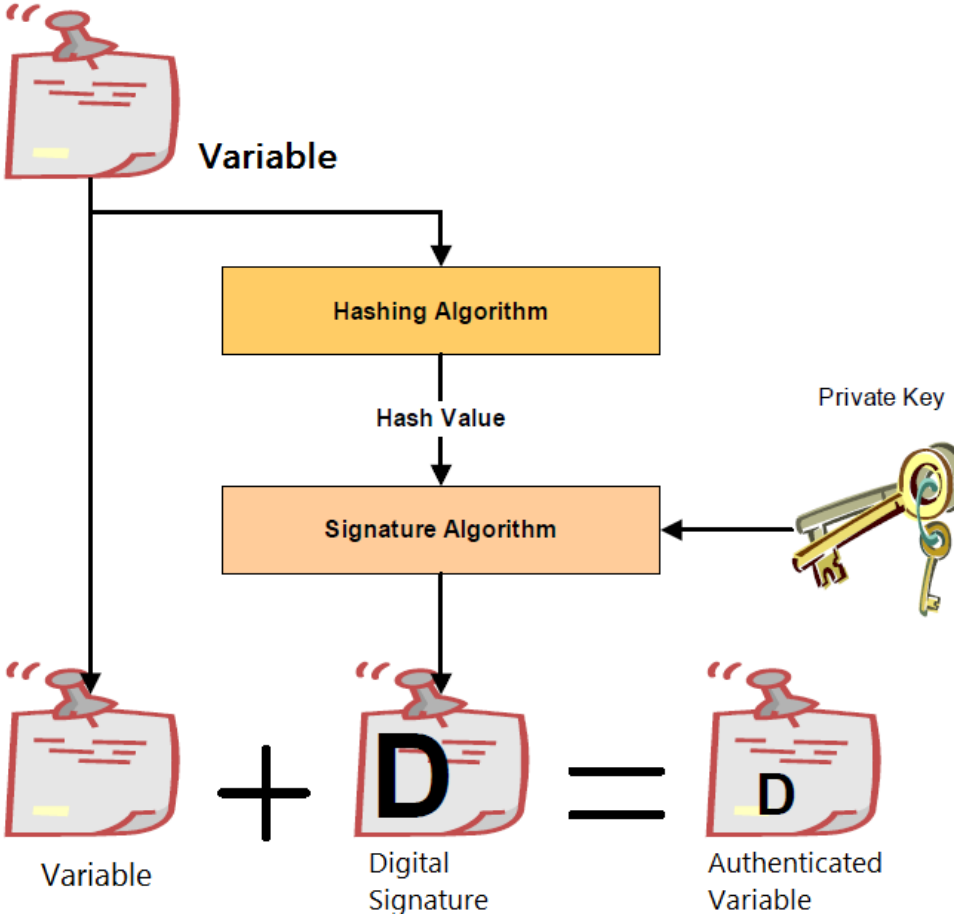


insyde®

IDF2011
INTEL DEVELOPER FORUM

UEFI Authenticated Variables

- Uses standard UEFI Variable Functions
- Available Pre-boot and also Runtime
- Typically stored in Flash
- Variable Creator signs Variable Hash with Private Key (PKCS-7 Format)
- Signature & Variable Passed Together for Create, Replace, Extend, or Delete
- Several System-defined variables for Secure Boot



Extensible Integrity Architecture

insyde®

IDF2011 INTEL DEVELOPER FORUM

Updating Authenticated Variable

New in UEFI 2.3.1

- Support for Append added (UEFI 2.3.1)
- Counter-based authenticated variable (UEFI 2.3)
  - Uses monotonic count to against suspicious replay attack
  - Hashing algorithm – SHA256
  - Signature algorithm – RSA-2048
- Time-based authenticated variable (UEFI 2.3.1)
  - Uses timestamp as rollback protection mechanism
  - Hashing algorithm – SHA256
  - Signature algorithm – X.509 certificate chains
    - Complete X.509 certificate chain
    - Intermediate certificate support (non-root certificate as trusted certificate.

New in UEFI 2.3.1

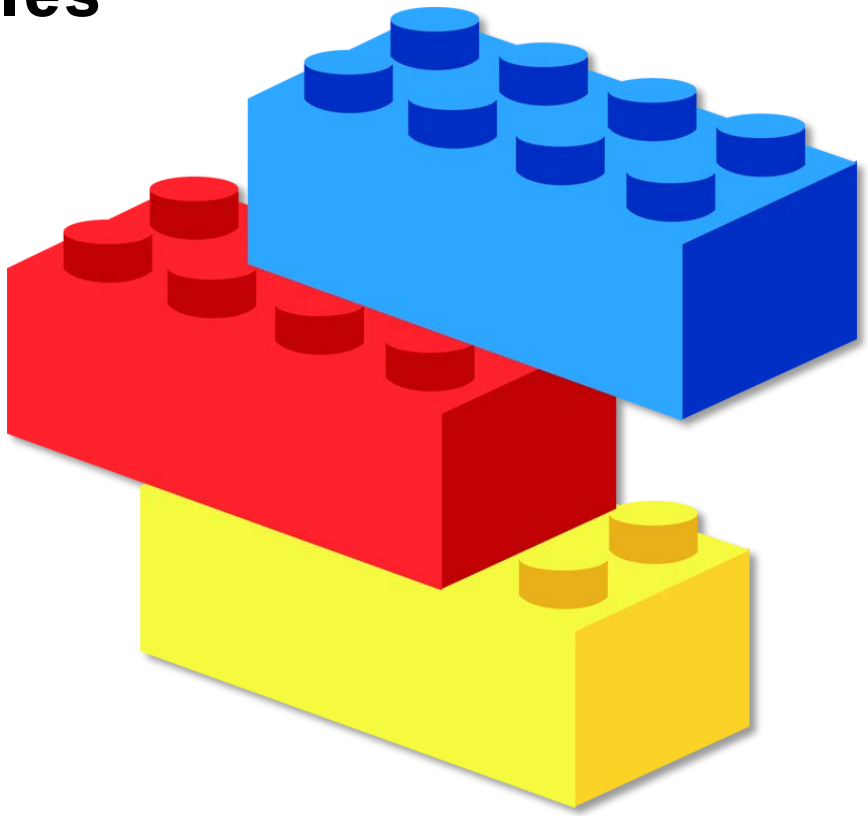
Protected Variables that can be Securely Updated

Secure Boot – Three Components

1. Authenticated Variables

2. Driver Signing

3. System-Defined Variables



UEFI Driver Signing

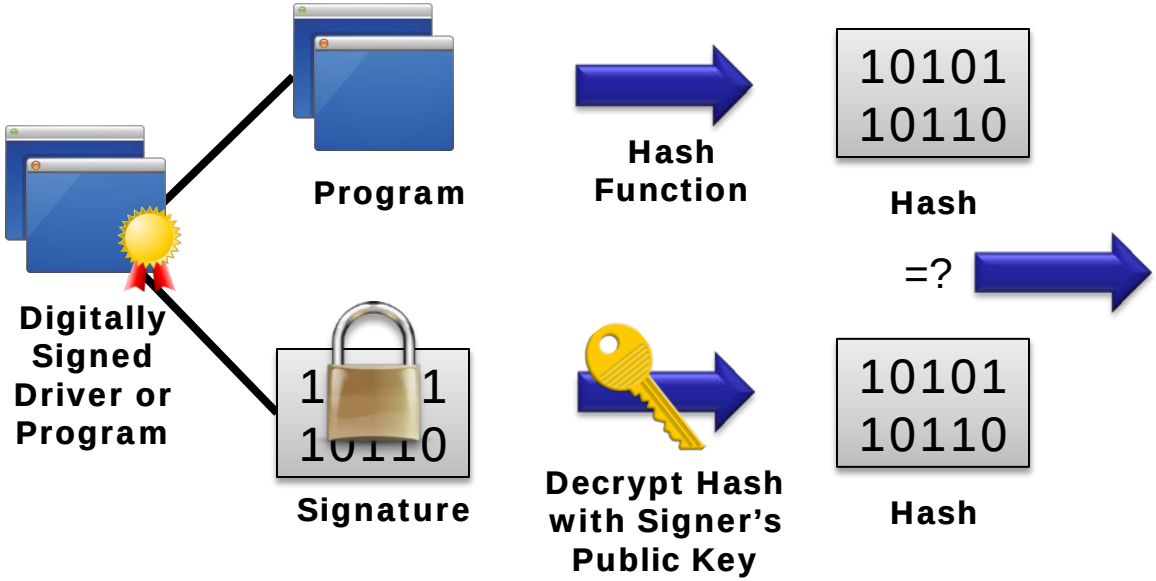
- UEFI Driver Signing Utilizes Microsoft* Authenticode* Technology to sign UEFI executables
- In Secure Boot, signatures should be checked:
  1. UEFI Drivers loaded from PCI-Express Cards
  2. Drivers loaded from mass storage
  3. Pre-boot EFI Shell Applications, f/w updaters
  4. OS UEFI Boot-loaders
- UEFI Signing is not applied to
  1. Drivers in the Factory BIOS
  2. Legacy components

Enhanced by UEFI 2.3.1

UEFI Driver Signing

Signing – by the creator:

Verification – In the PC:



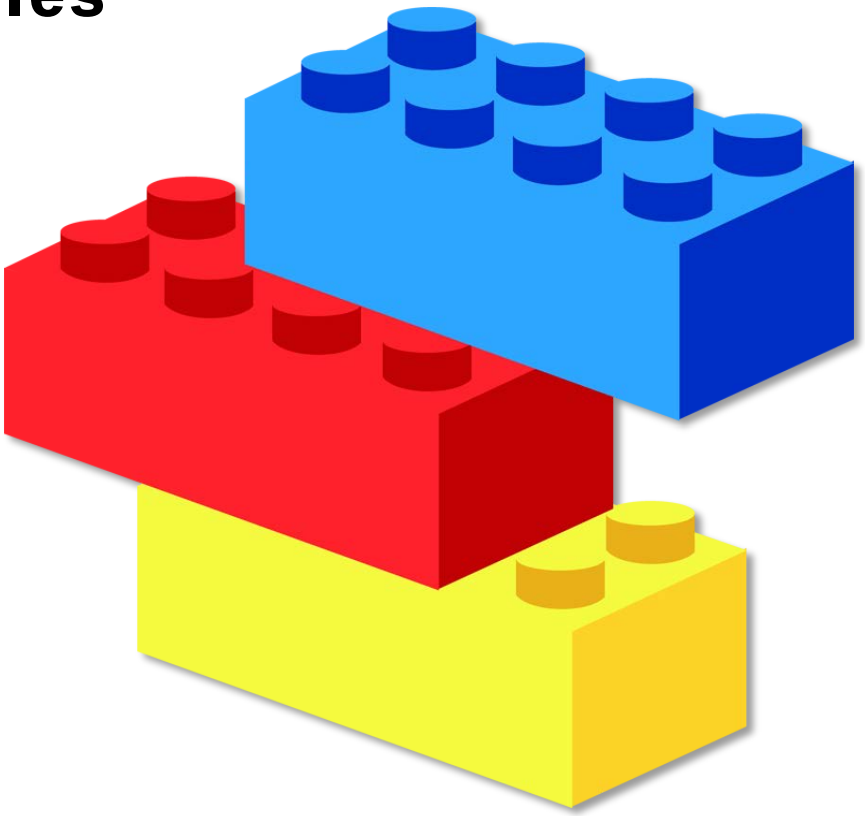
Check local databases for certificate. If certificate found and not revoked, run UEFI Executable.

Secure Boot – Three Components

1. Authenticated Variables

2. Driver Signing

3. System Defined Variables



Secure Boot Authenticated Variables

PK	**P**latform **K**ey – Root key set to enable Secure Boot
KEK	**K**ey **E**xchange **K**ey List of Cert. Owners with db, dbx update privilege
db	List of Allowed Driver or App. Signers (or hashes)
dbx	List of Revoked Signers (or hashes)
SetupMode	1= in Setup Mode, 0 = PK is Set (User Mode)
SecureBoot	1 = Secure Boot in force

Notes:

- Owner of cert. in KEK can update db, dbx
- Owner of cert. in PK can update KEK

UEFI Defines System Databases for Secure Boot

Secure Boot – Three Components

1. Authenticated Variables

+

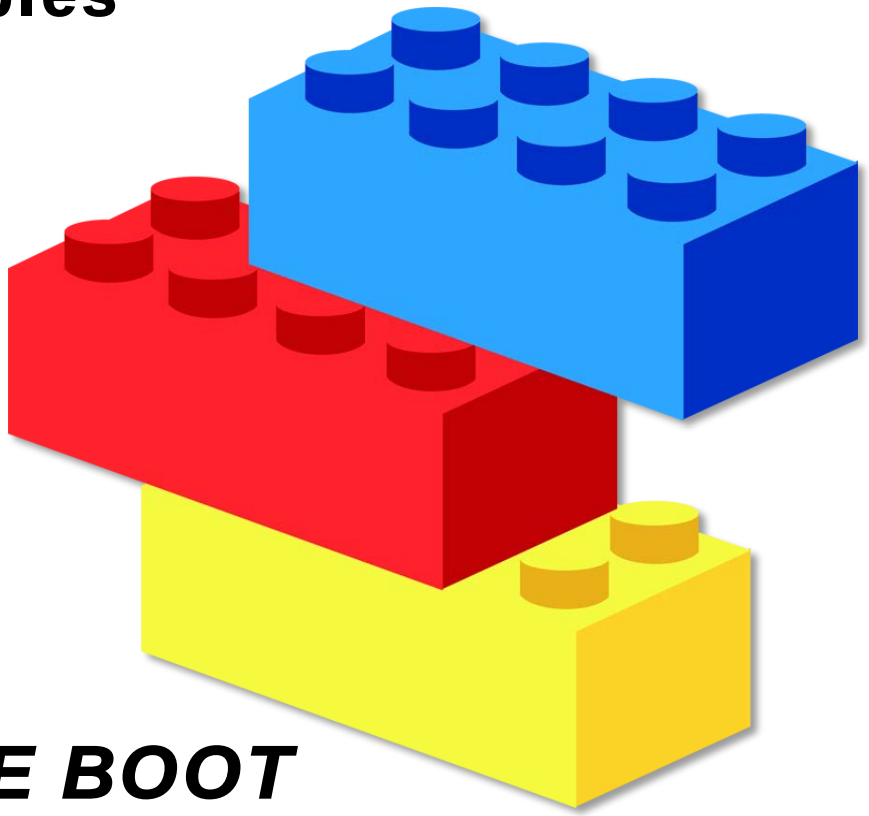
2. Driver Signing

+

3. System Defined Variables

=

UEFI 2.3.1 SECURE BOOT



insyde®

IDF2011
INTEL DEVELOPER FORUM

Secure Boot Begins @ the Factory

Pre-production — **Production** — **User**

Certificate Generating Station @ OEM

OEM collects certificates provided by OSVs, Partners, and OEM's own keys.

"DB Generator" creates the Initial Security Load for new computers.

Initial Security Load is installed onto each computer at the factory, enabling Secure Boot.
1) Initial db and dbx
2) KEK with allowed updaters
3) Platform Key (PK)

After delivery, the OEM or OSV can update with new certificates or revoked certificates*

OEM Responsible for Initializing Secure Boot

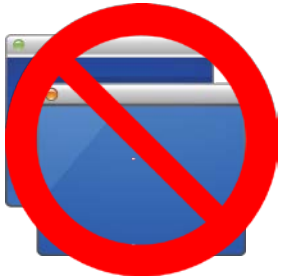
**And OEM can allow User To Disable Secure Boot in 'Setup'*

Secure Boot Protects the User

User attempts to boot a compromised system

OS Boot-loader image checked against pre-loaded database

Root-kit fails checks, user protected by Secure Boot

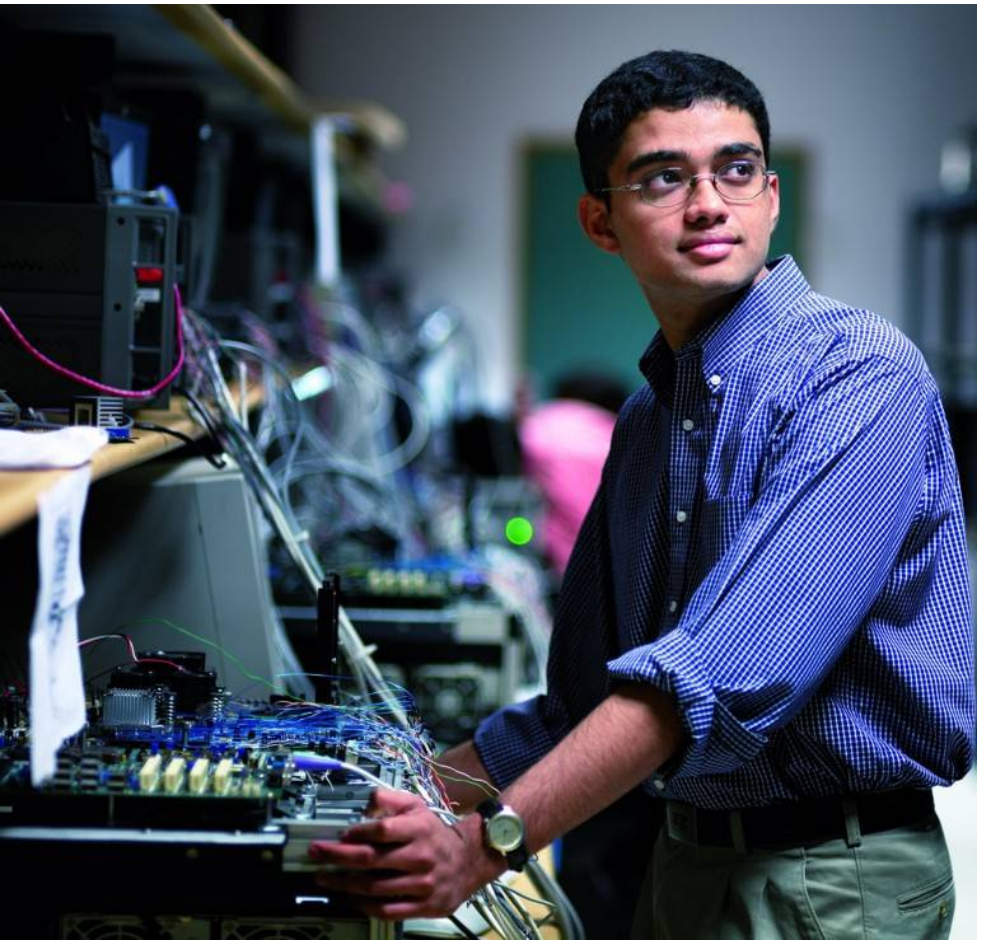


Secure Boot Tests Signatures to Reject Potential Threats

insyde®

IDF2011
INTEL DEVELOPER FORUM

Agenda



- UEFI Specification Updates
- Intel® UEFI Development Kit 2010 (Intel® UDK 2010) Key Features
- Drill Down: Secure Boot in UEFI 2.3.1
- **Implementing a Secure Boot Path with UEFI 2.3.1**

OEM / IHV Guide to UEFI 2.3.1 Secure Boot

- **<u>The Five Elements of Secure Boot Strategy:</u>**

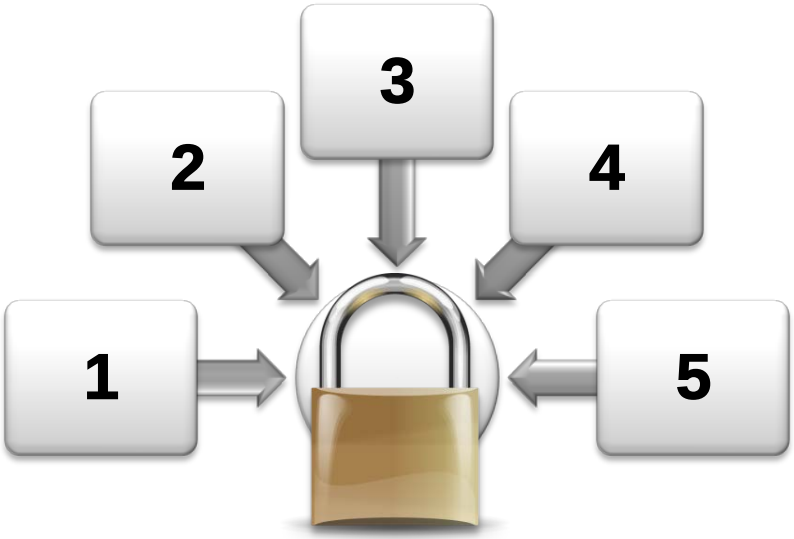
  1. **UEFI Platform Firmware with 2.3.1 implemented and backed by Strong Firmware Security Policies**

  2. **Hardware protection of critical security data**

  3. **Coordination from IBV, IHV and ISV partners**

  4. **UEFI Factory Provisioning and Field Support Tools**

  5. **Secure Firmware Update**



insyde®

IDF2011
INTEL DEVELOPER FORUM

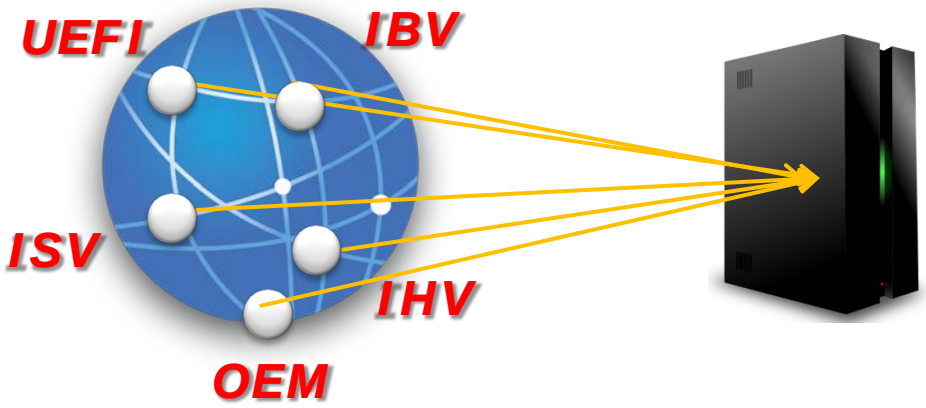
DEMO
Signing Test Tool

Summary

- UEFI 2.3.1 enables key networking and security technologies
- Intel UDK 2010 enables key UEFI features for the industry
- Driver signing and authenticated variables are key tools for constructing UEFI Secure Boot
- OEMs need to implement UEFI Secure Boot as part of an integrated strategy in concert with IHV and ISV partners

Call To Action

- Join UEFI if not already a member
- Download the UEFI 2.3.1 Spec: www.uefi.org
- OEMs need to implement UEFI boot and use UEFI 2.3.1 security features to harden systems
- OEMs must work with IBV, IHV and ISV partners in coordinated approach
- IHVs need to prepare for driver signing



Tunnel Mountain Intel DQTM57 UEFI 2.3.1 platform

Intel® UDK 2010 Compatible, supports UEFI 2.3.1

Pre-assembled systems available at HDNW, visit

http://www.Tunnelmountain.net

tomk@hdnw.com, (425) 943-5515 ext 42234. Use product name "Tunnel Mountain" when ordering

Comes with class 2 CSM and UEFI enabled firmware
Download site has Class 3 UEFI only firmware(nocsm)

Comes with serial port for debug
Can be ordered with optional ITP connector and socketed SPI flash - AC-SPEC4480

Visit **http://developer.intel.com/technology/efi/uefi-ihv.htm** for the latest information and other IHVs collateral

Fall 2011 UEFI Plugfest – Taipei, Oct 24-27

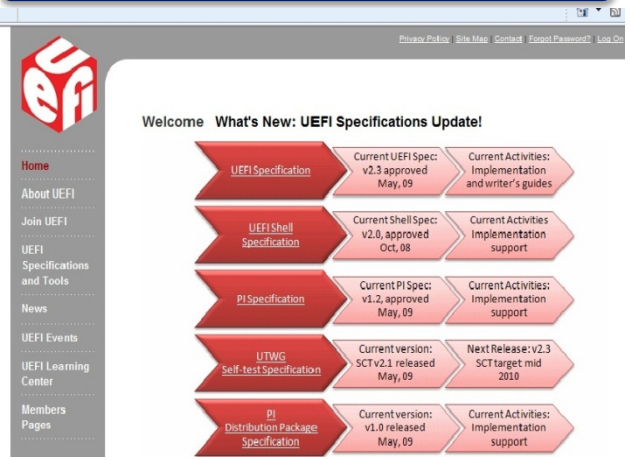
Visit www.UEFI.org for Event Info & Registration

insyde®

IDF2011
INTEL DEVELOPER FORUM

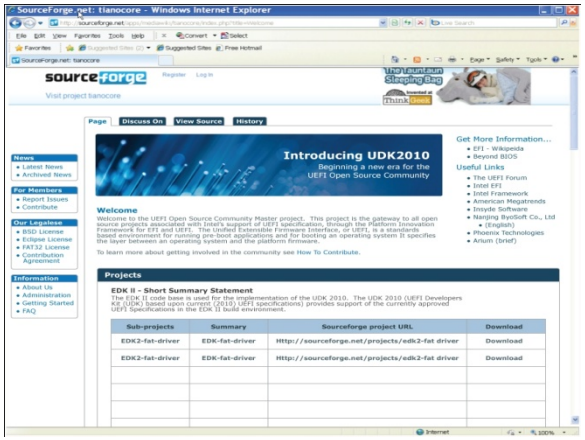
UEFI Industry Resources

UEFI Forum



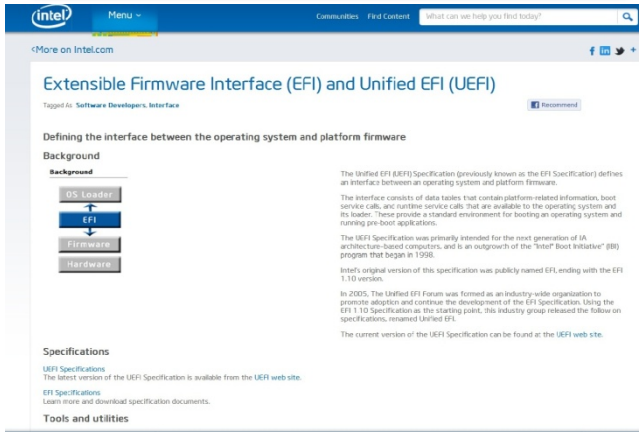
www.uefi.org

UEFI Open Source



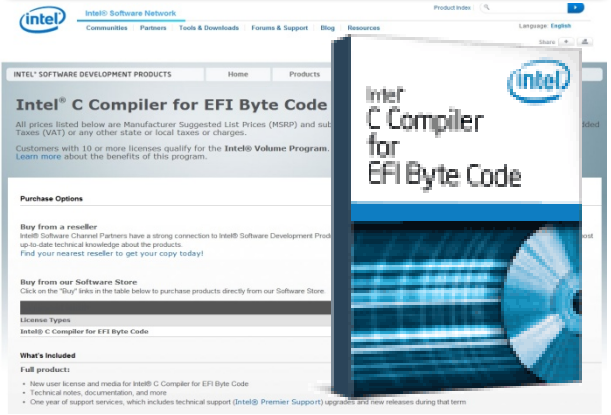
www.tianocore.org

Intel UEFI Resources



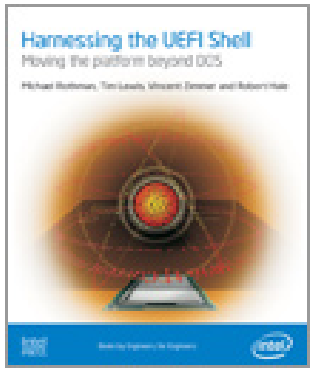
www.intel.com/technology/efi/index.htm

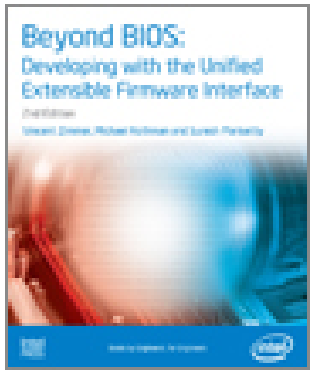
Intel EBC Compiler



http://software.intel.com/en-us/articles/intel-c-compiler-for-efi-byte-code-purchase/

UEFI Books





www.intel.com/intelpress

Training/IHVs Contact

Laurie Jarlstrom
- Intel UEFI Training
- Laurie.Jarlstrom@intel.com

Brian Richardson
- Intel IHVs UEFI Support
- Brian.Richardson@intel.com

IDF2011
INTEL DEVELOPER FORUM

UEFI Sessions Moscone SF IDF 2011

Session	Title	Company	Day / Time	Rm
✓ EFIS001	UEFI Security and Networking Advancements	Intel & Insyde	Tue 1:05 - 2:00	2009
EFIS002	UEFI Innovations for Platform Security	Intel & AMI	Tue 2:10 - 3:00	2009
EFIS003	Beyond DOS: UEFI Modern Pre-boot Application Development Environment	Intel & Phoenix Tech. LTD	Tue 3:20 - 4:10	2009
EFIS004	Designing for Next Generation Best-In-Class Platform Responsiveness	Intel	Tue 4:25 - 5:15	2009
EFIQ001	Hot Topic Q&A: UEFI in the Industry	All Speakers	Tue 5:25 - 6:00	2009
EFIS005	Microsoft* Windows* Platform Evolution and UEFI Requirements	Intel & Microsoft	Thu 1:05 - 1:55	2005
SPCQ003	Hot Topic Q&A: Intel & Microsoft - Windows * 8	Intel & Microsoft	Thu 2:05 - 2:55	2005

✓ = DONE

IDF2011 INTEL DEVELOPER FORUM

Please Fill out the Online Session Evaluation Form

Be entered to win fabulous prizes everyday!

Winners will be announced at 6pm (Day 1/2) and 3:30pm (Day 3)

You will receive an email prior to the end of this session.

Q&A

Legal Disclaimer

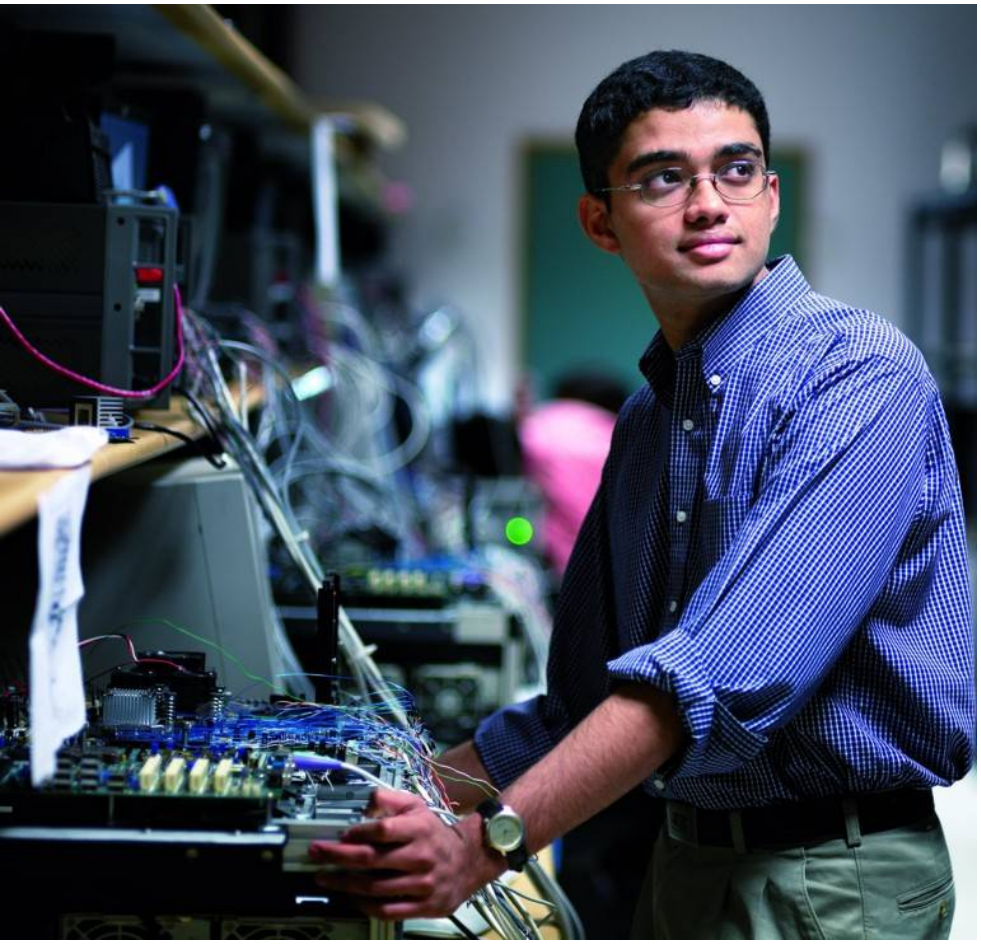
Risk Factors

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. Potential disruptions in the high technology supply chain resulting from the recent disaster in Japan could cause customer demand to be different from Intel’s expectations. 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 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. 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 April 2, 2011.

Rev. 5/9/11

Backup Slides

Agenda Backup



- UEFI Specification Updates
- Intel® UEFI Development Kit 2010 (Intel® UDK 2010) Key Features
- Drill Down: Secure Boot in UEFI 2.3.1
- **Implementing a Secure Boot Path with UEFI 2.3.1**

Element #1: UEFI Platform Firmware with 2.3.1 And Strong Firmware Security Policies

- **UEFI 2.3.1 is an architectural specification**
- **But real security strength is in the policy enforcement**
- **OEM-ACTION→ Policy must lock-out untrusted code including all legacy 16-bit code**
- **But User Experience is key to acceptance:**
  - ***We ship locked-down secure systems but how much freedom should I give users to reconfigure?***
  - ***How does my UI design minimize confusion from users familiar with "less secure" systems?***

insyde®

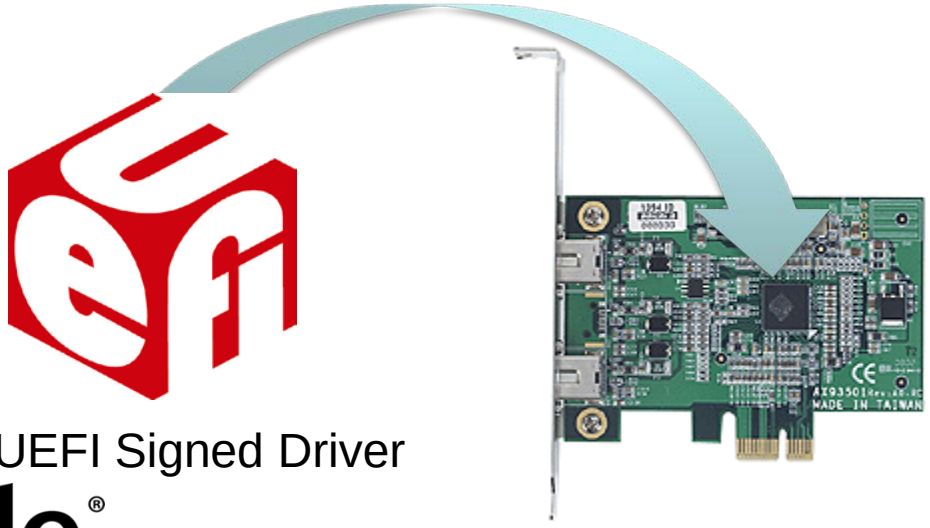
IDF2011 INTEL DEVELOPER FORUM

Element #2: Hardware Protection of Critical Data

- **Hardware protection of the key database is integral to a secure implementation**
- **OEM-ACTION→ Work with your chipset provider and IBV to implement strong protection of critical data**

Element #3: Support from IBV, IHV & ISV Partners

- **OEM-ACTION→ System ROM will need to contain UEFI drivers for all onboard devices (and no legacy drivers)**
- **IHV-ACTION→ Expansion cards will need Signed UEFI drivers**
- **ISV-ACTION→ Pre-boot software tools, for example bootable recovery disk, will need to be Signed**



Element #4: Factory Provisioning

- **Several new steps at the end of the factory flow will be required**

- **OEM-ACTION→ Provision with:**
  - **OSV Certificates**
  - **OEM Support and Update Certs.**
  - **Potentially other Partner Certs.**
  - **Install Platform Key to lock system**

Element #4: . . . And Field Support Tools

- **Any field support tools should be:**
  - **Signed UEFI executable (using UEFI Shell, not DOS)**
  - **Shipped pre-signed by the OEM key**
- **OEM-ACTION→ Examine field support flow, for example**
  - **Consider what users will do to reinitialize replacement motherboards?**
- **Support the future - Enterprise Administrator install of Enterprise key**
  - **Can Enterprise buyer unlock new system and re-provision using your tools?**

insyde®

IDF2011 INTEL DEVELOPER FORUM

Element #5: Secure Firmware Update

- Security level of the Firmware Update must match system goals for security

OEM-ACTION→

1. Sign all Firmware Updates Images
2. Firmware Update process must occur under control of secure firmware
3. H/W Flash Protection must reject any flash writes from unauthorized sources

insyde®

IDF2011
INTEL DEVELOPER FORUM

UEFI 2.3.1 Security Spec Update Backup

UEFI User Identification

Pre-boot Authentication

- **Facilitates appropriate user and platform administrator existence**
- **A standard framework for user-authentication devices**
- **Includes passwords, network auth. protocols, smart cards, USB key & biometric sensors**

Support for various pre-boot authenticators

IDF2011
INTEL DEVELOPER FORUM

UEFI 2.3.1 Security Spec Update

- **Key Management Service (KMS)**
  - Services to generate, store, retrieve, and manage cryptographic keys
  - Based on remote key server, or local Hardware Security Module (HSM), or software
- **Storage Security Command Protocol**
  - Send/receive security protocol defined data to/from mass storage devices
  - Supported command set
    - TRUSTED SEND/RECEIVE (ATA8-ACS)
    - SECURITY PROTOCOL IN/OUT (SPC-4)

UEFI 2.3.1 HII Spec Update

- **Forms Browser Default Behavior**
  - Series of clarifications and guidance for proper handling of default information
- **Modal Form Support**
  - Provide methods to better support UI abstractions that resemble error or confirmation dialogs
- **New opcode for event initiated refresh of browser**
  - Allows for a periodic event to occur which can make the browser aware of the need to refresh context
  - This avoids impractical periodic refreshes which otherwise might affect performance of the underlying firmware
- **Series of errata/clarifications**
  - Proper clarification of questions with no variable storage

Signed File

- **Microsoft* Authenticode* file format**