



UEFI Innovations for Platform Security

Vincent Zimmer, Principal Engineer, Intel Corporation

Zachary Bobroff, Technical Marketing Manager, AMI*

EFIS002

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.**

Agenda

- **Introduction**
 - Necessity of Secure Flash Update
 - NIST Background
- **Secure Flash Update Concepts**
 - Overview of Secure Flash Implementation
 - Demo of ASFU
- **Security and Platform Policy**
 - Overview of UEFI Platform Policy
 - Platform Policy Demonstration
- **Summary and Call to Action**

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

<http://intel.com/go/idfsessions>

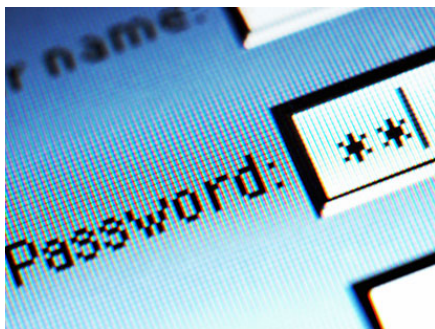
The URL is also in the Session Agenda Pages of the Pocket Guide

A photograph of a server room with rows of blue server racks. Two people are walking from left to right in the foreground, slightly blurred. The word "Introduction" is overlaid in white text on the right side of the image.

Introduction

Basic Introduction...

- **Platform security is a broad topic...**
 - Many technologies work together for platform security.
 - Includes TPM, TXT, secure boot, and secure flash update
- **Security Should...**
 - Prove the machine has booted in a trusted state
 - Protect the system against attacks
 - Provide a means for user authentication
- **From a usability standpoint security can be defined as:**
“Something you know, something you have, or something you are...”



Securing the Software Stack

- UEFI 2.3.1 security enhancements specifically address the “secure boot” issue
 - *See Session EFIS001 for more details...*
- Securing the firmware itself further strengthens the UEFI Secure Boot concept
 - *How is the firmware update protected?*
 - *How is the firmware put into “admin mode”?*
- NIST has created **BIOS Protection Guidelines**
 - Secure flash update requirements ([PDF](#))
 - Maintain firmware core root of trust
- UEFI 2.3.1 contains the framework to develop secure flash update on Intel silicon



NIST Implementation Requirements

The NIST BIOS Protection Guidelines break down to three basic requirements...

1. The BIOS must be protected
2. BIOS updates must be signed
3. BIOS protection cannot be bypassed



Achieving Secure Flash Update

- Intel chipsets already contain mechanisms to implement physical protection of the flash part
 - Features vary depending on chipset
 - Contact Intel for more details
- System firmware can leverage UEFI 2.3.1 concepts to implement image verification and non-bypassability for secure updates



UEFI 2.3.1 provides the security framework to implement secure flash update on Intel silicon

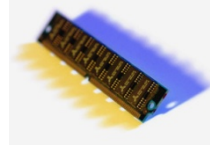


Secure Flash Update Concepts

Secure Flash Update Methods

- Implemented using capsules defined by UEFI spec

- *Capsule ("Capsule-in-Memory")*



- Capsule is put in memory by an application in the OS
- Mailbox event is set to inform BIOS of pending update
- System reboots, verifies the image and update is preformed securely by the BIOS

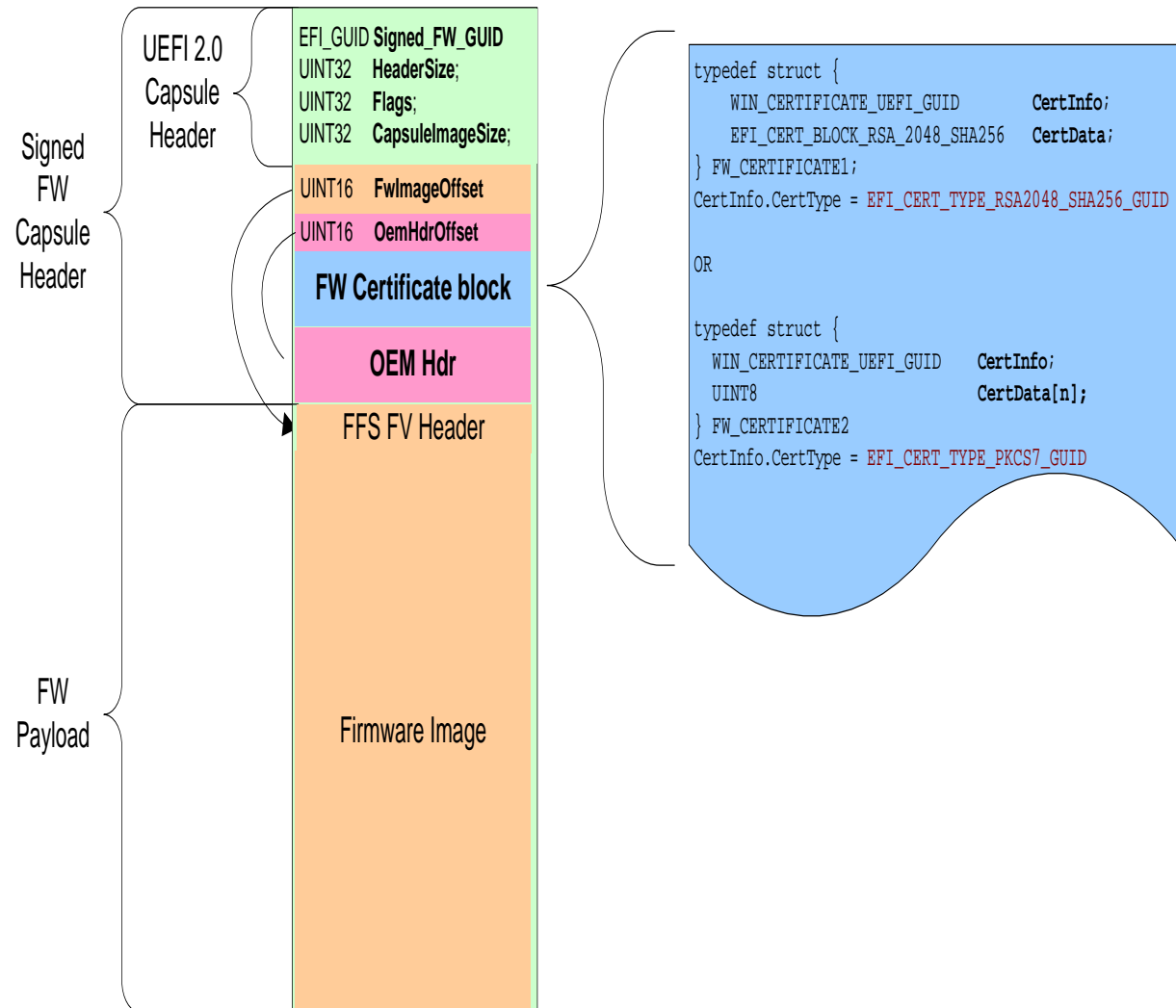
- *Recovery ("Capsule-on-Disk")*



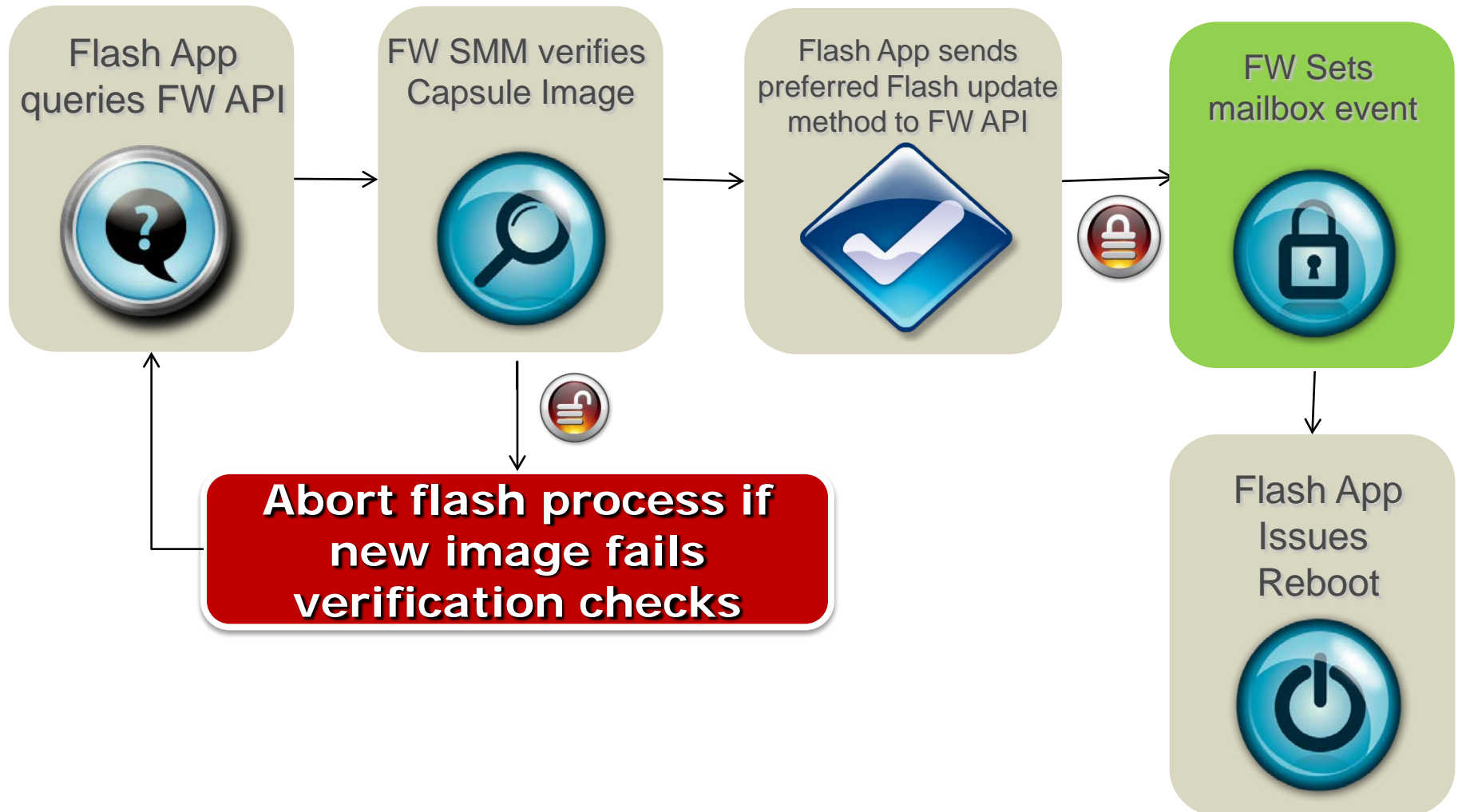
- Capsule is stored on a predefined disk and is loaded to memory during BIOS booting
- Mailbox event is set to inform BIOS of pending update
- System reboots, verifies the image and update is preformed securely by the BIOS

Signed FW Capsule

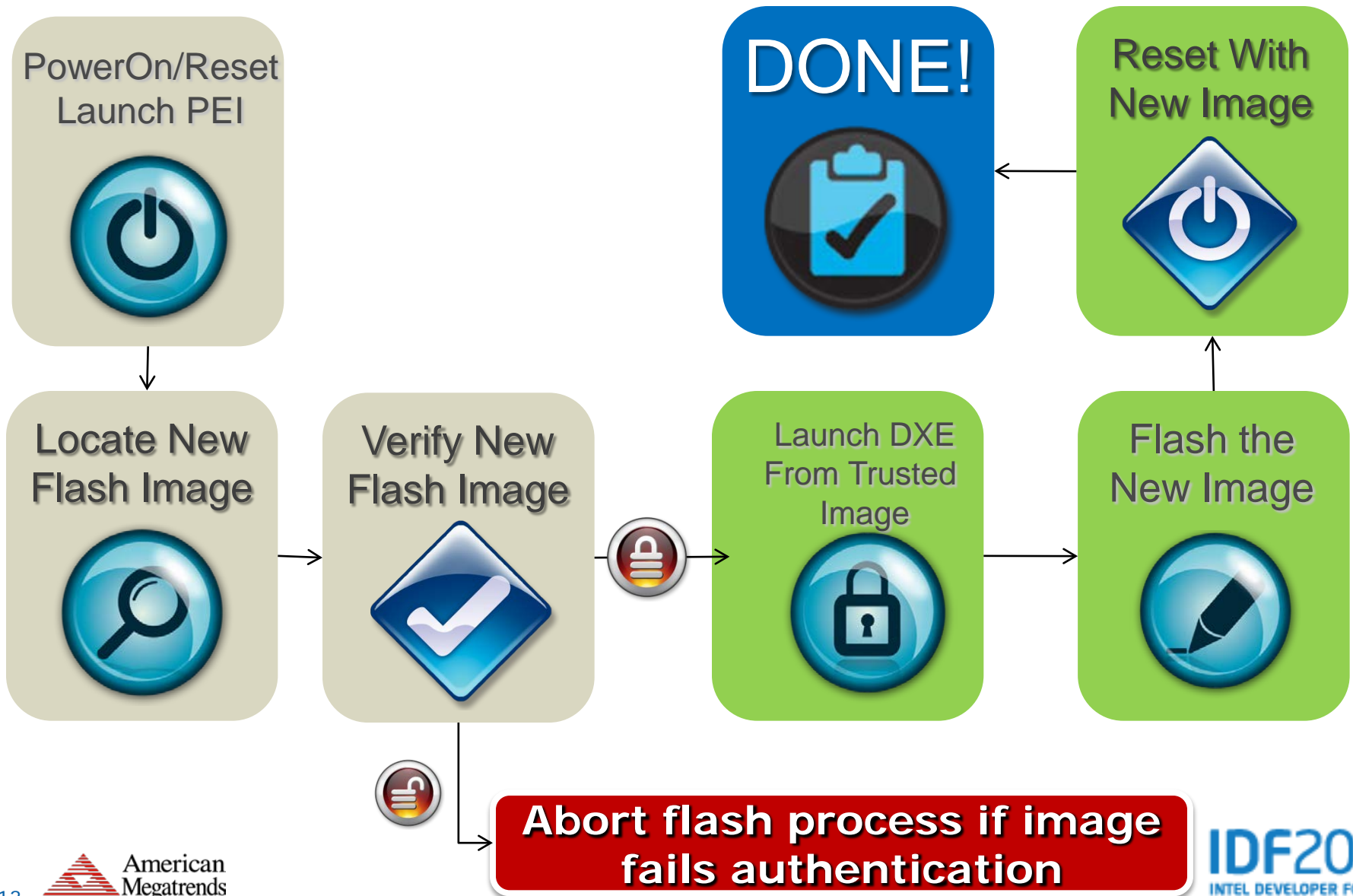
- Image is a combination of the firmware payload with the firmware certificate
- OEM Header and UEFI - defined Capsule Structure



Secure Flash Update Process



Secure Flash Update Process



Secure Flash Update Methodology

- Use UEFI Firmware Capsule method as the preferred image delivery mechanism
- Use digital signatures to authenticate the image as defined by UEFI 2.3.1
 - Industry approved Digital signature protocols
 - EMSA PKCS v1.15, RSA PSS signature schemas
 - 2048 bit RSA Key, SHA256 hash (NIST requirement)
- Use chipset features to prevent unauthorized updates to the flash part
 - Chipset dependent: check Intel specs for details



Secure flash update is an integral part of maintaining system security

Secure Flash Update Demonstration

- The following will be demonstrated:
 - The capsule update method using AMI ASFU (AMI Secure Flash Update) Utility
 - A modified binary will be used to simulate a malicious BIOS update
 - A binary modified after signing will have an invalid signature



American
Megatrends

Security and Platform Policy



Platform Policy Background

- Currently BIOS user authentication is used to check credentials to enable booting or choosing what type of information to display in setup
- Creating a UEFI credential provider allows to extend the usage of devices like fingerprint scanners to the preboot space
- Drivers and UEFI applications can be limited in usage and/or functionality to certain authorized users



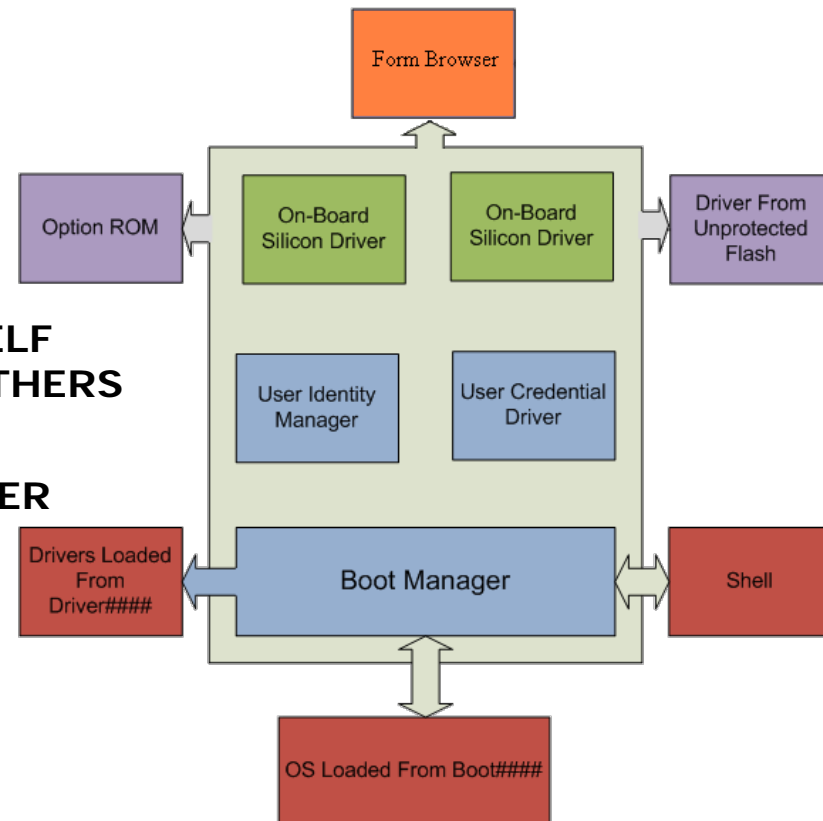
User Credentials Management

- Chapter 31 of the UEFI specification provides a standard method of user authentication and the defines following components:
 - User Identity Management Driver: Manages the process of determining the users identity
 - User Enrollment Manager: Application that enrolls new users
 - Deferred Image Load: Manages if drivers can be loaded by a user
 - Credential Provider Drivers: Manage authenticating a class of credentials
- There are different classes of credential providers listed in the specification. Examples are:
 - EFI_USER_CREDENTIAL_CLASS_PASSWORD
 - EFI_USER_CREDENTIAL_CLASS_SMART_CARD
 - EFI_USER_CREDENTIAL_CLASS_FINGERPRINT



User Management Drivers

- User identity managers, user credential drivers, and on-board drivers are located in the flash and are trusted
- User identity managers handle the users information and a user's associated capabilities
 - Ability to modify setup options
 - `EFI_USER_INFO_ACCESS_SETUP`
 - Execution of selected drivers
 - `EFI_DEFERRED_IMAGE_LOAD`
 - User Enrollment privileges
 - `EFI_USER_INFO_ACCESS_ENROLL_SELF`
 - `EFI_USER_INFO_ACCESS_ENROLL_OTHERS`
 - Control available boot order
 - `EFI_USER_INFO_ACCESS_BOOT_ORDER`



Platform Policy Implementations

- **BIOS user authentication can also be paired with operating systems to allow for a seamless single sign on**
- **Using UEFI provided abstractions for network, the user can also be authenticated with a corporate sever**

New authentication sources can be integrated by following the protocol definitions in the UEFI specification



Fingerprint Reader Demonstration

- Through fingerprint authentication the user can alter the boot flow with previously enrolled fingers.
- Depending on the finger swiped the system will take one of the following actions:
 - Not allow any action (the user is not verified)
 - Fingerprint enrollment
 - Boot to setup
 - Boot to windows



Summary and Call to Action

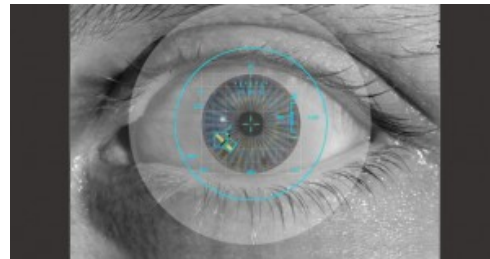


Summary

- **UEFI 2.3.1 provides the security framework to implement secure flash update on Intel silicon**
- **Secure flash update is an integral part of maintaining system security**
- **New authentication sources can be integrated by following the protocol definitions in the UEFI specification**

Call to Action

- Review NIST BIOS protection guidelines
 - NIST Special Publication [800-147](#)
- Secure flash update ensures that all BIOS updates come from a trusted source and are genuine
- Implementing user authentication according to the UEFI specification can enable an OEM or ODM the ability to allow users to authenticate using new sources
 - For assistance implementing your new credential sources please visit AMI's [website](#)



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

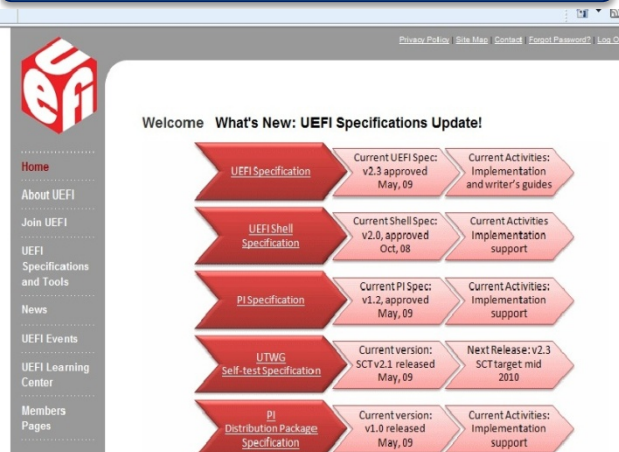
Fall 2011 UEFI Plugfest – Taipei, Oct 24-27



Visit www.UEFI.org for Event Info & Registration

UEFI Industry Resources

UEFI Forum

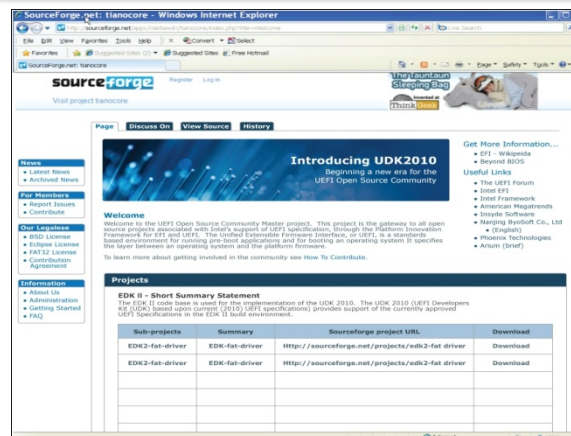


Welcome What's New: UEFI Specifications Update!

Specification	Current Version	Current Activities
UEFI Specification	Current UEFI Spec: v2.3 approved May, 09	Current Activities: Implementation and writer's guides
UEFI Shell Specification	Current Shell Spec: v2.0, approved Oct, 08	Current Activities: Implementation support
PI Specification	Current PI Spec: v1.2, approved May, 09	Current Activities: Implementation support
UTWG Self-test Specification	Current version: SCT v2.1 released May, 09	Next Release: v2.3 SCT target mid 2010
PI Distribution Package Specification	Current version: v1.0 released May, 09	Current Activities: Implementation support

www.uefi.org

UEFI Open Source



SourceForge.net: tianocore - Windows Internet Explorer

Introducing UDK2010
Beginning a new era for the UEFI Open Source Community

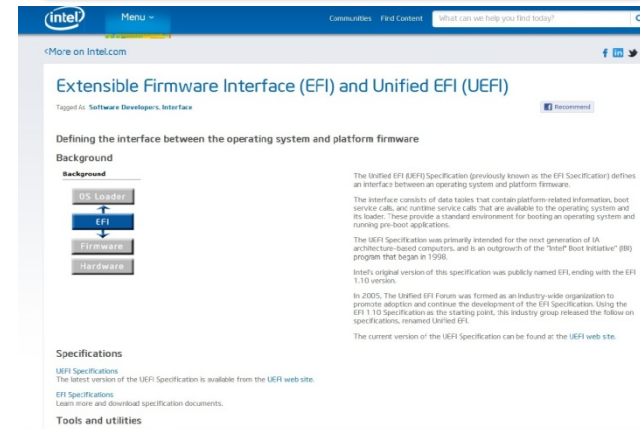
Welcome to the UEFI Open Source Community project. This project is the gateway to all open source projects associated with Intel's support of UEFI specifications, through the Platform Innovation Framework for EFI and UEFI. The Unified Extensible Firmware Interface, or UEFI, is a standards-based environment for running pre-boot applications and for booting an operating system. It specifies the layer between an operating system and the platform firmware.

To learn more about getting involved in the community see How To Contribute.

Sub-projects	Summary	Sourceforge project URL	Download
EDK2-fat-driver	EDK2-fat-driver	http://sourceforge.net/projects/edk2-fat-driver	Download
EDK2-fat-driver	EDK2-fat-driver	http://sourceforge.net/projects/edk2-fat-driver	Download

www.tianocore.org

Intel UEFI Resources



Extensible Firmware Interface (EFI) and Unified EFI (UEFI)

Tagged in: Software Developers, Interface

Defining the interface between the operating system and platform firmware

Background

OS Loader
↓
EFI
↓
Firmware
↓
Hardware

Specifications

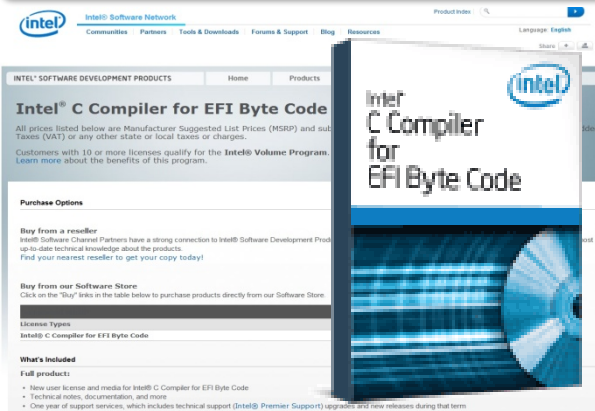
UEFI Specifications
The latest version of the UEFI Specification is available from the UEFI web site.

EFI Specifications
Learn more and download specification documents.

Tools and utilities

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

Intel EBC Compiler



Intel® Software Network

Intel® C Compiler for EFI Byte Code

All prices listed below are Manufacturer Suggested List Prices (MSRP) and not Taxes (VAT) or any other state or local taxes or charges.

Customers with 10 or more licenses qualify for the Intel® Volume Program. Learn more about the benefits of this program.

Purchase Options

Buy from a reseller
Intel® Software Channel Partners have a strong connection to Intel® Software Development Products up-to-date technical knowledge about the products.
Find your nearest reseller to get your copy today!

Buy from our Software Store
Click on the "Buy" links in the table below to purchase products directly from our Software Store.

License Types

Intel® C Compiler for EFI Byte Code

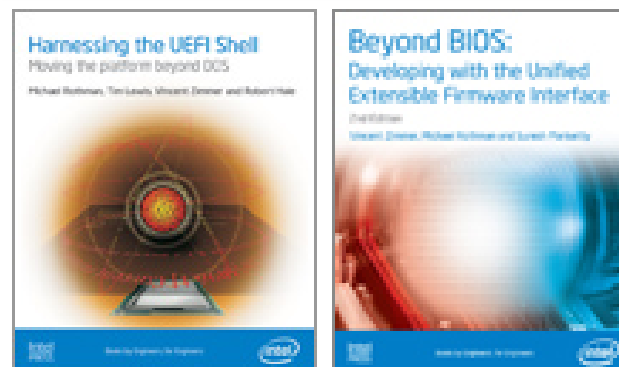
What's Included

Full product:

- New user license and media for Intel® C Compiler for EFI Byte Code
- Technical notes, documentation, and more
- One year of support services, which includes technical support (Intel® Premier Support) upgrades and new releases during that term

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

UEFI Books



Harnessing the UEFI Shell
Moving the platform beyond BIOS
Michael Hoffmann, Tim Leach, Vincent (Emerson) and Robert (Haller)

Beyond BIOS: Developing with the Unified Extensible Firmware Interface
David Williams
Steven Dimes, Michael Hoffmann and Loretta Moriarty

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

www.intel.com/intelpress

UEFI Sessions Moscone SF IDF 2011

Session ID	Title	Company	Day / Time	Rm
✓ EFIS001	UEFI Security and Networking Advancements	Intel & Insyde SW	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 8 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

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

- 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. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.
- Intel may make changes to specifications and product descriptions at any time, without notice.
- All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.
- Intel, processors, chipsets, and desktop boards 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.
- Other code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user
- Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.
- 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
- 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, 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.
- Copyright ©2011 Intel Corporation.

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