IDF13

Using UEFI for Secure Firmware Update of Expansion Cards

Brian Richardson – Sr. Technical Marketing Engineer, Intel Corporation

Jeff Bobzin – Vice President, Insyde Software

Terry Kirch – Senior Principal Engineer, Emulex

STTS003

intel Look Inside.™

Agenda

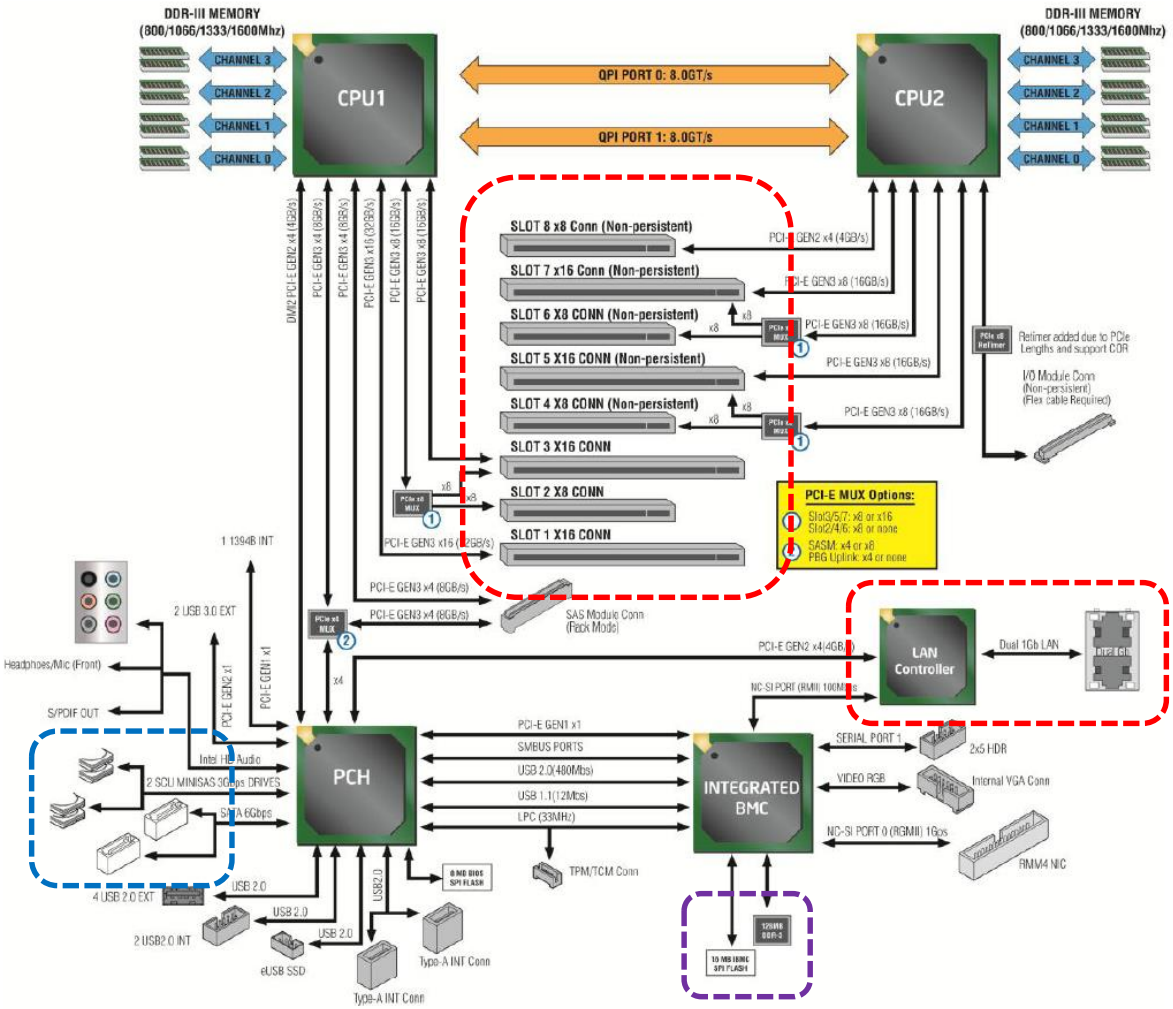
- Protecting the Firmware Update Process
- Security Enhancements in UEFI 2.4
- Securing the Firmware Update Process
- Pre-OS UEFI Secure Firmware Update with FMP

Agenda

- Protecting the Firmware Update Process
- Security Enhancements in UEFI 2.4
- Securing the Firmware Update Process
- Pre-OS UEFI Secure Firmware Update with FMP

Attacking "Other" Firmware

Enterprise systems use multiple firmware images…



Problems:

- Mixed update tools (Legacy & UEFI)
- Staging updates across enterprise environment
- Multiple attack surfaces exist before OS loads

- UEFI & Baseboard Management Controller (BMC) Firmware
- UEFI Driver & Option ROM (OpROM)
- Storage Firmware

Areas for Improvement

- Microsoft defines *EFI System Resource Table* (ESRT) for Windows* 8 systems
  - Described in "Windows UEFI Firmware Update Platform"
  - Currently used for "connected standby" devices

  Is a similar method applicable to other OS?

- Many vendors already use Firmware Management Protocol (FMP) for updates…
  Can FMP be hardened to meet NIST[1] requirements?

- UEFI provides an infrastructure for security…
  How can this be utilized in the update process?

Expansion board security is a key element of platform security

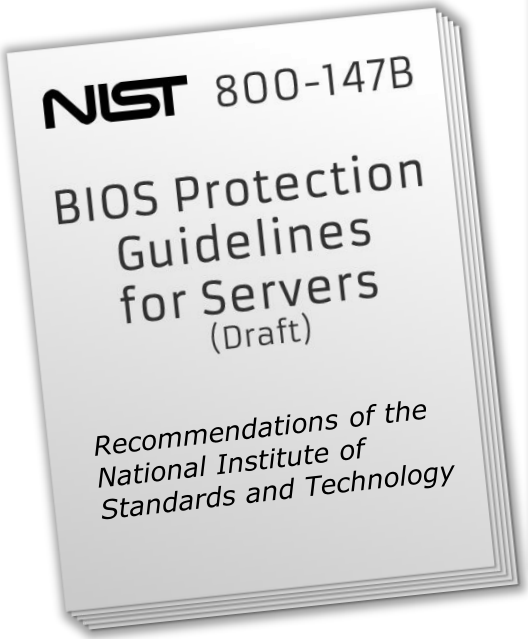
[1]National Institute of Standards Technology (NIST)

Agenda

- Current State of Firmware Security
- Security Enhancements in UEFI 2.4
- Securing the Firmware Update Process
- Pre-OS UEFI Secure Firmware Update with FMP

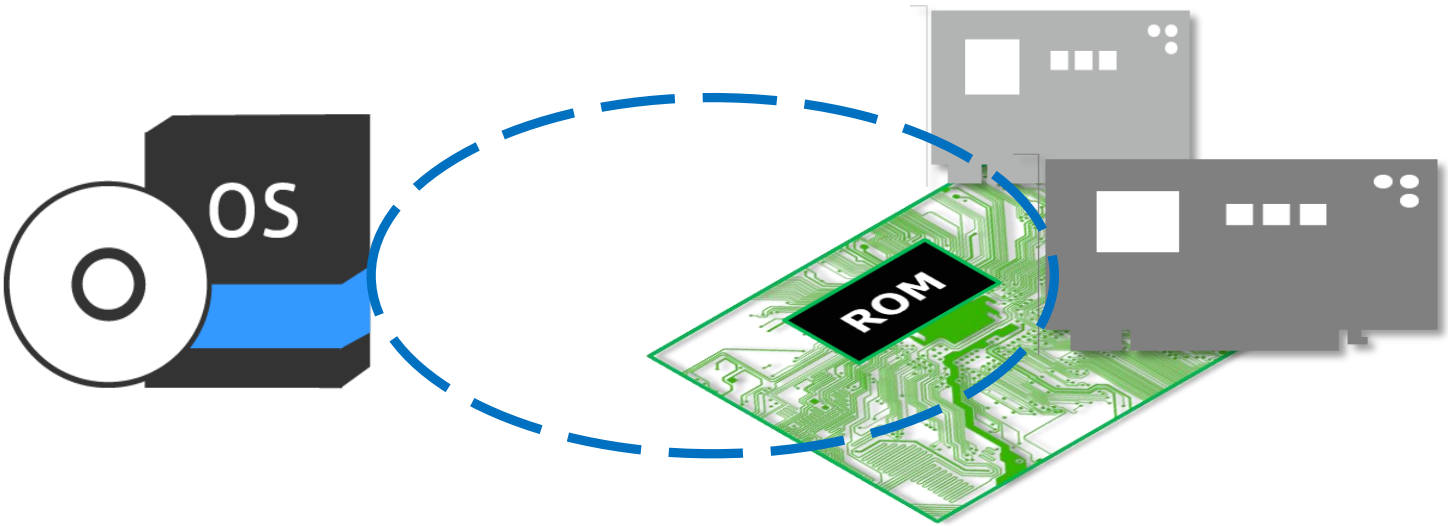
Industry Trend is for Increased Security

- System Manufacturers in Enterprise Segment must add security for
  - NIST Compliance
  - OS Requirements
  - Customer Demand

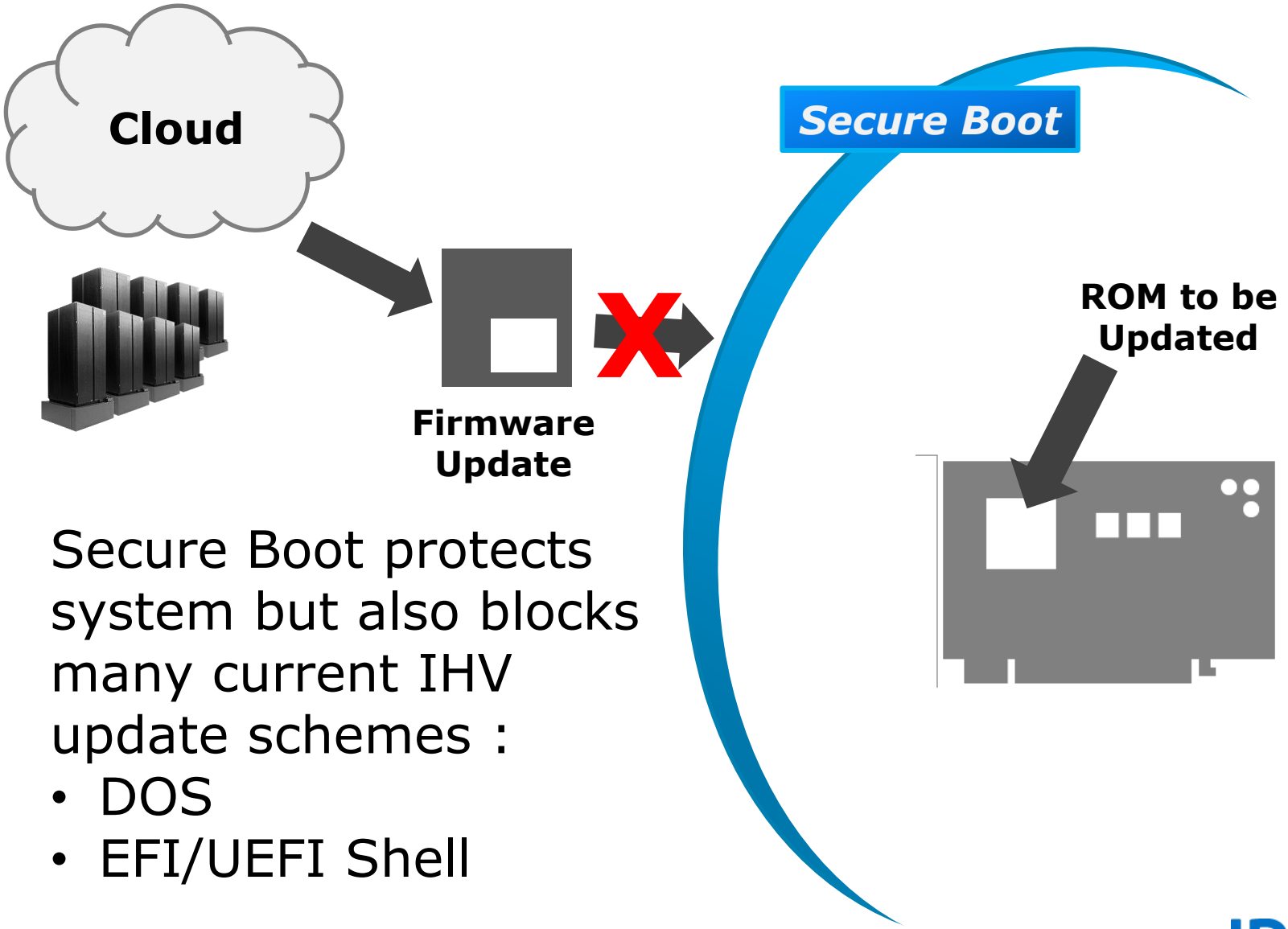


Added Security for Firmware Protection

- All firmware components must be protected from unauthorized alteration
  - System firmware
  - Option ROMs on expansion boards
- Still need to allow authorized firmware updates!



But IHV Firmware Update Methods Are Blocked



Secure Boot protects system but also blocks many current IHV update schemes :

- DOS
- EFI/UEFI Shell

How UEFI Secure Boot Protects

- UEFI Secure Boot is a technology to eliminate a major security hole during handoff from UEFI firmware to UEFI OS
- Option ROMs and OS boot-loaders need to be signed by private key corresponding to a certificate in the systems security database
- Database is always provisioned at factory and maintained by OS if required for revocation

Microsoft* hosts a CA for UEFI use

- UEFI Option ROMs need to be signed by a widely trusted Certificate Authority
- Microsoft* has CA experience and volunteered to host the first all-industry UEFI CA
- Manufacturers are encouraged to put MS CA certificate into "Allowed" database
- In addition to Signing Option ROM Images, MS CA can be used to sign Option ROM Secure Update Drivers

Microsoft CA Signing Makes Update Universal

IDF13

UEFI Supports IHV Firmware Management

1. UEFI has Firmware Management Protocol (FMP)
   - UEFI Specification defines a rich Firmware Management Protocol with functions for
     - Get Current Version and Update ID
     - Validate Update
     - Install an new image
     - Maintain Package Information

2. UEFI has UpdateCapsule Interface
   - Interface to deliver Updates to Firmware
   - Boot Services and Run Time Support
   - But Implementing Run Time Delivery has been challenging

UEFI 2.4 Spec Was Recently Released

New in UEFI 2.4 for Secure Firmware Update:

1. **Define capsule format containing FMP updates**

   Clarifies usage of Capsule for FMP

2. **Deliver capsule on boot disk**

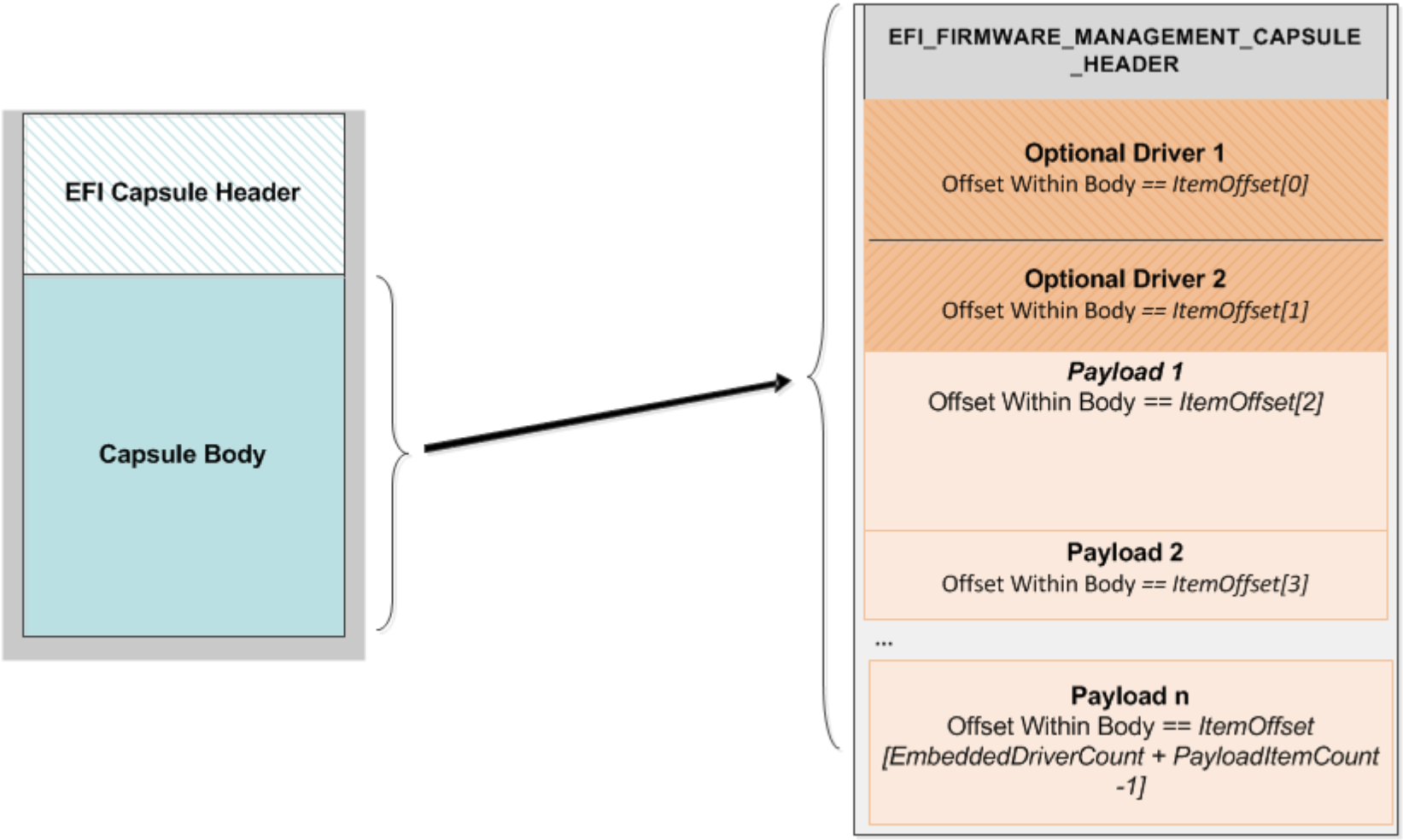
   Stage update in OS

   Process update in secure firmware state

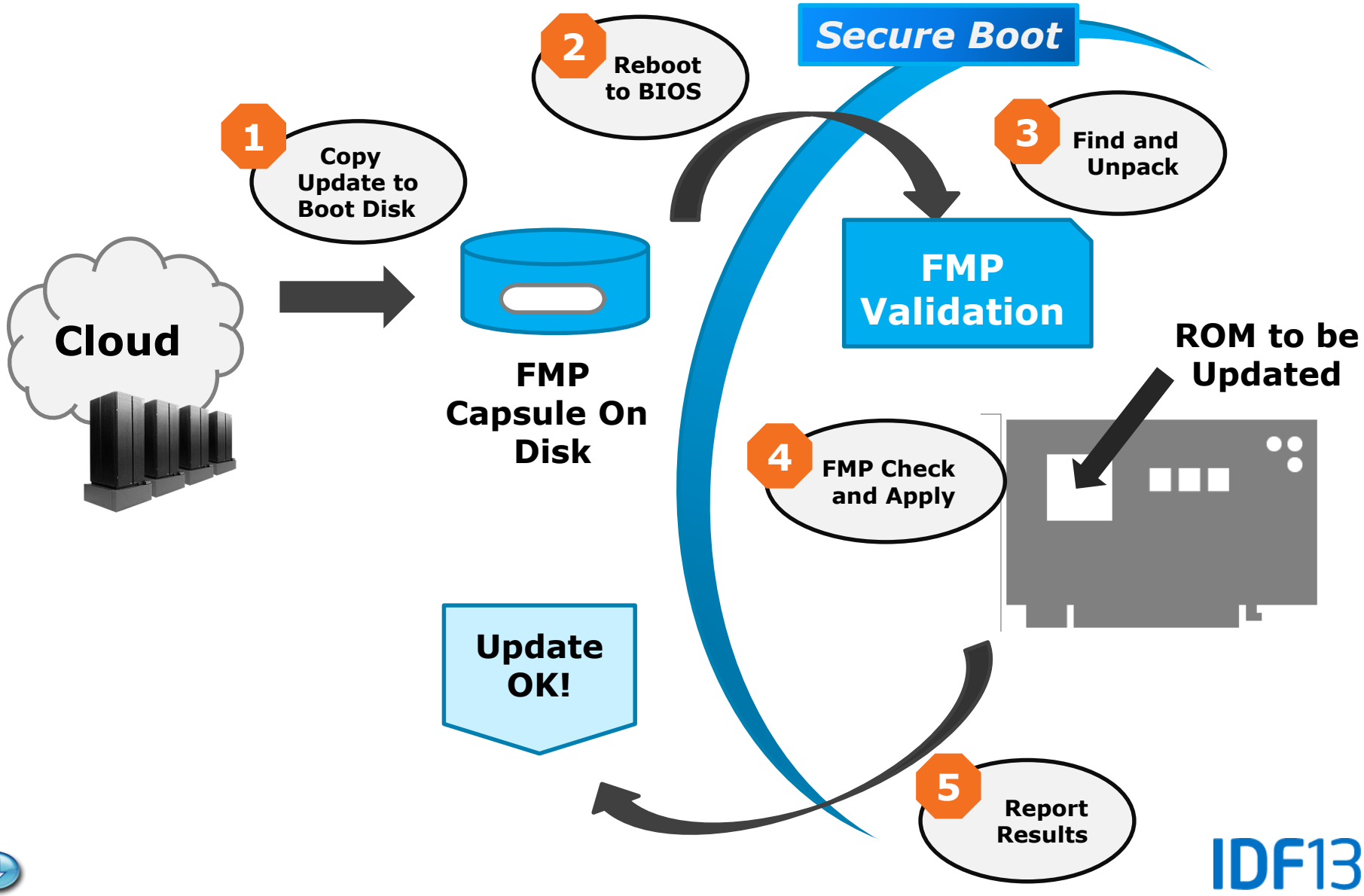
3. **Variable with capsule processing status**

   Report results back to OS context

New FMP Capsule Delivers - Optional Update Drivers and Multiple Payloads



Using UEFI 2.4, Update is Delivered Added Security



UEFI Responsive to Industry Needs

- Requirement for Secure Update for expansion cards
- UEFI WG brings together OS, OEM, IHV, and IBV
- Version 2.4 delivers workable solution

UEFI 2.4 Offers New Tools for Update

Agenda

- Current State of Firmware Security
- Security Enhancements in UEFI 2.4
- Securing the Firmware Update Process
- Pre-OS UEFI Secure Firmware Update with FMP

Requirement to Verify Update Image

- Chain of trust requires –
  1. Firmware checks signature of Option ROM and any Update Driver
  2. Trusted update code checks the signed update image

- Three examples follow to explain validation

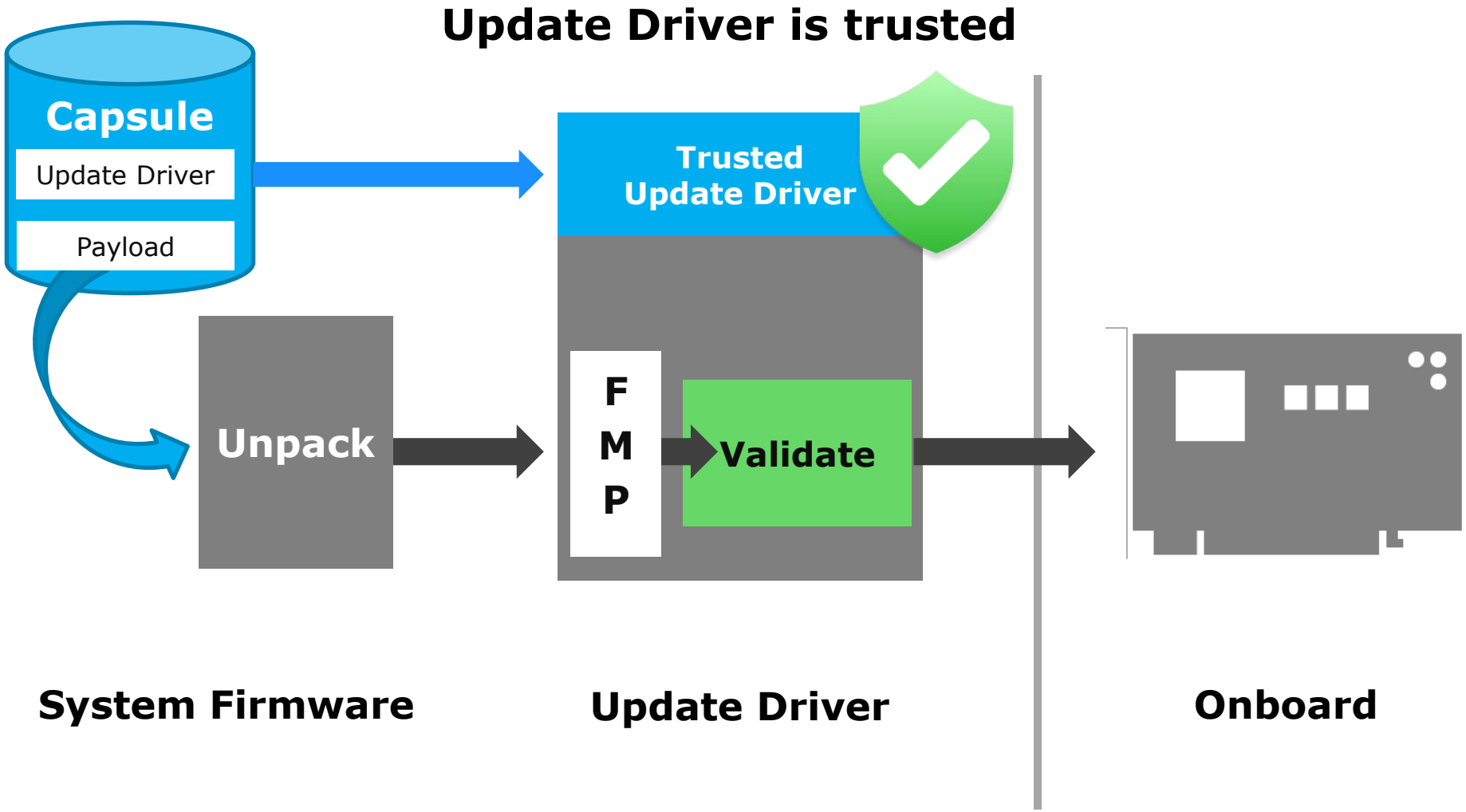
①**Protected.** Signed driver downloaded with update.

②**More Protected.** Signed option ROM on card.

③**Most Protected.** Device firmware.

Downloaded Driver Validation (No FMP Available in the Card)

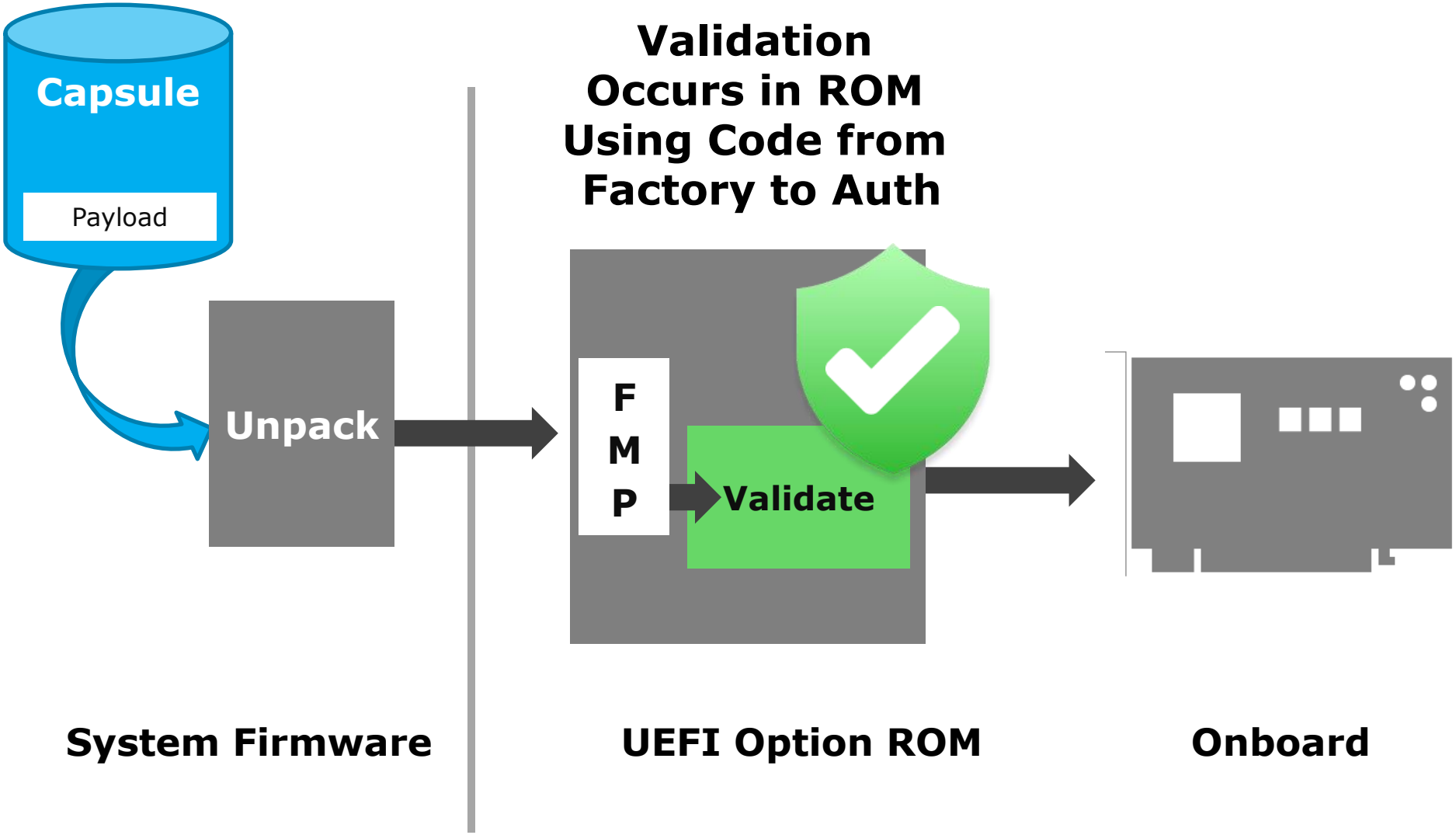
① Protected!



IDF13

Option ROM Does Validation (Secure FMP in Option ROM)

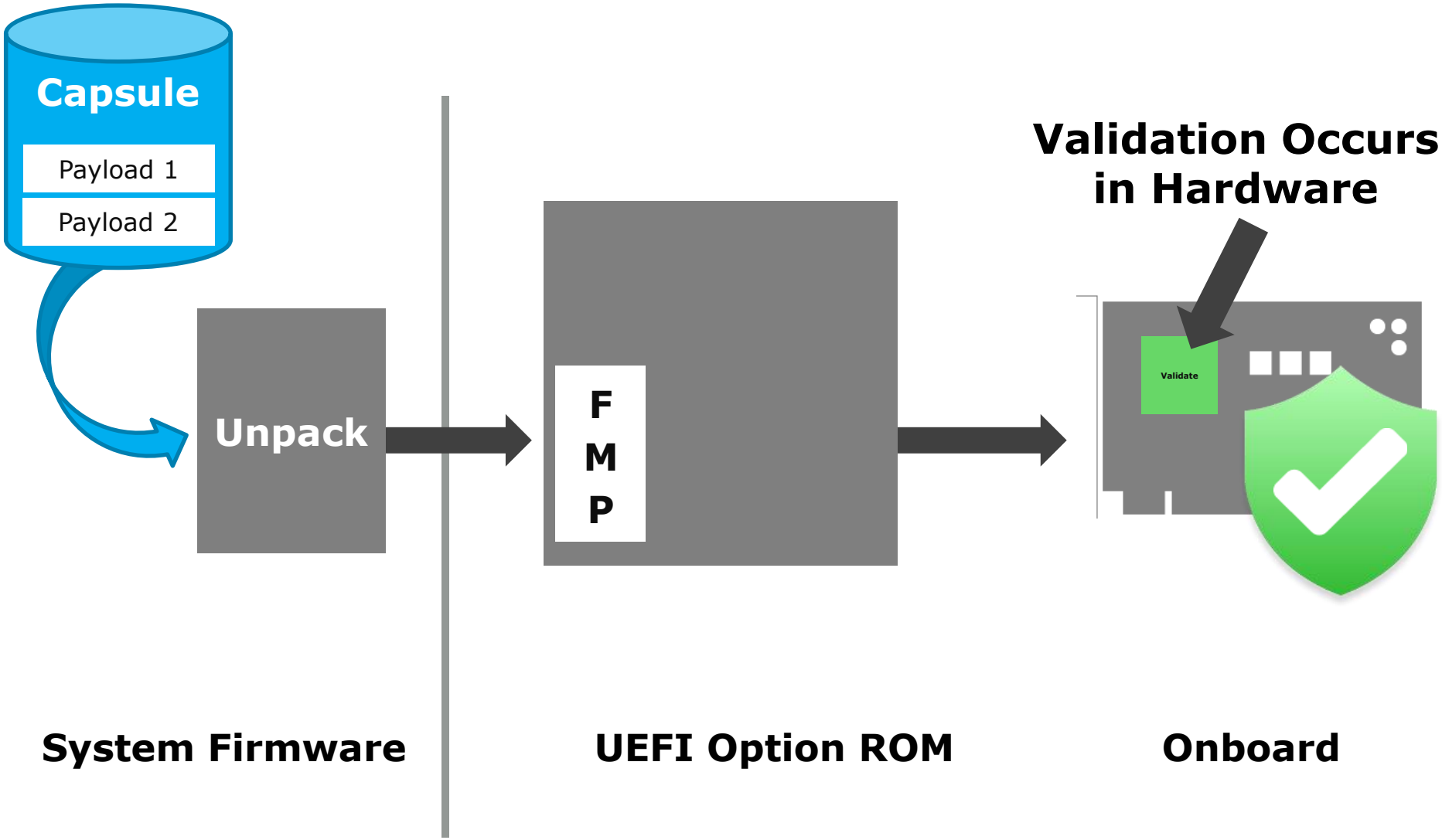
② MORE Protected!



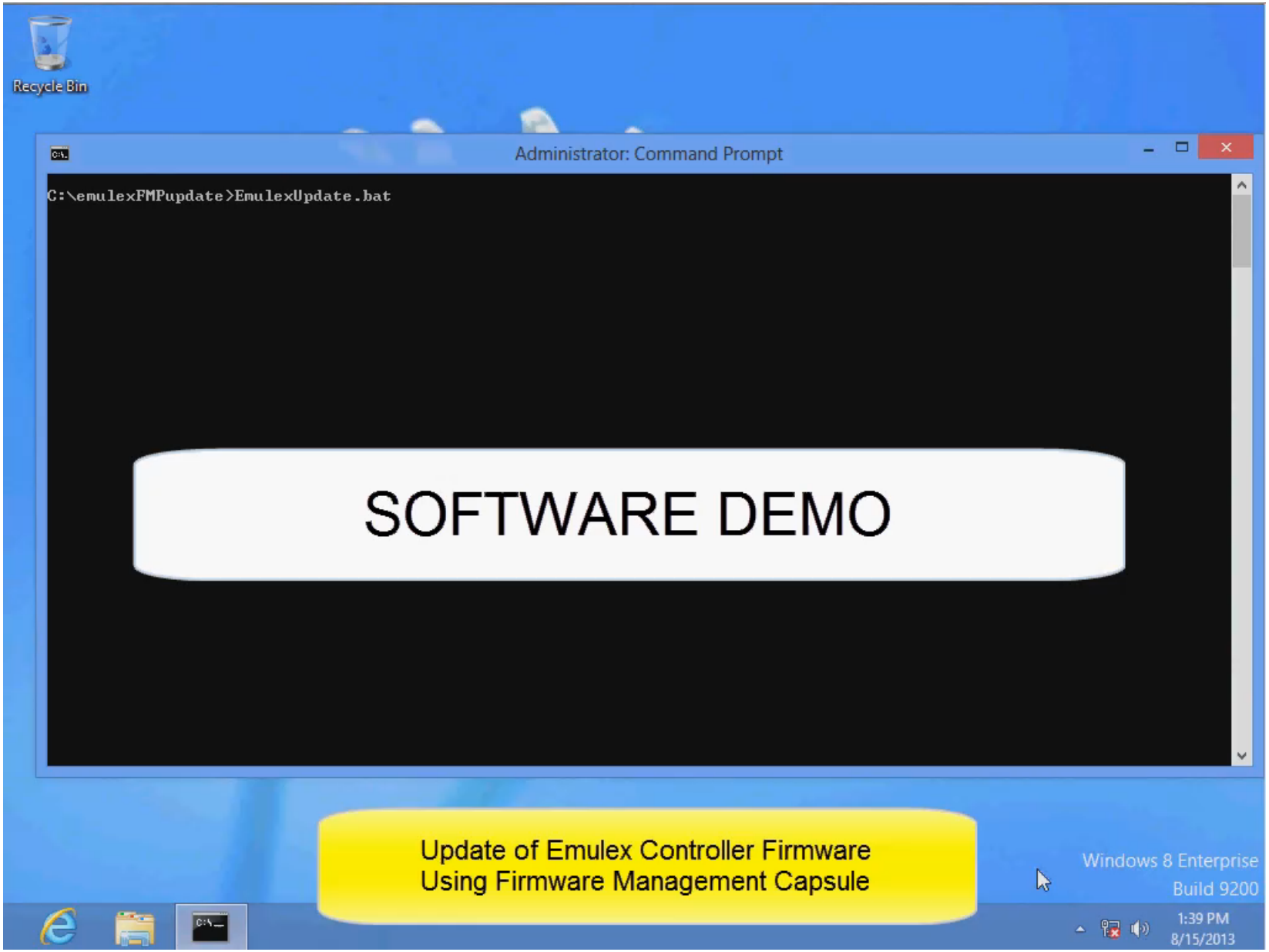
IDF13

③ MOST Protected!

Device Engine Does Validation



IDF13


Recycle Bin
Administrator: Command Prompt
C:\emulexFMPupdate>EmulexUpdate.bat
SOFTWARE DEMO
Update of Emulex Controller Firmware
Using Firmware Management Capsule
Windows 8 Enterprise
Build 9200
1:39 PM
8/15/2013

IHVs Feedback Needed

- Current design as reflected in UEFI 2.4 specification is powerful and flexible

- UEFI working group is looking for feedback from IHVs. For example, some ideas:
  - Platform firmware could expose generic validation routines to assist IHV code in authentication
  - Clarifications of methods for write-protecting firmware store before leaving root-of-trust environment
  - User Interface through DRIVER_HEALTH_PROTOCOL

- If your company is not a member – Join UEFI!
- IHVs – we need your input!

UEFI Offers Solutions for Security Requirements

Agenda

- Protecting the Firmware Update Process
- Security Enhancements in UEFI 2.4
- Securing the Firmware Update Process
- Pre-OS UEFI Secure Firmware Update using FMP

Vulnerable

Pre-OS UEFI Secure Firmware Update with FMP

Non-Secure Legacy Firmware Update Methods

- Utility in DOS
- EFI Shell with shell DRVCFG application (direct or through FMP)
- OS Runtime Utility from IHV

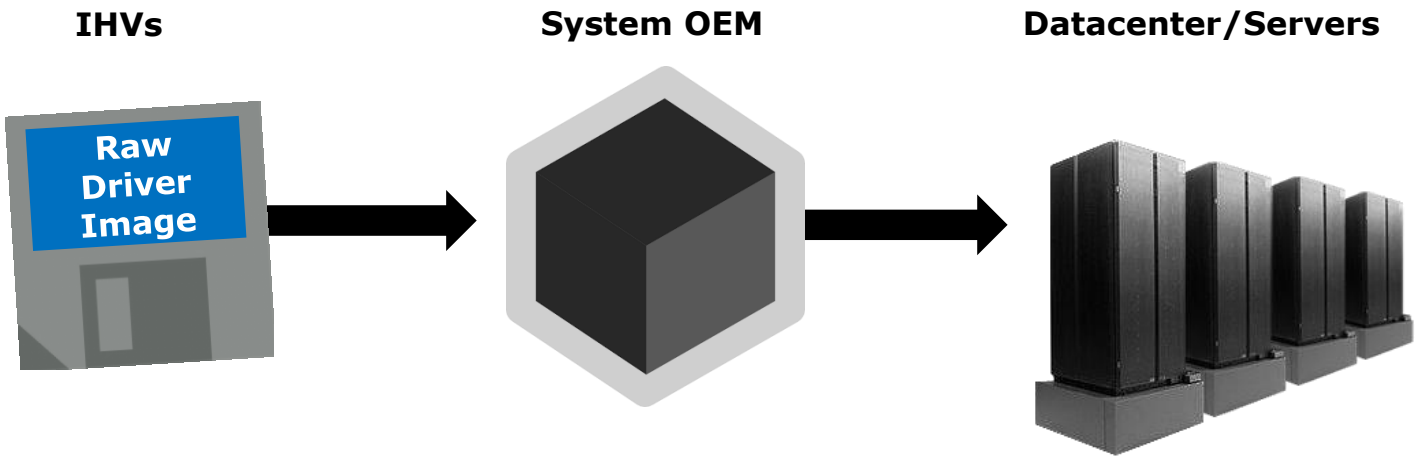
Pros

- Simple delivery method

Cons

- Untrusted OS with weak security methods
- Rogue binary can be substituted
- Difficult to implement hardware write protect

System OEM Handles Update Delivery



Pros

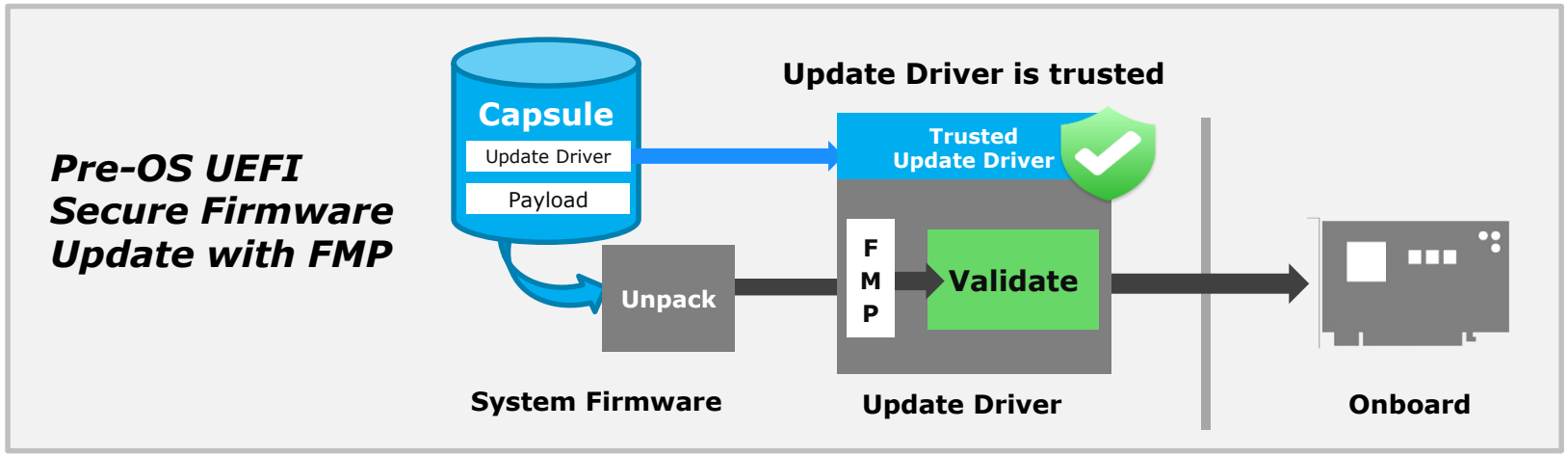
- Protected, but Chain of Trust is completely under OEM control
- Authentication doesn't burden every adapter driver

Cons

- Business Risk - IHV is vulnerable if OEM process is ever compromised

Good

Delivery and Authentication by Capsule



Pros

- Authentication is done by Capsule Driver and doesn't burden every adapter driver's FMP implementation

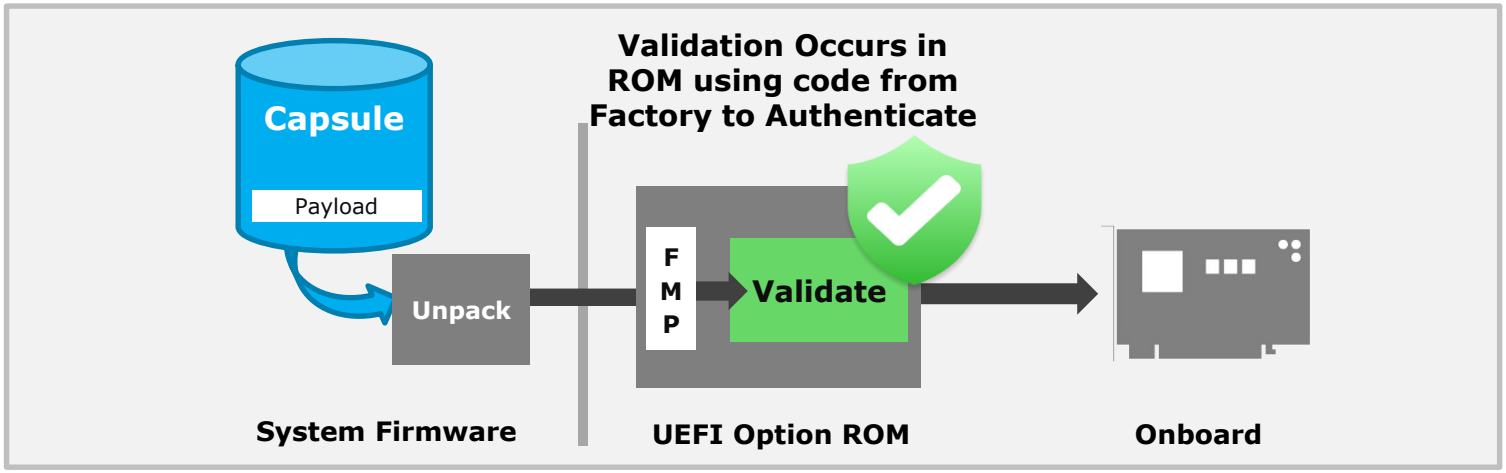
Cons

- Dependence upon Secure Boot leaves FMP vulnerable if Secure Boot is compromised

IDF13

Better

Authentication in UEFI Option ROM



Pros

- Protected – Authentication in factory image
- Eliminates need for IHV Update Driver
- Not dependent on OEM Secure Boot

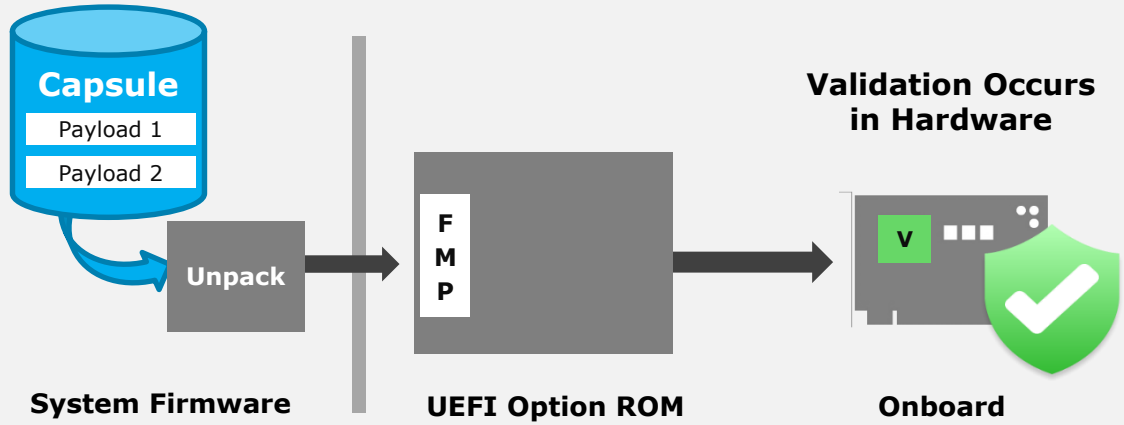
Cons

- Requires every UEFI adapter driver to include the authentication logic
- Requires UEFI adapter driver to manage keys

IDF13

BEST

Authentication on Adapter



Dependency:

- *Requires additional local storage on adapter card*
- *Adapter firmware must manage keys*

Pros

- Only one point of challenge
- Signed components not required in stack
- Authentication in protected environment

IHV Recommendations

- Safeguard your firmware and hardware from Pre-OS attacks!
- You have multiple options **Good** **Better** **Best**
- Contribute to overall system security
- New market opportunities for security solutions

IHVs need to evolve to meet update security requirements

IDF13

Summary

- Expansion board firmware security is a key element of platform security
- UEFI 2.4 offers new tools for update
- UEFI offers solutions for IHV security requirements
- IHVs need to evolve to meet update security requirements

Call to Action

- Evaluate the security of current update strategies
- For new designs, plan to include board resources that support strongest security
- Engage with your partners and the industry through participation in UEFI

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 UEFI Specification and the "UEFI Secure Boot in Modern Computer Security Solutions" whitepaper.

NIST Special Publications are available from
http://csrc.nist.gov/publications/PubsSPs.html

Intel UEFI Community Resource Center

Central resource for UEFI on Intel® Architecture

IDF13

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 409, 410, 411

✓ = DONE

IDF13

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!

Please Fill Out The Online Session Evaluation Form

Enter to win fabulous prizes!

You will receive an email with a link to the online session evaluation prior to the end of this session. Please submit the evaluation by 10am tomorrow to be entered to win.

Winners will be announced by email

Sweepstakes rules are available at the Help Desk on Level 2
All sessions evaluations must be submitted by Friday, September 13 at 5pm

IDF13

Q&A

Legal Disclaimer

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