
intel
Leap ahead™
Intel Developer
FORUM

Intel Advanced Technology in the Enterprise: UEFI Firmware and IBM

Cecil Lockett
IBM Systems and Technology Group
UEFI Development

Vincent Zimmer
Intel Corporation – Principal Engineer

Session ID EFIS004

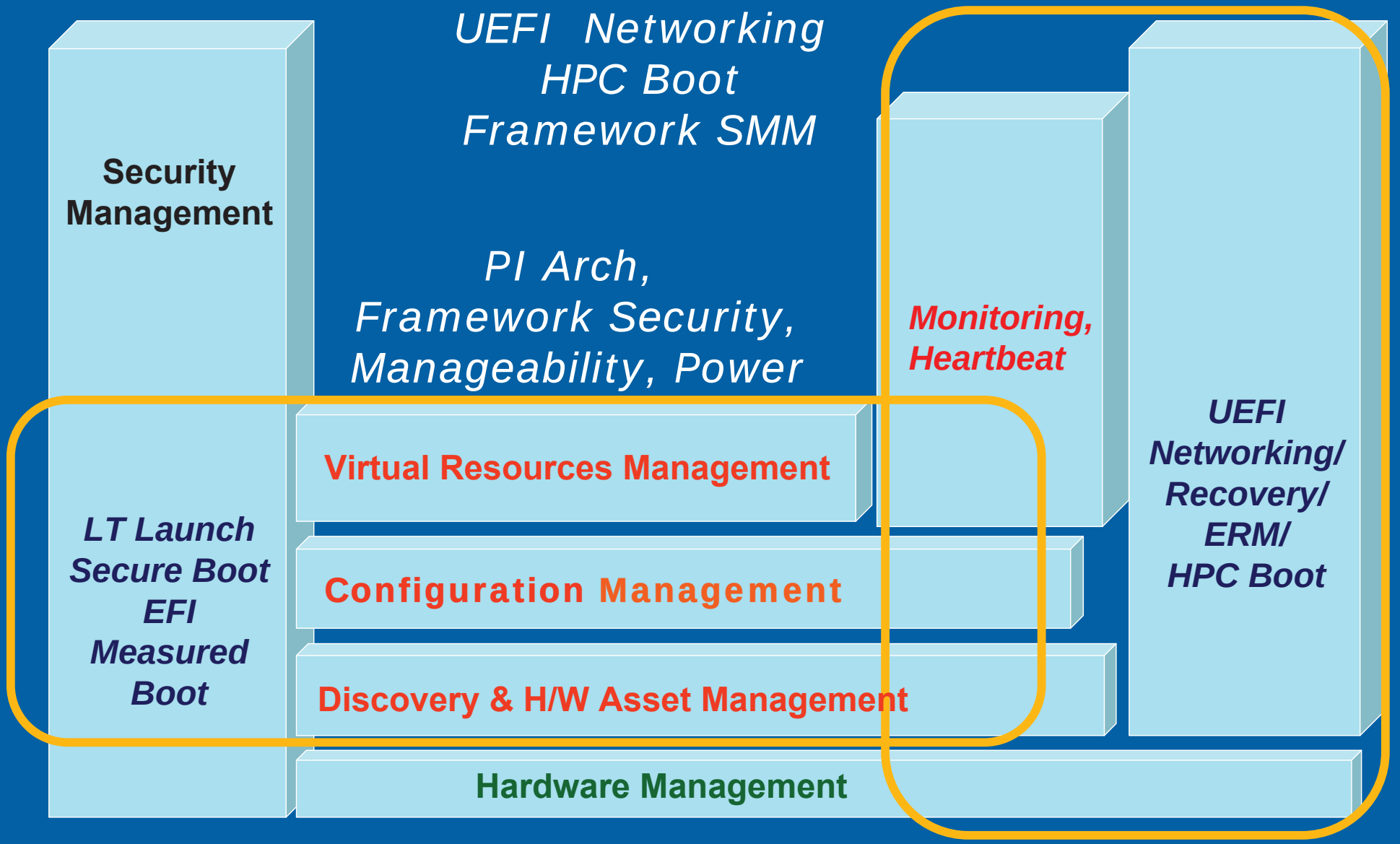
Intel Developer FORUM

© 2006 Intel Corporation

Agenda

- Overall Vision
- Platform Security
- Manageability
- The Enterprise

Vision: Enterprise Infrastructure



Pervasive UEFI

Platform Security – The Problem Statement

- **Protection Against Malicious Code**
  - Worms, patching
- **Business Process Compliance**
  - Regulatory requirements from EU Privacy, SarbOx, Basel II, HIPAA, GLB etc.
- **Internal/External Access and Data Protection**
  - Secure provisioning of Infrastructure/Users
  - Managing access/identity across disparate applications

Security isn't hype, but real market need

Dictionary Terminology

- **Trust**
  - An entity can be trusted if it always behaves in the expected manner for the intended purpose
- **Measurement**
  - The process of obtaining the identity of an entity
  - Hashes of software
- **Security**
  - ". . .[1]maintenance that ensure a state of inviolability from hostile acts or influences"

Trust needs an agreed upon lexicon

[1] www.wikipedia.org

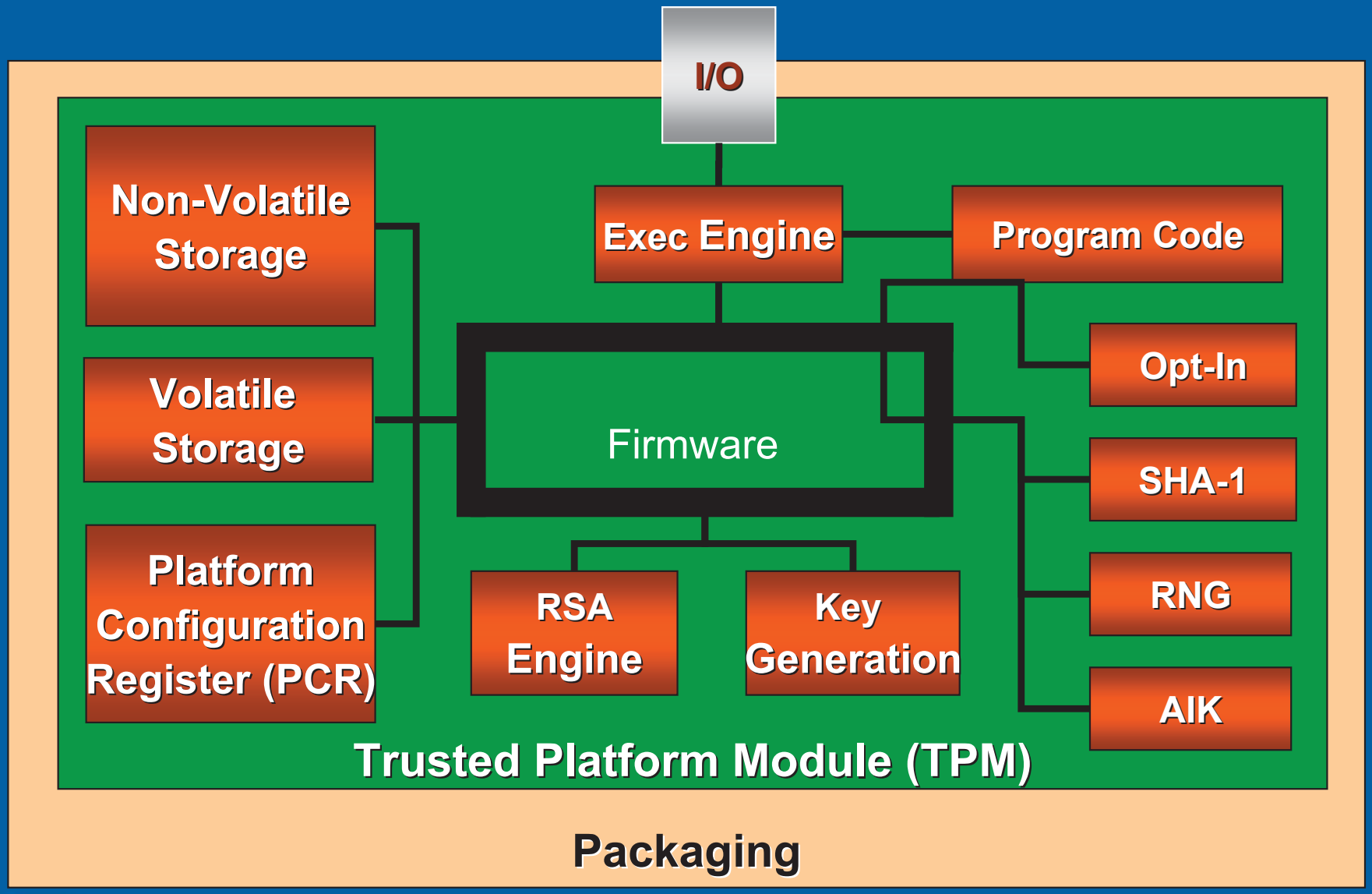
What is the heart of Trust

- TCG defines TPM's functionality
  - Protected capabilities
  - Shielded locations

- Not the implementation
  - Vendors are free to differentiate the TPM implementation
  - Must still meet the protected capabilities and shielded locations requirements

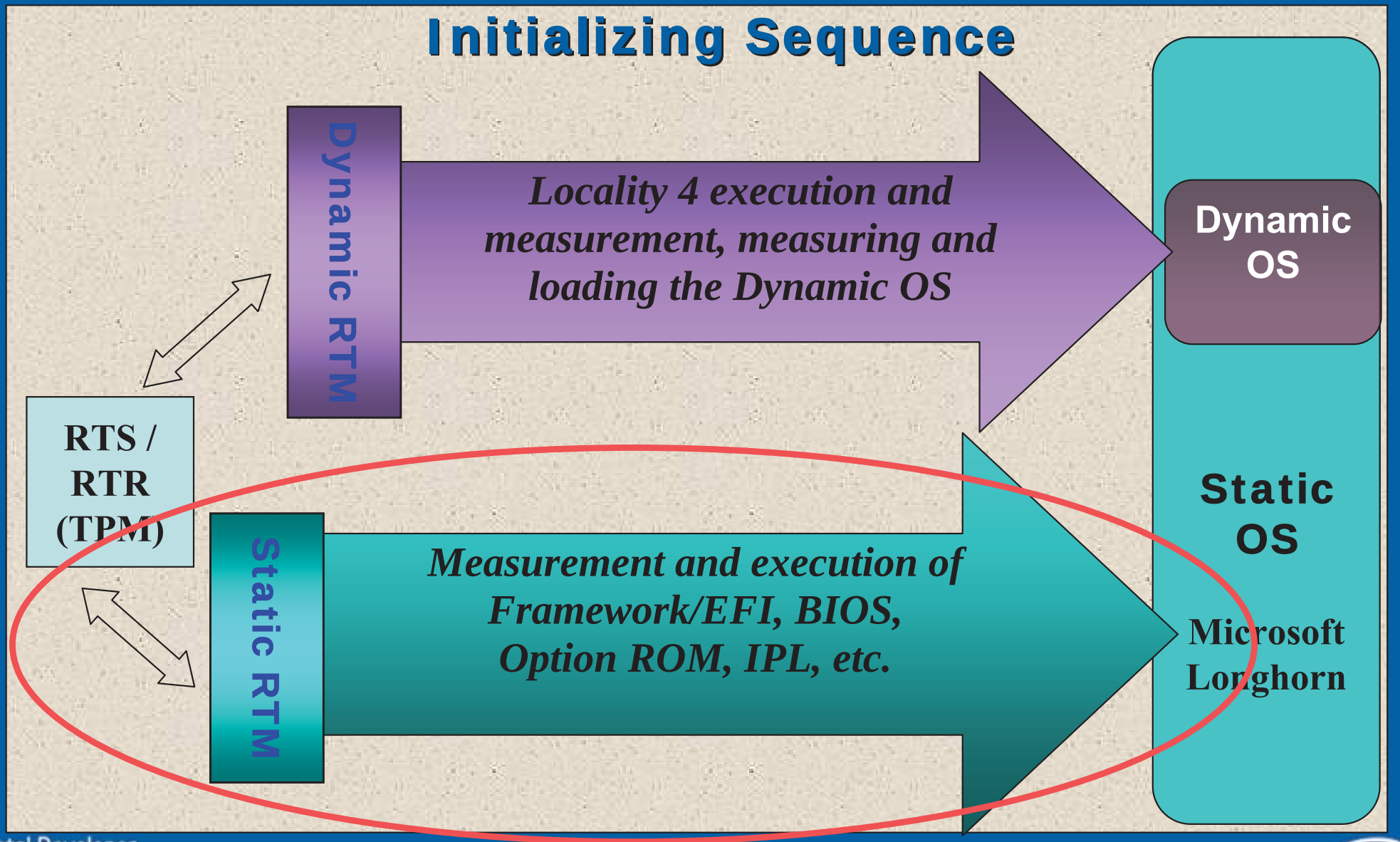
Need a hardware root of trust

Basic TPM Block Diagram



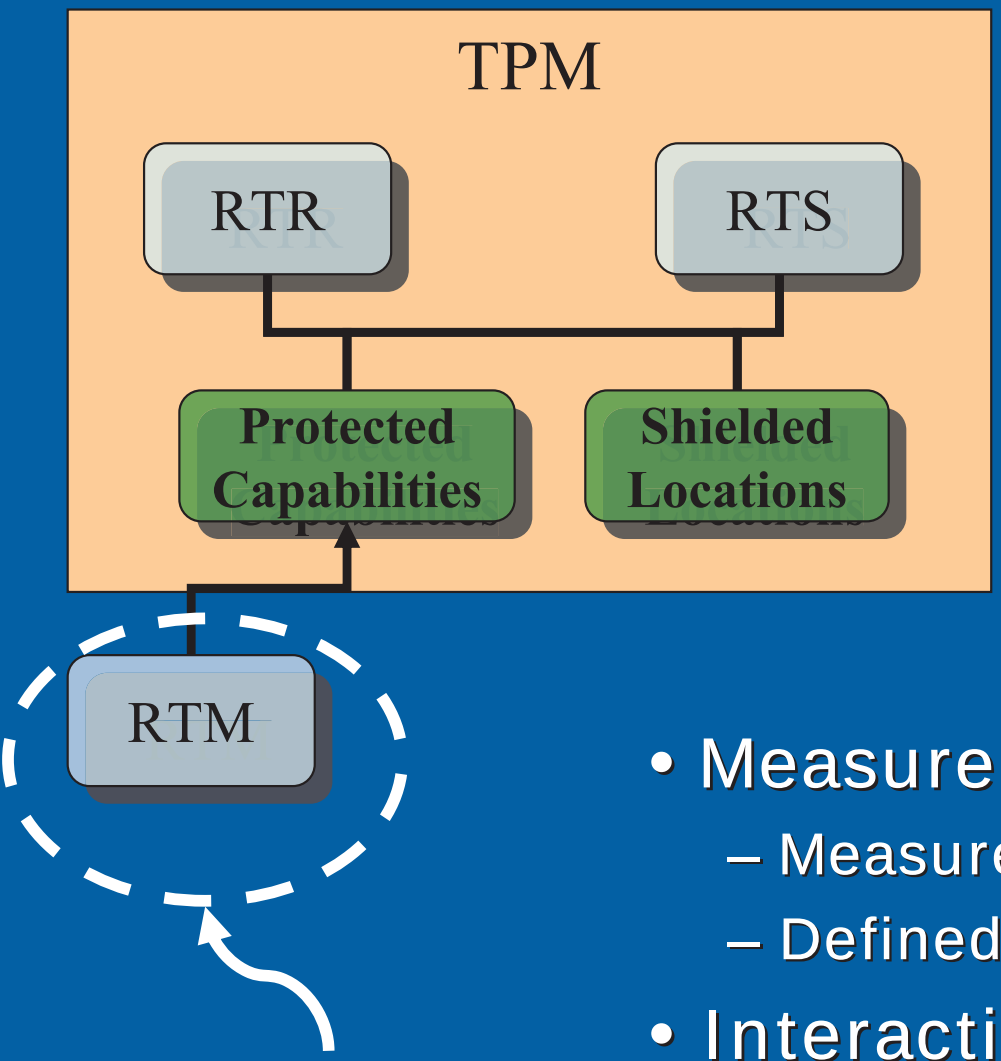
Shielded locations, including PCR's

We're talking about SRTM for Platform Firmware



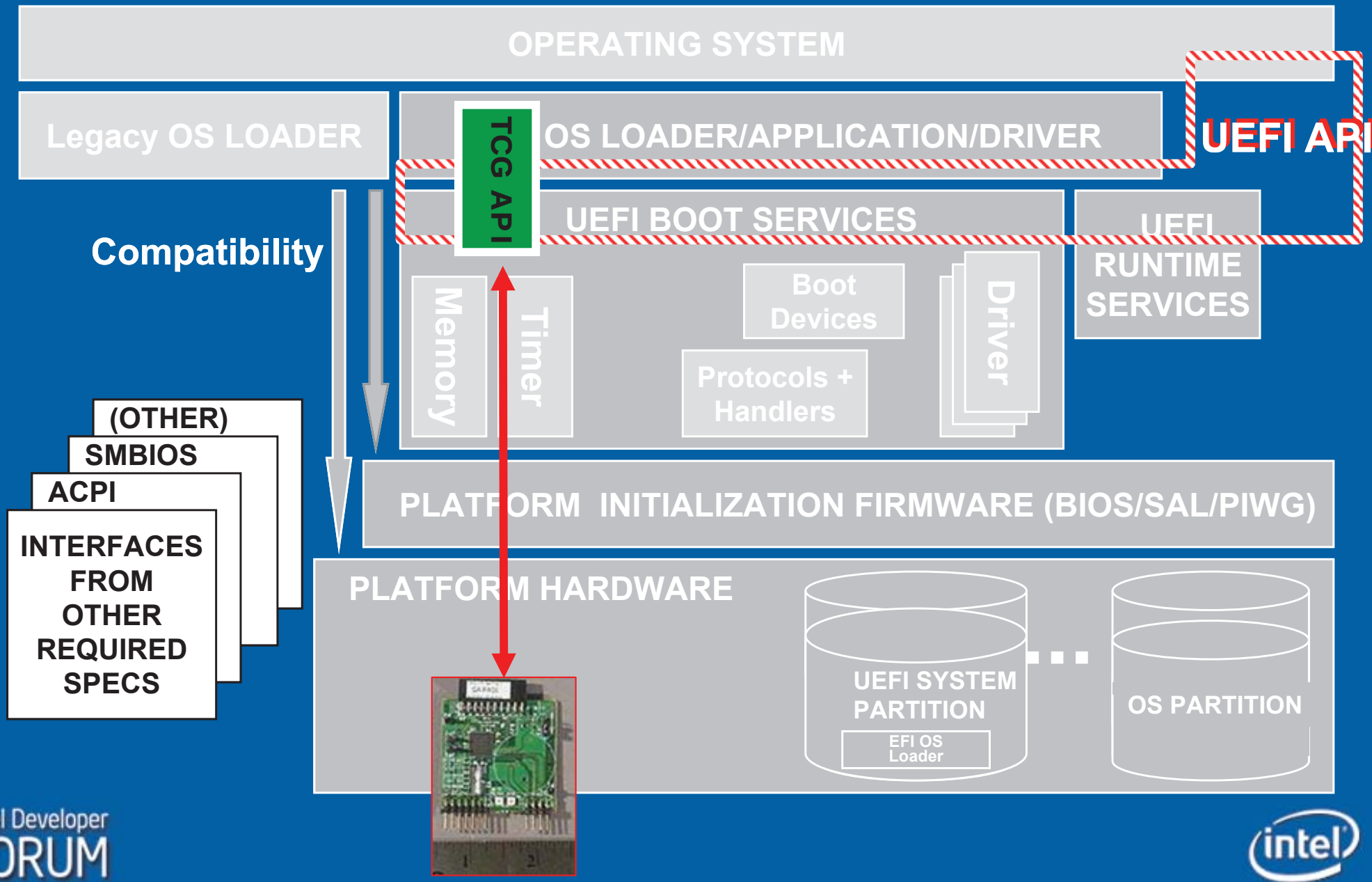
Firmware use of TPM and Measurements

Functional TPM Diagram

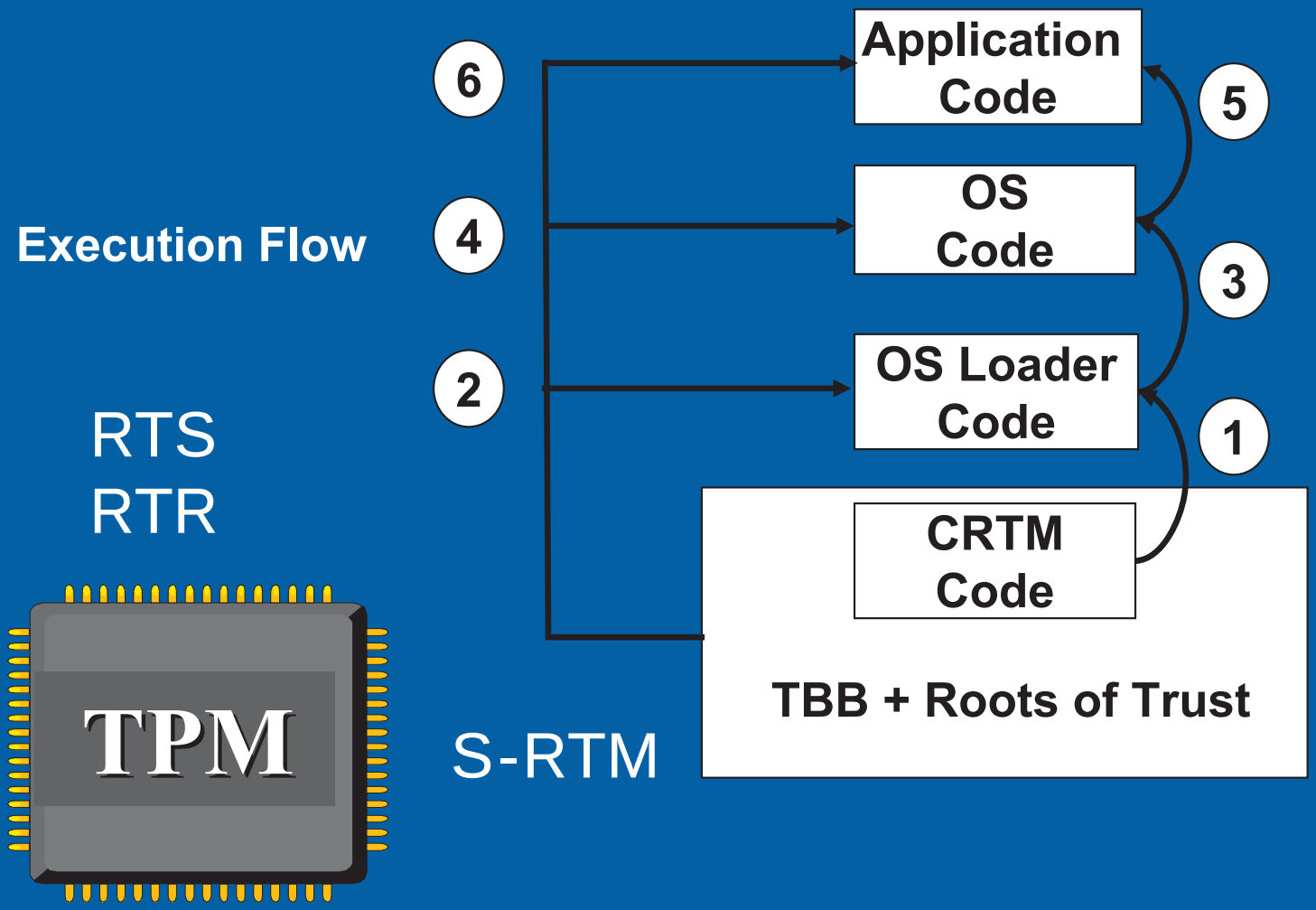


- Reporting RTR
  - Cryptographic mechanism to digitally sign TPM state
- Storage RTS
  - Cryptographic mechanism to protect information held outside of the TPM
- Measurement
  - Measure platform state
  - Defined by platform specification
- Interaction between RTR and RTS is important TPM capability
  - RTE/RTV in the future

UEFI Layered Implementation

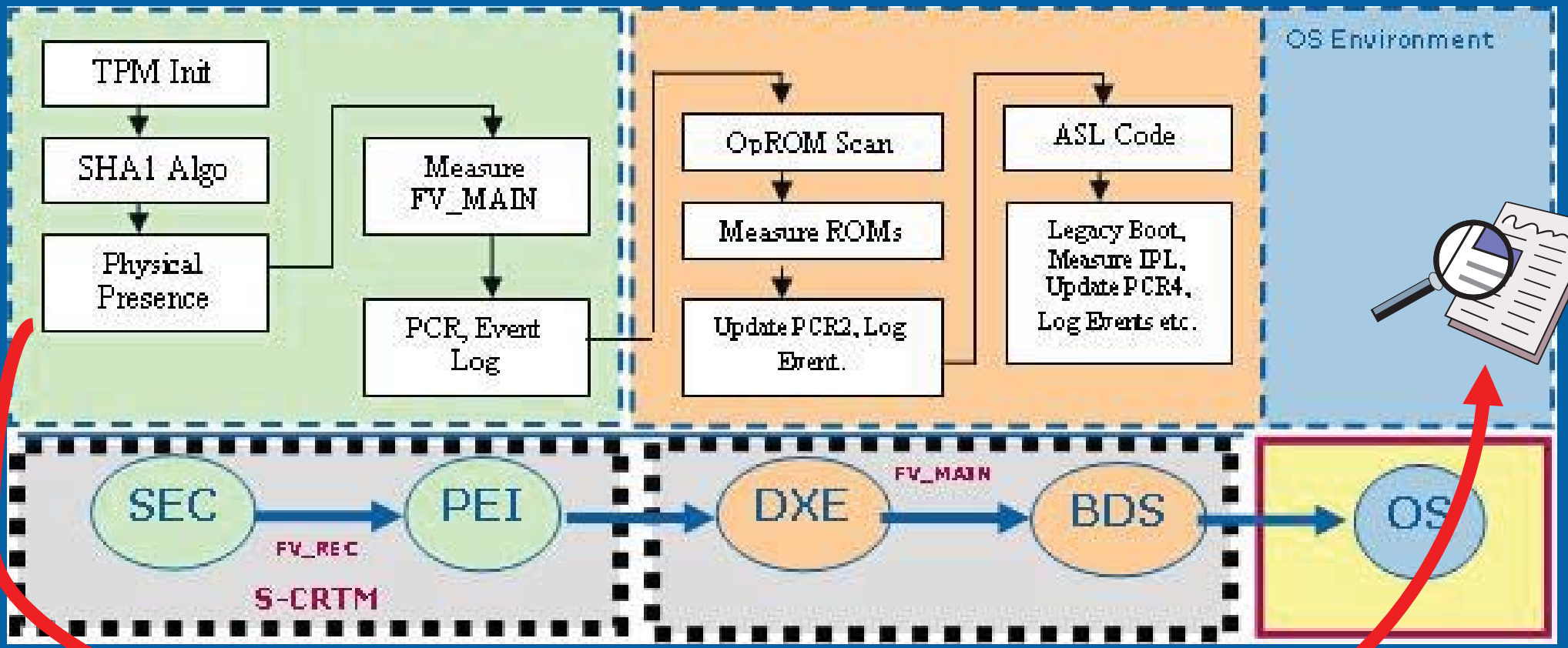


Today's TPM usage: Measure & Run-"Trusted Boot"

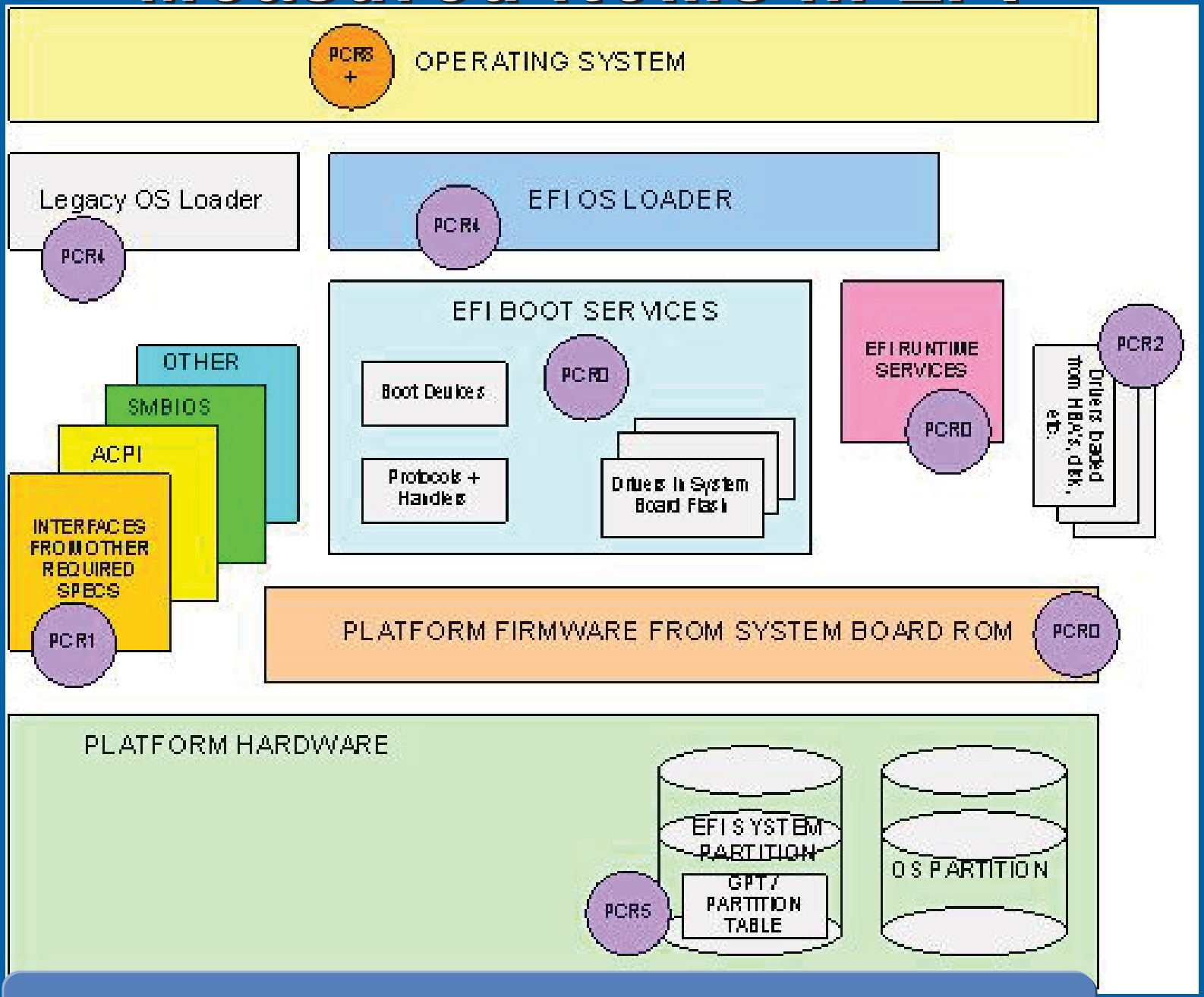


Just measure what you're running but don't enforce policy. Let someone later look at measurement.

UEFI / PI Architecture Boot Flow – Create / Evaluate Integrity List



Measured items in EFI



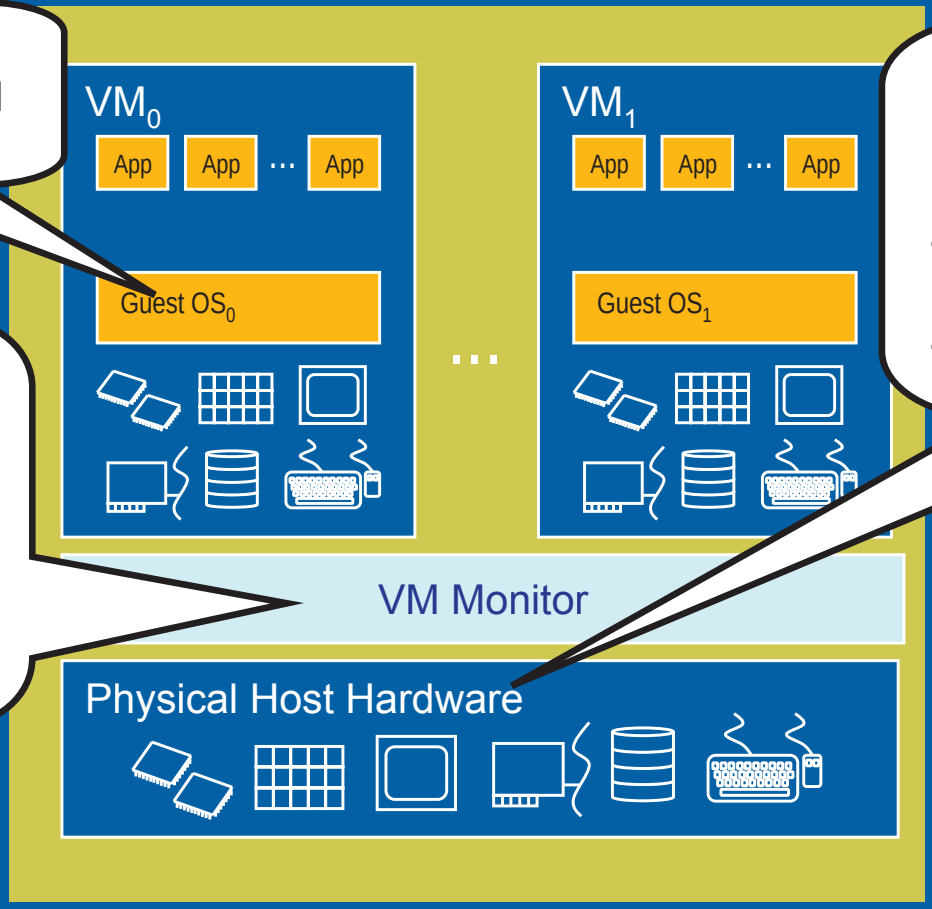
Standardized way to measure and report

Intel® Virtualization Technology

Guest OSs & Apps run in the intended ring

VMM runs in a new operation mode

VMM preempts guest execution via new HW transition mechanism



VT = HW support for Processor Virtualization

- New CPU execution mode
- HW-based mode transitions

- Less guest OS dependencies
- Simpler VMMs & Smaller TCB
- Less unwanted transitions

By design, VT eliminates virtualization holes and the need for unorthodox software methods

Cecil Lockett
IBM Systems and Technology Group
UEFI Development

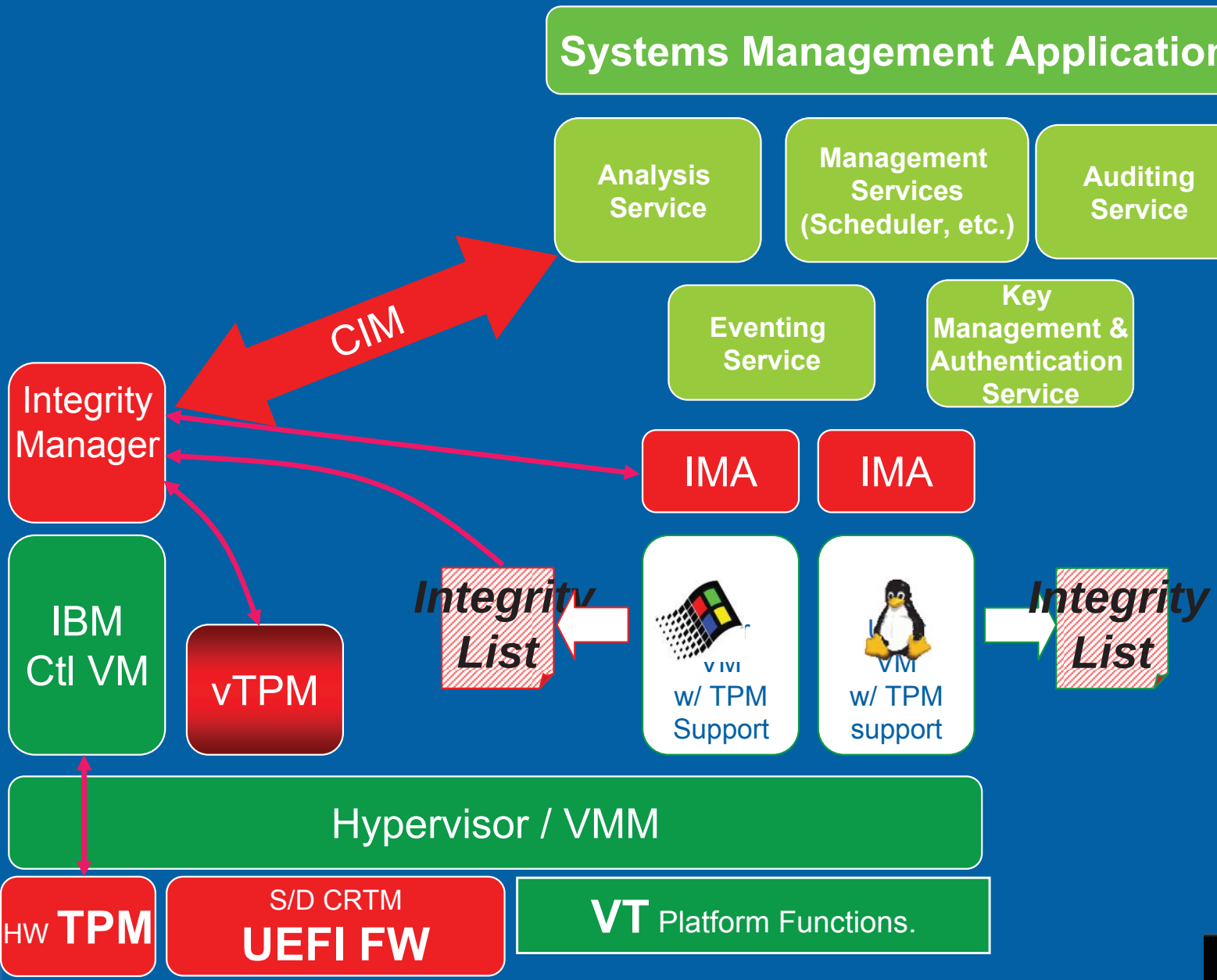
Intel Developer FORUM

© 2006 Intel Corporation

Top Problems based on IT survey

PRI	Problem	Solution Requirements
1	**Protecting from inside**	**Tamper-proof Agent and Circuit Breakers**
2	**Locating, Managing Systems**	**Asset Management**
3	**Controlling, Debugging Systems**	**Out of Band Management**
4	**Visibility into traffic**	**Network Visibility**

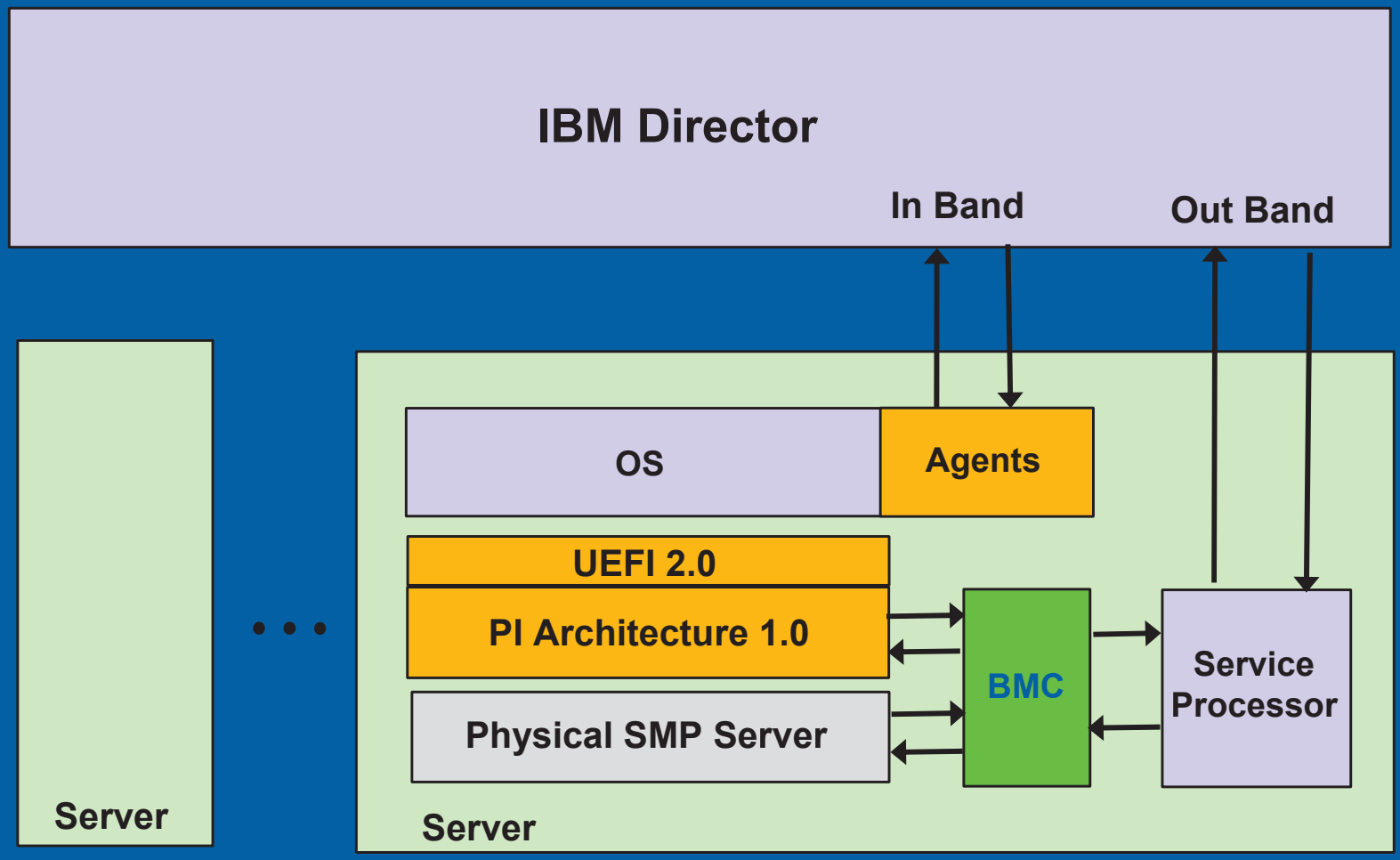
IBM Fidelity / Integrity Services Model



Systems Management and Industry Standards

- **UEFI, V-sig and DMTF**
- **CIM providers based on DMTF virtual resource model**
- **Move provider development into open source**
  - Domain State
  - Platform Instrumentation
  - CIM SMASH provider
- **Support of tools/interfaces in the control partition**
  - Update tools (Diagnostics, LFlash, etc…)
- **Virtual Management Module**
  - Develop and implement MM interface for Domain 0
  - Symmetric Interface Architecture and Management Framework

IBM Server Management Service Processor (SSP) / BMC



Platform Initialization Standards

Platform Initialization Working Group of UEFI Forum

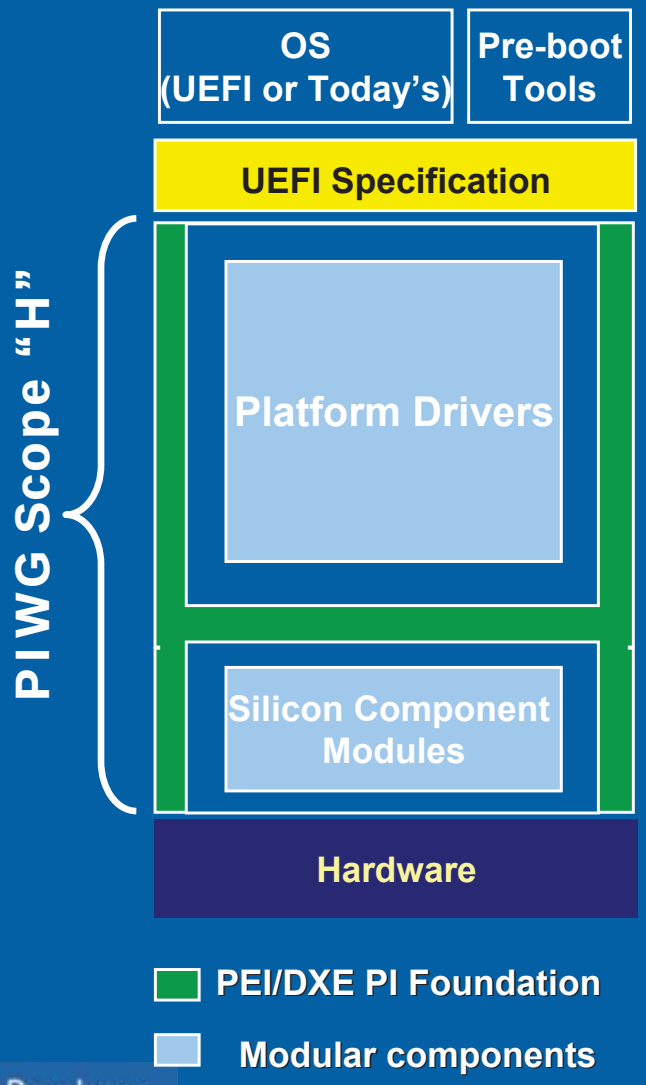
- Delivering the Platform Initialization Architecture Specifications
- Based on Intel PEI and DXE specs
- Independent of UEFI 2.0 Specification
- PI Architecture platforms can still boot today's OS's

Goal: Allow silicon vendors who create "reference code" today to package this reference code as modules that snap-into PI Architecture firmware implementations

Ownership: UEFI Forum

Promoters: AMD, AMI, Apple, Dell, HP, IBM, Insyde, Intel, Lenovo, Microsoft and Phoenix

PI Architecture Scope
(Pre-OS/Option ROM load – Int19h/EFI Boot)

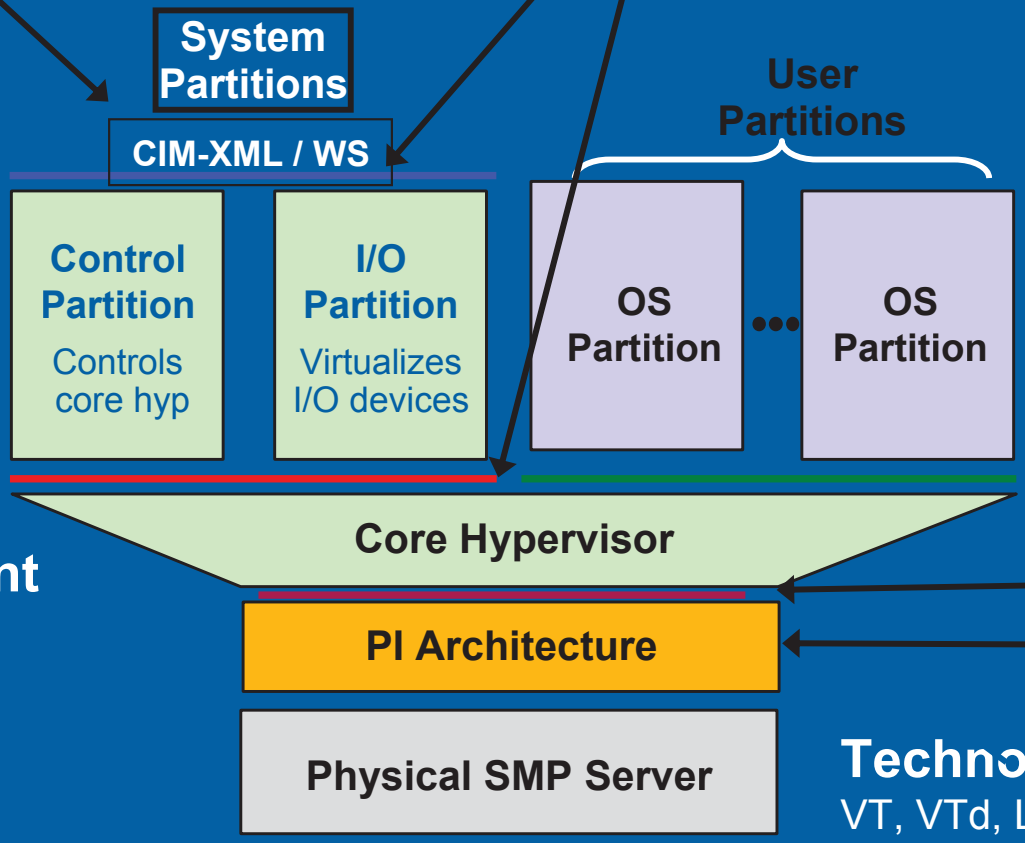


- UEFI 2.0 (published) specifies how firmware boots the OS loader
- UEFI's Platform Initialization Architecture specifies how modules initializing Si and the platform interact and provides common services for those modules
- PIWG has already voted to use Intel PEI/DXE specs as the baseline

IBM's Integration of Standards

Management capability

Industry Standards
-DMTF: Virt. CIM Models
-Virtualization SIG



System Management Infrastructure
SMASH extensions, CIM Brokers/Providers, etc…

Pre OS Environment
-UEFI 2.0 Interface
-PI Architecture

Technology Exploitation
VT, VTd, LT, UEFI

Standards at many layers of the stack

IBM UEFI Driver Requirements

- **UEFI 2.0 Boot Device Drivers**
  - Graphics
  - Storage RAID, SAS, Fibre-channel
  - Network UNDI
- **Formats**
  - Support for IA-32 and EMT64 platforms
  - EBC drivers preferred
- **Timeframe**
  - Beta 4Q06-
  - Production 4Q07-

UEFI Testing Event

- Purpose
  - Provide the an opportunity to allow implementers of UEFI to test their implementations among the UEFI community
- In Dupont WA – Week of December 11
  - Testing of UEFI systems and platforms with UEFI Add in Cards in different configurations for UEFI compliance as well
  - Testing install and boot to a variety of UEFI Operating systems
- Contact laurie.fleisher@intel.com
- More on this event: www.uefi.org

Your Opportunity to Test your Implementation

Summary

- UEFI impacts many layers
- Security is a platform issue
- Manageability futures need firmware
- Synthesize in the enterprise

Essential References and Resources

- Technical books from Intel Press:

  Beyond BIOS: Implementing the Unified Extensible Firmware Interface with Intel's Framework

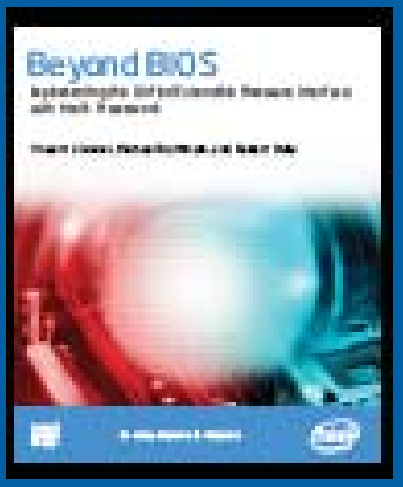
  by Vincent Zimmer, Michael Rothman, and Robert Hale

  The Intel Safer Computing Initiative

  by David Grawrock

  Applied Virtualization Technology

  by Sean Campbell and Michael Jeronimo



  For more info: www.intel.com/intelpress

Additional EFI /Framework Sessions Moscone West 2006:

Session	EFI #	Company	Time
Open Source Extensible Firmware Interface (EFI) Developer Kit - What it is and How to Use it	S005	Intel	Done
New Firmware Development at Hewlett Packard using EFI and the Framework	S001	Hewlett Packard	Done
Intel Advanced Technology in the Enterprise: UEFI Firmware & IBM	S004	Intel & IBM	4:00 Wed
Mobile Platform Usage of UEFI and the Framework Technology	S002	Intel Mobile	5:00 Wed
Benefits of Unified Extensible Firmware Interface (UEFI) with Microsoft and Other OS	S003	Intel	8:00 Thu
Q&A open forum	C001	Intel	11:00 Thu

More web based info: www.TianoCore.org

www.uefi.org

www.intel.com/technology/framework

Please fill out the Session Evaluation Form

Session presentation available in Content Catalog on the IDF web site –
when prompted enter:
Username: idf
Password: fall2006
(Please note these are case sensitive)

Thank You for your input, we use it to improve future Intel Developer Forums

Join us at the Spring 2007 IDF on March 20-22 in San Francisco!!

Intel Developer FORUM

intel