Seattle Meet-up Group October 4, 2012

UEFI and pre-OS Networking

Vincent Zimmer

Usual disclaimer-
These foils and opinions are mine and not necessarily those of my employer

Who am I? Vincent Zimmer

Principal Engineer at Intel
Industry since 1992
Intel since 1997
Chair of UEFI network subteam
Chair of UEFI PI security subteam
More –
http://sites.google.com/site/vincentzimmer/

Industry BIOS Transition

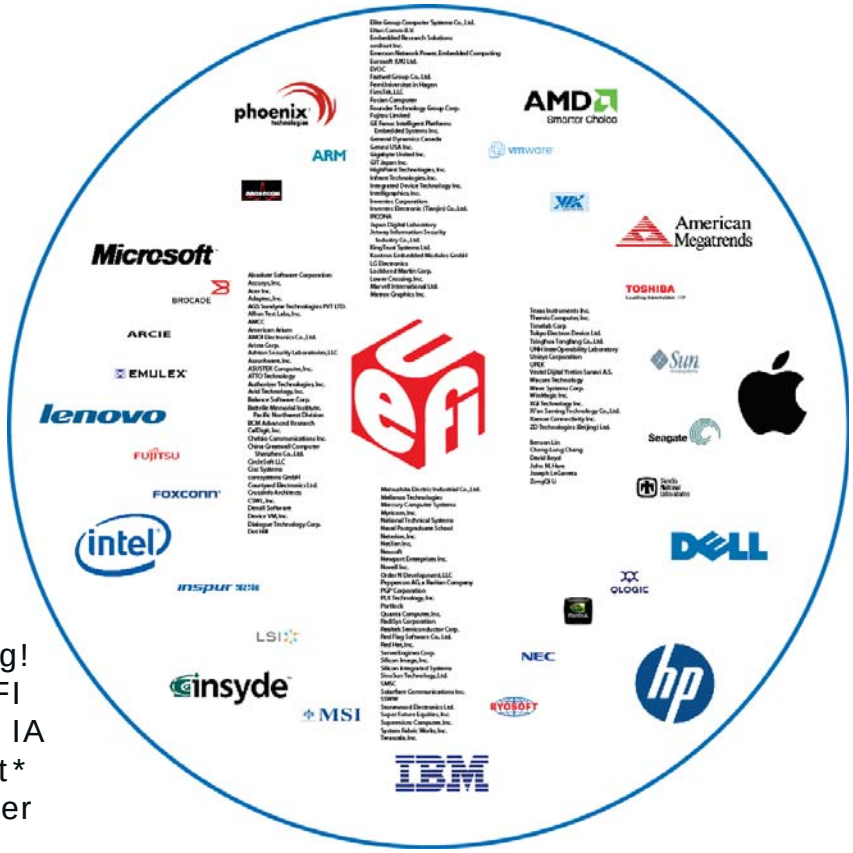
Pre-2000 — All Platforms BIOS were proprietary

2000 — Intel invented the Extensible Firmware Interface (EFI) and provided sample implementation under free BSD terms

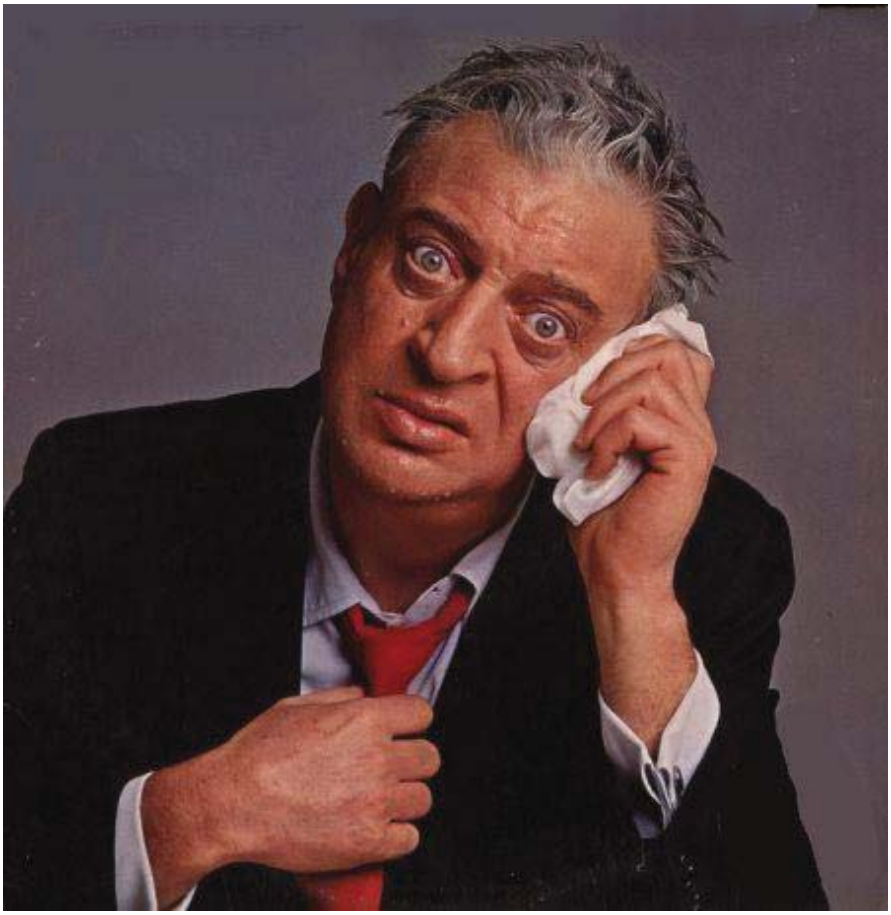
2004 — **tianocore.org**, open source EFI community launched

2005 — **Unified EFI (UEFI)** Industry forum, with 11 promoters, was formed to standardize EFI

2011 — 170 members and growing! Major MNCs shipping; UEFI platforms crossed 50% of IA worldwide units; Microsoft* UEFI x64 support in Server 2008, Vista* and Win7*; RedHat* and Novell* OS support



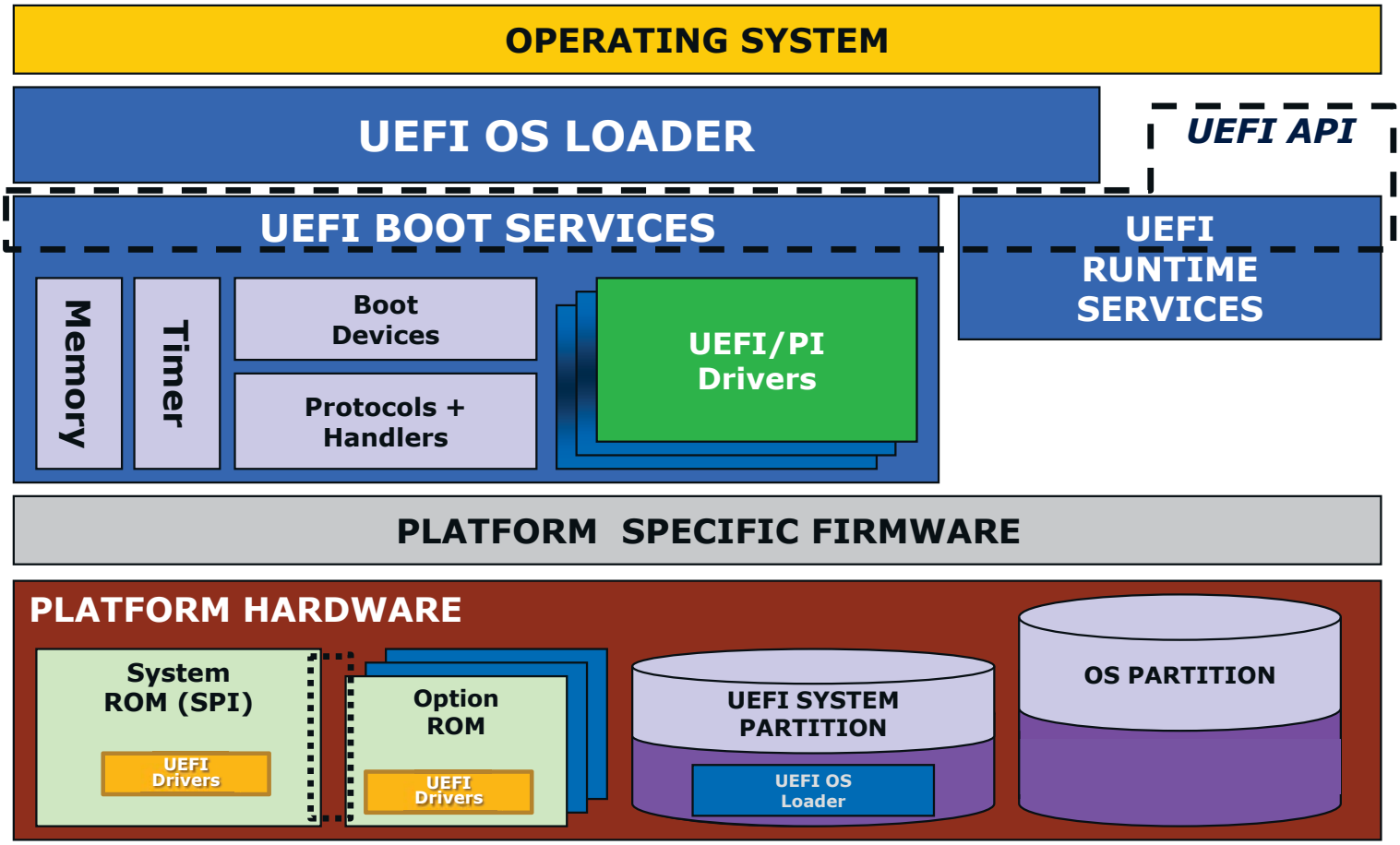
UEFI / PI is a type of BIOS
BIOS– aka. the Rodney Dangerfield of Software



"No respect"

http://www.noethics.net/News/index.php?option=com_content&view=article&id=1923:todays-rodney-dangerfield-award-winner-is-newt-gingrich&catid=121:rodney-dangerfield-award-winners&Itemid=96

Overview of the UEFI Boot Process



UEFI as an abstraction of the platform

Typical OS Loader Scenario for UEFI

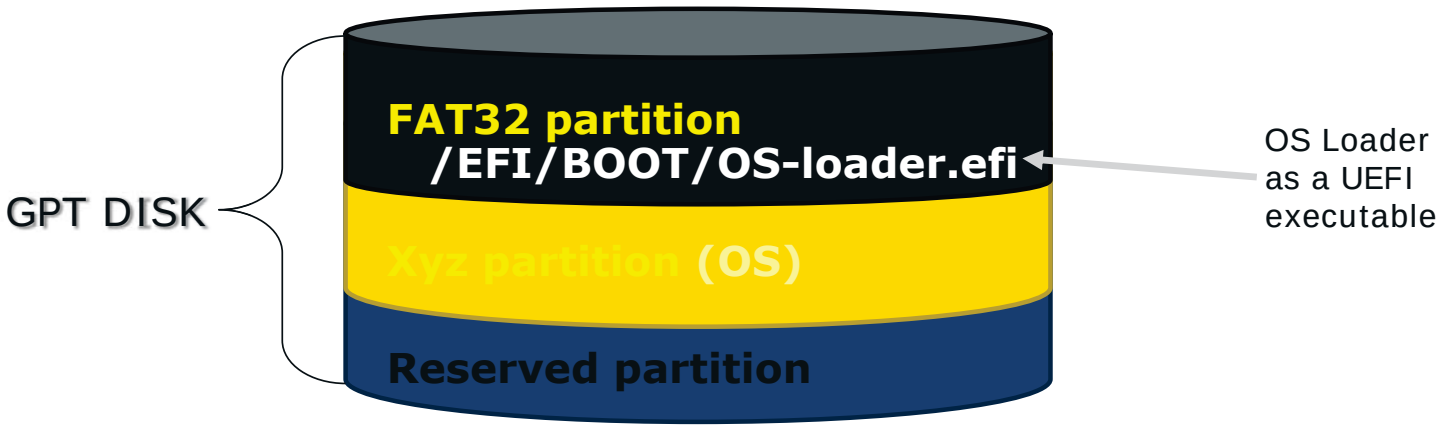
One GPT disk partition is FAT32 (service partition)

OS installer puts the loader on the service partition

- Under `/EFI/BOOT` or `/EFI/osname` directory
- Ex: **`/efi/boot/bootx64.efi`**, **`/efi/ubuntu/grubx64.efi`**

NVRAM `(Bootxxxx)` has a device path to OS loader

- Maps to specific device, GUID partition & filename



Advantages of UEFI Boot Process

Extensible across multiple boot devices

- SATA, SAS, USB, PXE/iSCSI (IPv4/IPv6), ...

Supports multi-boot operations

- Multi-boot loaders w/o MBR chain-loading
- UEFI Forum reserves directories to avoid collisions
- Use `/efi/boot` directory for removable media

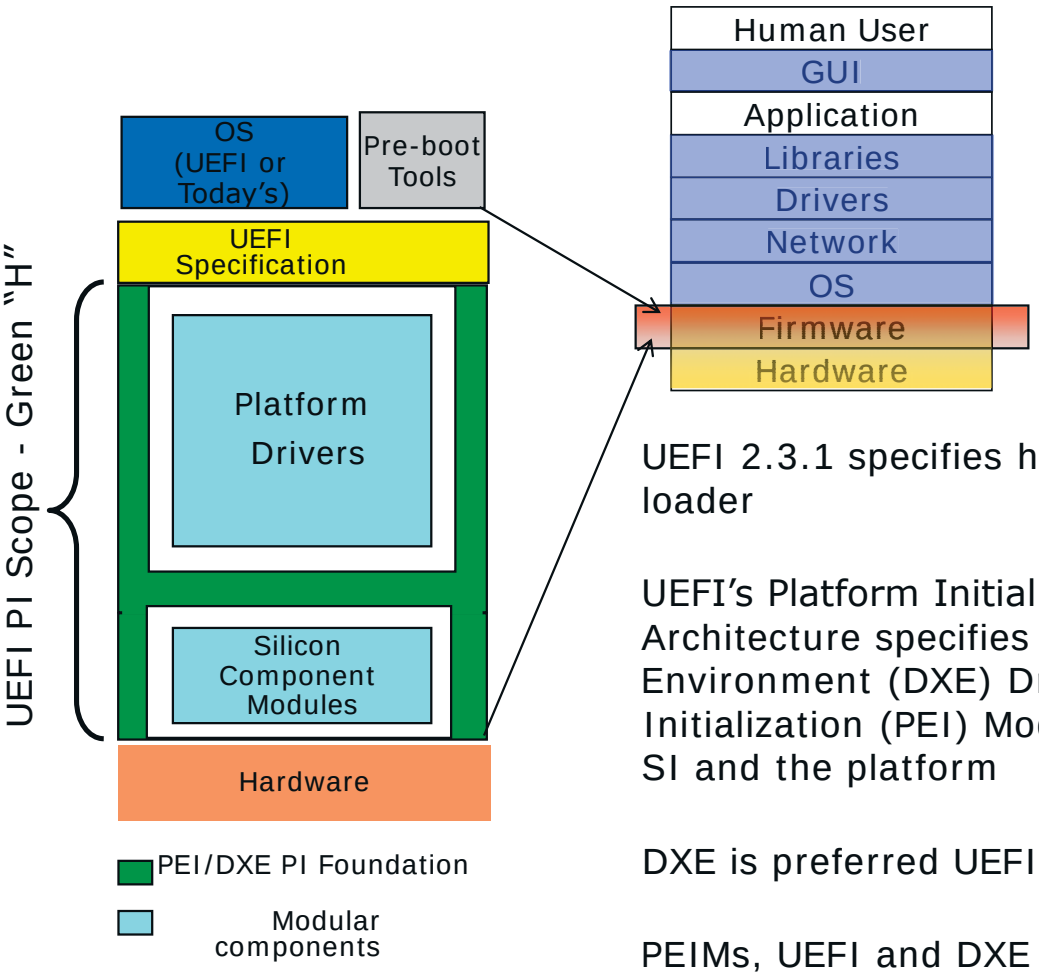
Device path stored in boot options (NVRAM)

- Pointer to specific boot device

Boot image can be validated when loaded

- Allows firmware loader to perform security checks

Building UEFI: UEFI Platform Initialization Overview



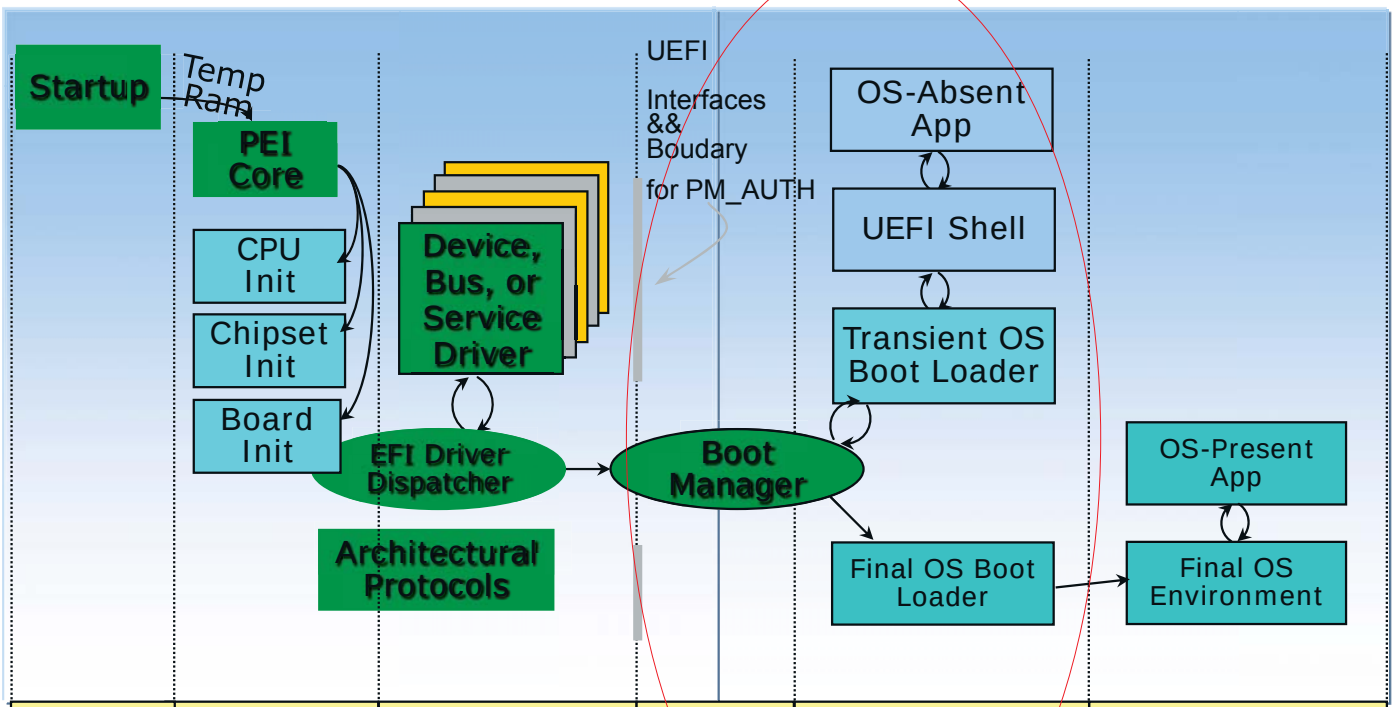
UEFI 2.3.1 specifies how firmware boots OS loader

UEFI's Platform Initialization (PI) 1.2 Architecture specifies how Driver Execution Environment (DXE) Drivers and Pre-EFI Initialization (PEI) Modules (PEIMs) initialize SI and the platform

DXE is preferred UEFI Implementation

PEIMs, UEFI and DXE drivers implements networking, Update, other security features

Temporal view of booting (more importantly, what problems we are not solving w/ this technology)



UEFI Development Kit -UDK2010

Industry Standards Compliance
- UEFI 2.0, UEFI 2.1, UEFI 2.2, UEFI 2.3; PI 1.0, PI 1.1, PI 1.2

Extensible Foundation for Advanced Capabilities
- Pre-OS Security
- Rich Networking
- Manageability

Support for UEFI Packages
- Import/export modules source/binaries to many build systems

Maximize Re-use of Source Code**
- Platform Configuration Database (PCD) provides "knobs" for binaries
- ECP provides for reuse of EDK1117 (EDK I) modules
- Improved modularity, library classes and instances
- Optimize for size or speed

Multiple Development Environments and Tool Chains**
- Windows, Linux, OSX
- VS2003, VS2005, WinDDK, Intel, GCC

Fast and Flexible Build Infrastructure**
- 4X+ Build Performance Improvement (vs EDKI)
- Targeted Module Build Flexibility

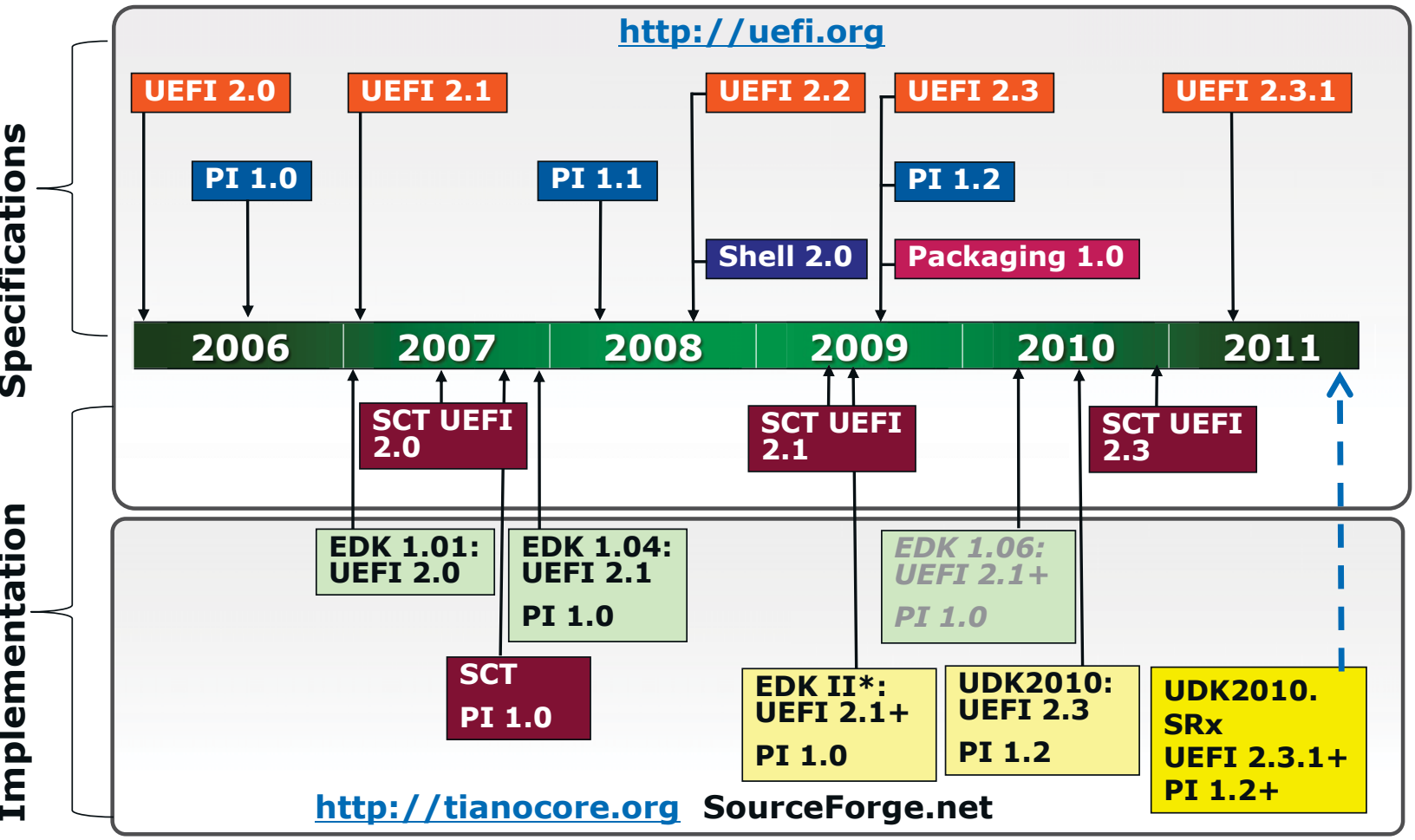
** *benefit of EDK II codebase*

Maximize the open source at www.tianocore.org

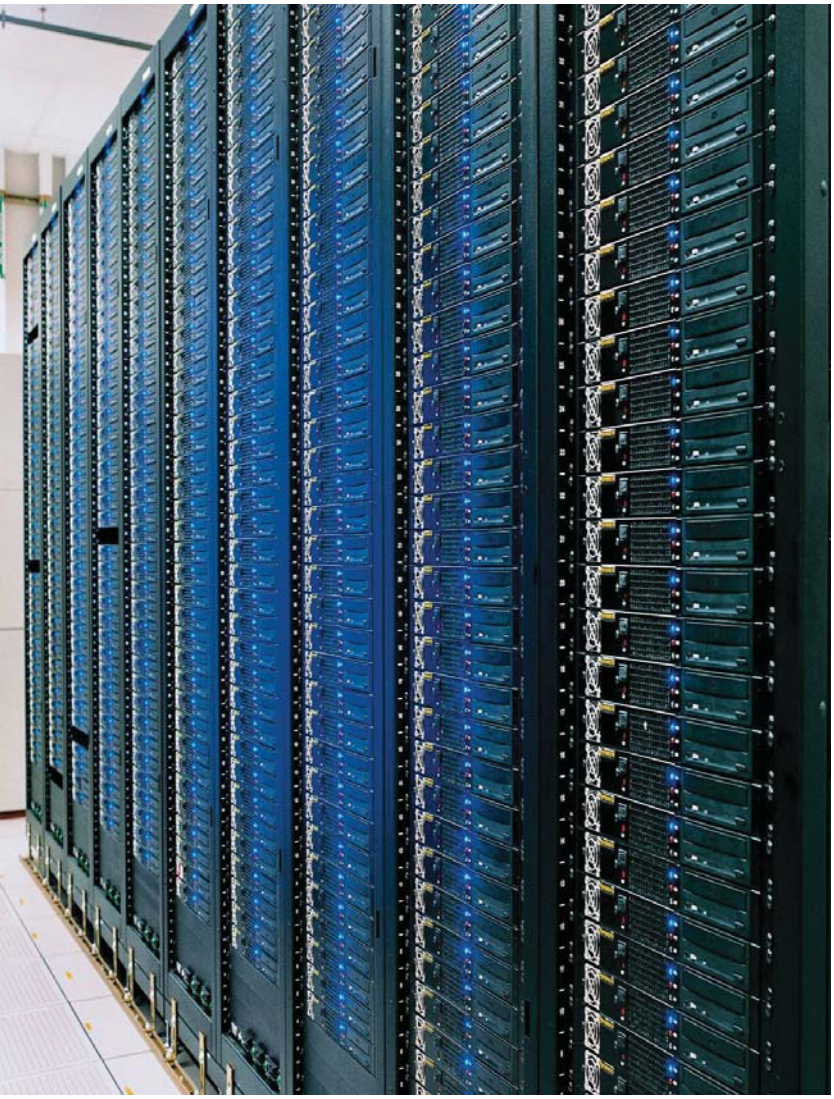
Intel® UDK2010 Enables a Common Firmware Development Foundation Across the Compute Continuum

Intel® UEFI Development Kit 2010 (Intel® UDK2010)

Specification & Tianocore.org Timeline



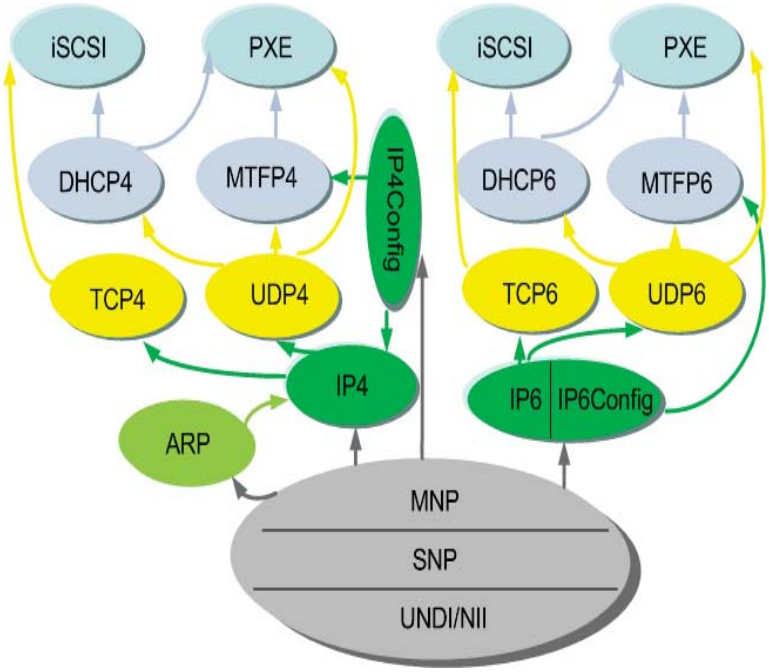
All products, dates, and programs are based on current expectations and subject to change without notice.



Rich Networking

IP6 Networking

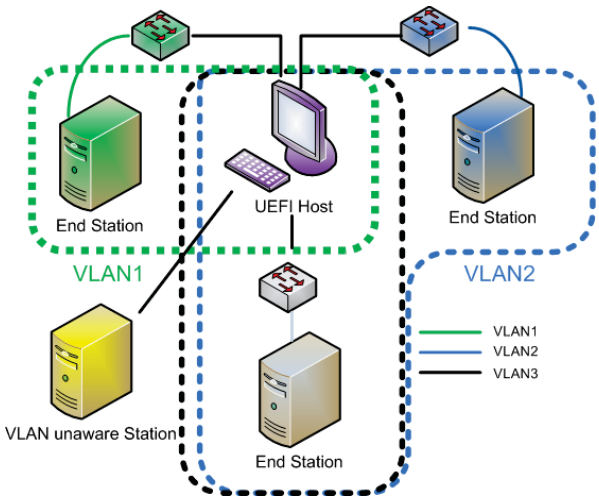
- IPv6 protocols compliance
  - IPv6 ready logo approved http://www.ipv6ready.org/db/index.php/public/
  - Requirements for IPv6 transition http://www.antd.nist.gov/usgv6/usgv6-v1.pdf
  - No IPv4 Addresses available
- Technology includes
  - IP4/6, UDP4/6, TCP4/6, DHCP4/6, MTFP4/6, iSCSI, PXE
    - Allows for concurrent network applications via design based upon MNP
    - Features dual stack: IP4, IP6, or both
- DUID-UUID support (UEFI 2.3.1)
  - Use SMBIOS system GUID as UUID

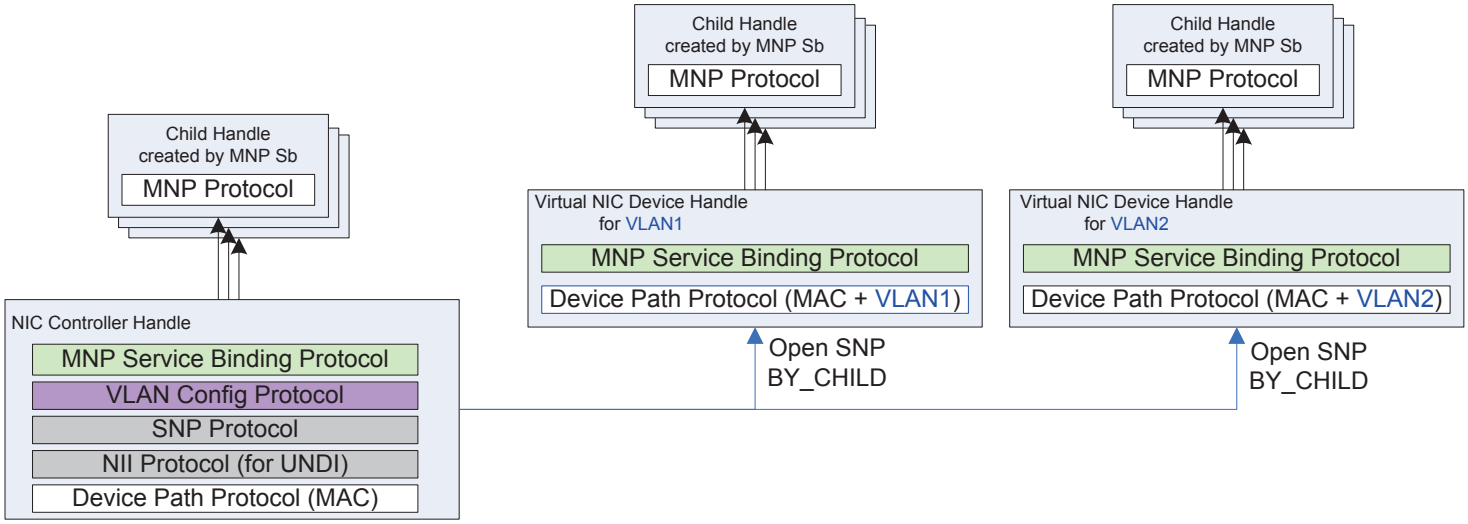


Industry moving to IPv6 for equipment procurement

VLAN Support

- Virtual Local Area Network
  - Defined in IEEE 802.1Q, to create logical groups of stations
  - Increased performance, security and improved manageability
- Technology includes
  - Support Hybrid LAN topology
  - Multiple VLAN for one station
  - VLAN configuration by HII

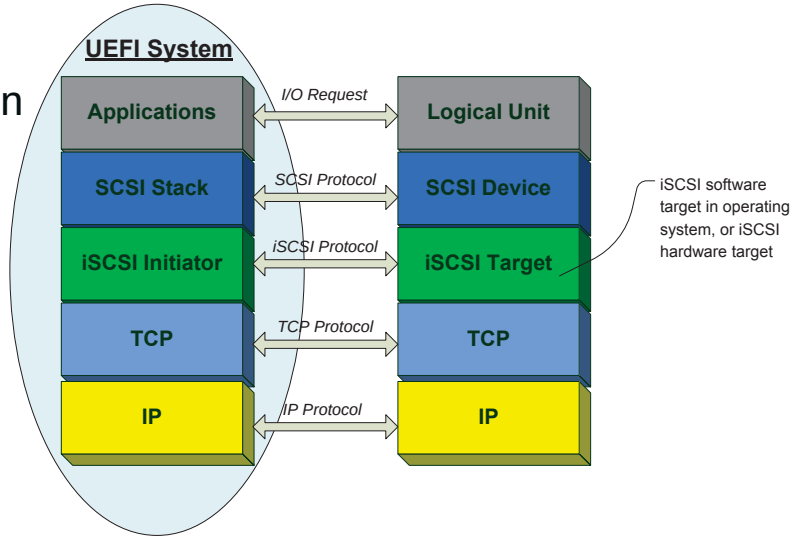


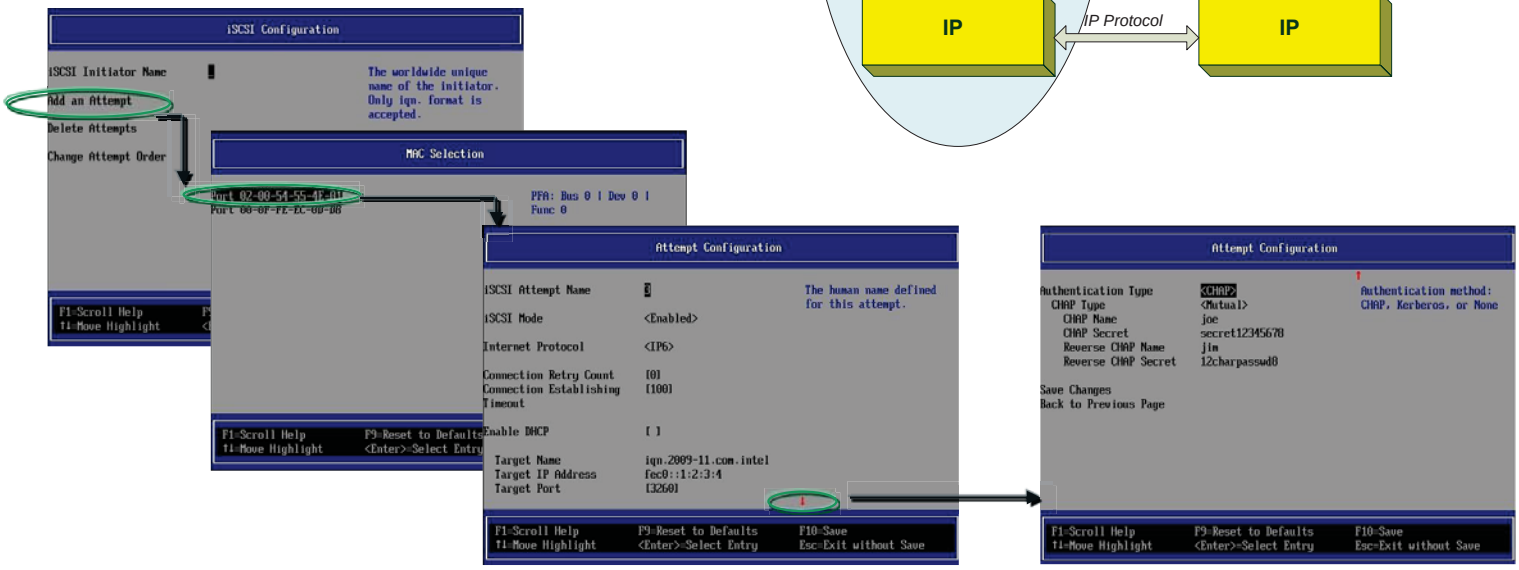


Enabling the quarantining of networks

UEFI iSCSI Solutions

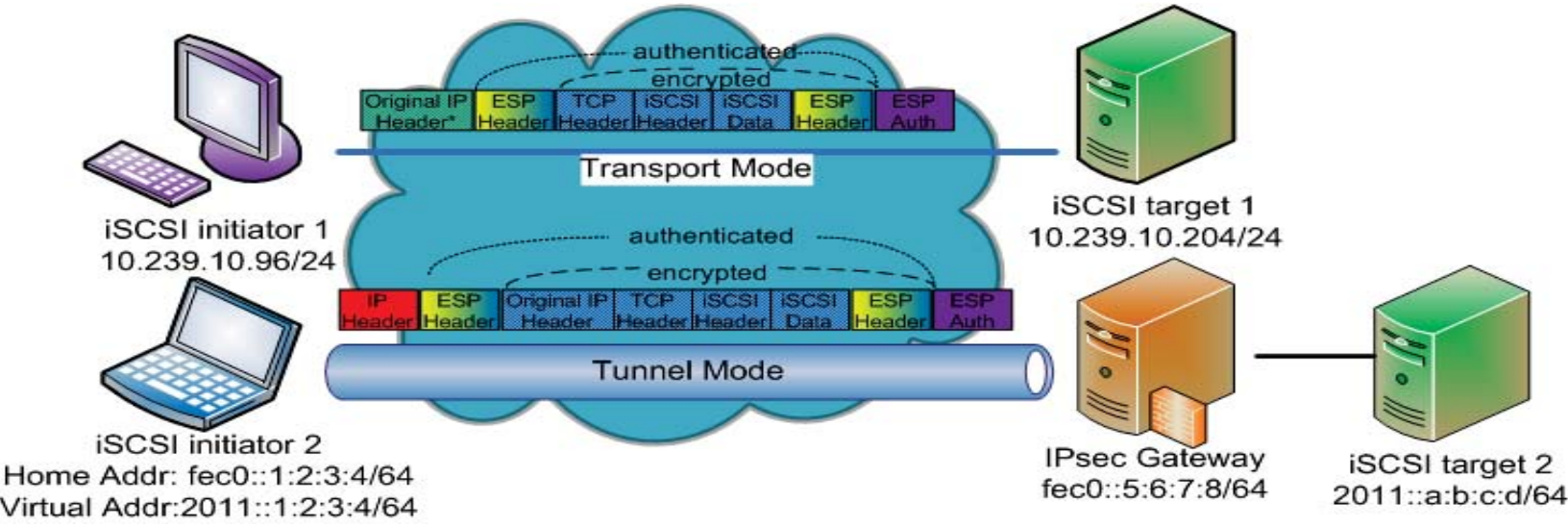
- SAN/Data center boot over iSCSI
  - Manual/DHCP based configuration allowed
  - Cryptographic logon with CHAP
  - Multi-path/fail-over capable
  - User Interface using HII





IPsec - Network Security

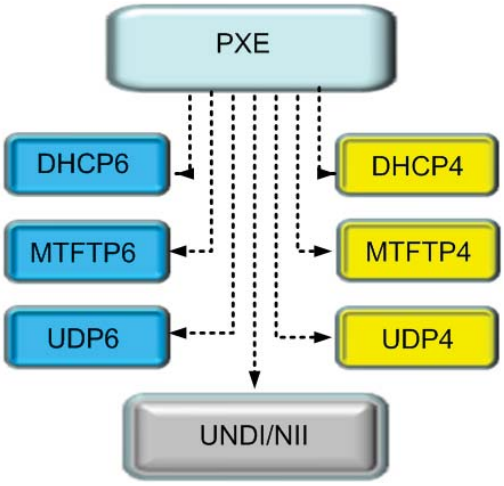
- Secure Internet Protocol Communication
  - Protects any application traffic across an IP network
  - Mandatory for IPv6
- Features include
  - AH, ESP, IKE version 2
  - HMAC-SHA1, TripleDES-CBC, AES-CBC
  - Transport/Tunnel mode
  - Pre shared Key/X.509 certificate authentication

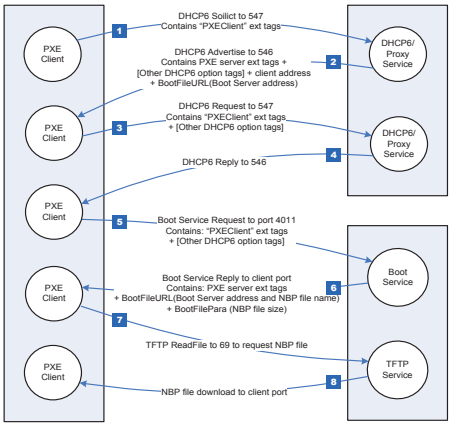


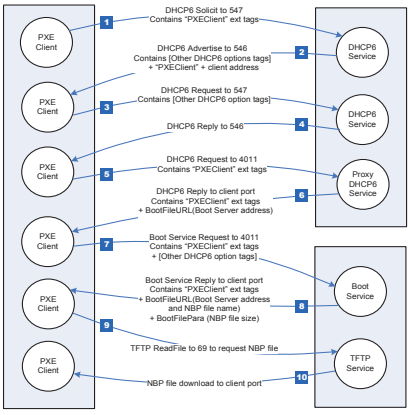
Improved Network Integrity

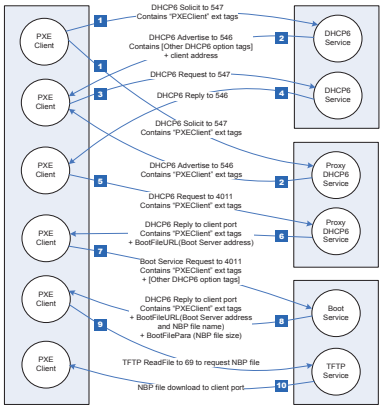
UEFI PXE Solutions

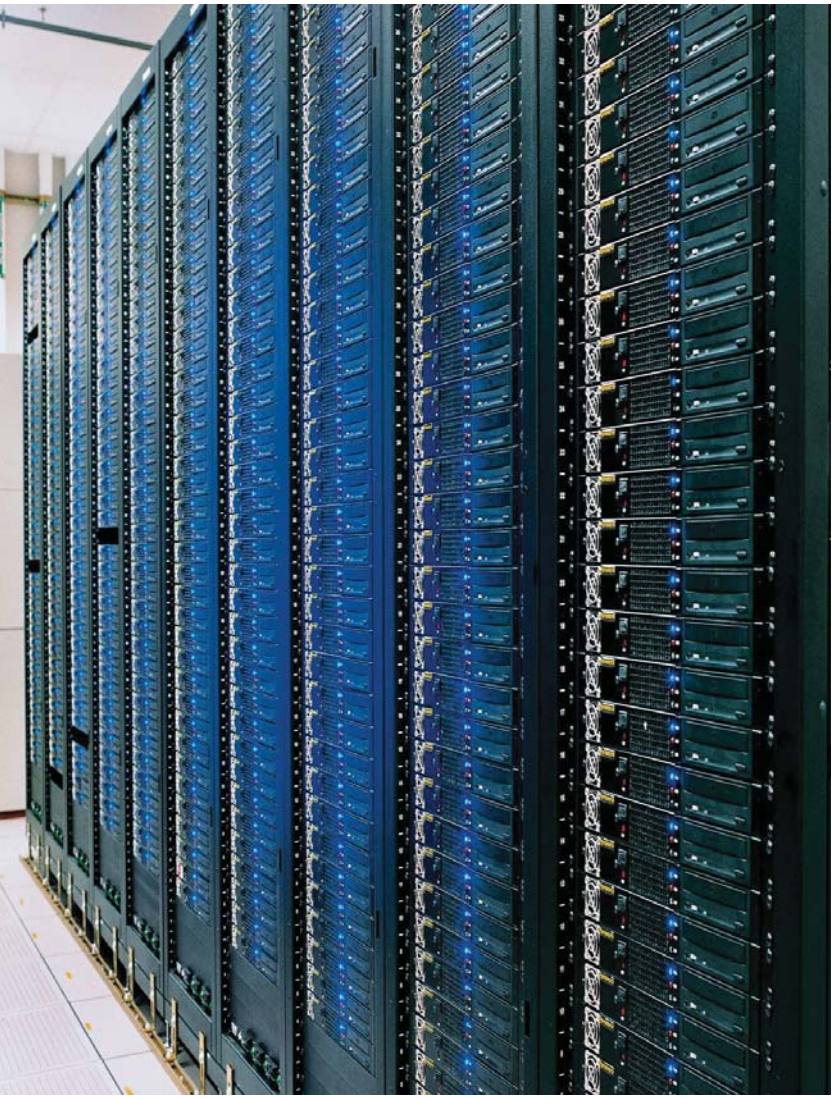
- Preboot eXecution Environment
  - General network booting
    - Independent of data storage device
  - IPv4 based PXE defined in PXE 2.1
  - IPv6 based PXE is defined in UEFI 2.3
- Technology includes
  - Dual network stack support
    - Evolution of network boot to IPv6 defin
      IETF RFC 5970
  - DUID-UUID support
    - Use SMBIOS system GUID as UUID







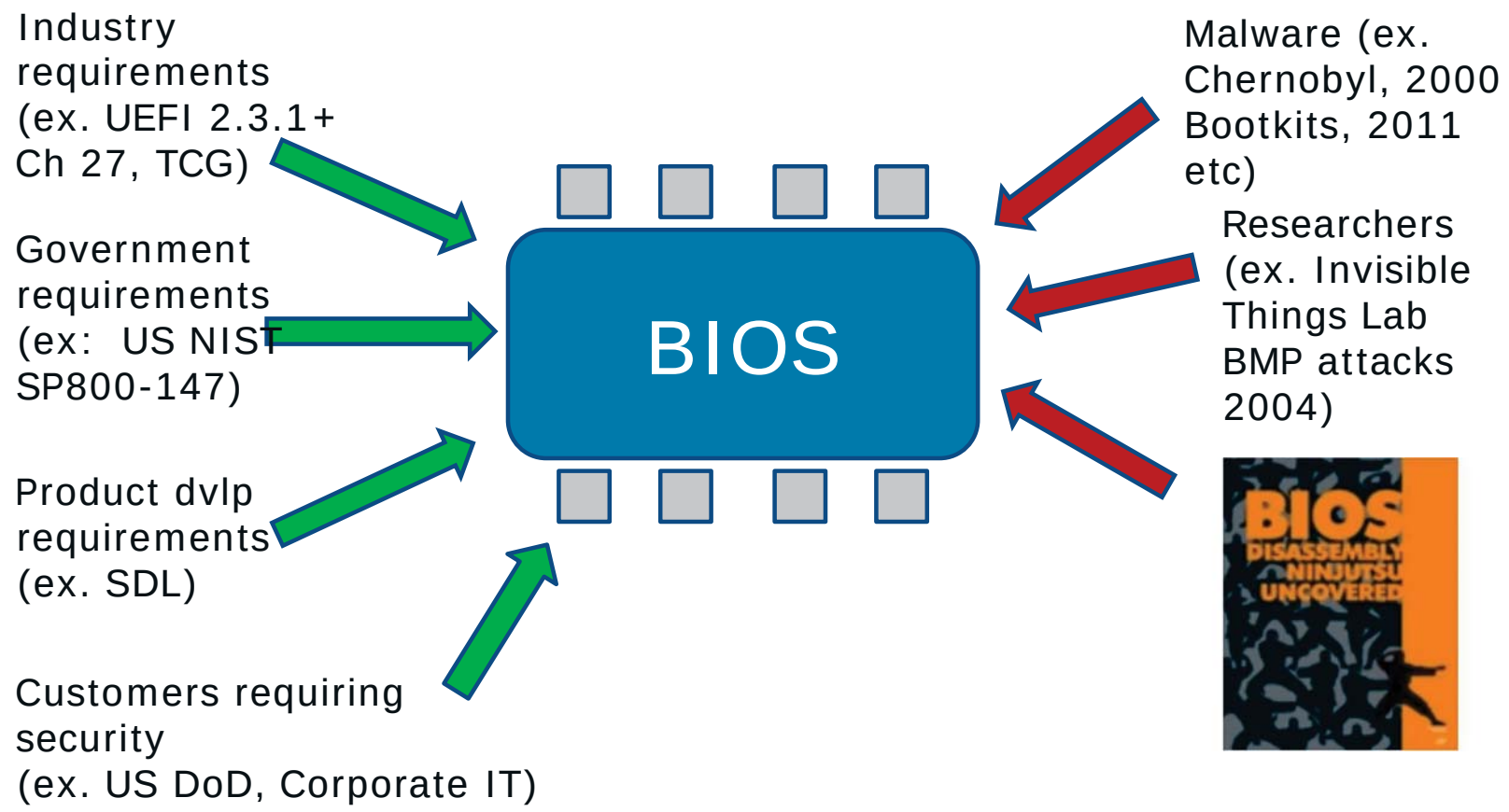




Security Features

Why

Pressure on BIOS



What

What is Security from BIOS Perspective

Secure Boot - UEFI

- Defined a policy for Image loading
  - Especially for network-loaded images
- Cryptographically signed
  - Private key at signing server, Public key in platform

Measured Boot -Trusted Computing Group (TCG)

- Trusted Platform Module (TPM) - Isolated storage and execution for Logging changes, attestation

NIST 800-147 -Security Guidelines for System BIOS Implementations - Capsule updates, firmware mngt protocol, authenticate user/admin w/ UID

UEFI User Identification

Pre-boot Authentication

- Facilitates appropriate user and platform administrator existence
- A standard framework for user-authentication devices
  - Static password, Network auth protocols, Smart cards, USB key & fingerprint sensors

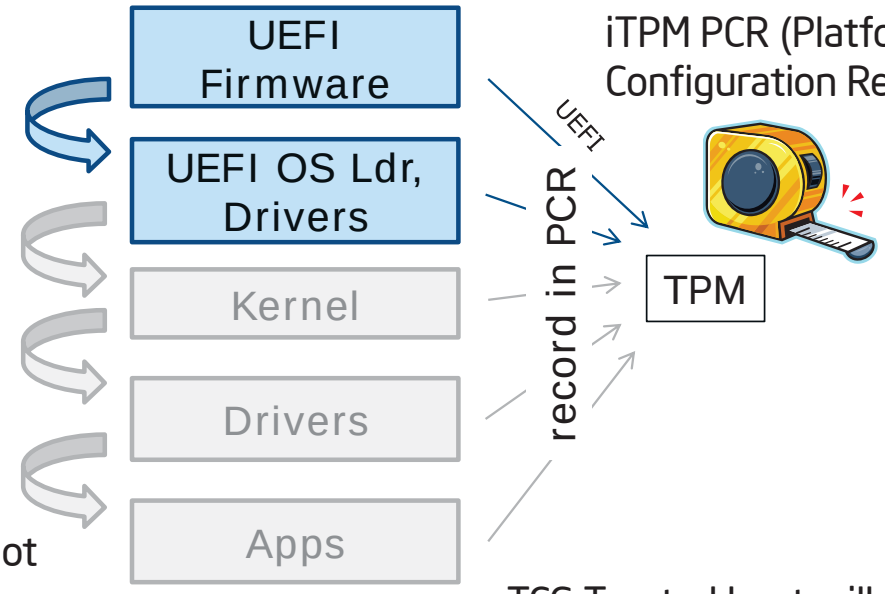
Support for various pre-boot authenticators

What

UEFI Secure Boot VS TCG Trusted Boot

UEFI authenticate OS loader
(pub key and policy)

Check signature of before loading



UEFI PI will measure OS loader & UEFI drivers into iTPM PCR (Platform Configuration Register)

- 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
- Incumbent upon other SW to make security decision using attestation

What

NIST Implementation Requirements

Make sure UEFI PI code is protected

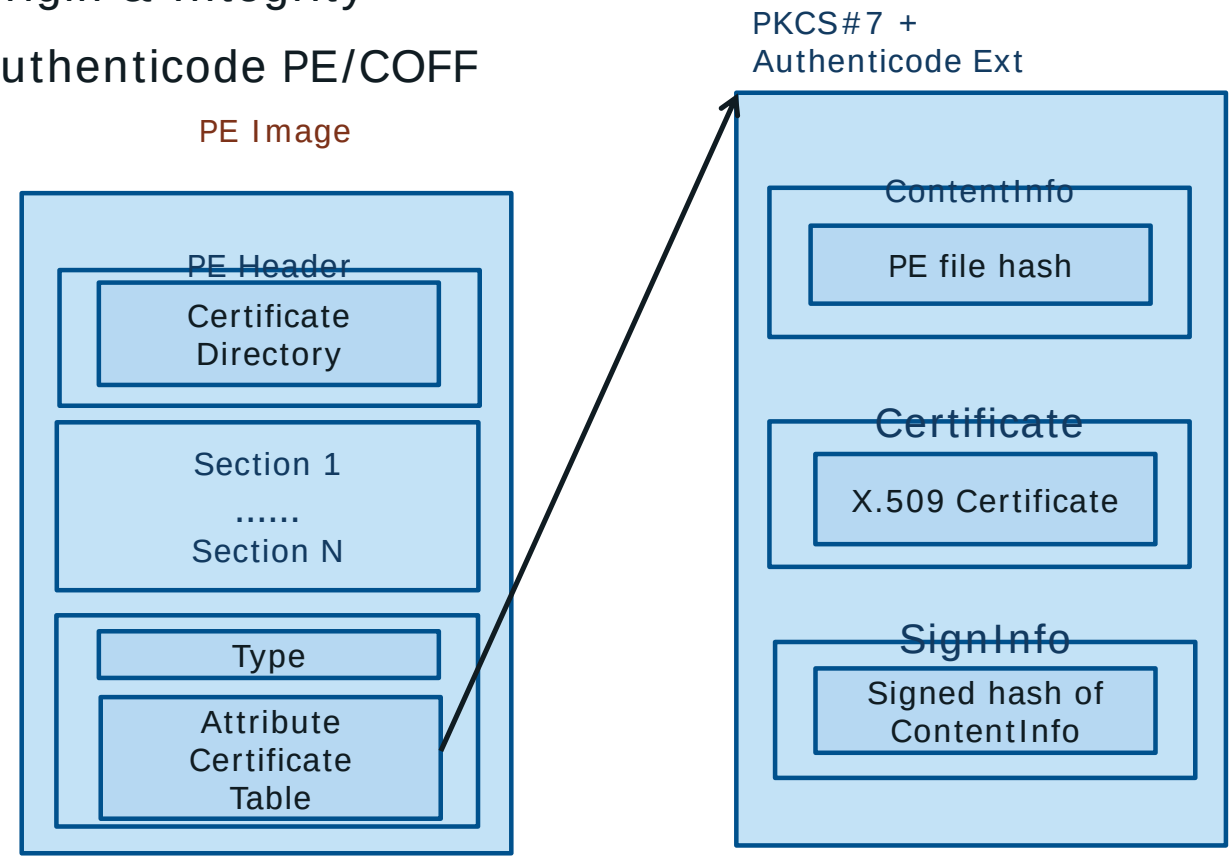
The NIST BIOS Protection Guidelines break down to three basic requirements...

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

UEFI Image (driver & application/OS loader) Signing

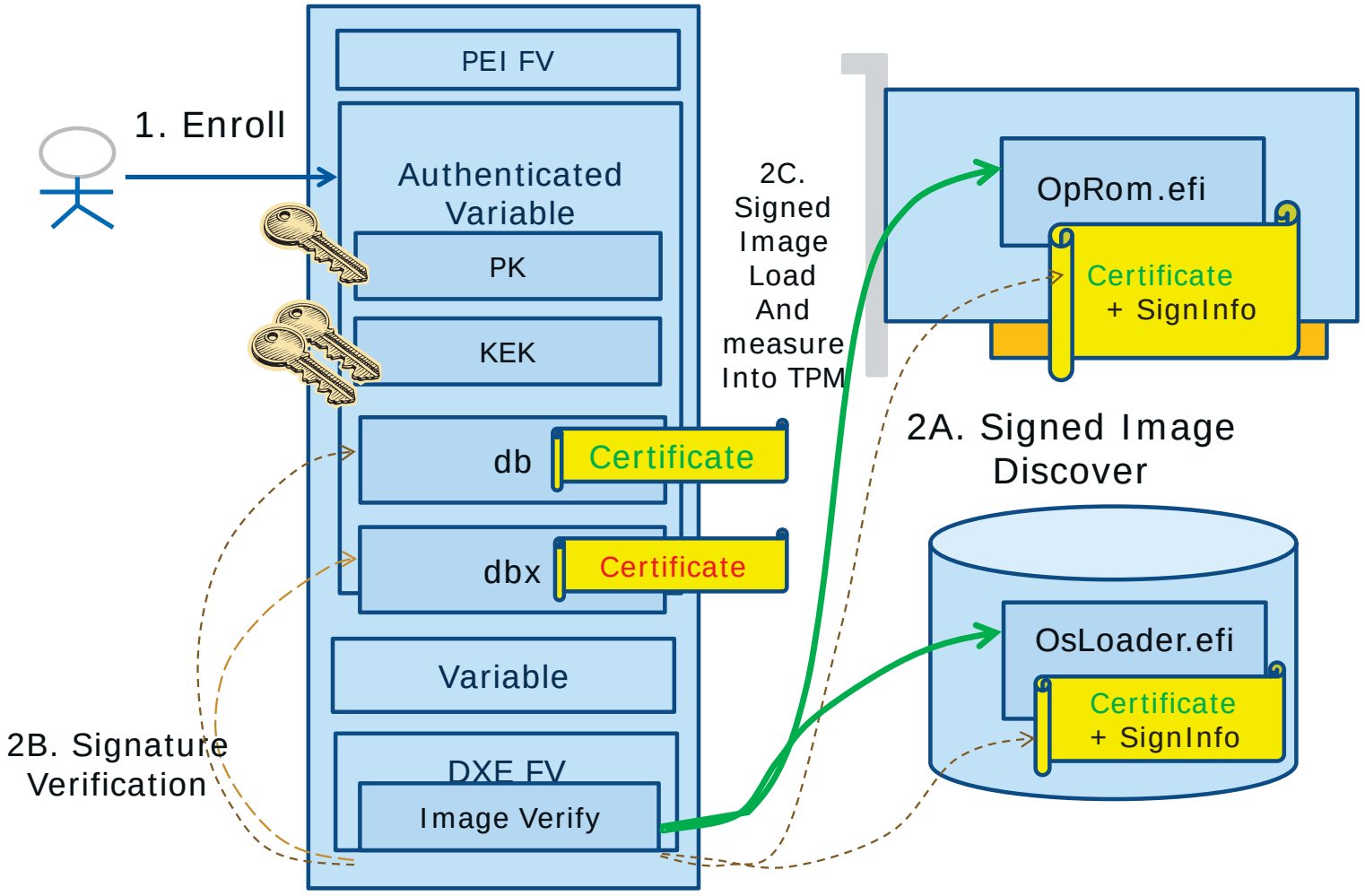
Why? – Origin & Integrity

How? – Authenticode PE/COFF

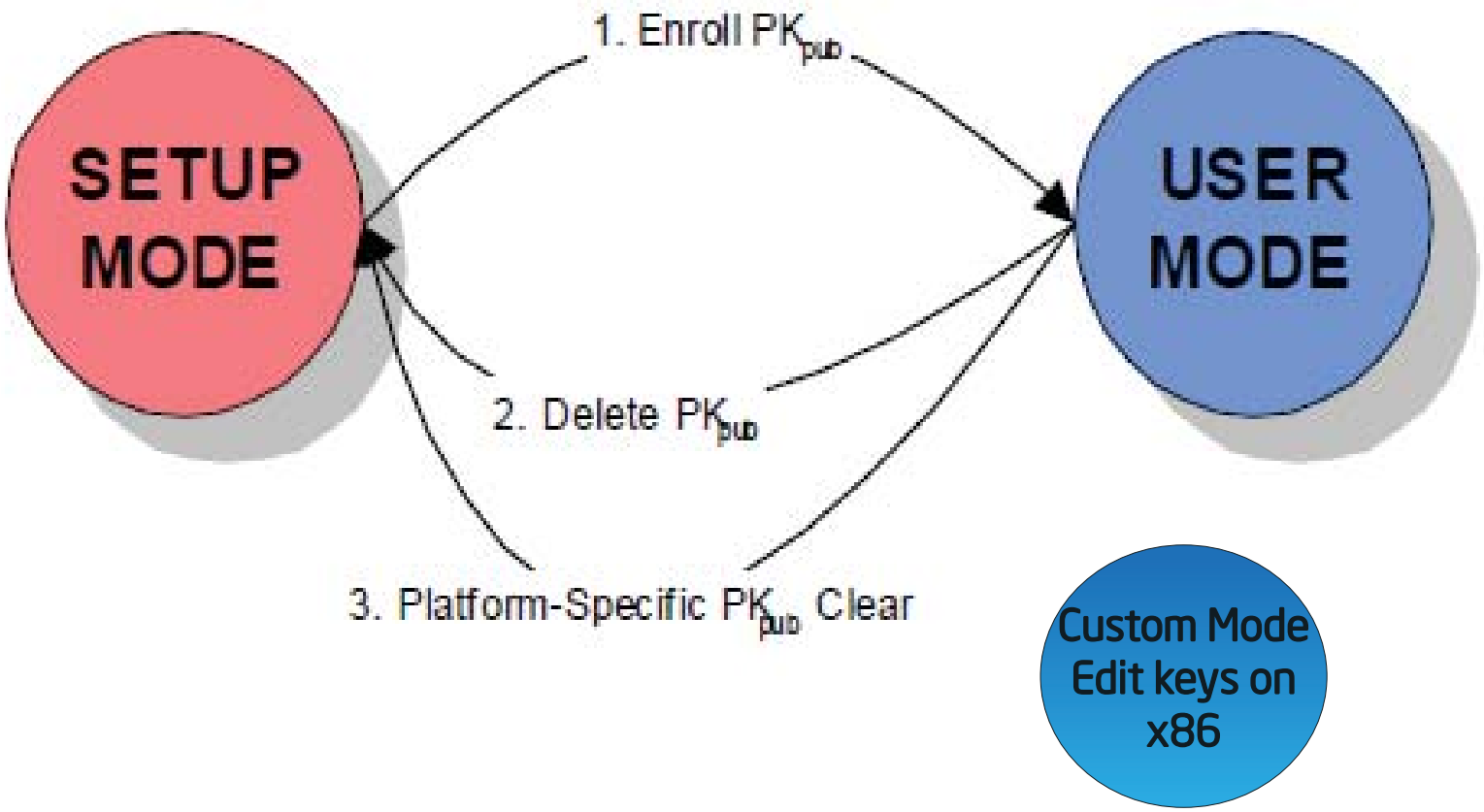


Authorization Flow

UEFI Secure Boot Flow



Put them altogether: UEFI Secure Boot



Summary

- OS absent networking important for deployment, provisioning, management, recovery
- Extensible architecture allows for rich pre-OS entworking
- Threats of UEFI extensibility are real
- Address w/ open standards and open source
- Netboot6 and Secure boot are coming w/ next OS wave (and like longevity of any shrinkwrap OS release, will continue for 10 yrs)
- Challenges in ecosystem enabling

For more information - UEFI Networking & Security

Intel Technology Journal, Volume 15, Issue 1, 2011, UEFI Today: Bootstrapping the Continuum, UEFI Networking and Pre-OS Security http://www.intel.com/technology/itj/2011/v15i1/pdfs/Intel-Technology-Journal-Volume-15-Issue-1-2011.pdf

UEFI 2.3.1a specification: chapters 15, 21-27 www.uefi.org

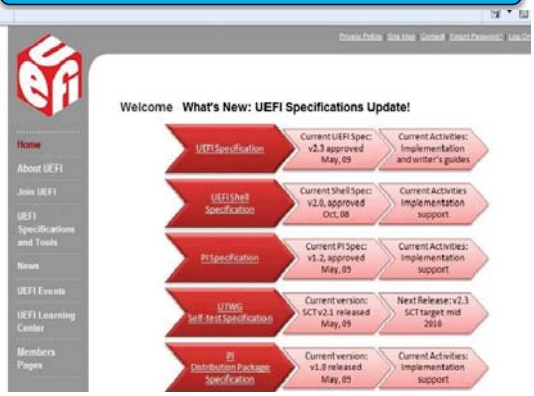
Beyond BIOS: Developing with the Unified Extensible Firmware Interface, 2nd Edition, Zimmer, et al, ISBN 13 978-1-934053-29-4 http://www.intel.com/intelpress

"DHCPv6 Options for Network Boot," Internet RFCs, ISSN 2070-1721, RFC 5970, September 2010, http://www.rfc-editor.org/rfc/rfc5970.txt

Zimmer, et al, "Trusted Platforms: UEFI, PI, and TCG-based firmware," Intel/IBM whitepaper, http://download.intel.com/technology/efi/SF09_EFIS001_UEFI_PI_TCG_White_Paper.pdf

UEFI Industry Resources

UEFI Forum



www.uefi.org

UEFI Open Source

www.tianocore.org

Intel UEFI Resources

www.intel.com/UDK

Intel EBC Compiler

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

UEFI Books/ Collateral

www.intel.com/intelpress

http://www.intel.com/technology/itj/2011/v15i1/index.htm

Seattle Meet-up

Thank You

Contact:
vincent.zimmer@intel.com
vincent.zimmer@gmail.com

Backup