UEFI Forum Update

UEFI Spring Plugfest – March 29-31, 2016
Presented by Dong Wei (The UEFI Forum)

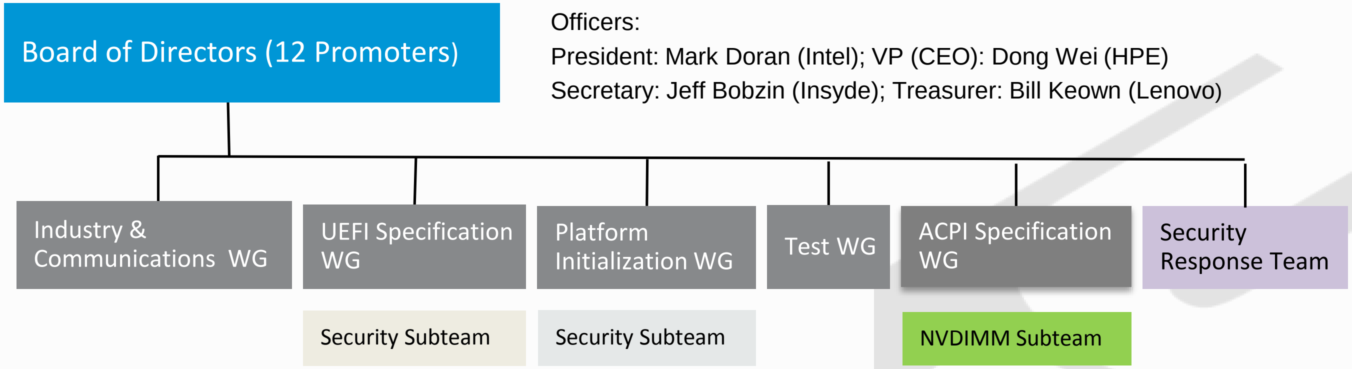
Updated 2011-06-01

Agenda

- Organization Update
- Specifications Update
- SCT Update
- Summary

Organization Update

The UEFI Forum



Board of Directors (12 Promoters)

Officers:
President: Mark Doran (Intel); VP (CEO): Dong Wei (HPE)
Secretary: Jeff Bobzin (Insyde); Treasurer: Bill Keown (Lenovo)

Industry & Communications WG

UEFI Specification WG

Platform Initialization WG

Test WG

ACPI Specification WG

Security Response Team

Security Subteam

Security Subteam

NVDIMM Subteam

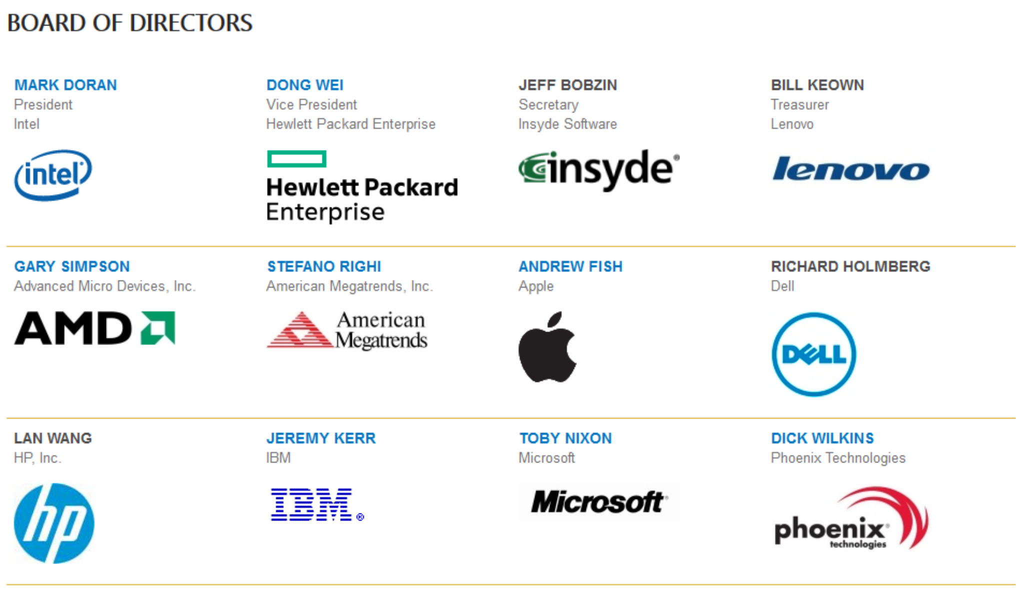
Configuration Subteam

Network Subteam

Shell Subteam

ARM Binding Subteam

12 Promoters
42 Contributors
218 Adopters
31 Individual Adopters
Total: 302



BOARD OF DIRECTORS

MARK DORAN
President
Intel

DONG WEI
Vice President
Hewlett Packard Enterprise

JEFF BOBZIN
Secretary
Insyde Software

BILL KEOWN
Treasurer
Lenovo

GARY SIMPSON
Advanced Micro Devices, Inc.

STEFANO RIGHI
American Megatrends, Inc.

ANDREW FISH
Apple

RICHARD HOLMBERG
Dell

LAN WANG
HP, Inc.

JEREMY KERR
IBM

TOBY NIXON
Microsoft

DICK WILKINS
Phoenix Technologies

Other Updates

- Updated UEFI/DMTF Work Register
  - Added Redfish coverage

Specification Update

Latest Specifications

- UEFI Specifications v2.6 (1/2016)
- ACPI Specification v6.1 (1/2016)
- UEFI Shell Specification v2.2 (1/2016)
- PI Packaging Specification v1.1 (1/2016)
- UEFI PI Specification v1.5 (Q2’2016)

What’s Not So New…

- But need to be tested
  - UEFI 2.5 Network Enhancements
    - Boot from HTTP
      - HTTP API
      - HTTP Helper API
      - DNS v4/6
      - RAM Disk Device Pat
    - WiFi
      - EAP Support
    - TLS
    - Bluetooth
    - REST Protocol

What’s New

- UEFI v2.6
  - Network Enhancements
    - Wireless MAC Connection II Protocol
    - RAM Disk Protocol
  - RAS
    - CPER Extension for ARM
  - User Interface
    - HII Font Ex, Glyph Generator, Image Ex and Image Generator Protocols
  - IO
    - SD/eMMC Pass Thru Protcol
    - Non-identity Mapped Address Translations in PCI Root Bridge and IO Protocols

What’s New

- ACPI v6.1
  - Persistent Memory
    - NFIT Updates
    - NFIT Root Device _DSM
  - RAS
    - APEI Extension for ARM
    - ERST/EINJ max wait time
  - Management
    - Graceful Shutdown Clarifications
    - Wireless Power Calibration Device
  - IO
    - Interrupt-signaled Events

What's New

- UEFI Shell v2.2
  - Network updates
  - Allow Execute() to not nest new shells
  - Add command line parameter to auto exit
  - New dh features
  - Setvar command re-factor
  - New command features for disconnect, comp, dmem, cls, reset, pci, bcfg, dmpstore

What’s New

- PI Packaging 1.1
  - Remove XSD reference
  - Ability to convey settings with discrete subsettings
  - Localized name to a package
  - Ability to convey detailed produces information
  - Ability to convey usage for PCDs from binary modules
  - Ability to convey detailed consumes information
  - Ability to convey PCD display information
  - Ability to convey enumeration-like information for PCD
  - Abstract type support
  - Ability to convey detailed BY_START/TO_START interaction
  - Ability to convey product limit information about Protocol/PPI/GUIDs

SCT Update

Latest SCTs

- UEFI SCT 2.4B
- Recommend FWTS Release 15.08.00 as ACPI SCT 5.1
- Under Development
  - UEFI SCT 2.5
  - FWTS Release as ACPI SCT 6.0
  - Alpha now, Beta@US Plugfest
  - Release by the end of 2016

SCTs for Taipei Plugfest

- UEFI
  - – SCT 2.5 Alpha
  - – Binaries/2016TaipeiPlugfest is located on the master branch of https://github.com/UEFI/UEFI-SCT.git
- ACPI
  - – FWTS 16.03.00
  - – https://wiki.ubuntu.com/FirmwareTestSuite/ReleaseNotes/16.03.00

PCIe Option ROM

PCIe Option ROM Alternative Architecture

Problem statement: **New server systems are in market based on alternate compute architectures** such as ARM, MIPS and Power… **today's PCIe add-in cards are unable to support this increased diversity and choice**

PCIe Option ROM Alternative Architecture

- X86 support already exists
  - Legacy BIOS
  - UEFI Native
- How many additional images are acceptable?
- Three options to support alternative architectures (in order of preference)
  - EBC Option ROM format
    - True cross architecture solution – adds a single image, could replace existing
  - Native ports to all target architectures
    - Requires multiple additional images and grows validation matrix too much
  - X86 emulation to run existing native option ROM format
    - Challenging during early boot and likely to incur compatibility issues
- Call to action: Connect with us here at the plugfest
  - Please attend the PCIe Option ROM Meeting
    (Room: This room (15F), Time: 15:00 (3:00 PM))

Summary

Summary

- The current State of the Forum is Strong
  - UEFI/ACPI are adopted on x64 Client and Server Systems
  - UEFI/ACPI are required for SB/SA/SBBR-compliant ARM Servers
- More opportunities in the IoT and embedded market
- Interests in more ISA bindings
  - Need to find a solution in the PCIe Option ROM space

Thanks for attending the UEFI Spring Plugfest 2016

For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org