Agenda

• Organization Update
• Specifications Update
• SCT Update
• Summary
Section Heading

Organization Update
The UEFI Forum

Board of Directors (12 Promoters)

- 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

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

12 Promoters
41 Contributors
221 Adopters
36 Individual Adopters
Total: 310

www.uefi.org

UEFI Plugfest – Sept 2016
Section Heading

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 (adoption postponed)
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/eMMMC Pass Thru Protocol
    • 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
What’s New

• PI v1.5 (current Final Draft)
  – SMM Environment to support newer architecture/platform designs
  – ARM extensions to Vol 4
  – Additional I2C PPIs
  – Add PPI to allow DEC to pass HOBs to PEI
  – Pre-DXE initialization of the SM Foundation
  – Handling PEI PPI descriptor notifications from SEC
  – SM stand-alone infrastructure
  – Communicate protocol enhancements
  – New MP protocol
  – Propagate PEI-phase FV verification status to DXE
  – Add SD/MMC GUID to DiskInfo protocol
  – Add EFI_FV_FILETYPE_SMM_CORE_STANDALONE file type
  – A number of errata
Section Heading

SCT Update
Latest SCTs

• UEFI SCT 2.4B
• Recommend FWTS Release 15.08.00 as ACPI SCT 5.1
Latest SCTs

• Under Development
  – UEFI SCT 2.5
    • Beta now, Release by the end of 2016
  – UEFI SCT 2.6
    • Alpha now, Beta@ Spring Plugfest
    • Release by mid 2017
  – FWTS Release as ACPI SCT 6.0/6.1
    • Recommend as ACPI SCT 6.0 by the end of 2016
    • Recommend as ACPI SCT 6.1 by mid 2017
SCTs for US Plugfest

• UEFI
  – SCT 2.5 Beta
    • Binaries/2016SeattlePlugfest is located on the master branch of https://github.com/UEFI/UEFI-SCT.git
  – SCT 2.6 Alpha
    • Binaries/2016SeattlePlugfest is located on the UEFI-2.6-SCT-DEV branch

• ACPI
  – FWTS 16.09.00
    • Tar: http://fwts.ubuntu.com/release/fwts-V16.09.00.tar.gz
    • PPA: https://launchpad.net/~firmware-testing-team/+archive/ubuntu/ppa-fwts-stable
    • Release notes: https://wiki.ubuntu.com/FirmwareTestSuite/ReleaseNotes/16.09.00
Section Heading

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 SBSA/SBBR-compliant ARM Servers

• However, the technology landscape is dramatically changing. UEFI/ACPI need to embrace the 3rd Platform era.
Thanks for attending the UEFI Spring Plugfest 2016

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