UEFI Forum Launches Non-volatile Memory and Boot from HTTP Support Across Three Specifications

Latest PI, ACPI, and UEFI Specifications Advance Firmware Programming and Management Capabilities

Beaverton, Ore.—April 30, 2015—Today, the UEFI Forum announced availability of the Platform Initialization (PI) Specification v1.4, the Advanced Configuration and Power Interface (ACPI) Specification v6.0 and the Unified Extensible Firmware Interface (UEFI) Specification v2.5. The Forum also released the UEFI v2.4B Self-Certification Test (SCT)—the test tool used to validate UEFI implementation conformance to the specification.

The new specifications introduce features that allow better access to and management of non-volatile memory (NVM) technologies.

"The next few years will see unprecedented system design innovation centered on advanced NVM. Defining the firmware hooks today is necessary to empower those system developers," said Mark Doran, president, UEFI Forum. "The UEFI community demonstrated an enormous commitment to this goal, updating its three specifications in parallel. This is a rare achievement for consortia. One that targets reliable NVM integration."

Individual Specification Updates
Beyond NVM support, the specifications include other new features required to keep the pre-boot environment current with the ongoing evolution of computing technology. Notably, many updates respond to industry member requests.

The PI Specification v1.4 now includes:

- **Graphics PPI:** Launches graphics subsystem and memory controller in the PI layer, providing access to various operating systems including those that do not require full UEFI conformance.
- **Multi-processor PPI:** Initializes processors in the PI layer, creating a prime environment for parallelization, giving the system full use of multi-processor machines.

- **Capsule PPI:** Discovers operating-system-initiated firmware updates during run time and allows updates to be handled in the driver execution environment (DXE).
- **No Execute Support:** Protects firmware against compromised hypervisor or operating system firmware.

The ACPI Specification v6.0 now includes:

- **CPU Topology Recognition:** Identifies different CPU topologies, enabling finer control of SoCs—thereby improving power efficiency.
- **Source Language Evolution:** Introduces high-level language including symbolic operations and expressions for intuitive programming.

The UEFI Specification v2.5 now includes:

- **Boot From HTTP:** Provides an improved UEFI replacement for iPXE.
- **Platform Recovery:** Explicitly defines standard (non-emergency) boot options as well as OS and platform firmware recovery options for when the system boot fails.
- **Connectivity Support:** Supports *Bluetooth*® technology and Wi-Fi/EAP2.
- **High Assurance Enterprise Replacement:** Allows automated platform deployment for higher security Secure Boot configurations.

Download the specifications here to learn more about these and other updates.

About The UEFI Forum
The Unified Extensible Firmware Interface (UEFI) Forum is a world-class non-profit industry standards body that works in partnership to enable the evolution of platform technologies. The UEFI Forum champions firmware innovation through industry collaboration and the advocacy of a standardized interface that simplifies and secures platform initialization and firmware bootstrap operations. Both developed and supported by representatives from industry-leading technology companies, UEFI specifications promote business and technological efficiency, improve performance and security, facilitate interoperability between devices, platforms and systems, and comply with next-generation technologies. To learn more about the UEFI Forum, visit www.uefi.org.