UEFI ARM Update

UEFI PlugFest – March 18-22, 2013
Andrew N. Sloss (ARM, Inc.)
AGENDA

• economics
• technology
• status
• summary
• questions
ECONOMICS

• What are the ARM numbers?

  – Processors shipped in 2012 : \( \sim 8.7 \text{ Bu} \) (~7.9 Bu `11)
  – Processors shipped in total : \( >30 \text{ Bu} \)
  – Processor licenses : \( \sim 960 \) (850’12)
  – Semiconductor partners : \( 310 \) (290’12)
  – Process technology : 14 – 250 nm
  – Connected community members : \( 1000+ \) (950’12)
ECOMONICS (1000+)
REASONS

• Driving forces for UEFI on ARM
  – Processor and system complexity increasing
  – Support for existing OEMs that are developing ARM processor-based solutions using UEFI
  – Help standardize the boot procedure for ARM processor-based platforms
  – On-going ARM goal is to improve the hardware-software interface for Operating Systems that target the ARM architecture

• Advantages to ARM partners and OEMs
  – Write once per platform and saves costs in boot loader development/engineering
  – UEFI specification written down and peer reviewed
  – Tested UEFI drivers available from 3rd party peripherals providers
  – Provides an environment for manufacturing tests
Cortex-A Series
“Low-Power Leadership”

Cortex-A9
Shipping since 2009
2nd generation 1-4X SMP
4x1750DMIPS@700MHz+ in 40LP

Cortex-A8

Cortex-A5

Cortex-A7
1/5 the power of Cortex-A15
Architectural alignment with Cortex-A15

Cortex-A15
>2GHz+ in 28HPM
Virtualization
1TB physical addressing
big.LITTLE with Cortex-A7

Cortex-A57
ARMv8 64-bit

Cortex-A53
ARMv8 64-bit

2011  2012  2013  2014  Future
NEW

• What new technologies have UEFI implications?

  • **Big.LITTLE** technology provide heterogeneous computing technology providing both high performance and extreme power efficiency – serving dynamic computing demands (32-bit & 64-bit)

  • **Virtualization** includes Large Physical Address Extensions (LPAE), second level of MMU page table translations and support for hypervisors (32-bit & 64-bit)

  • **ARMv8/Aarch64** brings 64-bit support to the ARM Architecture increasing the register file, media instructions, addressing range and cryptography instructions (64-bit)
What have UEFI ARM Binding Sub-Team (ABST) been doing?

• Proposed Aarch64 UEFI Bindings
  • adding support for the new architecture in the next UEFI specification

• Virtualization Protocol proposal
  • solve the way to start an hypervisor from ARM 32-bit UEFI

• Boot Architecture
  • Discussions around the standardization of the ARM Boot Architecture
IMPLEMENTATION

ARM focus:

- Add support for Aarch64 in Tianocore and SCT
  - Public when the Aarch64 UEFI Bindings is approved by USWG

- Implementation of the ARM Virtualization Protocol proposal
  - Linux KVM can be started from ARM 32-bit UEFI

- Focus on aligning the Open Source implementation
  - Tianocore with the UEFI Specification

- Support the Operating System requirements

- Enable the ARM Ecosystem through Open Source contributions
ECOSYSTEM

UEFI-in-ARM (the company):

- UEFI is the recommended ARM Boot Loader for Aarch64
- Strong interaction between the UEFI team and the different divisions in ARM (from the Linux kernel team to the compiler team) to enable UEFI
UEFI in Linaro:

- UEFI Platform bring-up on the Linaro's member platforms
  - ARM Versatile Express (from Cortex A5 to the latest big.LITTLE Cortex-A15 / Cortex-A7)
  - Pandaboard (TI OMAP 4 - Cortex A9)
  - Origen (Samsung Exynos 4 – Cortex A9x4)
  - Arndale (Samsung Exynos 5 – Cortex A15x2)

- Port Grub2 to ARM architectures

- Improve UEFI support to boot Linux kernel
SUMMARY

- UEFI brings a neutral boot loader capable of booting both open-source and non-open source Operating Systems
- UEFI is a framework that grows and shrinks depending upon requirements
- Specification written down and peer-reviewed
- Lots of validated software already
- Ability to support a 3rd party peripheral ecosystem
- Write-once, validate-once, support all OSes
- Next technology, support for Aarch64 and virtualization
QUESTIONS?
Thanks for attending the UEFI Spring PlugFest 2013

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

presented by