presented by





UEFI ARM Update

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

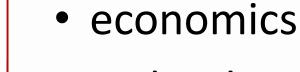
UEFI Spring PlugFest – March 2013

www.uefi.org

1

AGENDA





- technology
- status
- summary
- questions

ECONOMICS

• What are the ARM numbers?



- Processors shipped in 2012
- Processors shipped in total
- Processor licenses
- Semiconductor partners
- Process technology
- Connected community members

- : ~8.7 Bu (~7.9 Bu`11)
- : >30 Bu
- : ~960 (850'12)
- : **310** (290'12)
- : **14 250 nm**
- : 1000+ (950'12)

ECOMONICS (1000+)



Silicon Partners

Kater 🧐 OTTE Dalta 🕬 🐡 🖓 Alta CEVA ATTACA CAST dialog austranscrugations NVDM. alvaylew 5 5 6 CAMSYS Calestia Comes Uniquify B Donglas It Tak EPSON ETRI ARSNACON OCT- GER & MARCH COURSEN (2) BILL Interior State THE NUMBER OF THE STREET STREET TES Autors KEYRSIC NECENYERYYS AND ECI And Post of Lot 6 miczaL' MICRONAS /agnaCho+ NEC MASter QNETERICT Mediatek NOR NUMA PIXIM UMC Smith ? @ Aurres A constant and examine and an and a second SMT Wine SAND Gainspan. Silicon Hive SHARP SHARP SMIT 57 A SUBC. THOMSON TOSHIBA Scoled ARCHOS TONER SMIC Scours Transfer States WSOF Aurora VLSI Sectors de la companya de la company (intrinsity Territoria CHIPMUTS Of Centrality SHILL STEPHING () Chartored FOCUS G BIFELLS Hahan KABEN SALINEC THE ARCHOS Preescale SFAB totas Care OLA LSIS Nav Asic Annous Suppys Contention Rambus Digital Hocks MOXIC manoradio S RAPLUS PROSPEED THE MARKED MEMORY \$ FIOSCHP PHOSPHED THE MENENCE 2/log Stices Charles Con Her CONEX Armade Concessions ZTEIC ZARNAY (QUILLOWN OR COMPANY MORILEND REFERENCE PUBLIC





REASONS

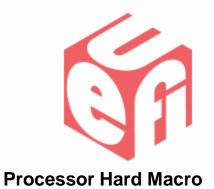


- Driving forces for UEFI on ARM
 - Processor and system complexity increasing
 - Support for existing OEMs that are developing ARM processor-based solutions using UEFI
 - Help standardize the boot procedure for ARM processor-based platforms
 - On-going ARM goal is to improve the hardware-software interface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



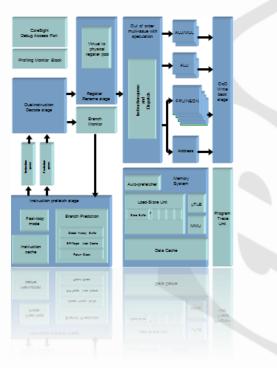
TECHNOLOGY

UEFI Spring PlugFest – March 2013



Dide Dide Bide Dide Bide





Architecture "ARMv8"

PROCESSORS

ARM[®] Architecture Reference Manual ARM[®]V7-A and ARM[®]V7-R edition

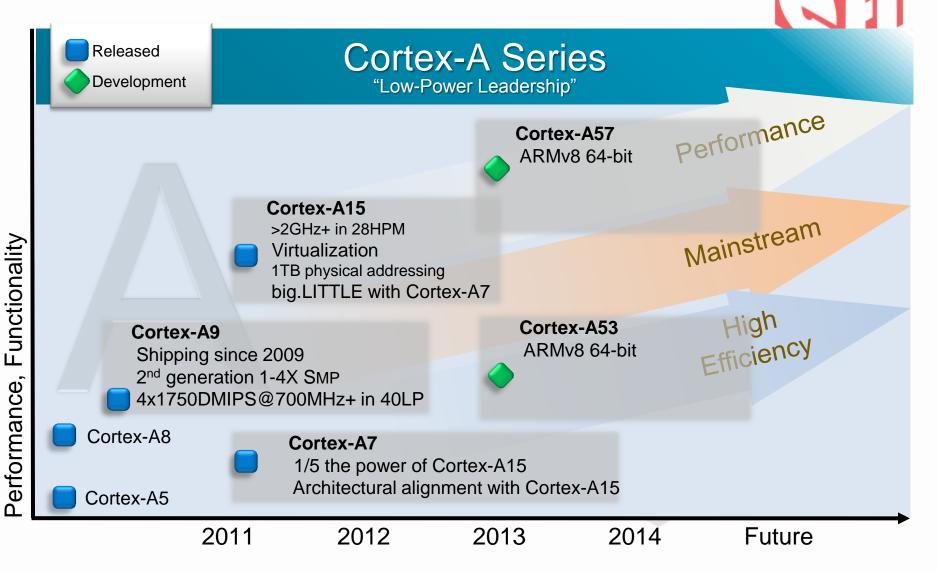


Copyright © 1996-1998, 2000, 2004-2010 ARM Limited. All rights reserved. ARM DDI 0406B_errata_2010_Q3 (ID100710)

Copyright @ 1996-1998, 2000, 2004-2010 ARM Limited. All rights reserved. ARM DDI 04068_emata_2010_Q3 (ID100710)

ARM'

APPLICATION ROADMAP







- 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)





STATUS

SPECIFICATION



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:

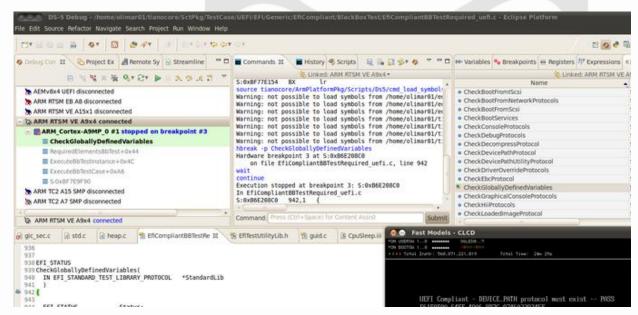
- Add support for Aarch64 in Tianocore and SCT
 - Public when the Aarch64 UEFI Bindings is approved by USWG
- Implementation of the ARM Virtualization Protocol proposal
 - Linux KVM can be started from ARM 32-bit UEFI
- Focus on aligning the Open Source implementation
 - Tianocore with the UEFI Specification
- Support the Operating System requirements
- Enable the ARM Ecosystem through Open Source contributions

ECOSYTEM¹



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



ECOSYSTEM²



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 Spring PlugFest – March 2013

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?

UEFI Spring PlugFest – March 2013

Thanks for attending the UEFI Spring PlugFest 2013

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

presented by

ARM

