OPEN POSSIBILITIES.

Arm & Ampere support for standards-based Open Source Firmware
Arm & Ampere support for standards-based Open Source Firmware

Samer El-Haj-Mahmoud, Sr Principal Architect, Arm
Peter Pouliot, Developer Advocate, Ampere Computing
Vision: “Software Can Just Work on Arm-based Devices”
Arm SystemReady Vision

**LS**
"Just Works" for Linux OSes on Arm server SoCs
- Program tailored to meet needs of many hyperscalers
- Ensures standard firmware interfaces to deploy and maintain
- Targets hyperscalers’ Linux environment

**SR**
"Just Works" on Arm server or workstation SoCs
- Program tailored to meet needs of Windows, VMware, Linux, and BSD ecosystem
- Ensures standard firmware interfaces to deploy and maintain
- Supports old OSes to run on new hardware and vice versa
- Targets generic off-the-shelf OSes
Arm SystemReady standards

Hardware requirements (BSA – Base System Architecture)
- **BSA v1.0 (Oct 2020)** – generic hardware target
- Documents a minimal set of CPU and system architecture necessary for an OS to boot and run. Includes aspects such as PCIe integration.

Server Hardware Supplement (SBSA)
- **SBSA**: Servers market segment specific hardware requirements
  - Mostly follows the Arm architecture enhancements
  - SBSA v7.0 (Jan 2021)

Firmware (BBR – Base Boot Requirements)
- Expands to include common firmware interfaces, but recognizes that different software stacks will require different recipes
- **BBR v1.0 (Oct 2020)**
- **SBBR, EBBR, LBBR Recipes** targeting different OSes

http://www.arm.com/systemready-certification-program
Arm Server Management Standards

- **SBMR** – Server Base Manageability Requirements
  [https://developer.arm.com/documentation/den0069/]
- Hardware and Firmware requirements for standard system management of Arm SystemReady SR or LS compliant servers.
- Co-developed with the Arm Servers ecosystem partners, with leadership from Ampere® Computing.
- Builds on top of prevalent management standards:
  - DMTF Redfish
  - DMTF MCTP, PLDM, SPDM, NC-SI
  - OCP Hardware Management
  - IPMI
Arm Standards-based server design

Standard HW Management
- OPEN
- Compute Project
- openstack
- ANSIBLE
- OpenBMC

Commercial
- BMC FW

Standard OSes and Hypervisors
- redhat
- SUSE
- Windows
- VMware ESXi
- ubuntu
- CentOS
- fedora
- Oracle Linux
- FreeBSD
- NetBSD
- tianocore

Commercial
- System FW

Arm Server Standards
- SBMR

arm SystemReady
- SBSA
- BSA
- BBR
- BBSR

Industry Standards
- DMTF
- IPMI
- OPEN
- Open Compute Project
- arm
- Trusted Computing Group
- CXL
- Compute Express Link
- NIST
- PCI SIG
- OPEN
- Compute Project
Ampere® Altra®: The First SystemReady SR Server Platform!

<table>
<thead>
<tr>
<th>Company</th>
<th>Ampere Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Mt. Jade Platform</td>
</tr>
<tr>
<td>SoC family</td>
<td>Ampere Altra 64-bit Multi-Core Arm processor</td>
</tr>
<tr>
<td>Firmware version</td>
<td>0A0Cl.1.01.20200923</td>
</tr>
<tr>
<td>ACS version</td>
<td>Enterprise ACS v2.5</td>
</tr>
<tr>
<td>BSA details</td>
<td>SBSA level 4</td>
</tr>
<tr>
<td>BBR details</td>
<td>SBBR (BBR 1.0)</td>
</tr>
<tr>
<td>Arm SystemReady certification</td>
<td>SystemReady SR v2.0</td>
</tr>
</tbody>
</table>

- Windows PE (from Windows ADK for Windows 10, version 2004)
- Ubuntu 20.04
- CentOS 8
- Debian 10 (buster)

https://developer.arm.com/architectures/system-architectures/arm-systemready/sr
Ampere® Mt. Jade Platform

- 2P/2U reference platform for Ampere® Altra®
- https://amperecomputing.com/altra/#jade
Ampere® Support for Open-Source Firmware

Ampere is committed to supporting open-source in the firmware ecosystem
• Enable open-source firmware on Ampere platforms
• Active engagement within the community

Firmware Projects
• TianoCore/EDK2 & LinuxBoot
• OpenBMC
• OpenOCD
• OCP/OSF Efforts

Ampere Github: https://github.com/AmpereComputing

OPEN POSSIBILITIES.
Ampere® OCP/OSF Efforts

• The OCP Open System Firmware project’s purpose is to allow platform owners to “own their firmware”. One of the central compliance requirements is that firmware be open-source (code) or freely redistributable (binaries).
• Ampere will be working towards certifying our Mt. Jade firmware to be OCP/OSF compliant in the next few months. Much of the stack is already open-source and Ampere is working to make the relevant binaries publicly redistributable.
• At the end of this process, the firmware components for Mt. Jade will be available from OCP’s website.
• Link: https://www.opencompute.org/projects/open-system-firmware
Arm and TianoCore

- TianoCore is an open-source community project with implementations of Firmware standards: UEFI, PI, ACPI, SMBIOS, TCG, UEFI Shell, etc..
  - Including support for Arm SBBR specification
- Growing Arm community (maintainers, contributors)
  - Complete and partial Arm64 platforms, silicon drivers, libraries, and support code
- https://github.com/tianocore/:
edk2, edk2-platforms, edk2-non-osi, uefi-sct
Support for Ampere® Altra® on Mt. Jade

- Ampere is committed to contributing at a frequent (monthly) cadence towards TianoCore/EDK2 opensource software
- Latest release is v1.07.300
- https://github.com/AmpereComputing/edk2-platforms/releases/tag/v1.07.300-ampere

Began support for Ampere® Altra Max in March 2021
Arm and LinuxBoot

Arm ecosystem working on defining LBBR (LinuxBoot Base Requirements) for Arm servers

• Foundation for Arm SystemReady LS class of servers
• Leveraging existing Arm server approach to fully open-source firmware
• Demos and PoCs on multiple arm platforms, including FVP, QEMU, RPi 4, as well as production offering from Ampere® (Mt Jade)

OPEN POSSIBILITIES.
What is LinuxBoot

- https://www.linuxboot.org/
- LinuxBoot is a firmware for modern servers that replaces specific firmware functionality like the UEFI DXE phase with a Linux kernel and runtime. Improves boot reliability and boot time.
- Old idea, but somewhat new in servers.

Ampere® Support

- Ampere EDK2 GitHub has a build option enabling LinuxBoot, which replaces the BDS shell with LinuxBoot & u-root UI.
- Will be working to integrate LinuxBoot into EDK2 upstream.
- LinuxBoot executable built directly from the GitHub repo (https://github.com/linuxboot/mainboards/tree/master/ampere/jade)
Arm and OpenBMC

- [https://www.openbmc.org/](https://www.openbmc.org/)
- Collaborative project for an open source BMC firmware stack
- Arm is on the OpenBMC Technical Steering Committee (TSC)
- Participating in upstream activity, enabling Arm specific PoC and SBMR functionality on OpenBMC
  - SBMR explicitly calls out OpenBMC for illustrating implementation guidance
  - MCTP/PLDM sensors and RAS error logging support for the Arm Side-Band Management Interface
  - Arm Remote Debug sample implementation using OpenBMC and OpenOCD
OpenBMC

Support for Mt. Jade
- linux: Linux kernel changes (including Ampere’s SM Pro MFD drivers and Ampere’s bmc-ssif driver)
- ssifbridge: Ampere’s SSIF Bridge implementation
- Monthly release cadence, latest release is v1.10.100

Upstreaming status
- Base meta-ampere and ssifbridge upstreamed
- Additional code under meta-ampere continues to be upstreamed over time
- SM Pro MFD drivers to be upstreamed for review - pending
- ssif-bmc driver to be upstreamed for review - pending
Ampere Open-Source Firmware Links

EDK2
- https://github.com/AmpereComputing/edk2
- https://github.com/AmpereComputing/edk2-platforms
- https://github.com/AmpereComputing/edk2-ampere-tools
- https://github.com/AmpereComputing/edk2-non-osi

OpenBMC
- https://github.com/ampere-openbmc

OpenOCD
- https://github.com/AmpereComputing/ampere-openocd

LinuxBoot
- https://github.com/linuxboot/mainboards/tree/master/ampere/jade
Call to Action

• How to get involved in Arm SystemReady
• www.arm.com/systemready-certification-program
• Visit Ampere and Arm booths and sessions @ OCP Global Summit 2021!
Visit Ampere @ OCP 2021

Booth (B13)
• Demos: Ampere® AI, CIDR, Android in the Cloud
• Platforms on display

Keynote Nov 9 @ 9:34 am PST
• Renee James, Ampere CEO: A New Era with Efficient Cloud-Native Processors: Open Collaboration for Rapid Innovation

Talks
• 11/9 @ 2:30pm Expo Hall Talk
• 11/9 @ 3:30pm Executive Talk – Jeff Wittich CPO
• 11/10 @ 9:30 am Tech Talk: The Era of Cloud Native platforms is here - presenting the Ampere Mt. Jade reference platform running Ampere Altra Max CPUs
• 11/10 @ 4pm Tech Talk: Arm and Ampere Support for Standards-Based Open System Firmware
Visit Arm @ OCP 2021

**Booth (B11)**
- Demos: Arm SystemReady Certified Hardware
  - Arm SystemReady, SR – ServerReady:
    - Ampere Altra ‘Mt Jade’ Platform (Wiwynn)
  - Arm SystemReady, ES – Embedded Server:
    - Hawkeye Tech HK-6010
    - SolidRun Macchiatobin
    - Arm SystemReady, IR – IoT:
      - Raspberry Pi

**Talks**
- Wed, Nov 10 @ 8:35am Room 211A-D
  Cost Modeling Analysis for Heterogeneous Integration of Chiplets, Javier DeLaCruz (Arm), Mudasir Ahmad (Google), Anu Ramamurthy (Microchip Technology)
- Wed, Nov 10 @ 10:00am Room 220C
  Confidential Compute Solutions in Arm Ecosystem, Sridhar Valluru (Arm)
- Wed, Nov 10 @ 1:00pm Room 210C
  Introduction to Open System Firmware (OSF) at OCP, Dong Wei (Arm), Ryan O’Leary (Google), Anjaneya “Reddy” Chagam (Intel)
- Wed, Nov 10 @ 2:30pm Room 210BF
  Arm and Ampere support for Standards-based OpenSource Firmware, Samer El-Haj-Mahmoud (Arm), Peter Pouliot (Ampere)
Thank you!