SystemReady
SR and ES
Standards for Servers and the Edge

Samer El-Haj-Mahmoud, Dong Wei
Arm Limited
Arm SystemReady

- SystemReady is a foundational compliance certification program that brings a level of consistency across broad range of devices, initially in the Server, Infrastructure Edge and IoT Edge sectors.
- Our vision is for software that works seamlessly across a vibrant, diverse ecosystem of hardware.
- Focusing on the common components of the software stack – the OS, hypervisor, and middleware components.
- Establishing a more uniform hardware system architecture and consistency around key processes like boot, through our standards-based approach.
- Enabling partners to focus on innovating & deploying the differentiating application layers of software, with a simplified and faster time to market.
Vision

Software Can Just Work on Arm-based Devices

EXTEND THE SUCCESS OF ARM SERVERREADY TO EMBEDDED SERVERS AND IOT

- App
- SDK
- FW/OS
- HW
- SIP "A"
- SIP "B"
- SIP "C"

- App
- SDK
- FW/OS
- HW
- SIP "A"
- SIP "B"
- SIP "C"

- App
- Common OSes
- FW Compliant
- HW Compliant
- SIP "A"
- SIP "B"
- SIP "C"
Key Specifications

Hardware Baseline (BSA – Base System Architecture)
- Documents a minimal set of CPU and system architecture necessary for an OS to boot and run. Includes aspects such as PCIe integration etc.
- Introduce BSA – generic hardware target

Hardware Supplements (xBSA)
- A roadmap of levels that document an increasing set of hardware features, largely following the progression of the CPU architecture
- Introduce xBSA, adds a roadmap for market segment hardware features
- Example: SBSA for servers

Firmware (BBR – Base Boot Requirements)
- Expand to include common firmware interfaces, but recognize that different software stacks will require different recipes

https://developer.arm.com/architectures/system-architectures/arm-systemready
BBR Specifications

**BBR Interfaces**

- PSCI, SMCCC (common for all)
- UEFI (for SBBR recipe)
- ACPI (for SBBR recipe)
- SMBIOS
- Exceptions (if needed)

**BBR Recipes Tailored to Various OSes**

**SBBR**
- Same requirements as current SBBR
  - UEFI, ACPI, SMBIOS, PSCI, SMCCC

**EBBR**
- UEFI, PSCI, SMCCC

**LBBR**
- LinuxBoot, ACPI, SMBIOS, PSCI, SMCCC

**Related Specifications**

**BBSR (Base Boot Security Requirements)**
- Secure Boot and Firmware Update

**EBBR (Embedded BBR)**
- Community development
  - BBR spec refers to EBBR spec as needed

## One Program, Multiple Bands

<table>
<thead>
<tr>
<th>Certification</th>
<th>Description</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>SystemReady SR</td>
<td>ServerReady</td>
<td>BSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SBSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BBR(SBBR)</td>
</tr>
<tr>
<td>SystemReady LS</td>
<td>LinuxBoot Server</td>
<td>BSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SBSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BBR(LBBR)</td>
</tr>
<tr>
<td>SystemReady ES</td>
<td>Embedded Server</td>
<td>BSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BBR(SBBR)</td>
</tr>
<tr>
<td>SystemReady IR</td>
<td>IoT</td>
<td>BSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BBR(EBBR)</td>
</tr>
<tr>
<td>Security</td>
<td>Security Option</td>
<td>BSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BBR (SBBR or EBBR)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BBSR</td>
</tr>
</tbody>
</table>
Focus of this Presentation

<table>
<thead>
<tr>
<th>Certification</th>
<th>Description</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>SystemReady SR</td>
<td>ServerReady</td>
<td>BSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SBSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BBR(SBBR)</td>
</tr>
<tr>
<td>SystemReady ES</td>
<td>Embedded Server</td>
<td>BSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BBR(SBBR)</td>
</tr>
</tbody>
</table>
SBBR Firmware Interfaces

OSes:
- Red Hat
- Windows
- VMware ESXi
- SUSE
- Fedora
- CentOS
- Ubuntu
- Oracle Linux
- FreeBSD

Interfaces:
- SR (SBBR)
- ES (SBBR)
- UEFI
- ACPI
- SMBIOS
- EDK2 or Commercial FW
- PSCI, SMCCC
- Trusted Firmware
Both SBBR! What is the Difference?

<table>
<thead>
<tr>
<th>Firmware Spec</th>
<th>ES (Embedded Server)</th>
<th>SR (ServerReady)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UEFI + ACPI + SMBIOS</td>
<td>UEFI + ACPI + SMBIOS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platform Hardware</th>
<th>64bit Arm</th>
<th>64bit Arm</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS/Hypervisor</td>
<td>Generic, off-the-shelf w/ exceptions: RAS, virtualization, etc.</td>
<td>Generic, off-the-shelf</td>
</tr>
</tbody>
</table>

| OS Distro (examples) | Windows IoT Enterprise, VMware ESXi, RHEL, SLES, Ubuntu, CentOS, Fedora, openSUSE, Debian, FreeBSD, NetBSD | VMware ESXi, Windows Client/Server, RHEL, SLES, Ubuntu, CentOS, Fedora, openSUSE, Debian, FreeBSD, NetBSD |

| Hardware Compliance Levels | BSA + waivers for existing HW initially | BSA+SBSA Levels 3 through 6 |

<table>
<thead>
<tr>
<th>BBR Recipe</th>
<th>SBBR</th>
<th>SBBR</th>
</tr>
</thead>
</table>

| Certification | Arm SystemReady ES + System Certification List | Arm SystemReady SR + System Certification List |

Can support UEFI SecureBoot and Secure Firmware Update via UEFI Capsule Service across (BBSR)
Certification Requirements

ServerReady (SR)

• V2.0
  • ACS 2.5 test results
  • BSA v1.0 + SBSA Supplement v6.0, or SBSA v6.0 (Level 3-5)
  • BBR v1.0 (SBBR) or SBBR v1.1

• OS installation logs
  • Windows PE (required)
  • VMware ESXi-Arm (recommended)
  • 2 Linux/BSD distros (required)

Embedded Server (ES)

• V1.0
  • ACS 2.5 test results
  • BSA v1.0, or SBSA v6.0 Level 3 (minus server features)
  • BBR v1.0 (SBBR), or SBBR v1.1 w/exceptions

• OS installation logs
  • Windows PE (recommended)
  • VMware ESXi-Arm (recommended)
  • 2 Linux/BSD distros (required)

https://developer.arm.com/documentation/den0109/latest
Architectural Compliance Suite (ACS)

ACS for SystemReady SR

- ACS v3.0 available
- Tests for SBBR + SBSA compliance

ACS for SystemReady ES and IR

- ACS-ES Development WIP (ETA: Q2 CY2021)
- Use ACS v2.5 w/ SBSA Level 3 to certify ES now
- New GitHub repository structure

https://github.com/arm-software/arm-enterprise-accs

https://github.com/arm-software/arm-systemready
SystemReady Certification List (SCL)

https://developer.arm.com/architectures/system-architectures/arm-systemready/sr

https://developer.arm.com/architectures/system-architectures/arm-systemready/es
SystemReady SR / ES

Devices Showcase
## Ampere Altra Mt Jade

<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>0ACOI 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>
<tr>
<td>Tested operating systems</td>
<td>• Windows PE (version 2004)</td>
</tr>
<tr>
<td></td>
<td>• Ubuntu Server 20.04</td>
</tr>
<tr>
<td></td>
<td>• CentOS 8</td>
</tr>
<tr>
<td></td>
<td>• Debian 10 (buster)</td>
</tr>
</tbody>
</table>
Ampere Altra Mt Jade - Firmware

- Firmware options both commercial (AMI Aptio UEFI and MegaRAC BMC FW) and open source
- UEFI EDK2 Firmware
  - Ampere EDK2 repository: https://github.com/AmpereComputing/edk2-platforms
  - TianoCore upstreaming is WIP
    - https://github.com/tianocore/edk2-platforms/tree/master/Platform/Ampere
    - Patches under review: https://edk2.groups.io/g/devel/search?q=ampere
- LinuxBoot Firmware
  - Upstreaming is WIP: https://github.com/linuxboot/mainboards/tree/master/ampere/jade
  - LinuxBoot payload carried in EDK2: edk2-platforms/tree/ampere/Platform/Ampere/LinuxBootPkg
- OpenBMC Firmware
  - Open source BMC firmware!
  - Ampere repository: https://github.com/ampere-openbmc/openbmc
  - Upstream is WIP: https://github.com/openbmc/openbmc/tree/master/meta-ampere
## Gigabyte Altra Mt Snow

<table>
<thead>
<tr>
<th>Company</th>
<th>GIGABYTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Ampere Mt. Snow 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>F06p</td>
</tr>
<tr>
<td>Additional information</td>
<td>GIGABYTE Ampere Altra Server Solution</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>
| Tested operating systems      | • Windows PE (20279 or newer)  
• Fedora Server 33  
• Debian 10  
• OpenSUSE Leap 15.2  
• Ubuntu Server 20.04 |
# Raspberry Pi 4 Model B

<table>
<thead>
<tr>
<th>Company</th>
<th>Raspberry Pi</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Raspberry Pi 4 Model B</td>
</tr>
<tr>
<td>SoC family</td>
<td>Broadcom BCM2711</td>
</tr>
<tr>
<td>Firmware version</td>
<td>UEFI: v1.19</td>
</tr>
<tr>
<td>Additional info</td>
<td>Firmware by Pi Firmware Taskforce (PFTF) Project</td>
</tr>
<tr>
<td>ACS version</td>
<td>Enterprise ACS v2.5</td>
</tr>
<tr>
<td>BSA details</td>
<td>BSA 1.0 (currently tested with ACS for SBSA Level 3)</td>
</tr>
<tr>
<td>BBR details</td>
<td>SBBR (BBR 1.0)</td>
</tr>
<tr>
<td>Arm SystemReady certification</td>
<td>SystemReady ES V1.0</td>
</tr>
</tbody>
</table>
| Tested operating systems | - VMware ESXi-Arm  
                          | - Windows 10 IoT Enterprise (Version 2004)  
                          | - Fedora Workstation 32   
                          | - CentOS 8.1              
                          | - Ubuntu Server 20.04    
                          | - OpenSUSE Leap 15.2     
                          | - OpenBSD 6.7            |
Raspberry Pi 4 Model B - Firmware

● Open source community effort, with many contributors: [https://rpi4-uefi.dev/about/](https://rpi4-uefi.dev/about/)
  ○ Arm Developer Ecosystem Discord community: [https://discord.gg/VfYbkfp](https://discord.gg/VfYbkfp) (#rpi4-uefi-dev)
  ○ TianoCore EDK2 based
  ○ Also works on the RPi3 (separate FW builds)
  ○ Ongoing work to add support to RPi 400, CM4

● UEFI EDK2 Firmware
  ○ All UEFI code built directly from [TianoCore Upstream](https://tianocore.org)
  ○ PI FW Taskforce (PFTF) GitHub: [https://github.com/pftf](https://github.com/pftf)
  ○ Issue and feature requests: [https://github.com/pftf/RPi4/issues](https://github.com/pftf/RPi4/issues)
  ○ ACS test reports: [https://github.com/pftf/acs-reports](https://github.com/pftf/acs-reports)

● TF-A Firmware:
# NXP Layerscape LX 2160A RDB

<table>
<thead>
<tr>
<th>Company</th>
<th>NXP</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Layerscape LX2160A Reference Design Board (RDB)</td>
</tr>
<tr>
<td>SoC family</td>
<td>NXP LX2160A</td>
</tr>
<tr>
<td>Firmware version</td>
<td>LX2RDB_SYS_READY_TAG_01</td>
</tr>
<tr>
<td>ACS version</td>
<td>Enterprise ACS v2.5</td>
</tr>
<tr>
<td>BSA details</td>
<td>BSA v1.0 (currently tested with ACS for SBSA Level 3)</td>
</tr>
<tr>
<td>BBR details</td>
<td>SBBR (BBR 1.0)</td>
</tr>
<tr>
<td>Arm SystemReady certification</td>
<td>SystemReady ES V1.0</td>
</tr>
</tbody>
</table>

## Tested operating systems

- VMware ESXi-Arm Fling v1.1
- Ubuntu Server 20.04
- Fedora Server 32
- Debian 10.4.0
- CentOS 8.2
- OpenSUSE Leap 15.2
- Windows PE (version 2004)
NXP Layerscape LX 2160A RDB - Firmware

- UEFI EDK2 Firmware
  - NXP Repository: https://source.codeaurora.org/external/qoriq/qoriq-components/edk2-platforms/tree/Platform/NXP/LX2160aRdbPkg
  - TianoCore Upstream (WIP): https://github.com/tianocore/edk2-platforms/tree/master/Platform/NXP/LX2160aRdbPkg

- TF-A Firmware:
  - NXP Repository: https://source.codeaurora.org/external/qoriq/qoriq-components/atf/tree/plat/nxp/soc-lx2160
    - Upstream WIP
SolidRun HoneyComb LX2

- **SolidRun** [HoneyComb LX2 Arm Workstation](https://www.solid-run.com/products/honeycomb-lx2)
  - Based on [NXP Layerscape LX2160A SoC](https://www.nxp.com/products/processors-and-processors-cores/layerscape-arm-processors/lx2160a)
  - Arm SystemReady ES Certification **In Progress**
  - Discord community: [https://discord.gg/VfYbkfp](https://discord.gg/VfYbkfp) (#solidrun)
- **Open source Firmware:**
  - UEFI FW Build script
  - EDK2 ([Solid Run Repository](https://github.com/SolidRun/edk2)
  - TF-A ([SolidRun Repository](https://github.com/SolidRun/tf-a)
  - Upstreaming (TianoCore and TrustedFirmware.org) planned
- **Tested with many OSes:**
  - ESXi-Arm 7.0.0 Fling v1.0
  - Windows PE (build 21286)
  - Fedora Workstation 33
  - Fedora Server 33
  - CentOS 8.1
  - SLES 15 SP2
  - OpenSUSE Leap 15.2
  - Debian 10.4.1
  - Ubuntu Server 20.04
  - Ubuntu Desktop 21.4
NXP Layerscape LX 2160A RDB and FRWY

- Arm SystemReady Certification **In Progress**
- Based on [NXP Layerscape LS1046A SoC](#)
- UEFI EDK2 Firmware
  - TianoCore Upstream
  - NXP Repository (code aurora)
- TF-A Firmware:
  - NXP Repository (code aurora)
  - TrustedFirmware.org Upstream WIP
SBESA QEMU

- Virtualization environment for Armv8-A, with support for Arm SBESA specifications
  - Available as “sbsa-ref” machine
  - Supports SBESA HW such as GICv3, generic timer, watchdog, etc..
- Choice as an environment for developing firmware and testing operating systems and compliance testing
- Linaro working on completing SBESA and SBBR support and testing compliance with the ACS test suite
- Upstreamed to:
  - QEMU
  - UEFI EDK2 FW (TianoCore)
  - TF-A FW (TrustedFirmware.org)
- Testing results: sbsa-acs and UEFI SCT tests
Marvell Octeon TX2 CN913x

- Work done by [SemiHalf](https://www.semihalf.com) to support UEFI+ACPI in EDK2
  - Work done on [SolidRun CN913 based boards](https://www.solidrun.com)
  - Firmware already available upstream
  - Boots most standard distros (Linux, ESXi-Arm, BSDs).
  - Testing with ACS test suites for more complete BSA+SBBR compliance
- [EDK2 FW](https://edk2.org) (TianoCore upstream)
- [TF-A FW](https://trustedfirmware.org) (TrustedFirmware.org upstream)
- Reference presentation in [OSFC 2020](https://osfc.org) by Marcin Wojtas
Thank you

Accelerating deployment in the Arm Ecosystem