Arm ServerReady Update

Dong Wei

Linaro Connect HKG
March 2018
Server Architecture
Server Architecture

Base System Architecture (BSA)
- Defines hardware requirements

Base Boot Requirements (BBR)
- Defines firmware requirements

These specifications require a minimum set of hardware and firmware implementations that will ensure OS and firmware will interoperate

SBSA/SBBR are the BSA/BBR for the server systems
- Developed using feedback from vendors across the industry (Silicon vendors, OSVs, Hypervisor vendors, BIOS vendors, OEMs and ODMs)
- SBBR defines the required, recommended and optional UEFI, ACPI and SMBIOS interfaces

SBSA and SBBR are now available at [https://developer.arm.com/](https://developer.arm.com/)
- Current versions are SBSA v3.1 and SBBR v1.0. No click through license required.
- SBSA v5.0 and SBBR v1.1 will be available soon

Server Base Manageability Guide (SBMG)
- Defines guidance for server management standardization
- Work In Progress
**Formalizing how to request spec content updates**

We have created an Engineering Change Request (ECR) process for SBSA / SBBR / SBMG

1. Partner submit the change requirement to Arm ([armserverac-request@arm.com](mailto:armserverac-request@arm.com)) using the template with the following info: Summary of Change, Benefits of the Change (justifications), Impact of the Change.

2. Partner and Arm work together to understand the change requirement and brainstorm the solution that meets the requirement. When the solution is defined, post it to an Arm Drop Zone for broader partners review.

3. External Mantis-based ECR tracking database Work In Progress

**Logistics:**

- **Two discussion channels:**
  - Partner to Arm over [armserverac-request@arm.com](mailto:armserverac-request@arm.com) protected by NDA
  - Anybody on the Arm server AC discussion group: [armserverac-discuss@arm.com](mailto:armserverac-discuss@arm.com)
    - If you are on ArmServerAC, you are already on [armserverac-discuss@arm.com](mailto:armserverac-discuss@arm.com), and if you are not then ask us
    - Weekly phone conferences on the as-needed basis would be the most scalable solution, complemented by ftf gathering
SBSA Status

Drafting SBSA v5.0 (BETA available on Dropzone)

Core / System:
- RAS requirements (AARCH-4638)
- ROP and JOB requirements for SBSA (AARCH-11320)
- SBSA and SVE (AARCH-11319)
- Nested virtualization (AARCH-12054)
- MPAM requirements for SBSA (AARCH-11323)
- Forced writeback (AARCH-11326)
- Add Activity Monitor Requirements to SBSA (AARCH-12044)
- Crypto Requirements to SBSA (AARCH-12058)
- 48bit mode (AARCH-12858)
- Ban non-standard interrupt controller (AARCH-11329)
- PPI assignments (AARCH-11753)
- Base frequency standardisation (AARCH-11324)
- Assign PPIs for new timers in v8.4 (AARCH-11321)
- Secure EL2 (AARCH-13144)
- TLBI-range (AARCH-12159)
- SVE heterogenity (AARCH-13132)

IO:
- PCIe clarifications (AARCH-12301)
- UART clarifications (AARCH-12701)
- PCIe requirements for assignable devices (AARCH-11610)
- PCIe Precision Time Measurement Root source (AARCH-12571)
- PCIe Deadlock (AARCH-4698)
- ACS and Peer to Peer (AARCH-12303)

Security:
- TCG TPM (AARCH-12312)

Cleanup:
- Deprecate old SBSA levels (AARCH-11330)
- Clean to point of persistence (AARCH-13385)
# PCIe improvements – SBSA

<table>
<thead>
<tr>
<th>PCIe feature</th>
<th>SBSA revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clarifications, 4G and Non-Prefetchable BARs</td>
<td>SBSA 5.0</td>
</tr>
<tr>
<td>PTM and system counter</td>
<td></td>
</tr>
<tr>
<td>Access control and Peer to Peer traffic</td>
<td></td>
</tr>
<tr>
<td>RCIE minimum requirements</td>
<td>SBSA - next</td>
</tr>
<tr>
<td>Error logging and reporting minimal requirements</td>
<td></td>
</tr>
<tr>
<td>Vendor defined message handling</td>
<td></td>
</tr>
<tr>
<td>DPC minimal requirements</td>
<td></td>
</tr>
<tr>
<td>Memory ordering requirements</td>
<td></td>
</tr>
</tbody>
</table>
Additional work on PCIe

We want to improve testability of SBSA rules relating to PCIe

• Our current approach is based on modified drivers (SATA) and this limits coverage
  • Very hard to use pre-silicon

• We are working with pre-silicon and post-silicon solutions to generate test IP
  • Enables us to generate specific traffic patterns and increase coverage in areas such as coherency, deadlocks and interrupts

We are also working on PCIe guidance (as opposed to mandates):

• PCIe integration guide - currently trying to nail topic list
• PCIe performance verification guide – alpha is in dropzone
SBBR Status

SBBR 1.1 (EAC available on Dropzone)

**UEFI:**
- UEFI PCI Root Bridge IO Protocol Address Translation clarifications
- UEFI GOP implementation clarifications
- UEFI REST Protocol support
- UEFI Capsule Service clarification
- Native AArch64 image requirements for UEFI applications and drivers
- UEFI RNG Protocol*

**ACPI:**
- ACPI Interrupt-signaled Events support
- ACPI Generic Event Devices support
- ACPI PCI IO Address Translation clarifications*
- IORT implementation guidelines

**SMBIOS/Management:**
- SMBIOS Processor Information
- SMBIOS structure data requirements clarification
- SMBIOS Redfish Host Interface support
- SPMI recommendation removal

**Cleanup:**
- Clarifications of SSDT being optional
- Clarifications on UEFI Load File and Load File 2 Protocols
- Updated referenced specifications to: UEFI 2.7, ACPI 6.2, SMBIOS 3.1.1
- Secondary core boot standardization with PSCI

**Security:**
- Secure and Trusted Boot
- Secure Firmware Update
UEFI Option ROM Availability

Architecturally Arm requires the support of AArch64 native binary UEFI drivers.

Arm testing room will be open at UEFI Plugfest next week to provide:

• Real HW Setup in which to test native AArch64 drivers
• Help and suggestions on how to get your driver recompiled for AArch64

Arm is creating a “getting started guide” and a list of off-the-shelf systems that can be used for continuous testing.

Arm is collecting a list of vendors/cards with AArch64 drivers:

• Contact us (uefi@arm.com) if you would like to be on it or if you’d like more information.
Secure Server Profile

What are included:
• Verified Boot (Reset - Arm TF - UEFI Secure Boot -OS)
• Measured Boot (TPM, TCG Trusted Boot)
• Secure Firmware Update

What else?
SBMG Status and Plans

LM0: current implementation
LM1: Redfish
LM2: Redfish enabled PLDM/MCTP
IPMI support: optional in addition
SBSA/SBBR roadmap

<table>
<thead>
<tr>
<th>Available</th>
<th>FY2018H1</th>
<th>FY2018H2</th>
<th>FY2019H1</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBSA 5.0 BETA</td>
<td>SBSA 5.0 EAC</td>
<td>SBSA 5.0 REL</td>
<td>SBSA-next EAC</td>
<td>SBSA-next-next Alpha</td>
</tr>
<tr>
<td>SBSA 5.0 REL</td>
<td>SBSA next Alpha</td>
<td>SBSA-next EAC</td>
<td>SBSA-next-next Alpha</td>
<td></td>
</tr>
<tr>
<td>SBSA next Alpha</td>
<td>SBSA-next EAC</td>
<td>SBSA-next-next Alpha</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SBSA-next EAC</td>
<td>SBSA-next-next Alpha</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SBBR 1.1 EAC</td>
<td>ECR Database</td>
<td>SBMG-1.0 EAC</td>
<td>PCIe perf verification guide EAC</td>
<td></td>
</tr>
<tr>
<td>SBMG-1.0 EAC</td>
<td>SBMG-1.0 Beta</td>
<td>PCIe perf verification guide Beta</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SBMG-1.0 Beta</td>
<td>PCIe perf verification guide Alpha</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SBMG-1.0 Alpha</td>
<td>PCIe Integration guide Alpha</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCIE perf verification guide Alpha</td>
<td>PCIe Integration guide Beta</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCIE perf verification guide Beta</td>
<td>SBMG-1.0 Beta</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise ACS</td>
<td>Enterprise ACS for Server Ready 2.0</td>
<td>Enterprise ACS</td>
<td>SBMG-1.0 Alpha</td>
<td></td>
</tr>
<tr>
<td>Enterprise ACS</td>
<td>Enterprise ACS for Server Ready 2.0</td>
<td>Enterprise ACS</td>
<td>SBMG-1.0 Beta</td>
<td></td>
</tr>
<tr>
<td>Enterprise ACS</td>
<td>Enterprise ACS for Server Ready 2.0</td>
<td>Enterprise ACS for Server Ready 2.0</td>
<td>SBMG-1.0 EAC</td>
<td></td>
</tr>
<tr>
<td>Enterprise ACS</td>
<td>Enterprise ACS for Server Ready 2.0</td>
<td>Enterprise ACS for Server Ready 2.0</td>
<td>SBMG-1.0 EAC</td>
<td></td>
</tr>
<tr>
<td>Enterprise ACS</td>
<td>Enterprise ACS for Server Ready 2.0</td>
<td>Enterprise ACS for Server Ready 2.0</td>
<td>SBMG-1.0 EAC</td>
<td></td>
</tr>
</tbody>
</table>

Specs
- SBSA/SBBR
- Enterprise ACS 1.3
- SBMG-1.0 Alpha
- PCIe perf verification guide Alpha

Compliance test suites
- SBMG-1.0 Alpha
- PCIe perf verification guide Alpha

Future
- Released
- Development
- Adv. Planning
- Concept
- Ongoing updates
Vision

• Arm servers everywhere and easy to deploy

Mission

• We provide the tools to enable customers to deploy Arm servers with confidence

Elevator

• **ServerReady** gives the confidence that your server works out of the box.
SBBA and SBBR Architectural Compliance Suites

SBBA test covers

• SBBA CPU properties
• SBBA defined system components
• SBBA rules for PCIe integration
  – Based on the PCIe specification
  – Based on standard OS drivers with no quirks enabled

SBBR test covers

• UEFI testing based on the UEFI SCT
• ACPI testing based on FWTS
• SMBIOS testing

V1.4 released! Apache v2 licensed

• https://github.com/ARM-software/sbsa-acs
• https://github.com/ARM-software/arm-enterprise-acs
Server Ready testing

We are engaging with silicon vendors, ODMs, OEMs and BIOS vendors to run the tests.

Tests are developed by our architecture team, which also develops the specifications.

We have a support team that helps in running of test, debugging etc.
Inputs for certification

Certification request document (CRD) contains

- Board information table
- Enterprise ACS logs
  - Explanation for fails and skips
- OS boot logs
  - CentOS x.x (Kernel version y.y)
  - Or RHEL x.x (Kernel version y.y)
  - Suse Linux x.x (Kernel version y.y)
  - Ubuntu x.x

<table>
<thead>
<tr>
<th>Board Information table</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODM Name</td>
</tr>
<tr>
<td>Board Name</td>
</tr>
<tr>
<td>Silicon provider</td>
</tr>
<tr>
<td>Silicon version</td>
</tr>
<tr>
<td>Bios vendor</td>
</tr>
<tr>
<td>Target market</td>
</tr>
<tr>
<td>Is it a SKU of a previously certified board? If yes, name of the board.</td>
</tr>
</tbody>
</table>

Arm Server Ready Program Launch

Likely to Launch in Q4’2018

Call to Action

- Partners continue to work with Arm to evaluate the tests
- Partners invited to write guest blogs promoting the program
- Partners get ready to co-launch
The trademarks featured in this presentation are registered and/or unregistered trademarks of Arm Limited (or its subsidiaries) in the EU and/or elsewhere. All rights reserved. All other marks featured may be trademarks of their respective owners.
Thank You!
Danke!
Merci!
谢谢!
ありがとう!
Gracias!
Kiitos!