presented by

ARM

The Role UEFI Technologies Play in ARM Platform Architecture

Spring 2017 UEFI Seminar and Plugfest

March 27 - 31, 2017

Presented by Dong Wei (ARM)

Agenda

- ARM Ecosystem Update
- Specification Updates
- SBSA/SBBR
- SBSA/SBBR Tests
- Questions
  - ODM/OEM/ISV Badge Program?
  - UEFI Driver Binary Format

Section Heading

ARM Ecosystem Update

Economics

- What are the ARM numbers?
  - Silicon with ARM IP shipped in 2016 : 16.7 Bu
  - Cumulative total shipped : 100+ Bu
  - Processor + GPU licenses : 1400+
  - Licensees : 450+
  - Foundry partners : 5+
  - Process technology : 7 – 250 nm
  - Connected community members[1] : 1000+

[1] Important for a collaborative business model

Connected Community

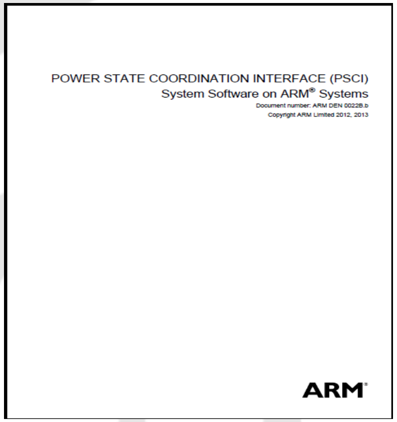
Specification Updates

ACPI Next

- New introduction chapter
- NUMA SRAT (System Resource Affinity Table) support for ITS (Interrupt Translation Service)
- CPPC (Collaborative Processor Performance Control) Support for multiple PCC (Platform Communication Channels)
- Processor Properties and Topology Table (PPTT)
- Extended PCC subspaces – bidirectional interface between the OSPM and the platform
- SDE (Software Delegated Exception) hardware error notification and SDEI (SDE Interface) table
- IORT, and ARM ACPI Table, will have an update soon
- Heterogeneous Memory Attribute Table (HMAT)
- NVM Label, ARS (Address Range Scrubbing) Updates, Translate SPA (System Physical Address), Platform RAS Capabilities Updates, ARS Error Injection

PSCI

- Power State Coordination Interface is the ARM standard for core and system power management
  - Supported by all major OSs, UEFI and ACPI
- Expect to release PSCI v1.1 in 17Q2
  - Improves reset support, and allows implementing system warm resets

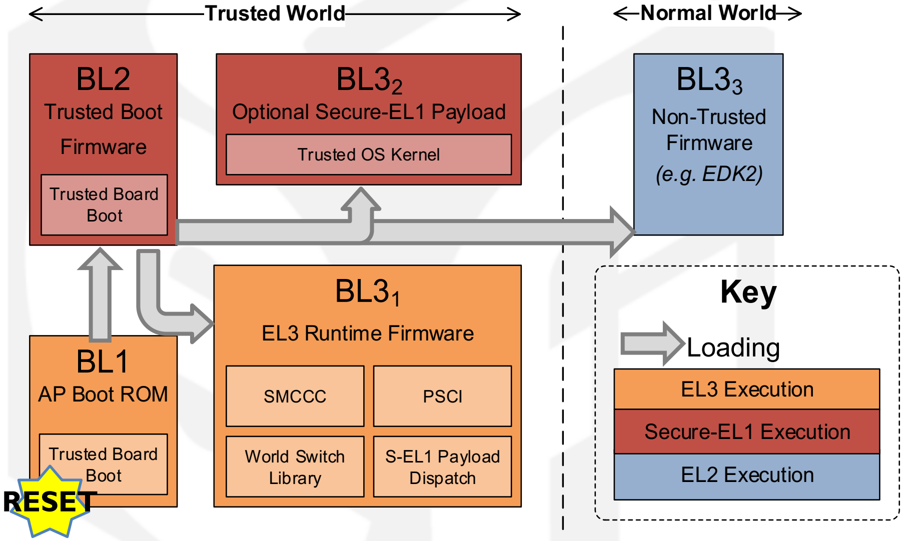


POWER STATE COORDINATION INTERFACE (PSCI)
System Software on ARM® Systems
Document number: ARM DEN 0022B.b
Copyright ARM Limited 2012, 2013

ARM®

ARM Trusted Firmware (TF)

- Standardized ARMv8-A EL3 firmware
  - Optional trusted boot firmware
- BSD licensed, contributions welcome
  - No CLA (Contributor License Agreement) needed
- Reusable reference code
  - Including PSCI…

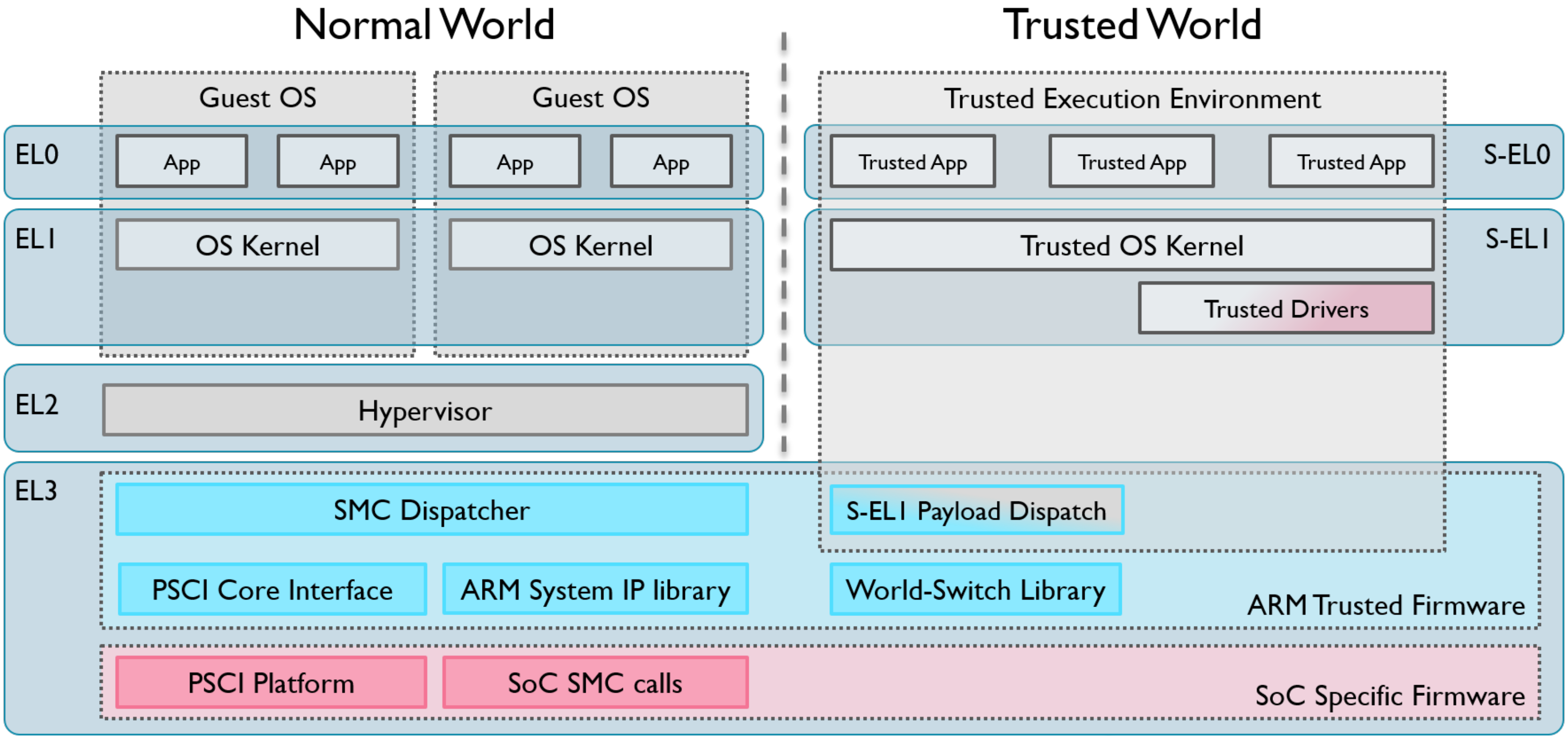


https://github.com/ARM-software/arm-trusted-firmware

ARM TF and PSCI

- AArch64 and AArch32 library
- Mostly generic with thin platform layer
- Supports all mandatory PSCI v1.0 functions
  - and most optional ones
- Latest TF v1.3 adds
  - Power state residency statistics functions
  - Instrumentation of key PSCI operations
- TF implementation will track specification

ARM TF Runtime Stack



ACPI View

- A UEFI Shell utility
  - Provides a human readable output of the installed ACPI tables
  - Similar to SmbiosView
  - Provides extensive interface to validate ACPI tables
  - Useful for firmware developers to diagnose ACPI table issues that cause an OS to fail to boot
  - Assists in prototyping implementations against specification proposals
  - ARM initiated, collaborations welcome
  - https://github.com/tianocore/edk2-staging

SBSA/SBBR

Platform Architecture

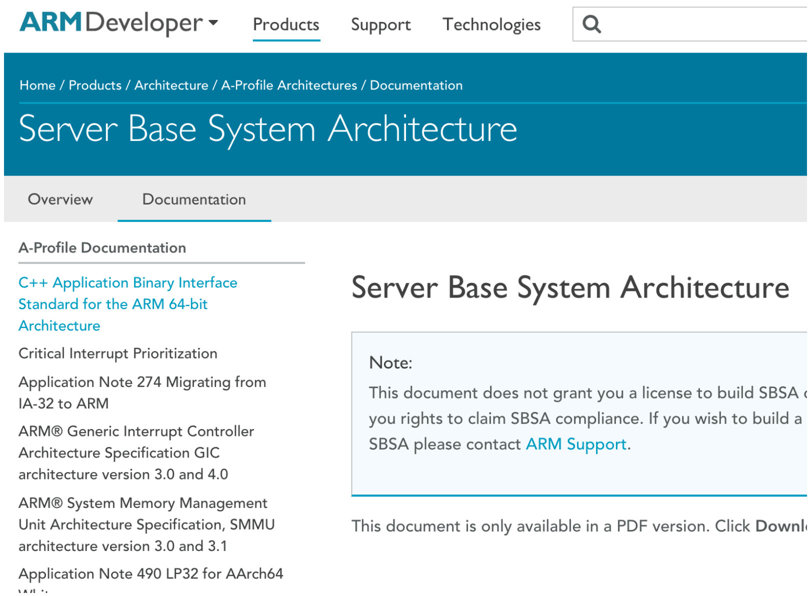
- Base System Architecture (BSA)
  - Defines hardware requirements
- Base Boot Requirements (BBR)
  - Defines firmware requirements
- These specifications require a minimum set of hardware and firmware implementations that will ensure OS and firmware will interoperate

SBSA/SBBR

- SBSA/SBBR are the BSA/BBR for the enterprise 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/SBBR

- SBSA are SBBR are now available at https://developer.arm.com/
  - Current versions are SBSA v3.0 and SBBR v1.0
  - No click through license required



Home / Products / Architecture / A-Profile Architectures / Documentation

Server Base System Architecture

A-Profile Documentation

C++ Application Binary Interface Standard for the ARM 64-bit Architecture

Critical Interrupt Prioritization

Application Note 274 Migrating from IA-32 to ARM

ARM® Generic Interrupt Controller Architecture Specification GIC architecture version 3.0 and 4.0

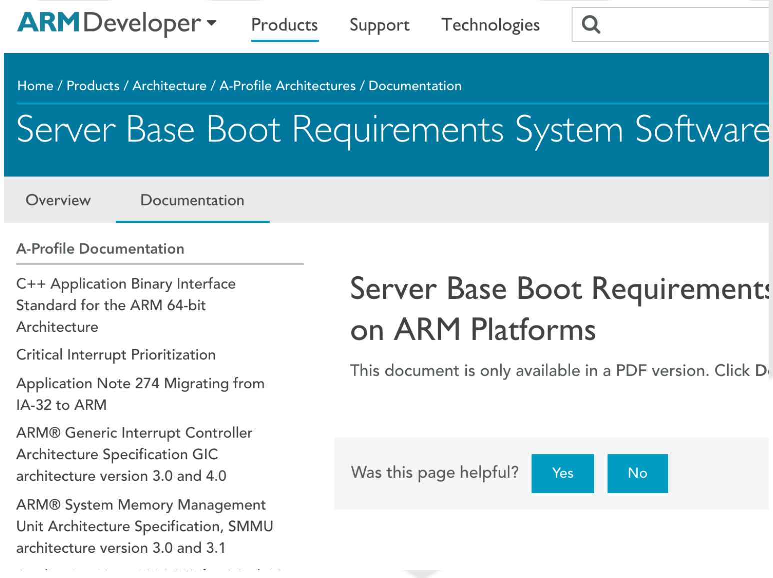
ARM® System Memory Management Unit Architecture Specification, SMMU architecture version 3.0 and 3.1

Application Note 490 LP32 for AArch64

Server Base System Architecture

Note:
This document does not grant you a license to build SBSA c
you rights to claim SBSA compliance. If you wish to build a
SBSA please contact ARM Support.

This document is only available in a PDF version. Click Downl



Home / Products / Architecture / A-Profile Architectures / Documentation

Server Base Boot Requirements System Software

A-Profile Documentation

C++ Application Binary Interface Standard for the ARM 64-bit Architecture

Critical Interrupt Prioritization

Application Note 274 Migrating from IA-32 to ARM

ARM® Generic Interrupt Controller Architecture Specification GIC architecture version 3.0 and 4.0

ARM® System Memory Management Unit Architecture Specification, SMMU architecture version 3.0 and 3.1

Server Base Boot Requirements on ARM Platforms

This document is only available in a PDF version. Click D

Was this page helpful?

SBSA/SBBR Compliance Tests

SBSA/SBBR Compliance Tests

- SBSA test suite covers
  - SBSA PE properties
  - SBSA defined system components
  - SBSA rules for PCIe integration
    - Based on the PCIe specification
    - Based on standard OS drivers with no quirks enabled
- SBBR test suite covers
  - UEFI testing based on the UEFI SCT
  - ACPI testing based on FWTS
  - SMBIOS testing

SBSA Tests

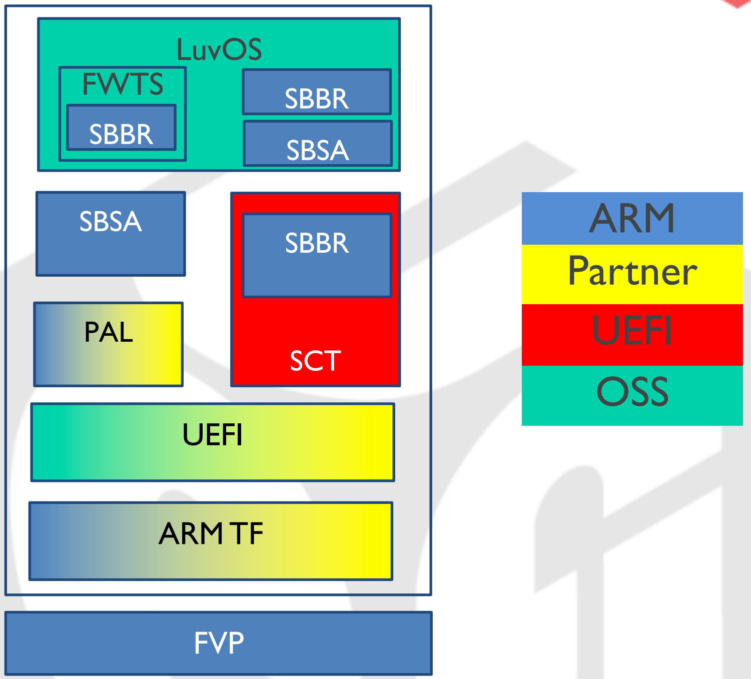
- Provided as open source
  - Apache v2 License
- Built on top of a Platform Adaptation Layer
  - ARM will support one based on UEFI and ARM Trusted Firmware
  - A silicon vendor can also port to a bare metal environment

SBBR Tests

- From 3 sources (all open source)
  - UEFI SCT* (ARM will upstream into SCT)
  - FWTS (ARM + Linaro will upstream)
  - Standalone (ARM provides through github and packages into LuvOS image)
- Note: UEFI SCT is currently for UEFI member only. Would like to see it open source

Unified Release

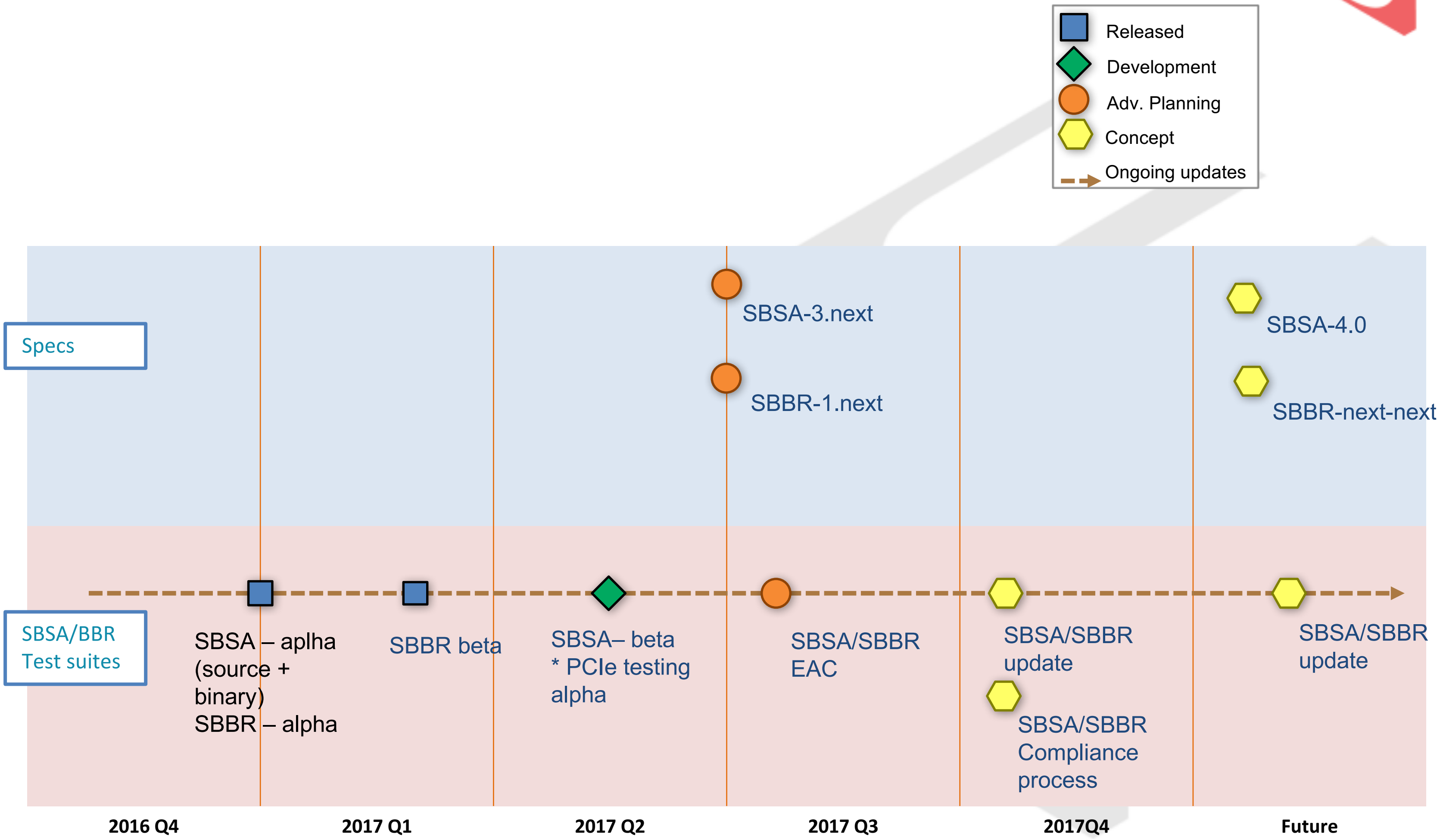
- A unified software release, to tie all of these deliverables together with the enterprise FVP model
- Planned for future



SBSA/SBBR Tests Release

- Overarching github including SBBR
  - https://github.com/ARM-software/arm-enterprise-acs
- SBSA github
  - https://github.com/ARM-software/sbsa-acs

SBSA/SBBR Roadmap



🟦 Released
◆ Development
● Adv. Planning
⬡ Concept
⇢ Ongoing updates

Specs

SBSA-3.next

SBBR-1.next

SBSA-4.0

SBBR-next-next

SBSA/BBR
Test suites

SBSA – aplha
(source +
binary)
SBBR – alpha

SBBR beta

SBSA– beta
* PCIe testing
alpha

SBSA/SBBR
EAC

SBSA/SBBR
update

SBSA/SBBR
Compliance
process

SBSA/SBBR
update

2016 Q4

2017 Q1

2017 Q2

2017 Q3

2017Q4

Future

Questions to the ARM Community

SBSA/SBBR Certification

- To improve the out-of-box experience for OS vendors and system users, ARM received feedback that a badge program certifying the SBSA/SBBR Compliance can be useful
- Feedback?

UEFI Driver Binary Format

- EBC is a cross-architecture solution
  - One driver image for all ISAs
  - Open-source EBC Interpreter for ARM upstreamed to tianocore
- However,
  - Benefit cannot be realized if x86 uses its native format, unless more ISAs become relevant
  - No supported EBC Compiler
  - No Secure Boot Signing for EBC Drivers
- Can the industry come together to solve these problems?
  - If not, propose that ARM AArch64 native binary format be used for UEFI Drivers on ARM systems
  - Feedback?

Summary

Conclusion

- UEFI Technologies play significant roles in the ARM Platform Architecture
- ARM SBBR requires UEFI, ACPI and SMBIOS implementations
- SBSA/SBBR Tests can be used for compliance tests
- Drive closure on a remaining questions

Thanks for attending the Spring 2017 UEFI Seminar and Plugfest

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

presented by

ARM