presented by

arm

UEFI and ACPI in Arm System Architecture

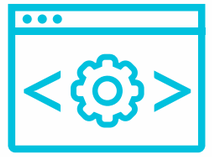
UEFI Fall 2023 Developers Conference & Plugfest
October 9-12, 2023
Presented by Dong Wei (Arm)

Agenda

- Arm Base Boot Requirements
- Three Recipes
- Arm SystemReady

Arm Base Boot Requirements

Arm Base Boot Requirements (BBR)



Firmware (BBR – Base Boot Requirements)

- Expands to include common firmware interfaces, but recognizes that different software stacks will require different recipes
- BBR v2.0 (May 2022)
- SBBR, EBBR, LBBR Recipes targeting different OSes

BBSR (Base Boot Security Requirements)

- Secure Boot and Firmware Update
- V1.2 (Jan 2023)
  - Add platform security checklist
  - Cleanup

EBBR Specification

- Community development
- BBR spec refers to EBBR spec as needed
- V2.1.0 (Dec 2022)

Uboot is EBBR compliant

BBR Related Arm FW Specifications

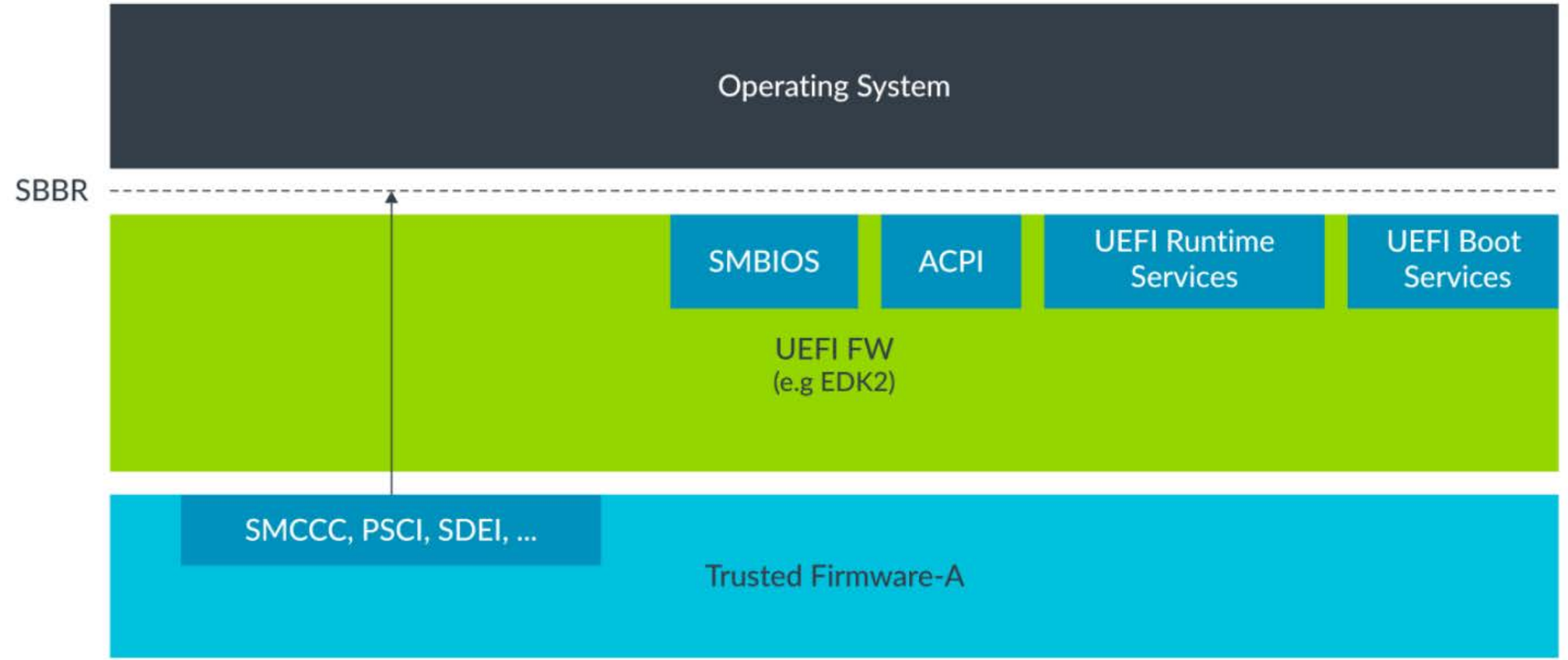
Document	Title	Version	Released	URL
DEN0028	SMC Calling Convention (SMCCC)	1.4 EAC0	May 2022	https://developer.arm.com/documentation/den0028/
DEN0077	Arm Firmware Framework (FFA)	1.1 REL0	Nov 2022	https://developer.arm.com/documentation/den0077/
DEN0022	Power State Coordination Interface (PSCI)	Issue E	July 2022	https://developer.arm.com/documentation/den0022/
DEN0054	Software Delegated Exception Interface (SDEI)	1.1 REL0	Jan 2023	https://developer.arm.com/documentation/den0054/
DEN0060	Management Mode Interface (MM)	Issue A	Dec 2016	https://developer.arm.com/documentation/den0060/
DEN0113	DRTM Architecture for Arm	BET1	Nov 2022	https://developer.arm.com/documentation/den0113/
DEN0098	TRNG Firmware Interface	1.0 REL0	Jan 2022	https://developer.arm.com/documentation/den0098/
DEN0118	Secure FW Update ABI	1.0 BET0	May 2021	https://developer.arm.com/documentation/den0118/
DEN0100	SMC Errata ABI	1.0 EAC1	Oct 2022	https://developer.arm.com/documentation/den0100/
DEN0115	PCIe Config Access ABI	1.0 Beta 1	May 2021	https://developer.arm.com/documentation/den0115/

BBR Related Arm FW Specifications

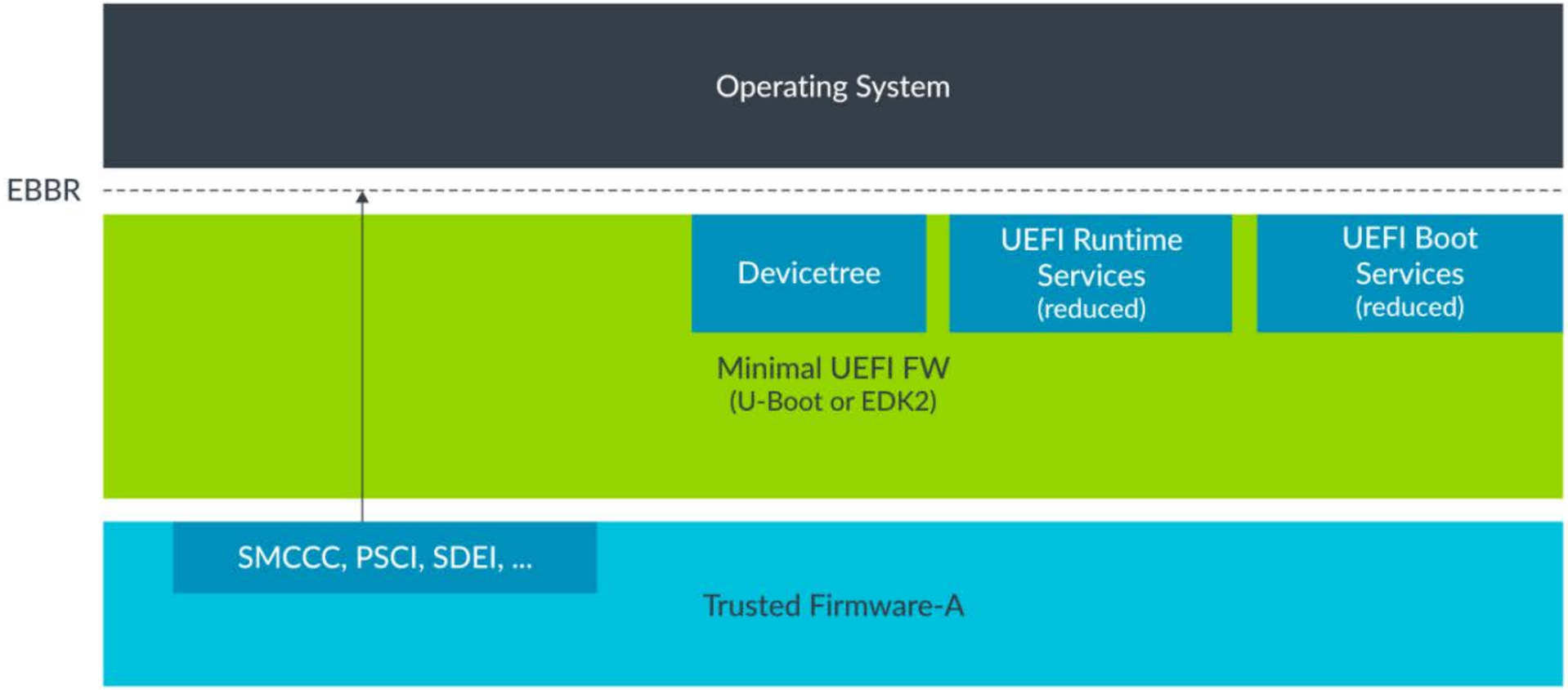
Document	Title	Version	Released	URL
DEN0049	IO Remapping Table (IORT)	Issue E.e	Sep 2022	https://developer.arm.com/documentation/den0049/
DEN0085	ACPI for Arm RAS Extensions (AEST)	1.1	Sept 2020	https://developer.arm.com/documentation/den0085/
DEN0117	ACPI for CoreSight PMU (APMT)	1.0	Jan 2022	https://developer.arm.com/documentation/den0117/
DEN0065	ACPI for MPAM (MPAM)	2.0	Nov 2022	https://developer.arm.com/documentation/den0065/
DEN0093	ACPI for Arm Components (AGDI)	1.1	Nov 2021	https://developer.arm.com/documentation/den0093/
DEN0048	ARM Functional Fixed Hardware (FFH)	1.2	Sep 2022	https://developer.arm.com/documentation/den0048/
DEN0056	System Control and Management Interface (SCMI)	3.2	Dec 2022	https://developer.arm.com/documentation/den0056/

Three BBR Recipes

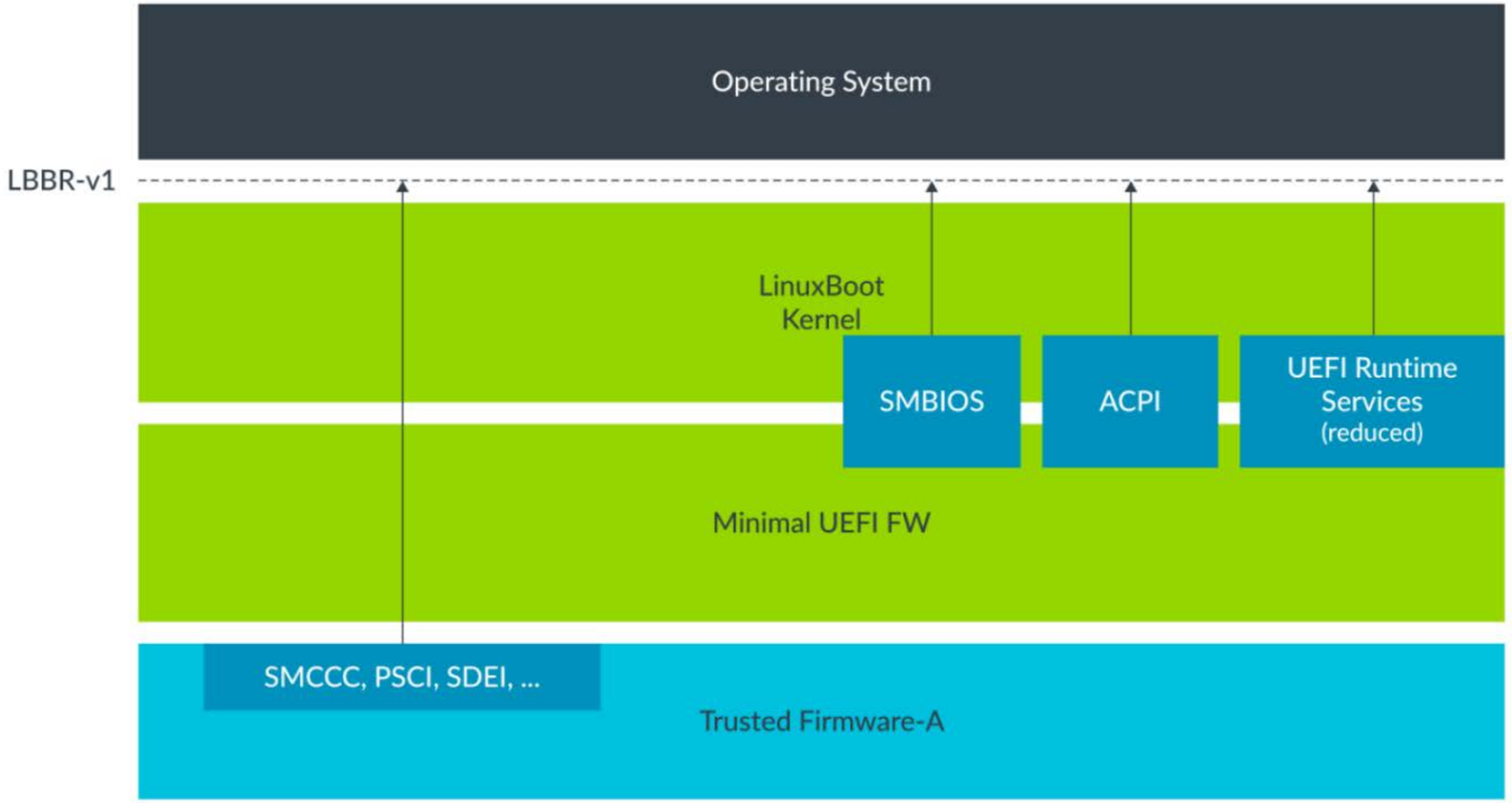
BBR Recipe - SBBR



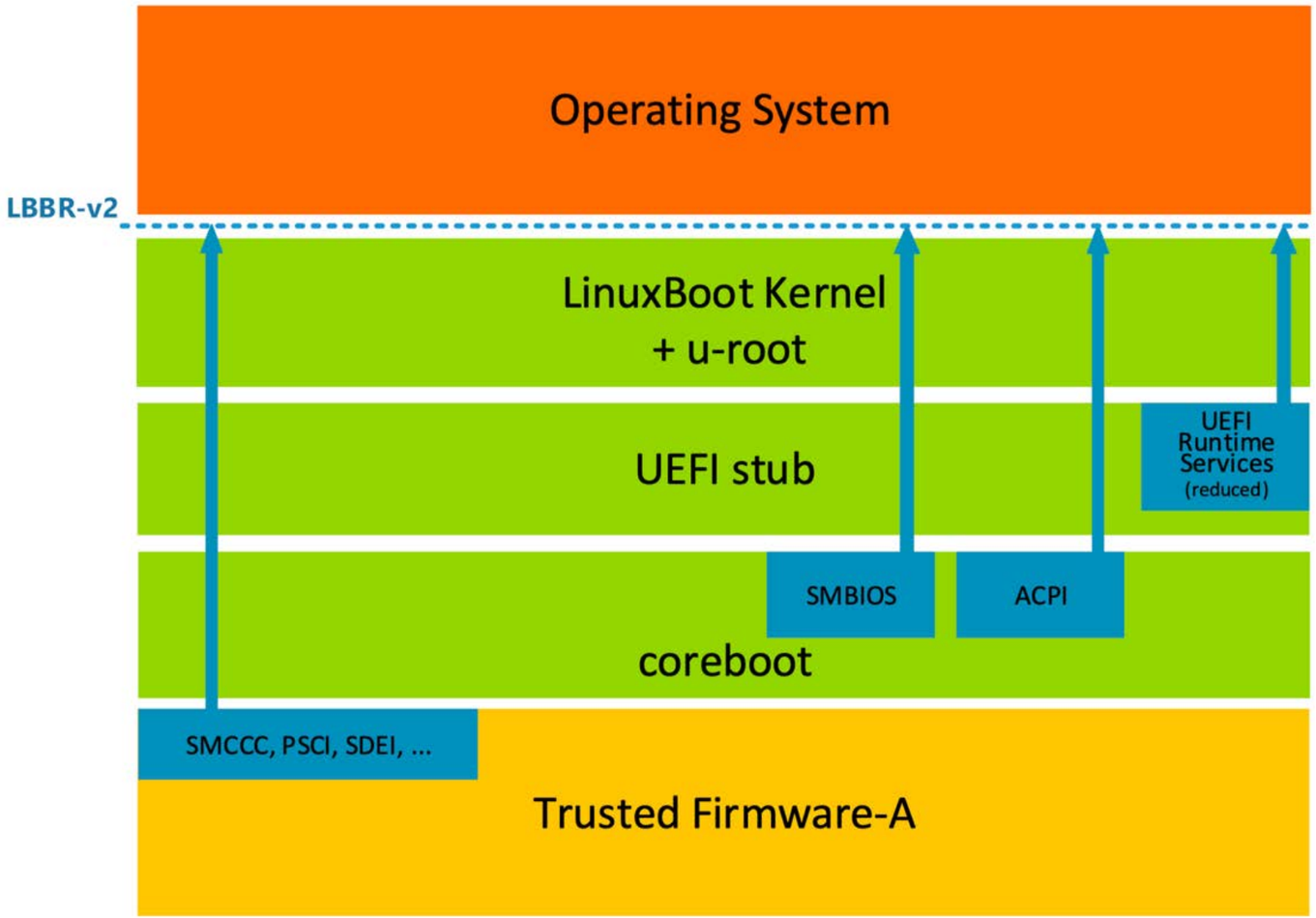
BBR Recipe - EBBR



BBR Recipe – LBBR (v1)



BBR Recipe – LBBR (v2)



Wed, October 18, 1:10pm - 1:30pm | SJCC - Concourse Level - 210CG

Enabling coreboot for Open System Firmware on Arm servers

- Open System Firmware (OSF)

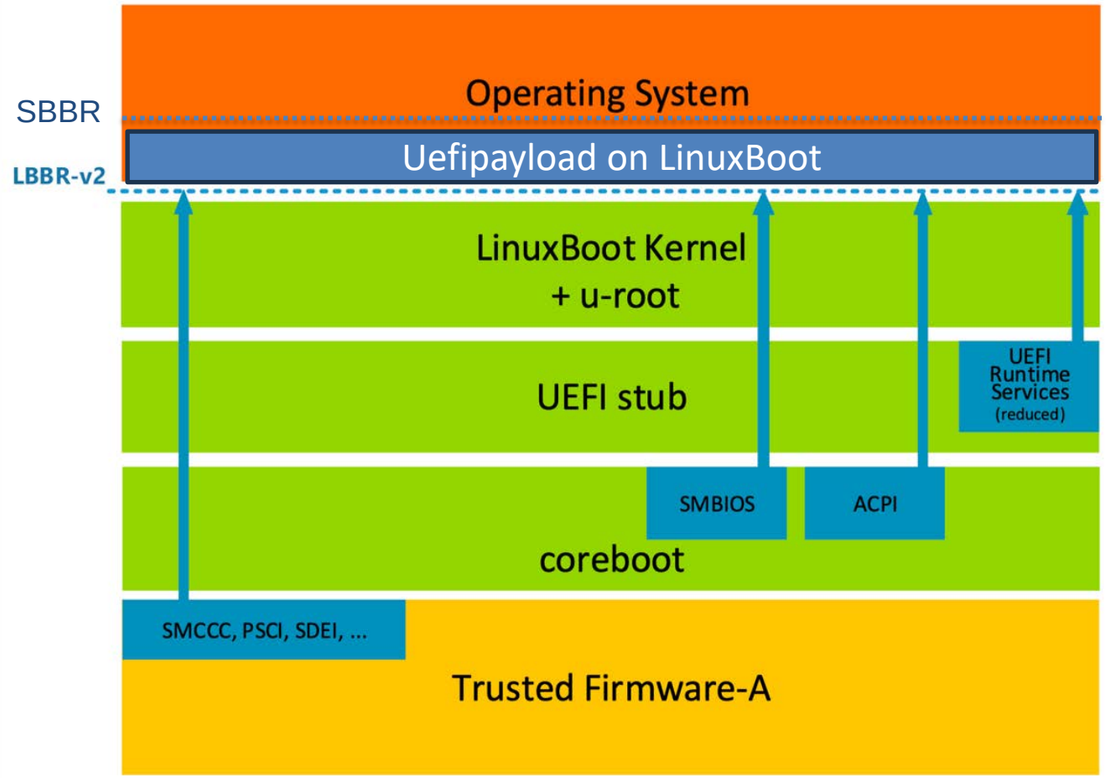
The Arm Base Boot Requirements (BBR) Specification defines standard firmware requirements for Arm systems. It outlines the firmware interfaces needed for system software interoperability. Arm servers commonly rely on the SBBR recipe, which is typically built using EDK2 open source firmware or derived commercial UEFI solutions. Recently, there is increased interest in coreboot + LinuxBoot firmware from cloud operators as an alternative open-source firmware. Arm created the LBBR recipe to outline the interfaces needed for LinuxBoot on Arm systems. In this session, Arm and 9elements will share our progress towards developing a coreboot firmware stack for Arm servers. We will showcase proof of concepts, and discuss the challenges faced when developing a new firmware stack to fit existing software expectations. Finally, we will share how this work influenced the evolution of the LBBR specification, and the work ahead to give partners more open firmware options for deploying Arm servers.

Speakers

Jeff Booher-Kaeding
Systems Architecture Engineer - Arm

David Milosevic
Firmware Developer - 9elements Agency

Merge LBBR into SBBR



Wed, October 18, 12:50pm - 1:10pm | SJCC - Concourse Level - 210CG

Different Path: Uefipayload on Linuxboot

- Open System Firmware (OSF)

1. Why This Solution?

-coreboot/Linuxboot echosystem still missing the last piece: booting windows. For now, there is no possible solution to build UEFI environment in Linuxboot that the windows needed, so intel provide a solution to boot uefipayload on coreboot, this can build the UEFI environment and boot into windows successfully, but also this solution missing the good stuff: Linuxboot and golang, all feature development on u-root will gone. Now we are trying to find a better way to keep Linuxboot in this windows boot solution.

2. Current Status Update

-Booting into Windows 2022 on Intel EagleStream platform with Sapphire Rapids processor.

3. Future Plan

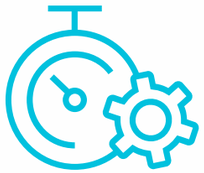
-Solve the remaing issue and enabling it on intel BrichStream platform

Speakers

GuangYao Cao
Senior BIOS Mananger - Lenovo

Arm SystemReady

Arm Base System Architecture



Hardware Baseline (BSA – Base System Architecture)

- Common standard architecture for 64-bit A-profile applicable to all market segment
- defining a minimal set of CPU and System architecture necessary for an OS to boot and run.
- BSA v1.0c (Oct 2022)

Hardware Supplements (xBSA)

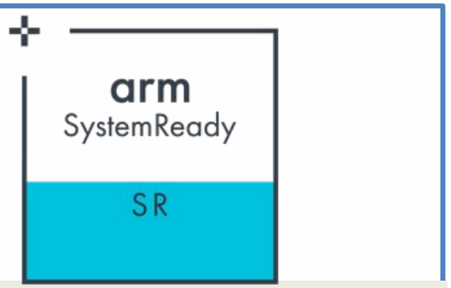
- Provides market segment specific hardware requirements
- Server BSA for server requirements
  - SBSA v7.1 (Oct 2022)
- PC BSA, Auto BSA?

arm SystemReady

"Just Works" for **Linux** and **BSD** on **embedded** Arm SoCs

- For the embedded Linux ecosystem
- Forward compatibility
- **Mainline Linux support for SoC**
- Targets both custom (Yocto, OpenWRT, Buildroot) and pre-build (Debian, Fedora, SUSE, Ubuntu)

"Just Works" on **embedded** and **DPU/IPU** Arm SoCs



"Just Works" on **server or workstation** Arm SoCs

- For the **Windows**, **VMware,** Linux, and BSD ecosystems

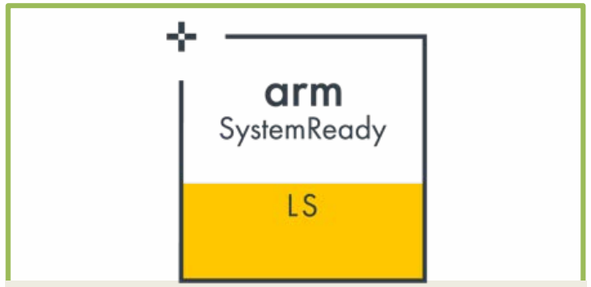
- **Supports old OSes to run on new hardware and vice versa**
- Targets generic off-the-shelf Oses
- Forward/backward compatibility

Ensures standard firmware interfaces to deploy and maintain

arm SystemReady

	arm SystemReady IR	arm SystemReady ES	arm SystemReady SR
Firmware Spec	UEFI + Devicetree	UEFI + ACPI + SMBIOS	UEFI + ACPI + SMBIOS
Platform Hardware	32bit/64bit Arm	64bit Arm	64bit Arm
	Can support UEFI SecureBoot and Secure Firmware Update via UEFI Capsule Service across (**BBSR**)		
OS/Hypervisor	Linux, etc. →	Generic, off-the-shelf w/ exceptions: RAS, I/O virtualization, etc. →	Generic, off-the-shelf
OS Distro *(examples)*	Fedora, openSUSE, SLES, Debian, Ubuntu, Yocto	Windows IoT Enterprise, VMware ESXi, RHEL, SLES, Ubuntu, CentOS, AlmaLinux, Rocky Linux, Oracle Linux, Anolis OS, Fedora, openSUSE, Debian, CBL-Mariner, FreeBSD, NetBSD, OpenBSD	VMware ESXi, Windows Client/Server, RHEL, SLES, Ubuntu, CentOS, AlmaLinux, Rocky Linux, Oracle Linux, Anolis OS, Fedora, openSUSE, Debian, CBL-Mariner, FreeBSD, NetBSD, OpenBSD
Hardware Compliance Levels	**BSA Recommended** + BSA required if hardware targeting both IR and ES	**BSA** + waivers for existing HW initially	**BSA+SBSA** Levels 3 through 6
BBR Recipe	**EBBR**	**SBBR**	**SBBR**
Certification	**Arm SystemReady IR** + System Certification List	**Arm SystemReady ES** + System Certification List	**Arm SystemReady SR** + System Certification List

arm SystemReady



"Just Works" for **Linux** OSes on **server** Arm SoCs

- For hyperscalers
- Targets hyperscalers' Linux environment
- BSA+SBSA
- LBBR (ACPI+SMBIOS)

"Just Works" for **virtual environments**

- For cloud instances
- For desktop virtual platforms
- Can be certified with or without a specific band

Extension for secure boot and secure firmware update

- Recommended as an extension for SR, ES and IR bands
- Required for SR, ES and IR in the future

SystemReady Requirements Spec v2.1

IR

V2.0

- IR ACS v2.0.0 test results
- BSA v1.0c
- BBR v1.0 (EBBR v2.1.0)
- Devicetree v0.3
  - Require 100% of nodes to have a json-schema in the Linux kernel
- BBSR 140/150
- Waiver Levels 0-2

SIE recommended

OS installation and boot logs

- 2 Linux/BSD distros required
- Recommended list:
  - Fedora, Debian, openSUSE, Ubuntu

ES

V1.4

- ES ACS v1.2.0 test results
- BSA v1.0c
- BBR v1.0 (SBBR)
- Waiver Levels 0-2

SIE recommended

OS installation and boot logs

- Either WinPE (GPT) or VMware ESXi-Arm required
- 2 Linux/BSD distros based on heritage required

Heritage: RHEL/Fedora/CentOS/AlmaLinux/ Rocky Linux/Oracle Linux/Anolis OS, or SLES/openSUSE, or Ubuntu/Debian, or CBL-Mariner, or NetBSD/OpenBSD/FreeBSD

SR

V2.4

- SR ACS v2.0.0 Beta0 test results
- BSA v1.0c + SBSA Supplement v7.1 Level 3-6
- BBR v1.0 (SBBR)

SIE recommended

OS installation and boot logs

- WinPE (GPT) required
- VMware ESXi-Arm (recommended)
- 2 Linux/BSD distros based on heritage required

Heritage:RHEL/Fedora/CentOS/AlmaLinux/ Rocky Linux/Oracle Linux/Anolis OS, or SLES/openSUSE, or Ubuntu/Debian, or CBL-Mariner, or NetBSD/OpenBSD/FreeBSD

SystemReady Requirements Spec v2.1

Virtual Environment (VE)

V1.0

The Arm SystemReady Virtual Envirnment (VE) is designed for the certification of virtual environments that can demonstrate the same software “just works” user experience as other SystemReady certifications.

- VE
- VE SR
- VE ES

LS

V1.0 ALPHA

- test results following the SystemReady LS ACS instructions
- BSA v1.0c + SBSA Supplement v6.1 Level 3-6.
- LBBR-v1 recipe in BBR v2.0

OS installation and boot logs

- 2 Linux distros required

Recommended distros: CentOS, Debian, Ubuntu or Fedora

Arm SystemReady Supporters

arm SystemReady

ISVs

CANONICAL, Microsoft, ORACLE, Parallels Enabled by Alludo, Red Hat, SUSE, vmware

SiPs

AMPERE., BROADCOM, CIX, FUJITSU, MARVELL, MEDIATEK, nuvoTon, NVIDIA, NXP, RENESAS, Rockchip 瑞芯微电子, SIPEARL The Silicon Pearl, socionext for better quality of experience, AMD XILINX

Hyperscale Cloud Service Providers

Alibaba Cloud, aws, Baidu 百度, Google Cloud, Microsoft Azure, ORACLE CLOUD Infrastructure

OEMs/ODMs

AAEON an ASUS company, ADLINK TECHNOLOGY INC., ADVANTECH Enabling an Intelligent Planet, AMD XILINX, ARDUINO, ASUS IoT, AVANTEK COMPUTER, Compulab, congatec, CyberTAN, DIGI, EUROTECH Imagine. Build. Succeed., Foxconn Industrial Internet, GIGA COMPUTING, Google, HAWKEYE TECH, Hewlett Packard Enterprise, 华辰连科 HuachenLink, inspur, kontron S&T Group, Lanner, Lenovo, 联泰集群 LTHPC, NEXCOM, NORCO, PEGATRON, PHYTEC, radxa, Raspberry Pi, Scalys, SECO, 天固信安 SKYSOLIDISS, SolidRun Embedded Edge Computing, SUPERMICRO, 日海飞信, Toradex Swiss. Embedded. Computing., Variscite, WINSYSTEMS, wiwynn

EDAs

cadence, SYNOPSYS

IFVs

9ELEMENTS Cyber Security, ami, BYOSOFT 百数软件, insyde, phoenix technologies, PureSoftware, Semihalf

Communities

AlmaLinux, Linaro, OpenAnolis 龙蜥社区, OPEN Compute Project, OpenGCC, Rocky Linux, yocto PROJECT PARTICIPANT

Test Labs

GlobalLogic A Hitachi Group Company, iol University of New Hampshire InterOperability Laboratory

arm SystemReady

Band	Certified Systems
arm SystemReady SR	ADLINK TECHNOLOGY INC. • AVA Developer Platform • Ampere Altra Developer Platform (AADP-64 + 1x GbE) • Ampere Altra Developer Platform (AADP-32 + 4x 10GbE + 1x GbE) • AVA Developer Platform (AVADP-32 + 4x 10GbE + 1x GbE) • Ampere Altra Developer Platform (Altra Max, AADP-128 + 1xGbE) AMPERE. • Mt Jade Platform & Refresh • Mt Mitchell (with SIE) AVANTEK COMPUTER • Ampere Altra Server 2U Mt. Jade • Ampere Altra Server 2U Mt. Snow NVMe • Ampere Altra Arm Workstation Alibaba Cloud • Cloud Server M Series ASXXXXMG1 arm • Morello System Development Platform Foxconn Industrial Internet • 2U Mt. Collins 2S NVMe (R-2211) • 1U Mt. Collins 2S (R-2110)

arm SystemReady

Band	Certified Systems
arm SystemReady SR	**GIGA COMPUTING** • Ampere Mt. Snow Platform • Gigabyte R152-P30 • Gigabyte R152-P31 • Gigabyte R182-P91 • Gigabyte G242-P31 • Gigabyte E252-P30 • Gigabyte H262-P60 • Gigabyte R272-P30 • Gigabyte R282-P91 **Hewlett Packard Enterprise** • ProLiant RL300 Gen11 (Ampere Altra) • ProLiant RL300 Gen11 (Ampere Altra Max) **inspur** • NF5280R6 **联泰集群 LTHPC** • GR2134 • SR223 **Microsoft Azure** • Azure Ampere Altra Arm-based server **NVIDIA** • MGX Grace CPU Superchip Reference System & with SIE • MGX GH200 Reference System & with SIE • GH200 P4351 Reference System (with SIE) (Nvidia & Insyde FW) • Grace Superchip P4352 Reference System

arm SystemReady

Band	Certified Systems
arm SystemReady SR	• ARS-210M-NR • ARS-110M-NR

arm SystemReady

Band	Certified Systems
arm SystemReady LS	AMPERE. • Mt Jade Platform

arm SystemReady

Band	Certified Systems
arm SystemReady ES	**arm** • Morello System Development Platform **HAWKEYE TECH** • HK-6010 • HK-5120 • HK-6100 **MARVELL** • OCTEON TX2 CN9130 DB • OCTEON TX2 CN96XX-CRB • OCTEON TX2 CN98XX-CRB • CN106xx CRB (crb106 r1p0) • CN106XX-PCIe-CRB DPU **NEXCOM** • NSA 6310 • DTA 1376 **NVIDIA** • BlueField-2 DPU (MT42822) **NXP** • LX2160A RDB (LX2160A and LX2080A SoC) • LS1046A FRWY & Refresh • LS1046A RDB & Refresh **Raspberry Pi** • Raspberry Pi 4 Model B • Raspberry Pi 400 **SolidRun** Embedded Edge Computing • HoneyComb LX2 Workstation • MACCHIATObin Double Shot • CEx7 CN9132 Eval Board

arm SystemReady

Band	Certified Systems		
+ arm SystemReady IR	AAEON an ASUS company • SRG-IM8P	ADLINK TECHNOLOGY INC. • I-Pi SMARC IMX8M Plus & refresh	ADVANTECH Enabling an Intelligent Planet • RSB-3720
	ARDUINO • Portenta-X8 and ASX00031 Portenta Breakout	arm Corstone • Corstone-1000 MPS3	ASUS • PE100A
	Compulab • IOT-GATE-iMX8 & Refresh	congatec • SMX8-Plus w/ SMC1/SMARC-ARM	EUROTECH Imagine. Build. Succeed. • ReliaGATE 10-14-35
	Google • Coral Dev Board	kontron S&T Group • KBox A-230-LS • pITX-iMX8M Quad • Baseboard BL i.MX8M MINI	Lenovo • Leez P710 Gateway

arm SystemReady

Band	Certified Systems
arm SystemReady IR	• i.MX8M Mini EVK • i.MX8M Mini EVK (w/SIE) • i.MX8M Nano EVK • i.MX8M Plus EVK • i.MX8M Quad EVK • i.MX8M Quad EVK (w/SIE) • i.MX8M Plus EVK(w/SIE)
	• RockPro64
	• Rock PI 4B Plus
	• Raspberry Pi 4 Model B • Raspberry Pi 400
	• HiHope RZ/G2M
	• Toybrick TB-RK3399ProD
	• SBC-C61
	• SynQuacer E-Series
	• DART-MX8M-PLUS with VAR-DT8MCustomBoard (Quad-core @1.8 GHz, 4 GB LPDDR4, 16 GB eMMC) • DART-MX8M-PLUS with VAR-DT8MCustomBoard (Quad-core @1.8 GHz, 2 GB LPDDR4, 16 GB eMMC)
	• ITX-P-C444
	• Zynq UltraScale+ MPSoC ZCU102 Evaluation Kit

arm SystemReady

Band	Certified Systems
arm SystemReady IR	2MP157C-DK2 2MP157C-EV1

arm SystemReady

VE	Certified Virtual Environments
arm SystemReady VE	• (VE) EC2 C6g Virtual Machines • (VE) EC2 M6g Virtual Machines • (VE) EC2 R6g Virtual Machines • (VE) EC2 T4g Virtual Machines • (VE) EC2 C7g Virtual Machines • (VE) EC2 M7g Virtual Machines • (VE) EC2 R7g Virtual Machines • (VE) EC2 Im4gn Virtual Machines • (VE) EC2 C6gn Virtual Machines • (VE) EC2 C7gn Virtual Machines

arm SystemReady

VE	Certified Virtual Environments
	Google Cloud • (VE and VE SR) Tau T2A Compute Engine VM Microsoft Azure • (VE) Azure Virtual Machines series featuring the Ampere Altra Arm-based processor ORACLE CLOUD Infrastructure • (VE) OCI Ampere A1 Compute Instances

arm SystemReady

VE	Certified Virtual Environments
	arm • (VE SR) Neoverse N2 reference design FVP (RD-N2 FVP 11.17.33) Linaro • (VE ES) QEMU sbsa-ref 7.0.50 (v7.0.0-1589-g6d940eff47) Parallels Enabled by Alludo • (VE) Parallels Desktop 18 vmware • (VE ES) ESXi-Arm Fling • (VE ES) Fusion 13

Thanks for attending the UEFI Fall 2023 Developers Conference & Plugfest

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

presented by

arm