presented by

arm

Arm System Firmware Architecture

UEFI 2025 Developers Conference & Plugfest

October 10, 2025

Dong Wei

Meet the Presenters

Dong Wei

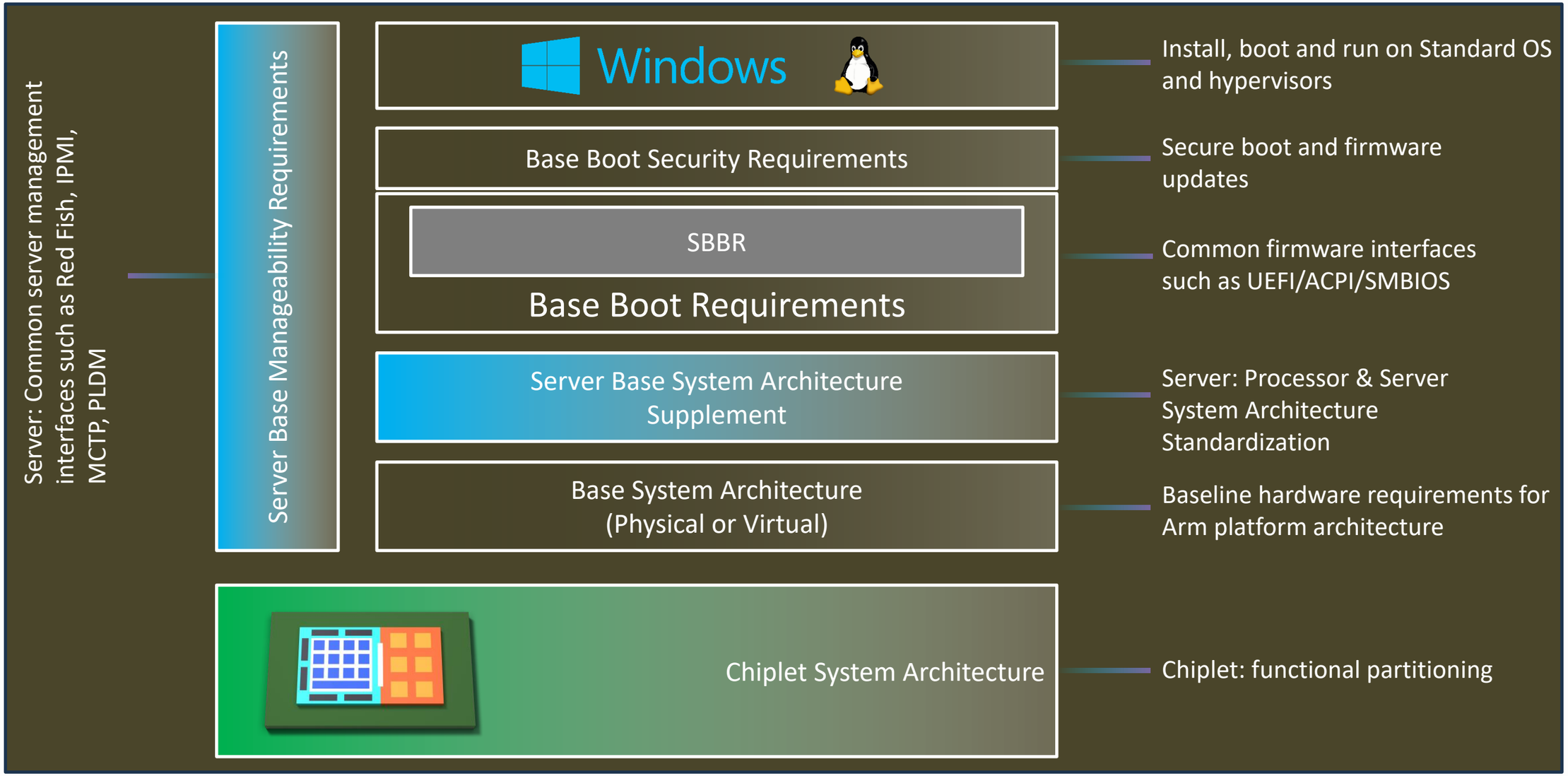
Arm Fellow

Dong Wei is an Arm Fellow and Lead Standards Architect of the Architecture and Technology Group in Arm Limited. He leads the Arm SystemReady compliance program with definitions of the hardware, firmware requirements for the Arm-based systems. He also leads the system manageability and security requirements for these systems. He is the Vice President of the UEFI Forum and a Board member at PCI-SIG, TCG, UEFI Forum, CXL and UCIe Consortium. He is also the Steering Committee rep for the OCP Open Platform Firmware project.

Agenda

- Arm System Firmware Architecture
- UEFI and ACPI on Arm
- Typical Arm Server Firmware

Arm System Architecture



Arm System Architecture

Install, boot and run on Standard OS and hypervisors

Base Boot Security Requirements

Secure boot and firmware updates

EBBR and Devicetree

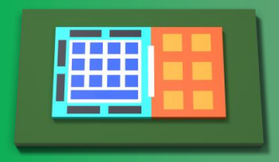
Base Boot Requirements

Common firmware interfaces such as UEFI and Devicetree

Platform Fault Detection Interface

Platform fault detection

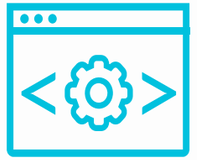
Physical or Virtual



Chiplet System Architecture

Chiplet: functional partitioning

Firmware Requirements



Firmware (BBR – Base Boot Requirements)

- Expands to include common firmware interfaces, but recognizes that different software stacks will require different recipes
- BBR v2.2 (June 2025)

BBSR (Base Boot Security Requirements)

- Secure Boot and Firmware Update
- V1.4 (March 2025)
- Maintenance Mode
- Merge with BBR in the future

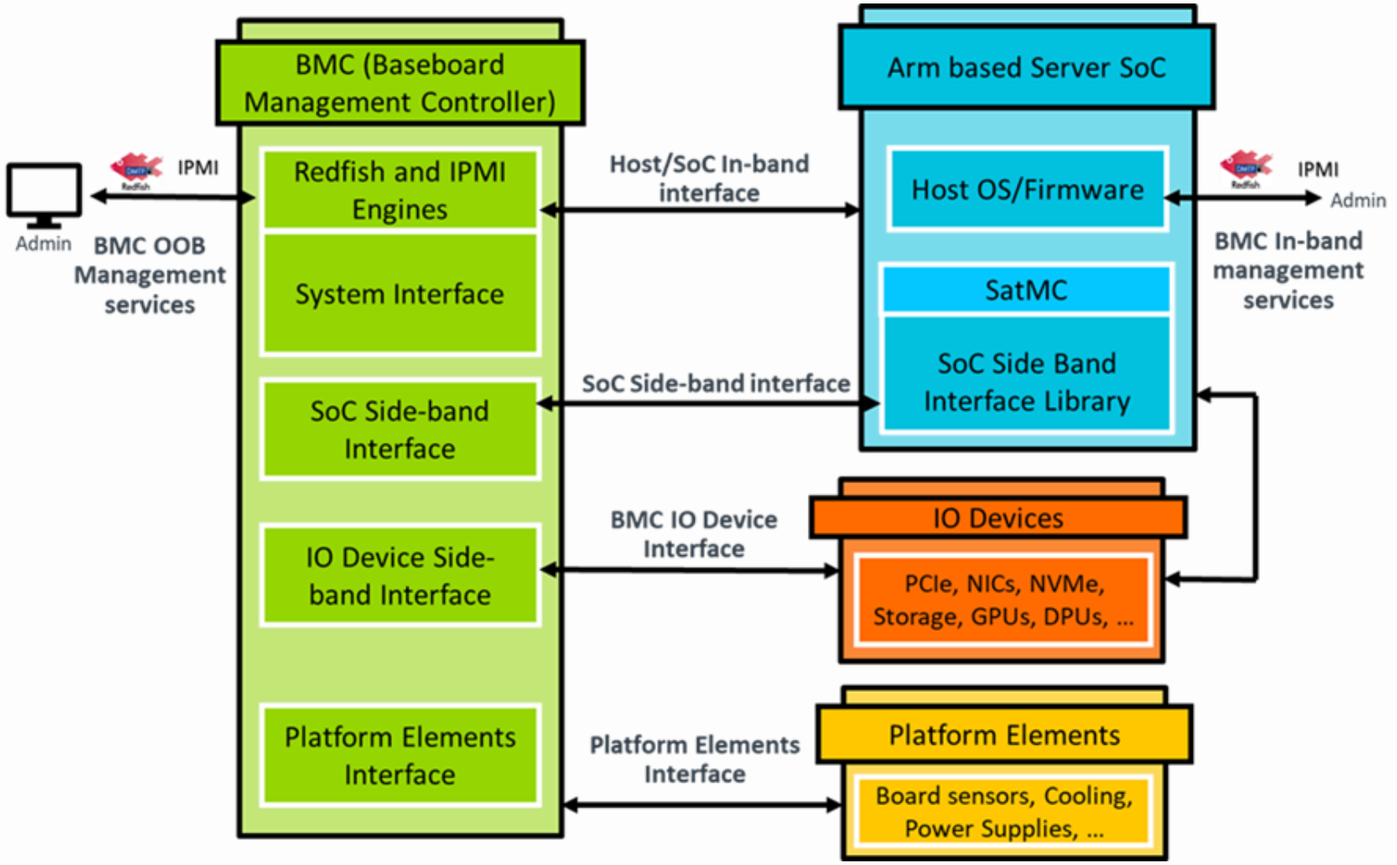
System Architecture Compliance Suite (ACS)

- Verify that the DUT is compliant with the system architecture specifications
- Encourage partner certifications to include the use of ACS
  - Collaborating with Nvidia NVSSVT

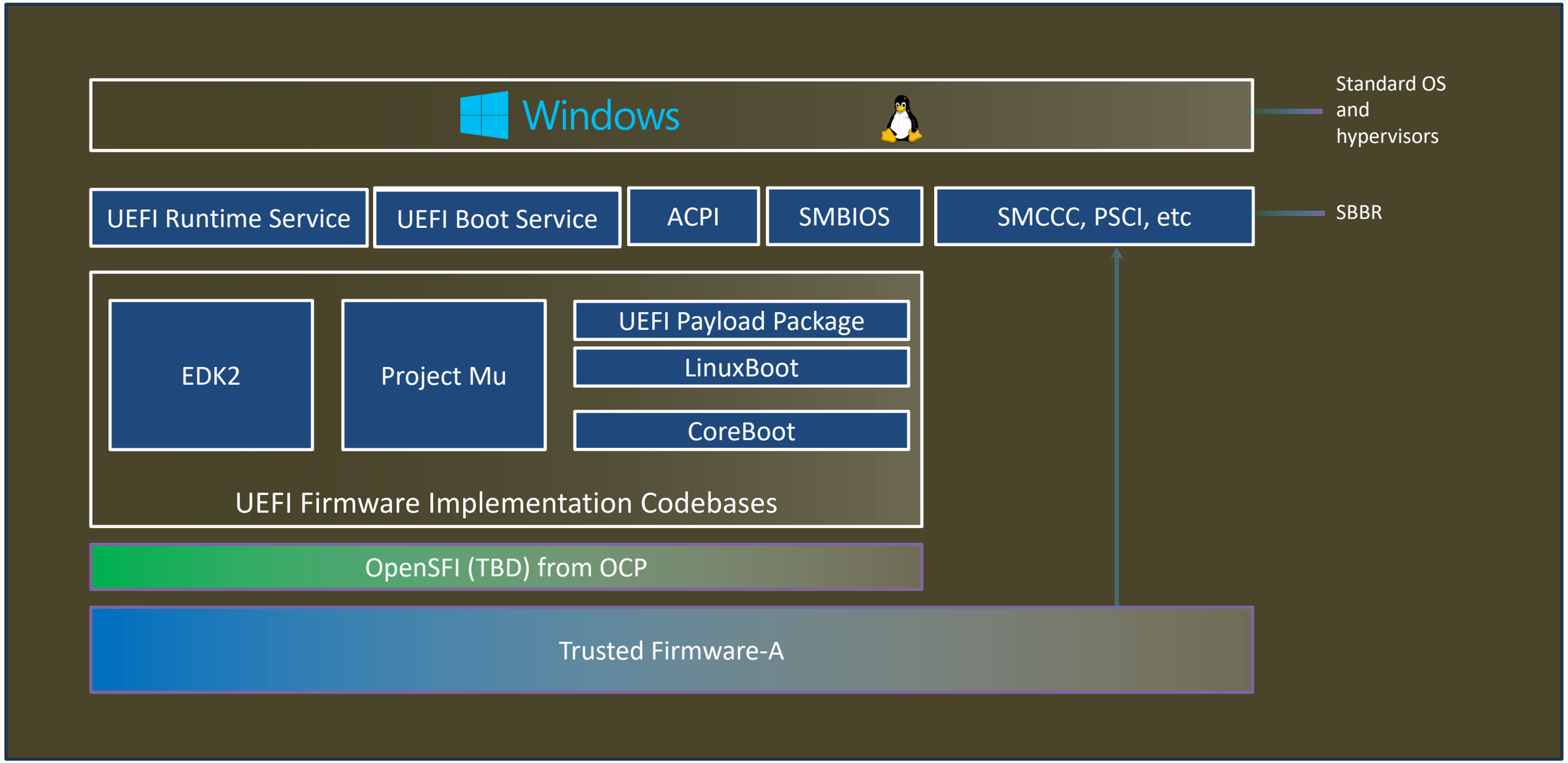
Server Manageability

Server Base Manageability Requirements

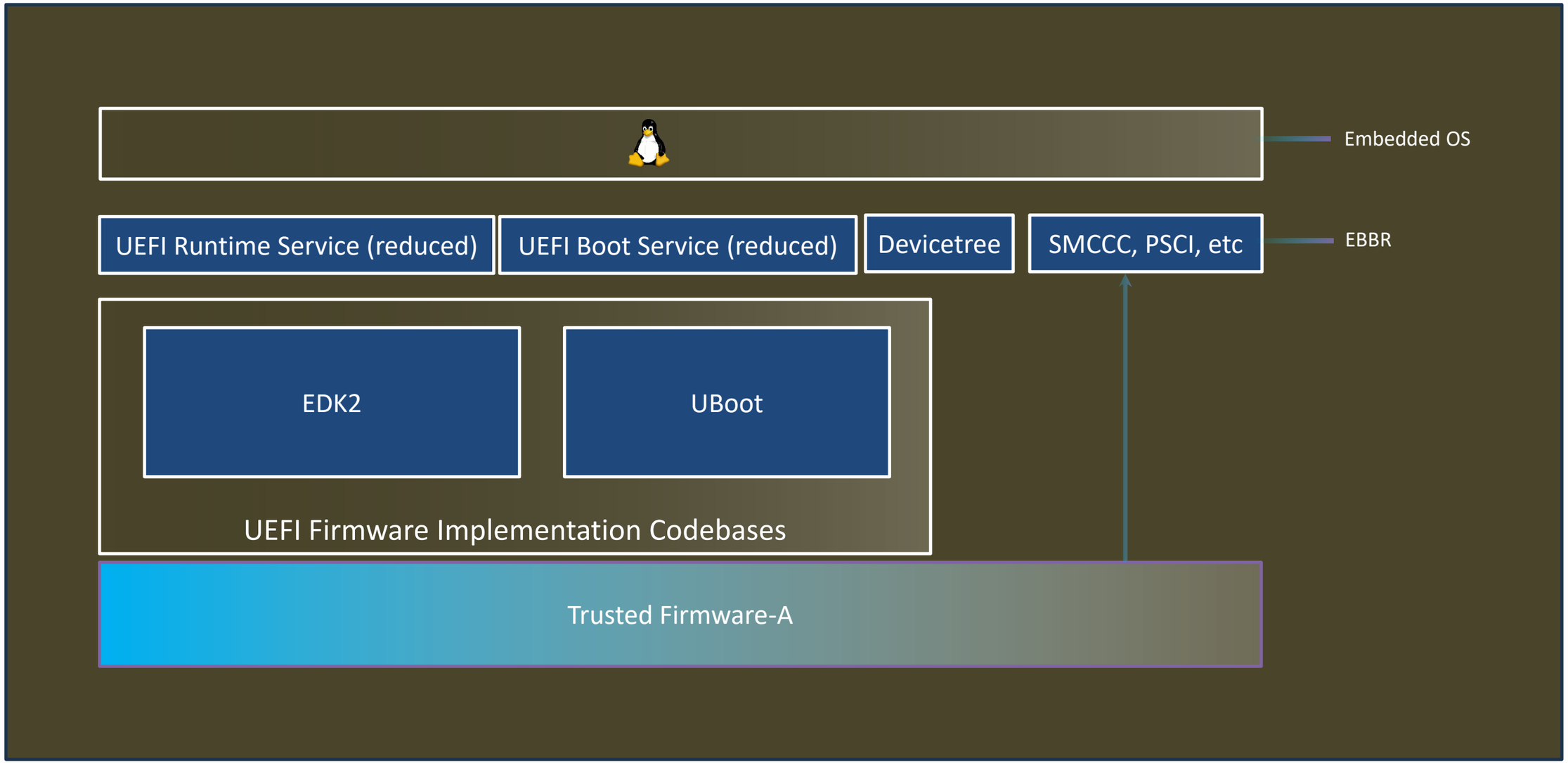
- Hardware and firmware requirements for system management for servers
- Builds on top of prevalent management industry standards: DMTF (Redfish, MCTP, PLDM, SPDM), OCP (HW Mgmt, DC-SCM, HW Fault Mgmt), IPMI
- SBMR v2.1 (Oct 2024)



SBBR Recipe (Servers, PCs, Windows IoT)



EBBR Recipe (Embedded Linux Devices)



BBR Related Arm Firmware Specifications

SMCCC & FF-A ABIs

Document	Title	Version	Released	URL
DEN0028	SMC Calling Convention (SMCCC)	1.6 G	Jul 2025	https://developer.arm.com/documentation/den0028/
DEN0022	Power State Coordination Interface (PSCI)	1.3 F.b	Oct 2024	https://developer.arm.com/documentation/den0022/
DEN0054	Software Delegated Exception Interface (SDEI)	C REL	Jan 2023	https://developer.arm.com/documentation/den0054/
DEN0113	DRTM Architecture for Arm	1.2	Jul 2025	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 A EAC1	Oct 2024	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/
DEN0060	Management Mode Interface (MM)	1.0 Issue A	Dec 2016	https://developer.arm.com/documentation/den0060/
DEN0077	Arm Firmware Framework (FF-A)	1.3 ALP2	Jul 2025	https://developer.arm.com/documentation/den0077/
DEN0140	FF-A Memory Management Protocol	1.3 ALP2	Jul 2025	https://developer.arm.com/documentation/den0140/latest/
DEN0143	FF-A SP Lifecycle	1.2 ALP0	Dec 2023	https://developer.arm.com/documentation/den0143/latest/

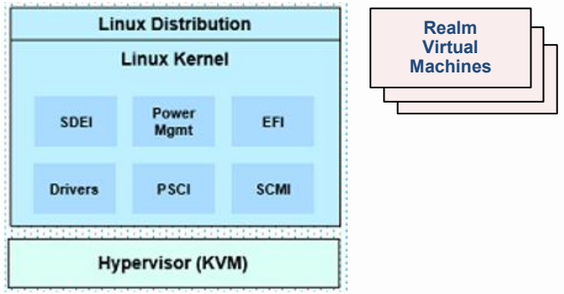
BBR related Arm Firmware Specifications

ACPI

Document	Title	Version	Released	URL
DEN0049	IO Remapping Table (IORT)	Issue E.g	Jul 2025	https://developer.arm.com/documentation/den0049/
DEN0085	ACPI for Arm RAS Extensions (AEST)	2.0 BET1	May 2024	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)	3.0 BET	Jul 2025	https://developer.arm.com/documentation/den0065/
DEN0067	ACPI for CoreSight	1.3	Apr 2024	https://developer.arm.com/documentation/den0067
DEN0093	ACPI for Arm Components (AGDI)	1.2 EAC1	Jul 2025	https://developer.arm.com/documentation/den0093/
DEN0048	ARM Functional Fixed Hardware (FFH)	1.3 ALP0	Sep 2025	https://developer.arm.com/documentation/den0048/

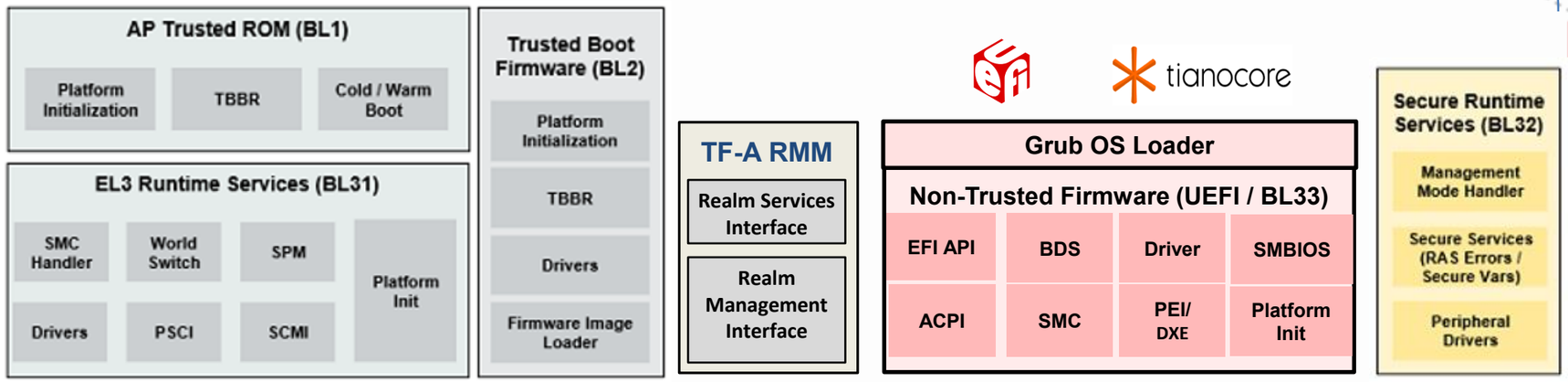
Example Server System Software

Host Operating System



Application Processor Firmware

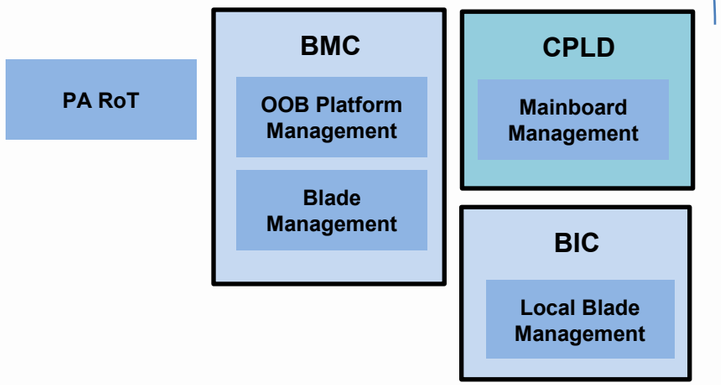
TrustedFirmware.org



Root world firmware (TF-A) | Realm Management | UEFI EDK2 / OS Loader | Secure Partitions

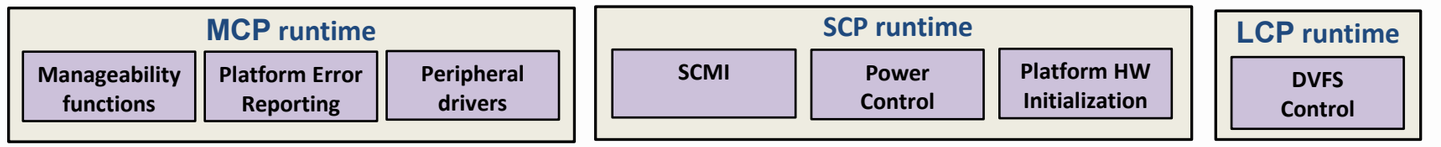
Platform Management

OpenBMC



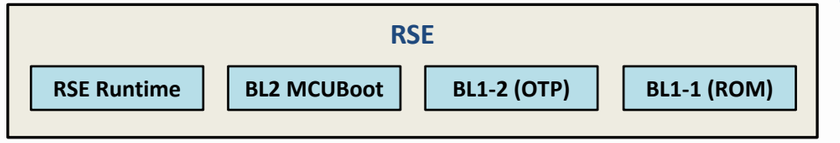
Supervisory Firmware

ARM-software / SCP-firmware Public



SoC RoT

TrustedFirmware.org



AP Boot Stages

- BL1 (TF-A Boot Loader stage 1)
- BL2 (TF-A Boot Loader stage 2)
- BL31 (TF-A BL31) – Root Monitor/EL3 Runtime Firmware
- BL32 – SPM / Hafnium
- RMM – TF-RMM Realm Monitor
- BL33 – UEFI (Non-trusted Firmware)
- OSPM – Linux, Windows

Questions?

References

- Arm SystemReady
- Arm ARM