Linaro Connect
MADRID 2024 | MAY 14-17 2024

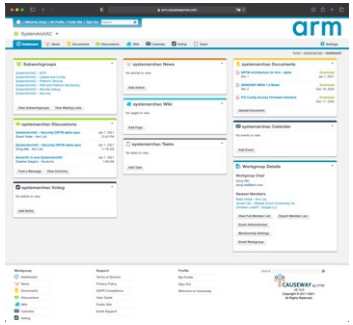
Arm System Architecture and SystemReady Update

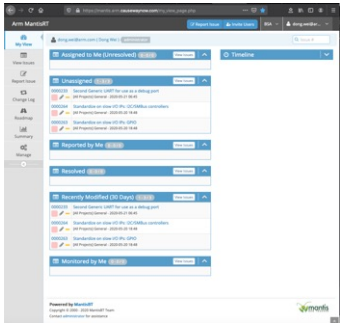
Dong Wei, Lead Standard Architect and Fellow, Arm

System Architecture Advisory Committee (SystemArchAC)

Where BSA/SBSA/BBR/BBSR/SBMR Specifications are Developed

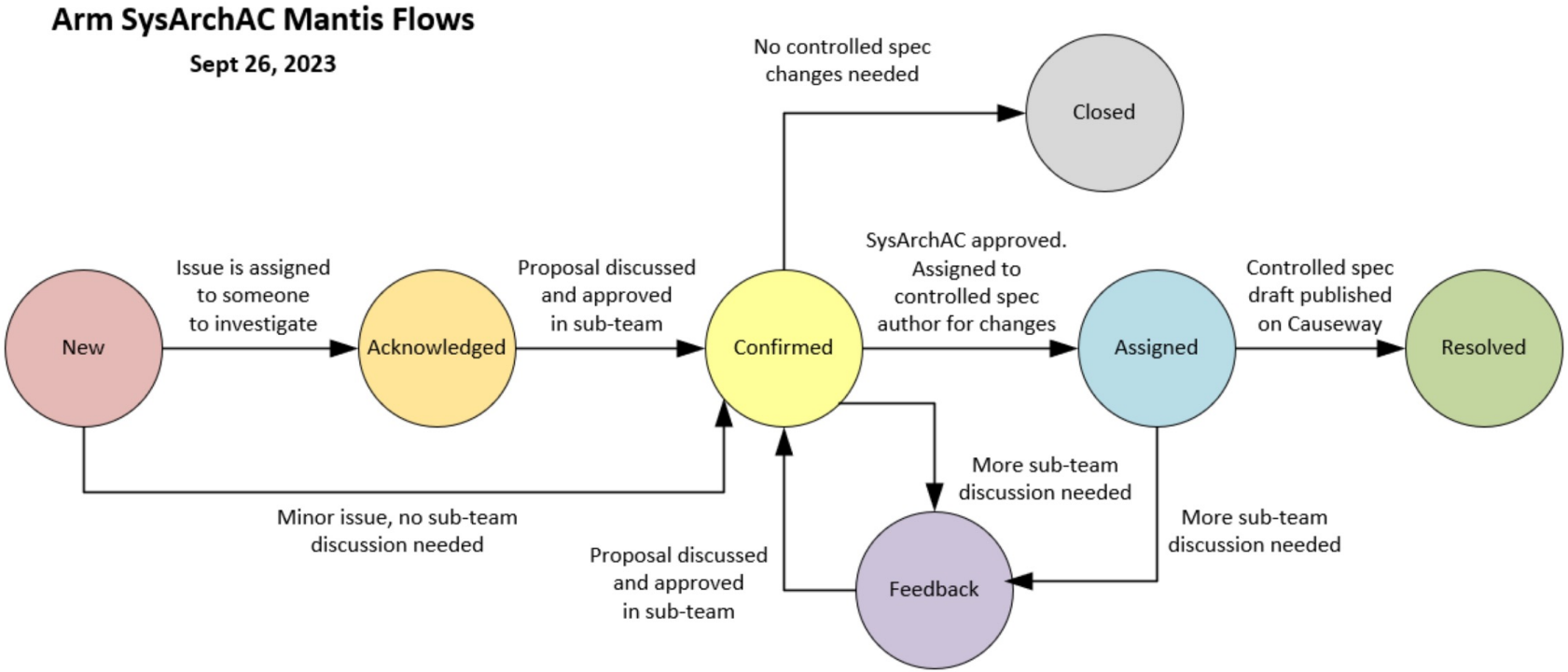
Facility: Causeway/Mantis



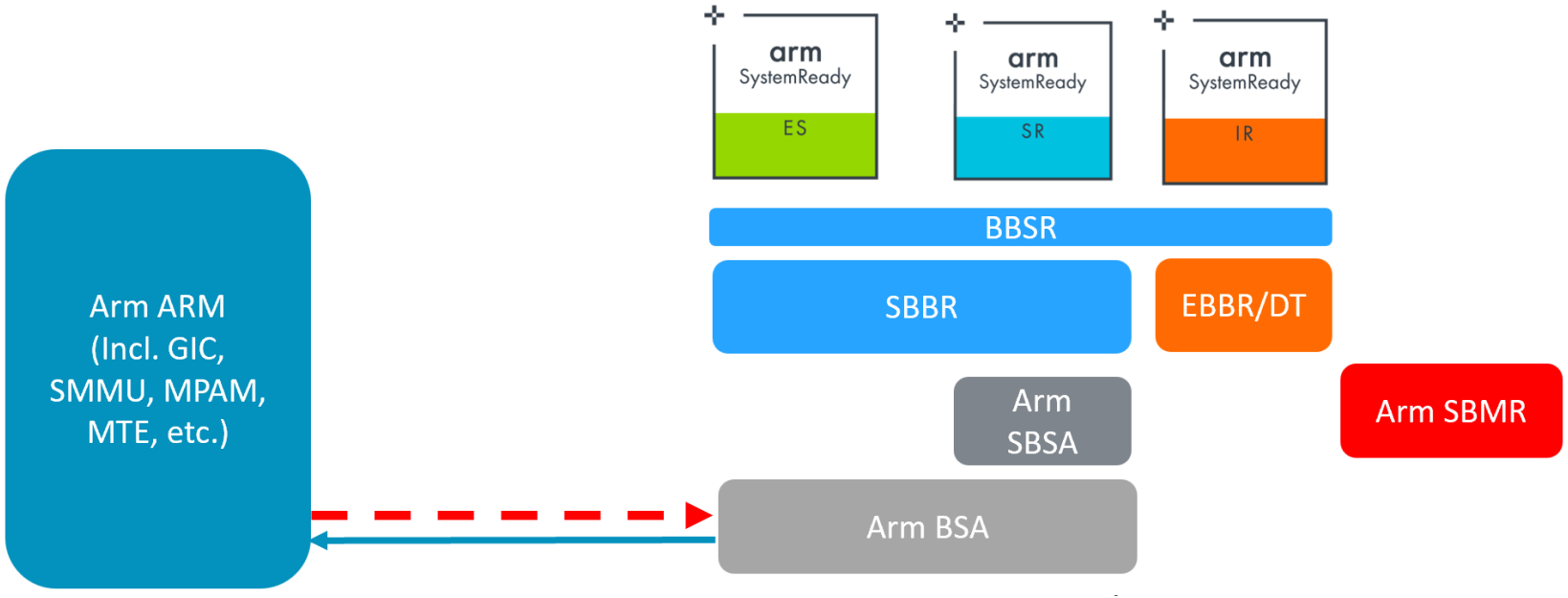


- 60+ companies
- Silicon Providers, OS Vendors, IP Providers, OEMs, ODMs, Firmware Vendors, IHVs, ISVs, Hyperscalers
- Standards approach for maximum compatibility and consistency
- Current subteams: ACPI, FF-A, LinuxBoot, Management, RAS, Real-time & Safety, Remote Debug, SBSA/SBBR, Security, UCIe, Update & Config, IO (PCI SIG members/CXL Promoters/Contributors), Rich IoT Edge
- Under consideration: PC

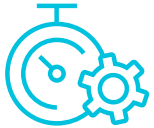
ECR Approval Flow



Specification Relationships

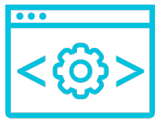


Key Specifications (OS install and Boot)



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)



Firmware (BBR – Base Boot Requirements)

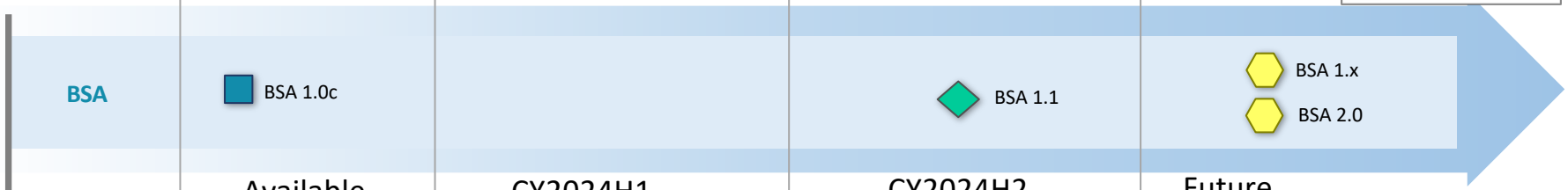
- Expands to include common firmware interfaces, but recognizes that different software stacks will require different recipes
- BBR v2.1 (April 2024)
- SBBR, EBBR, LBBR Recipes targeting different OSes

EBBR Specification

- Community development
- BBR spec refers to EBBR spec as needed
- V2.1.0 (Dec 2022)
- V2.2.0-Pre1 (April 2024)

Uboot is EBBR compliant

BSA Specification Roadmap



BSA 1.0c

(Oct 2022)

- Minor errata for BSA 1.0b

BSA 1.1

(2H CY2024)

Errata for BSA 1.0

- Require SVE2 for Armv9 (574)
- Recommend PTM (595)
- Remove CBSA reference (650)
- Remove LPI for Timer/WD/UART (656)
- PE PAuth errata (590), (596)
- GIC related errata (553), (576)
- PCIe related errata (518), (521), (588), (643), (620)
- SMMU related errata (631), (624)
- + any newly approved errata

"Future Requirements" for BSA Level 2

- Require FEAT_LSE (598)
- Recommend FEAT_LRCPC (599)

New Content:

- Minimal BSA rules for OS Install & Boot
- Criteria for new requirements & recommendations.
- Initial list of "VBSA" exceptions to BSA rules for virtual environments.

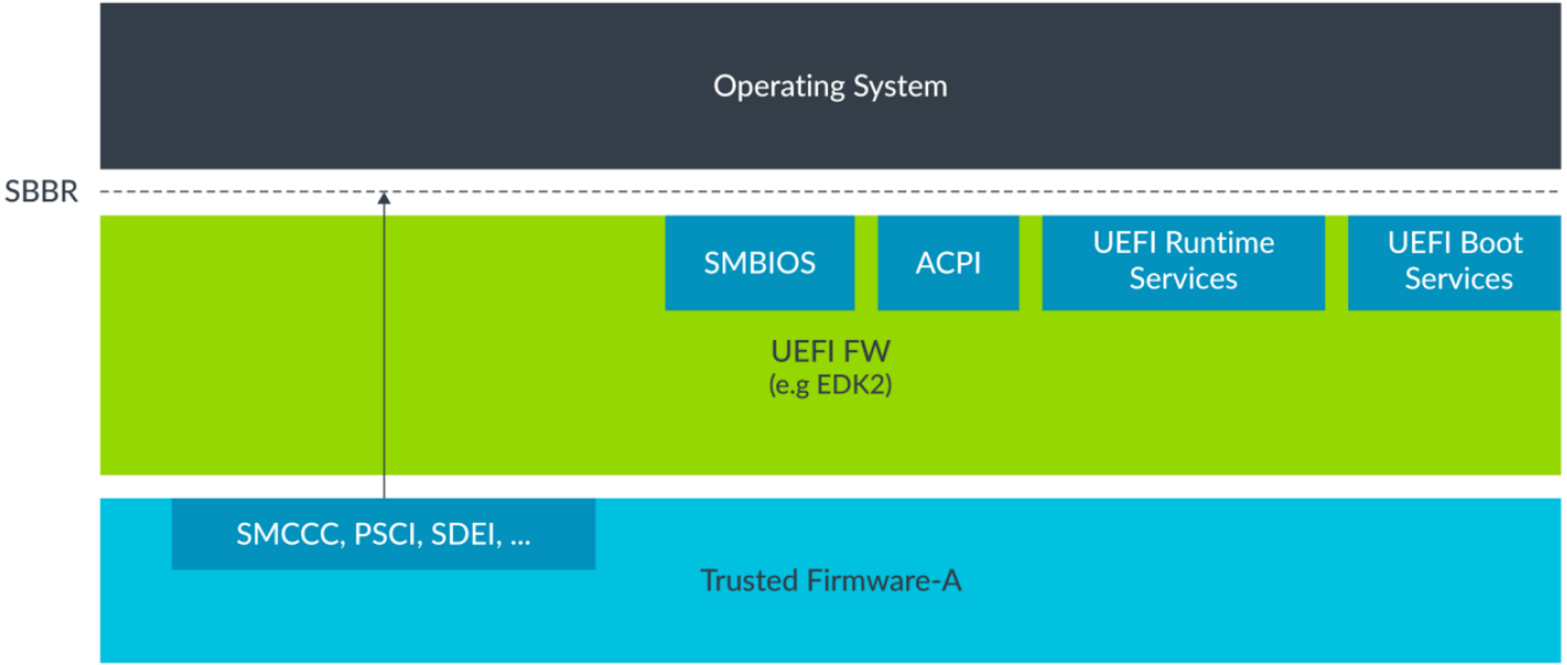
BSA 1.x

- Errata, as needed
- Future Requirements, as needed
- Continue "VBSA" exceptions

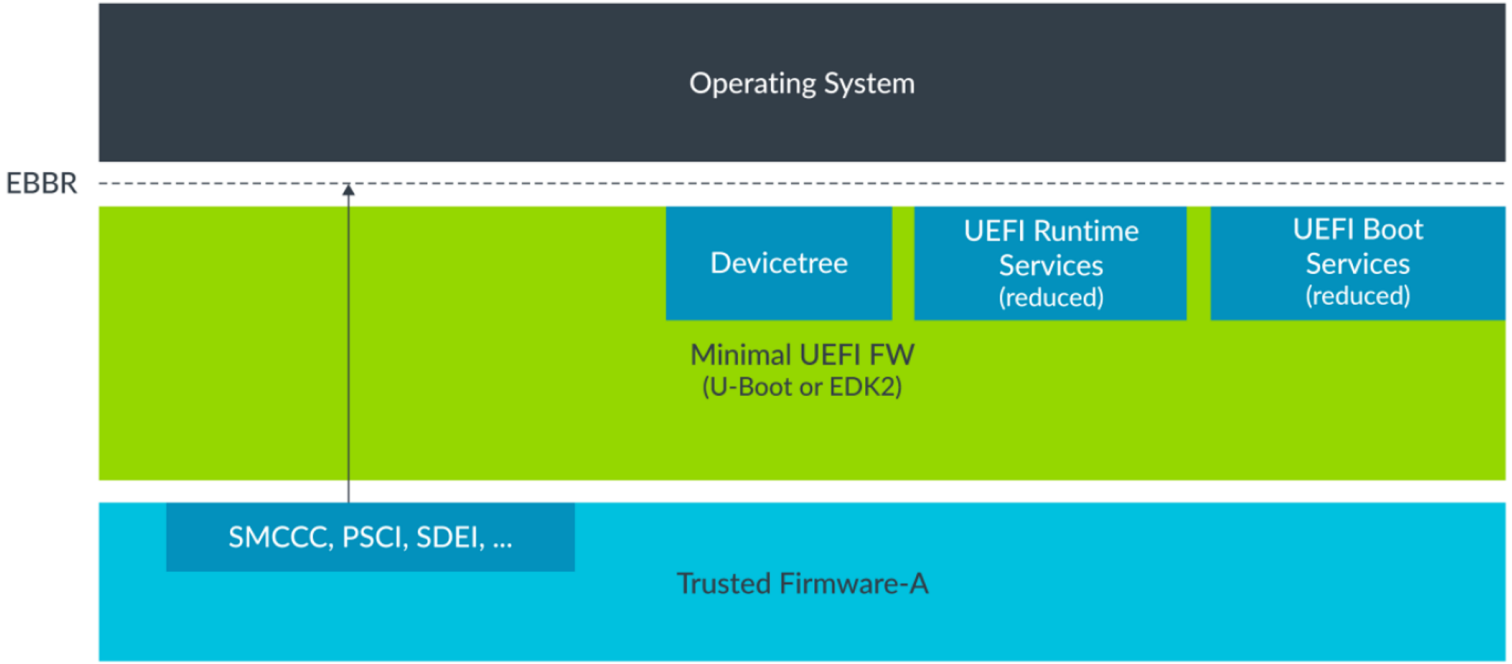
BSA 2.0

- "BSA Level 2" based on all the approved Future Requirements from BSA 1.x
- Release when enough requirements for BSA Level 2, and ecosystem readiness

BBR Recipe - SBBR

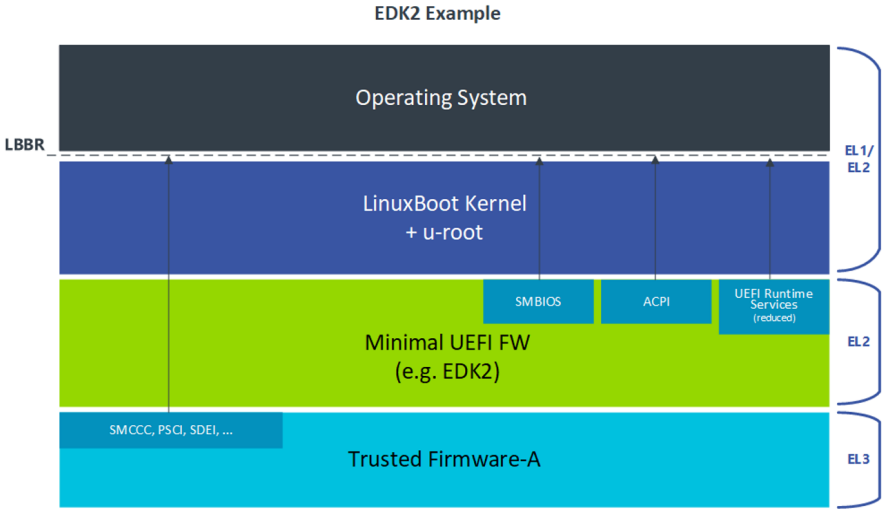


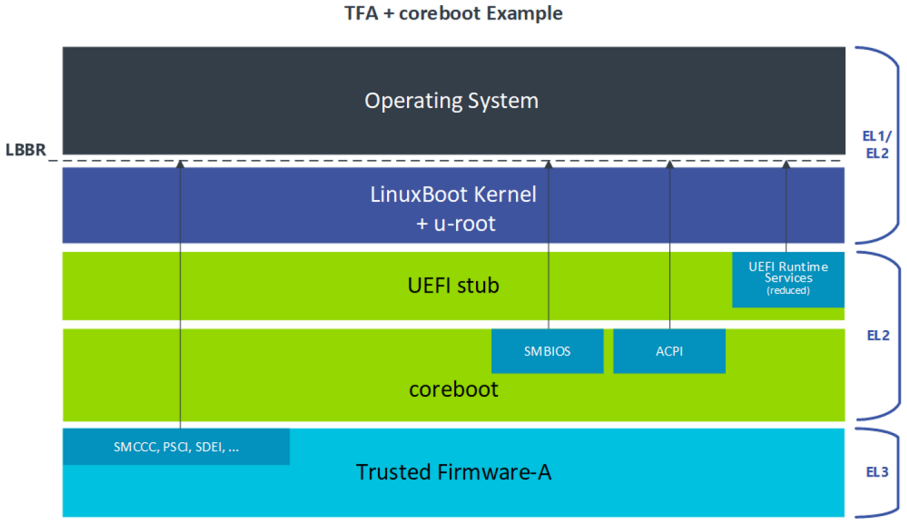
BBR Recipe - EBBR



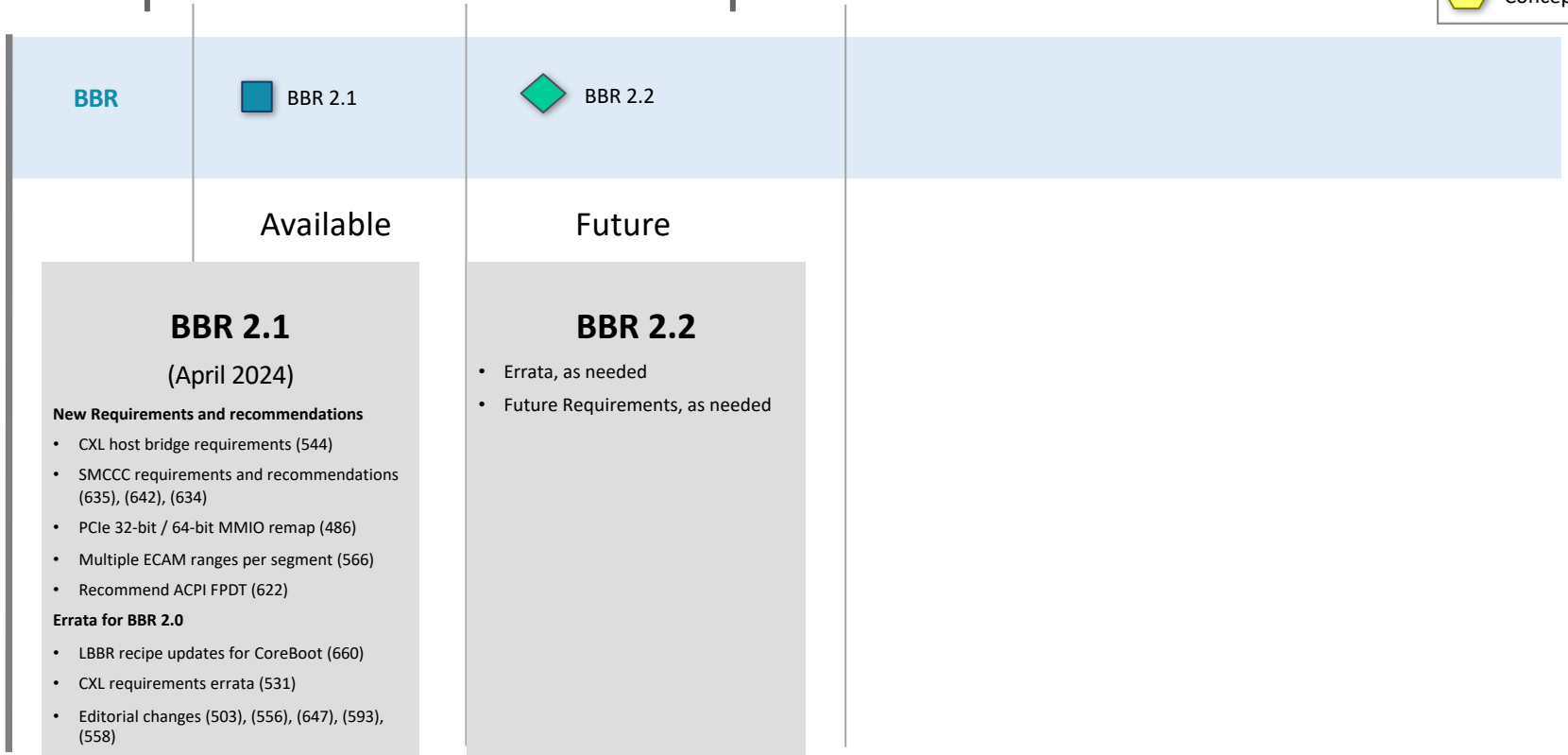
BBR Recipe - LBBR

Towards merging LBBR with SBBR





BBR Specification Roadmap

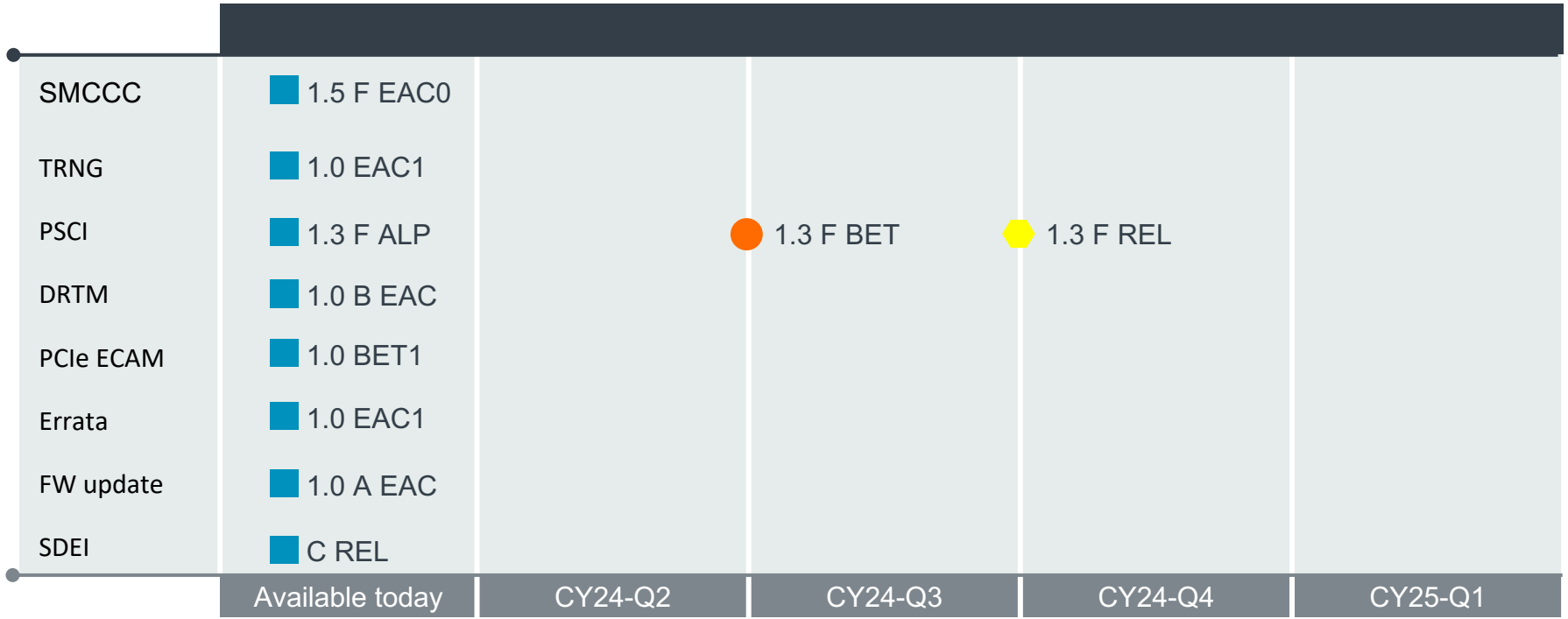


BBR related Arm FW specifications – SMCCC & FF-A ABIs

https://developer.arm.com/Architectures/Secure%20Monitor%20Calling%20Convention

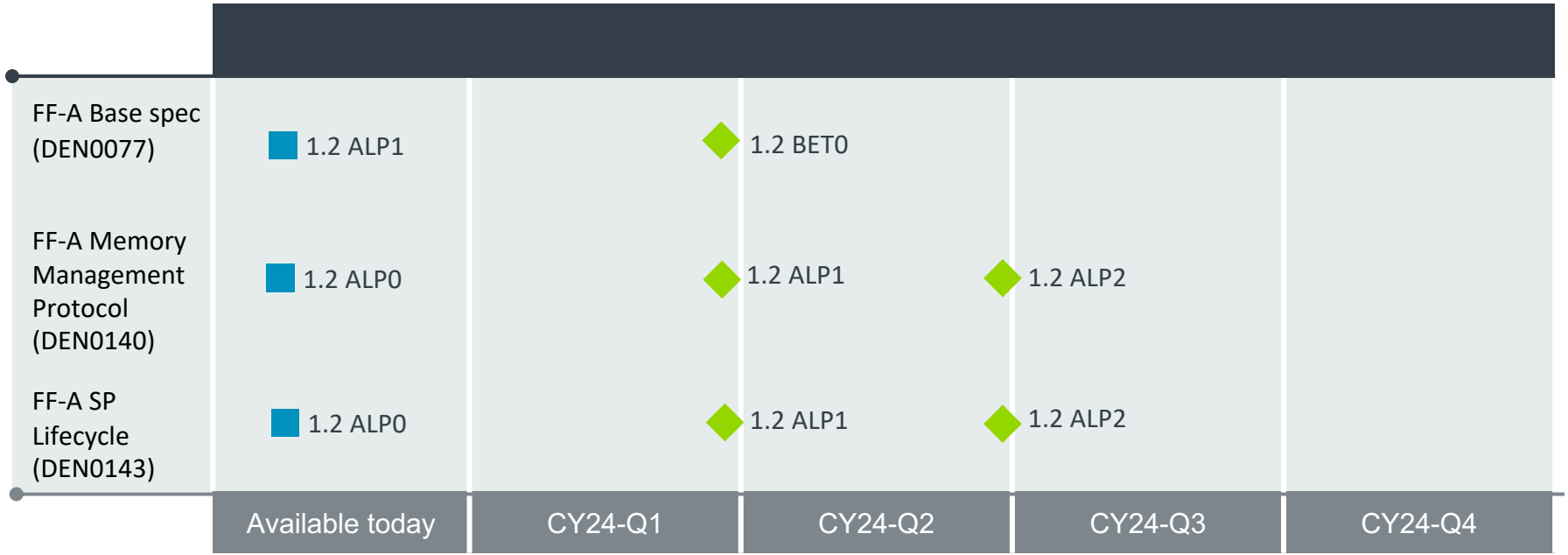
Document	Title	Version	Released	URL
DEN0028	SMC Calling Convention (SMCCC)	1.5 F EAC0	April 2024	https://developer.arm.com/documentation/den0028/
DEN0022	Power State Coordination Interface (PSCI)	1.3 F ALP	Feb 2024	https://developer.arm.com/documentation/den0022/
DEN0054	Software Delegated Exception Interface (SDEI)	C REL	Jan 2023	https://developer.arm.com/documentation/den0054/
DEN0113	DRTM Architecture for Arm	1.0 B REL	May 2024	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 EAC	Mar 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 (FFA)	1.2 ALP1	Oct 2023	https://developer.arm.com/documentation/den0077/
DEN0140	FF-A Memory Management Protocol	1.2 ALP0	Nov 2023	https://developer.arm.com/documentation/den0140/latest/
DEN0143	FF-A SP Lifecycle	1.2 ALP0	Dec 2023	https://developer.arm.com/documentation/den0143/latest/

SMCCC ABIs roadmap



Last Update: April 24, 2024

FF-A ABIs roadmap



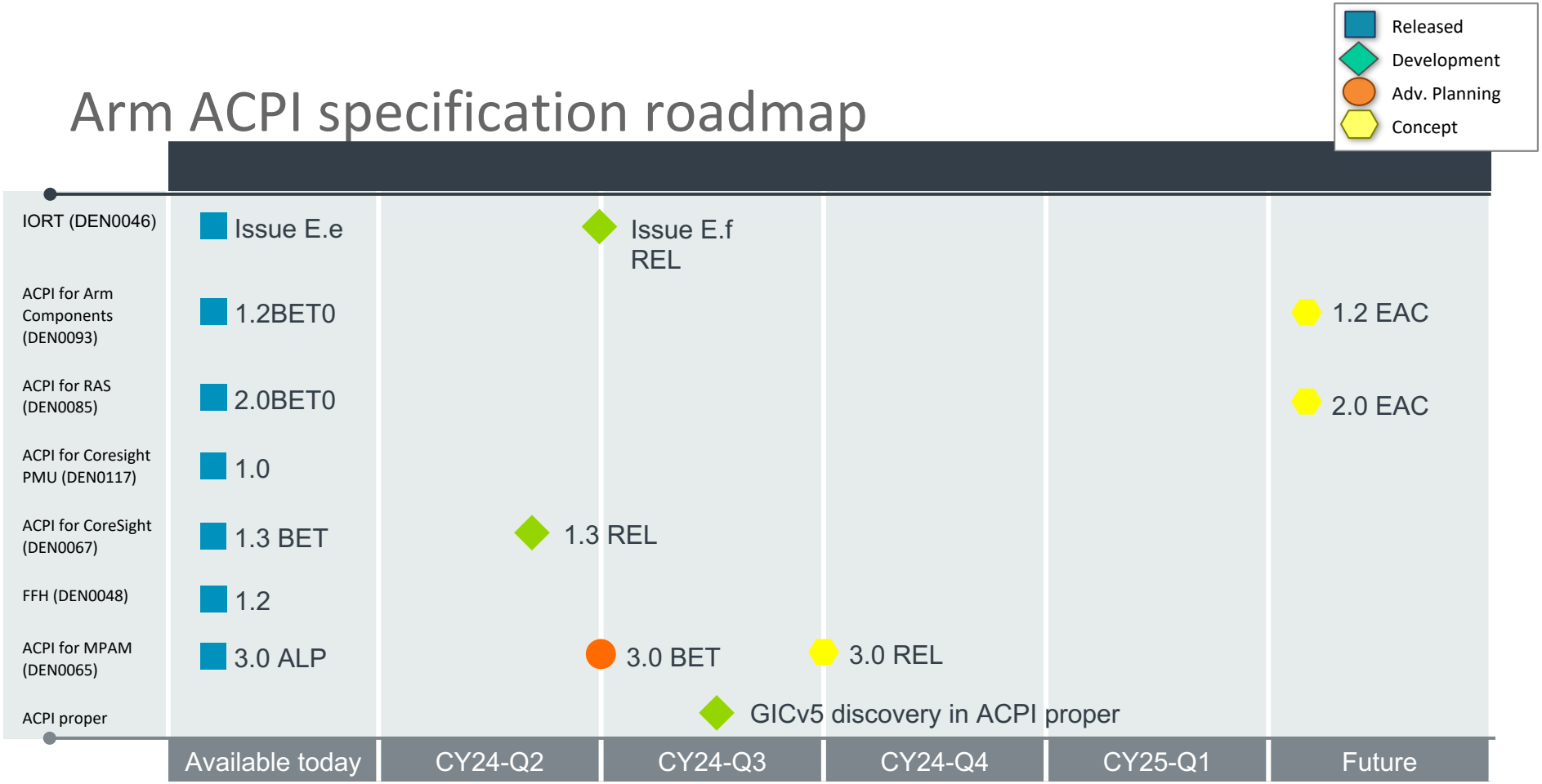
Last Update: January 10, 2024

BBR related Arm FW specifications – ACPI

https://developer.arm.com/Architectures/Advanced%20Configuration%20and%20Power%20Interface

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)	2.0 BET0	May 2023	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 ALP	Dec 2023	https://developer.arm.com/documentation/den0065/
DEN0067	ACPI for CoreSight	1.3 BET	Dec 2023	https://developer.arm.com/documentation/den0067
DEN0093	ACPI for Arm Components (AGDI)	1.2 BET0	May 2023	https://developer.arm.com/documentation/den0093/
DEN0048	ARM Functional Fixed Hardware (FFH)	1.2	Sep 2022	https://developer.arm.com/documentation/den0048/

Arm ACPI specification roadmap



Last Update: April 24, 2024

Other Specifications (beyond OS installation and boot)

Hardware Supplements (xBSA)

- Provides market segment specific hardware requirements
- Server BSA supplement for software standardization of server hardware features
  - SBSA v7.1 (Oct 2022)
  - Arm v8.7 or v9.x

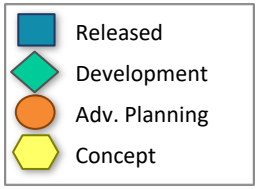
BBSR (Base Boot Security Requirements)

- Secure Boot and Firmware Update
- V1.3 (March 2024)

SBMR (Server Base Manageability Requirements)

- Server Management standardization
- V2.0 (May 2022)

xBSA Specifications Roadmap



SBSA

SBSA 7.1

SBSA 7.2

CXL Integration Guide 1.0

SBSA 7.x

SBSA.next

Available

SBSA 7.1

(Oct 2022)

- SBSA 7.0 errata
- Arm v8.7/v9.x requirements
- Self-hosted debug for Arm v9
- PCIe integration for GPU accelerated compute
- PCIe integration and error handling requirements (updates)
- PMU updates

2024

SBSA 7.2

(2H CY2024)

Errata for SBSA 7.1

- Relax NV2 to conditional requirement (659)
- Relax AMUv1p1 to recommendation (668)
- Lower RPMU_SYS_5 to a recommendation (607)
- Clarify FEAT_LPA / FEAT_LPA2 requirements (669)
- Clean up “Level 3 Firmware Requirements” section (648)
- SMMU related errata (625), (636)
- PAuth errata (581), (582), (610)
- RAS errata (557), (535), (580), (546), (623), (522), (295)
- PCIe related errata (587), (594)
- Other minor edits (579), (629), (623), (657)

“Future SBSA Level Requirements”

- RME System Architecture Requirements (511)
- TRNG/DRNG rates recommendations (539)
- TPM FIFO recommendation (567)
- Mandate minimum Architected Timer frequency (577)
- Require GICv4.1 (589)

New Content:

- Criteria for new requirements & recommendations.
- Initial list of “VSBSA” exceptions to BSA rules for virtual environments.

Future

SBSA 7.x , SBSA.next

- Will continue as 7.x with errata + Future Requirements, until there is partner request to publish Level 8

CXL Integration Guide

(2H CY2024)

- Initial version of Arm CXL Integration Guide and requirements

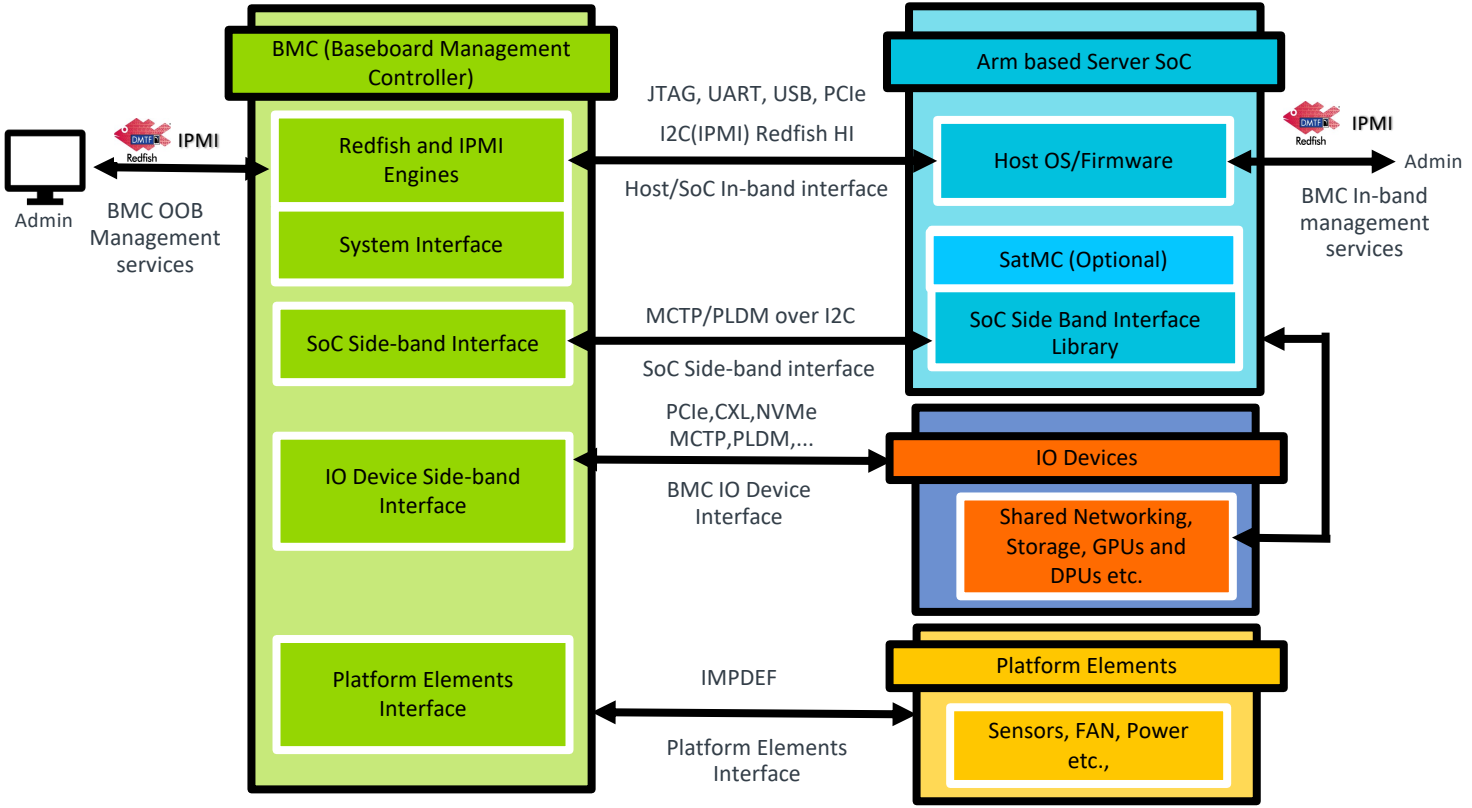
Base Boot Security Requirements (BBSR)

- Secure Boot, Firmware Update and TPM
- Version 1.3 is published on March 6, 2024
  - Contains 8 ECRs approved by SystemArchAC
- BBSR Architecture Compliance Suite
  - Integrated into the main SystemReady ACS in September 2023 release
- Spec is in maintenance mode, will address enhancements as they come up from Arm and partners.
- Future discussion topics in SystemArchAC security workgroup
  - Security assessment tooling
  - Firmware SBOM

BSA/xBSA/BBR for virtual environment

- Form hardware and firmware requirements for the virtual environments to support standard OSes running as guests on the hypervisors
- Approach
  - Run ACS on Google Cloud, Microsoft Azure, Alibaba Cloud and Parallels Desktop to understand the virtualized hardware and firmware implementations to define the proper requirements
  - The requirements may result in modifications to BSA/SBSA/BBR specs for the virtual environment
  - Currently under discussion in SystemArchAC Virtual Environment subteam

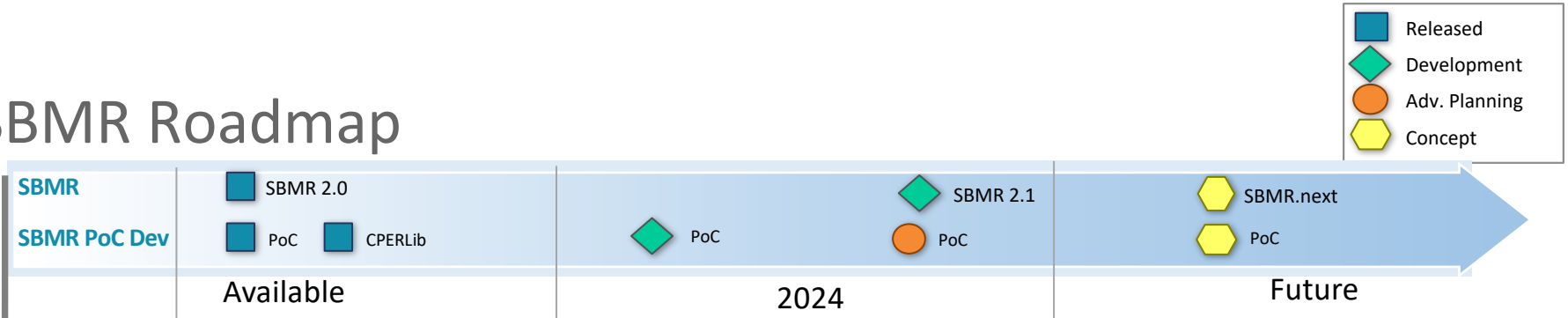
SBMR Overview



SBMR Compliance Levels

	Level	Out-of-band Interface	SoC Side-band Interface	Host/SoC In-band Interface	BMC-IO Device Interface	BMC Platform Element Interface
SBMR 1.0/1.1	**M0**	IMPLEMENTATION DEFINED	IMPLEMENTATION DEFINED	IMPLEMENTATION DEFINED	IMPLEMENTATION DEFINED	IMPLEMENTATION DEFINED
	M1	**Required:** IPMI	IMPIMPLEMENTATION DEFINED	**Required:** IPMI SSIF	IMPLEMENTATION DEFINED	IMPLEMENTATION DEFINED
	M2/ M2.1	**Required:** Redfish **and** IPMI	IMPIMPLEMENTATION DEFINED	**Required:** IPMI SSIF, **and** Redfish Host Interface	**Conditional Requirement:** NC-SI	IMPIMPLEMENTATION DEFINED
SBMR 2.0	**M3**	**Required**: Redfish	**Required:** MCTP/PLDM over I2C/SMBus or a higher bandwidth interface	**Required:** IPMI SSIF and Redfish Host Interface	**Conditional Requirement:** NC-SI **Recommended:** MCTP/PLDM for PCIe devices, and NVMe-MI over MCTP, using I2C/SMBus or a higher bandwidth interface.	IMPLEMENTATION DEFINED. Refer to OCP and IPMI specs for guidance
	M4	**Required:** Redfish	**Required**: MCTP/PLDM over I3C	**Required**: IPMI SSIF and Redfish Host Interface	**Conditional Requirement:** NC-SI **Conditional Requirement:** MCTP/PLDM for PCIe devices, and NVMe-MI over MCTP, using I3C or PCIe VDM, with I2C as fallback **Recommended**: CXL FM and CCI over MCTP for CXL devices, using I2C or PCIe VDM, with I2C as fallback	IMPLEMENTATION DEFINED. Refer to OCP and IPMI specs for guidance **Recommended:** PLDM/MCTP

SBMR Roadmap



SBMR 2.0

(April 2022)

- M3/M4 requirements
- Formalize the Side-band interface (SatMC – BMC) using MCTP/PLDM
- Platform monitoring updates
- RAS error logging updates
- OCP DC-SCM and HW Management requirements
- SPDM recommendations
- JTAG requirements updates
- DMTF specifications updates: Redfish, MCTP, SPDM, PLDM

SBMR 2.1

(H2 CY2024)

- Errata for SBMR 2.0
- Level M5 – alpha
- Platform AC-RoT and HES requirements
- Faster in-band interfaces (MMBI over PCIe MMIO)
- Faster side-band and BMC-IO interfaces (MCTP-over-USB)
- Multi-node systems support (1 BMC, multiple hosts)
- MCTP-over-PCC support (Host to SatMC)
- Update to industry standards

SBMR.next

(Future)

- Errata for SBMR 2.1
- Level M5 – BET / final
- DMTF PMCI Test Interface (PTTI) support
- RAS management enhancements
- Etc...

SBMR PoC Dev

- CPER library (generate and parse RAS error logs using CPER format)
- PoC – SBMR side-band development using MCTP/PLDM on physical platforms (ASPEED 2600 BMC) and virtual platforms (QEMU, Arm Neoverse Infra RF FVP)

SBMR PoC Dev

- PoC – OpenBMC on Arm Base FVP (as a BMC) + Neoverse Infra RD FVP (As a host & SatMC)
- PoCs (future) - MCTP Host Interface (on MMBI, I3C, PCC)
- PoCs (future) - Redfish HI on Arm Infra RD FVP

SBMR PoC Dev

- PoCs (future) - PTTI enablement in BMC, and SBMR+ACS to test MCTP inside the system (including SatMC side-band)

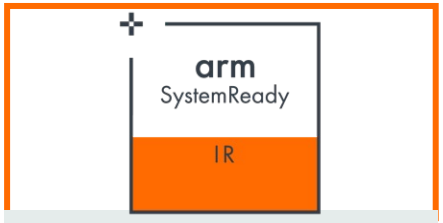
Manageability Compliance (SBMR-ACS)

- New open-source test suite for SBMR Compliance
  - https://github.com/ARM-software/sbmr-acs
- Automated HW Management compliance testing
  - Based on openbmc-test-automation and robot framework
  - Applies to any Arm server implementation (OpenBMC or other FW)
  - In-band (IB) and out-of-band (OOB)
  - Redfish, Redfish Host Interface, IPMI-over-LAN, IPMI Host Interface, USB/PCIe, KVM, UART (console redirection), …
  - Including compliance testing for OCP HW Management Profiles
- Ongoing collaborating with Arm server partners to verify their implementations

DRTM

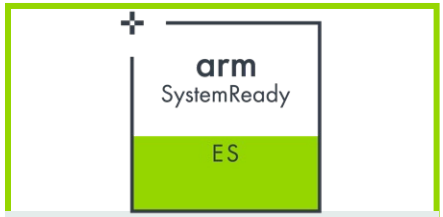
- Microsoft requested in 2019
- v1.0 B complete May 2024
- Future research topics
  - DRTM with TPM on RME-based system
  - Fine grained DMA protection
- ACS to evaluate compliance with the DRTM architecture
  - Plan in place and being executed for alpha release in Q2 CY24
- Trusted Firmware-A
  - Patch set to updated support to 1.0 in review

arm SystemReady

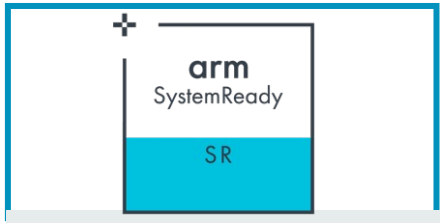


"Just Works" for **Linux** and **BSD** on **embedded** Arm SoCs

- 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

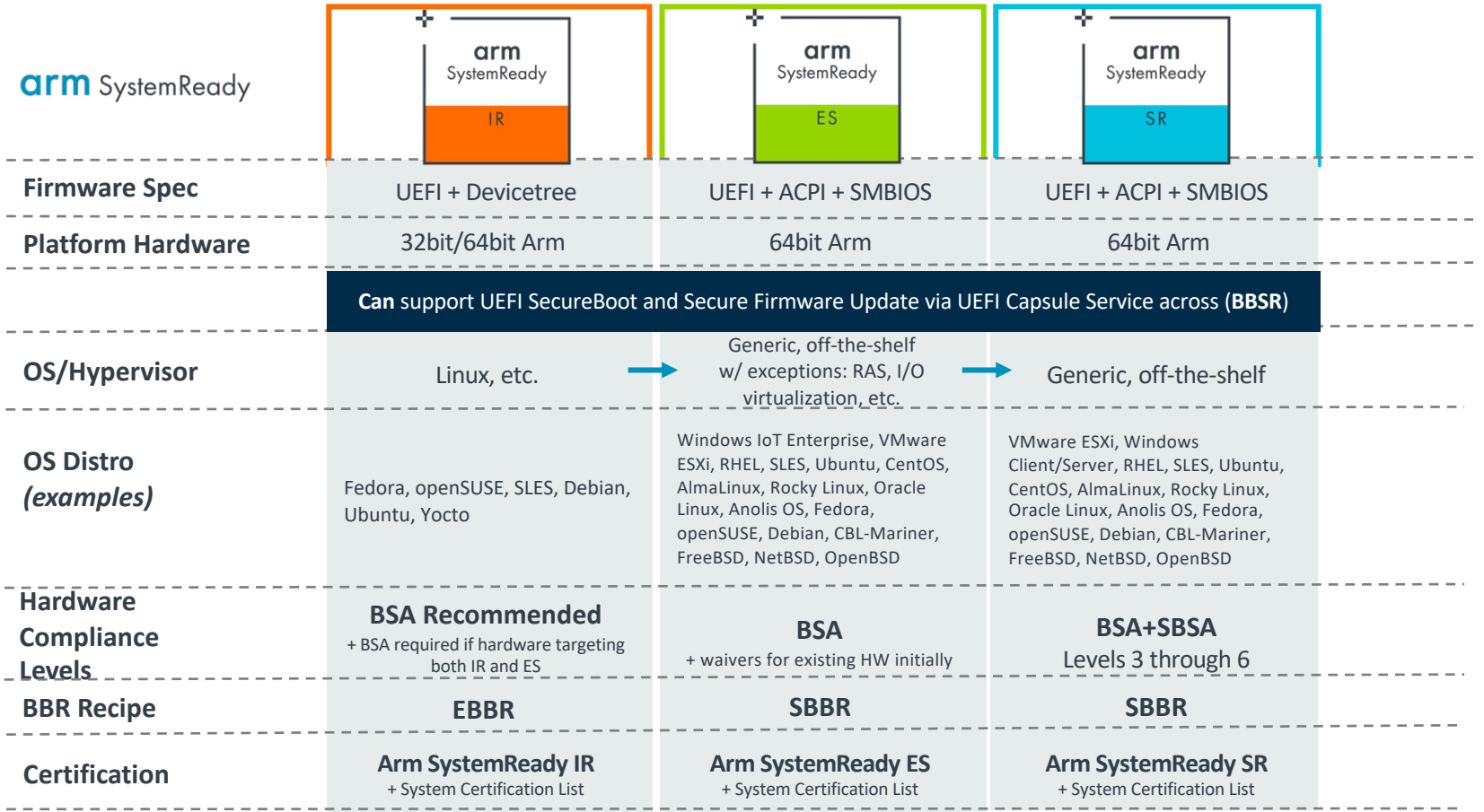


"Just Works" on **server or workstation** Arm SoCs

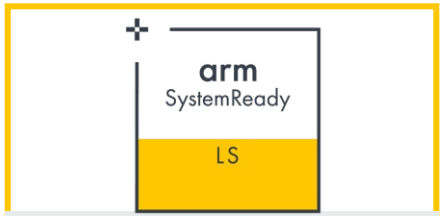
- For the **Windows**, **VMware,** Linux, and BSD ecosystems

- **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

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

SystemReady Requirements Spec v2.2 (Oct, 2023)

IR

V2.1

- **IR ACS v2.1.0 test results**
- BSA v1.0c recommended
- BBR v2.0 (EBBR v2.1.0)
- BBSR 140/150
- **Ethernet port requirements**
- **Boot sources stated by the vendor**
- Devicetree v0.3
- Waiver Levels 0-2

SIE recommended

OS installation and boot logs

- **3 Linux/BSD distros required**
- Recommended list:
  - Fedora, Debian, **RHEL, Rocky Linux, SLES, openSUSE**, Ubuntu, **OpenWRT**

ES

V1.5

- ES ACS v1.3.0 test results
- BSA v1.0c
- BBR v1.0 (SBBR)
- **Hardware functionality requirements**
- 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

V2.5

- **SR ACS v2.0.0 test results**
- BSA v1.0c + SBSA Supplement **v7.1** Level 3-7
- BBR v1.0 (SBBR)
- **Hardware functionality requirements**

SIE recommended

OS installation and boot logs

- WinPE (GPT) required
- **RHEL and SLES required**
- VMware ESXi-Arm (recommended)
- Other Linux/BSD distros recommended

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

SystemReady Requirements Spec v2.2 (Oct, 2023)

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

ISVs

SiPs

Hyperscale Cloud Service Providers

OEMs/ODMs

EDAs

IFVs

Communities

Test Labs

The Growing Standard for Software on Arm

arm SystemReady

144

Published SystemReady certificates ensuring software just works on Arm

53 SystemReady SR devices certified

25 SystemReady ES devices certified

43 SystemReady IR devices certified

22 SystemReady VE virtual environment certified


LinaroConnect
MADRID 2024 | MAY 12-17 2024
Thank you