Arm SystemReady Compliance

System Requirements Specification v3.0

Document number: DEN0109H

Arm SystemReady Compliance System Requirements Specification

Release information

The Change History table lists the changes made to this document.

Table 1 Change History

Date	Issue	Confidentiality	Change
6 Oct 2020	A	Non-Confidential	Arm SystemReady Requirements Specification version 1.0
27 April 2021	B	Non-Confidential	Arm SystemReady Requirements Specification version 1.1 • Updated requirements for SystemReady SR v2.0, ES v1.0 and IR v1.0 • Reformatted the guidance for possible requirements for future versions • Renamed “security option” to “security extension” • Removed the Pre-silicon Certification as Pre-silicon is an enabler and tool not a requirement or certification program • Added waiver levels for SystemReady ES and IR • Added certification process flow chart
19 Oct 2021	C	Non-Confidential	Arm SystemReady Requirements Specification version 1.2 • Updated requirements for SystemReady SR v2.1, ES v1.1, and IR v1.1 • Updated the guidance for possible requirements for future versions • Renamed the “Security Extension” to “Security Interface Extension” • Added certification process for the updated and derivative devices
16 May 2022	D	Non-Confidential	Arm SystemReady Requirements Specification version 1.3 • Updated requirements for SystemReady SR v2.2 and ES v1.2 • Defined requirements for SystemReady LS v0.9 • Defined requirements for SystemReady Virtual Environment (VE) v0.5 • Created Appendix C exclusion to BSA for the ES and IR bands
28 Oct 2022	E	Non-Confidential	Arm SystemReady Certification System Requirements Specification version 2.0 • Updated requirements for SystemReady IR v1.2 & v2.0 ALPHA • Updated requirements for SystemReady Virtual Environment (VE) v1.0 • Updated requirements for SystemReady SR v2.3 and ES v1.3 • Renamed SystemReady LS v0.9 to SystemReady LS v1.0 ALPHA to be consistent with the IR version naming • Removed Appendix C exclusion to BSA for the ES and IR bands with the changes made to BSA 1.0c

26 April 2023	F	Non-Confidential	Arm SystemReady Certification System Requirements Specification version 2.1 • Updated requirements for SystemReady SR v2.4, ES v1.4, IR v2.0 and SIE v1.2 • Updated the Waiver Levels • Updated the Certification Process
30 Oct 2023	G	Non-Confidential	Arm SystemReady Certification System Requirements Specification version 2.2 • Improved the description of the SystemReady program and its bands • Updated requirements for SystemReady SR v2.5, ES v1.5, and IR v2.1 • Added SystemReady IR Certification Policy Guide
21 Nov 2024	H	Non-Confidential	Arm SystemReady Compliance System Requirements Specification version 3.0 • Move from Certification to Compliance • Merge SystemReady ES and SR into the new SystemReady • Change the SystemReady IR name to SystemReady Devicetree • Deprecate SystemReady LS

CONTENTS

NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS LICENSE, TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, IN CONTRACT, TORT OR OTHERWISE, IN CONNECTION WITH THE SUBJECT MATTER OF THIS LICENSE (INCLUDING WITHOUT LIMITATION) (I) LICENSEE'S USE OF THE DOCUMENT; AND (II) THE IMPLEMENTATION OF THE DOCUMENT IN ANY PRODUCT CREATED BY LICENSEE UNDER THIS LICENSE). THE EXISTENCE OF MORE THAN ONE CLAIM OR SUIT WILL NOT ENLARGE OR EXTEND THE LIMIT. LICENSEE RELEASES ARM FROM ALL OBLIGATIONS, LIABILITY, CLAIMS OR DEMANDS IN EXCESS OF THIS LIMITATION.

This License shall remain in force until terminated by Licensee or by Arm. Without prejudice to any of its other rights, if Licensee is in breach of any of the terms and conditions of this License then Arm may terminate this License immediately upon giving written notice to Licensee. Licensee may terminate this License at any time. Upon termination of this License by Licensee or by Arm, Licensee shall stop using the Document and destroy all copies of the Document in its possession. Upon termination of this License, all terms shall survive except for the License grants.

Any breach of this License by a Subsidiary shall entitle Arm to terminate this License as if you were the party in breach. Any termination of this License shall be effective in respect of all Subsidiaries. Any rights granted to any Subsidiary hereunder shall automatically terminate upon such Subsidiary ceasing to be a Subsidiary.

The Document consists solely of commercial items. Licensee shall be responsible for ensuring that any use, duplication or disclosure of the Document complies fully with any relevant export laws and regulations to assure that the Document or any portion thereof is not exported, directly or indirectly, in violation of such export laws.

This License may be translated into other languages for convenience, and Licensee agrees that if there is any conflict between the English version of this License and any translation, the terms of the English version of this License shall prevail.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. No License, express, implied or otherwise, is granted to Licensee under this License, to use the Arm trade marks in connection with the Document or any products based thereon. Visit Arm's website at https://www.arm.com/company/policies/trademarks for more information about Arm's trademarks.

The validity, construction and performance of this License shall be governed by English Law.

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

Arm document reference: PRE-21585 Version 5.0, March 2024

1 Arm SystemReady program

Arm SystemReady program is a compliance program for Arm A-profile CPU-based systems with two bands targeting different user experiences.

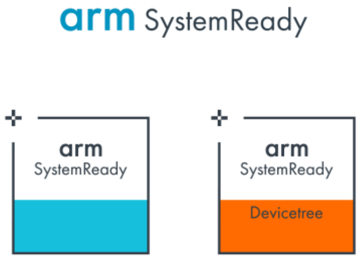

Figure 1: SystemReady program and its two bands

1.1 SystemReady band

SystemReady band is for systems that are designed for end users who would like to install and run generic unmodified off-the-shelf standard operating system images on their systems with forward and backward compatibility. This means that old operating systems can install and run on new hardware and vice versa.

To ensure these capabilities, these systems must provide Advanced Configuration and Power Interface (ACPI) firmware abstraction and follow a set of minimum hardware and firmware requirements in the Base System Architecture (BSA) specification and the SBBR recipe defined in the Base Boot Requirements (BBR) specification.

SystemReady band is market-segment agnostic. For example, servers, DPUs, PCs, or Windows IoT devices all need to meet these requirements if the above user experience is expected. There might be additional market segment-specific requirements necessary for operating systems to support hardware features in a standard manner. For example, the Server Base System Architecture (SBSA) supplement specification defines these additional requirements for the server segment. For servers, Trusted Platform Module (TPM) must be used and the related requirements in Base Boot Security Requirements (BBSR) must be met.

Note: SystemReady ES and SR bands in the previous versions of this document are now merged into this SystemReady band.

1.2 SystemReady Devicetree band

Separately, SystemReady Devicetree band is for systems that are built to support embedded Linux or embedded BSD operating systems only. These systems can still benefit from having standard boot loader, secure boot and secure firmware update features. These systems must follow the EBBR recipe defined in the Base Boot Requirements (BBR) specification. BSA compliance is recommended but not required for these systems.

Systems compliant with SystemReady Devicetree band typically do not aim for forward compatibility, meaning there is no expectation that old operating systems can install and run on new systems without modifications. However, backward compatibility is pursued, meaning newer operating systems are expected to install and run on older systems without modifications. To ensure the backward compatibility, these systems can provide Devicetree firmware description rather than ACPI firmware abstraction. However, the support of the SoC in these systems must be upstreamed to the mainline Linux or BSD.

Note: SystemReady IR band in the previous versions of this document is now this SystemReady Devicetree band.

1.3 SystemReady compliance summary

The Arm SystemReady compliance program currently embraces these differences in the Arm ecosystem. This specification describes the requirements for the program.

SystemReady band and SystemReady Devicetree band are supported by a common Architecture Compliance Suite (ACS) that is modular, to support testing against different combinations of specifications required.

Disclaimer: Arm Limited disclaims any responsibility for determining or assuring that any product actually passes the ACS or that representations of compliance by partner company are true or accurate. See the Arm SystemReady Band Policy Guidelines and the Arm SystemReady Devicetree Band Policy Guidelines for clarifications on the compliance process.

Table 2 summarizes the specifications that the devices need to comply with.

Compliance	Specifications		
SystemReady band	BSA	SBSA if server	SBBR Recipe in BBR
SystemReady Devicetree band	-	-	EBBR Recipe in BBR and Devicetree

Table 2: Arm SystemReady band and SystemReady Devicetree band

Note: IoT devices that are BSA compliant can be either SystemReady band or SystemReady Devicetree band depending on the firmware recipe supported for the targeted operating systems.

1.4 SystemReady major and minor versions

Major versions of SystemReady band or SystemReady Devicetree band signify substantial advancements in the evolution of compliance requirements, introducing significant changes, enhancements, or expansions to the compliance criteria. An example is the ability to test new technologies required by SystemReady.

Minor versions occur more frequently within the context of major versions. These minor versions denote smaller, yet valuable, steps forward in development. They typically involve incremental changes, refinements, or additions to existing compliance requirements.

2 SystemReady band compliance

2.1 SystemReady band v3.0 requirements

SystemReady band v3.0 requires that the systems are compliant to the following specifications:

- BSA v1.0c or later
- SBBR recipe in BBR v2.0 or later
- For servers, SBSA Supplement v7.1 or later

SystemReady band v3.0 recommends that the systems are compliant to the following specification:

- BBSR Specification v1.2 or later:
  - When a TPM is present, the related requirements in BBSR are required.
  - For servers, TPM must be present.

SystemReady band ACS v3.0.0, or later, must be used to test the systems for compliance.

Also, SystemReady band v3.0 recommends that OS installation and boot logs are used to check for compliance:

- Windows 11 or WinPE boot log, from a GPT partitioned disk
- Installation and boot logs from Linux distros or BSDs. When selecting Linux distributions or BSDs, maximize coverage by installing an OS from different groups in the following list:
  - RHEL, Fedora, CentOS, AlmaLinux, Rocky Linux, Oracle Linux, Anolis OS
  - SLES, openSUSE, Ubuntu, Debian
  - CBL-Mariner
  - NetBSD, OpenBSD, FreeBSD
- VMware ESXi-Arm installation and boot logs

Note: some classes of devices, such as DPUs, might require special methods for deploying operating systems. This might include reformatting off-the-shelf OS distros in a device-specific format, or using non-standard deployment frameworks.

SystemReady band v3.0 requires the following hardware functionality:

Hardware or Peripheral	Functionality	Minimum required	Recommended or aspirational
Console in and out	Console for the user to interact with the system to install and boot the OS	At least one input and one output console: • Local USB keyboard and video graphics • Local UART console • For servers, BMC remote keyboard and video graphics • For servers, Remote UART such as IPMI Serial-over-LAN (SOL)	All of the following: • If present, Local USB keyboard and video graphics • Local UART console Servers that support BMC: • If present, BMC remote keyboard and video graphics • Remote UART such as IPMI SOL
OS installation media	Media used for OS installation source	For server, at least two separate media sources from the following groups. For others, at least one	All of the following if present: • Local USB • NVMe drive

		media source from the following groups: • Local USB, or BMC remote USB virtual media • NVMe drive, or SATA drive, or SAS drive • Network (PXE, HTTP, HTTPS, iSCSI, or FCoE, or NVMoF) • eMMC or internal SSD	• SATA drive • SAS drive • Network (PXE, HTTP, HTTPS or iSCSI) • eMMC or internal SSD Servers that support BMC: • BMC remote USB virtual media • FCoE, or NVMoF
OS boot media	Media used for installing and booting the target OS	For server, at least two separate media destinations from the following groups. For others, at least one media destination from the following groups: • Local USB • NVMe drive • SATA drive • SAS drive • Network (iSCSI or FCoE or NVMoF)	All of the following if present: • Local USB • NVMe drive • SATA drive • SAS drive
Network boot	Network device for OS boot	None	Support for network boot from at least one network device, using at least one of the following boot protocols: • PXE Boot • HTTP or HTTPS Boot • iSCSI Boot • NVMeoF
OS Network support	Network device for OS usage	At least one network device: • Integrated Network controller • PCIe network card • USB network device	OS support for network access to at least one network device, other than USB network devices

Table 3: SystemReady band hardware functionality requirements

2.2 SystemReady band pre-silicon testing

Arm SystemReady pre-silicon is a program that helps silicon vendors achieve hardware compliance as defined in the SystemReady band requirements prior to taping out. This is a well-defined and low-risk path to SystemReady.

The latest tagged releases of BSA ACS, and for servers SBSA ACS in addition, must be used to test for compliance. See SystemReady Pre-Silicon Reference Guide BSA integration and compliance.

Note: BSA compliant system can support either band.

Note: For a complete compliance coverage of the BSA and SBSA specifications, a PCIe exerciser is needed. This is particularly important for PCIe integration rules. This exerciser is typically implemented as a controllable PCIe endpoint, transactor or verification IP (VIP). Arm collaborates with EDA vendors who develop and commercialize these exercisers.

3 SystemReady Devicetree band compliance

3.1 SystemReady Devicetree band v3.0 requirements

SystemReady Devicetree band v3.0 requires that the systems are compliant to the following specifications:

- EBBR recipe in BBR v2.1 or later

Note: the EBBR recipe is based on the EBBR Specification 2.2.0 or later.

- Devicetree v0.4, or later, with additional clarifications defined in the forthcoming table
- The following rules from BBSR Specification v1.2 or later:
  - R140_BBSR: Capsule payloads for updating system firmware must be digitally signed.
  - R150_BBSR: Before updates to system firmware are applied, images must be verified using digital signatures.
  - When a TPM is present, the related requirements in BBSR are required.

SystemReady Devicetree band v3.0 recommends that the systems are compliant to the following specification:

- Section 8 (SMBIOS requirements) of the BBR 2.1 or later
- BBSR Specification v1.2 or later
- BSA v1.0c or later

SystemReady Devicetree band ACS v3.0.0, or later, must be used to test for compliance.

Also, SystemReady Devicetree band v3.0 requires that installation and boot test logs from three of the actively supported versions of Linux or BSD are used to check for compliance. The recommended distributions are Fedora, Debian, Ubuntu, RHEL, Rocky Linux, SLES, openSUSE, OpenWrt, and Yocto.

When selecting Linux distributions or BSDs, maximize coverage by installing an OS from different groups in the following list. Avoid repetition within groups unless all four groups are covered:

- RHEL, Fedora, or Rocky Linux
- SLES or openSUSE
- Ubuntu or Debian
- OpenWrt or Yocto

SystemReady Devicetree band v3.0 requires and recommends the following system capabilities:

System item	Capability	Requirements	Recommendation
Console in and out	Console for the user to interact with the system to install and boot OS	Local UART console	Local USB keyboard and video graphics
Devicetree conformance	Long term compatibility between platforms and	All of nodes meant to be used by the OS must have a JSON-Schema in the Linux kernel.	All warnings from JSON-Schema in the test report are fixed.

	OS. Backwards compatibility: new OSes do not break on older platforms	**Clarification**: Non-OS nodes, that is, nodes not meant to be used by the OS, may be checked but are not required. This includes but is not limited to: • specific U-boot nodes • Medium nodes to be used by the firmware but not by the OS. For example, a storage device not meant to be accessible by the OS	
Network boot	Network device support for operating systems boot	None	Network boot support using the UEFI HTTP/HTTPS boot protocol.
OS boot media	Support for media used for installing and booting the target OS	All block devices claimed by the vendor as a destination storage media must be tested as such, This includes but is not limited to: • Local USB • eMMC • SD • NVMe	All of the following if present: • Local USB • NVMe drive • SATA drive • SAS drive • eMMC
OS installation media	Support for media used for OS installation source	All block devices claimed by the vendor as a source storage media must be tested as such, This includes but is not limited to: • Local USB • eMMC • SD • NVMe	All of the following if present: • Local USB • NVMe drive • SATA drive • SAS drive • eMMC
OS Network support	Network device support for operating system usage	At least one configuration enabling the following devices to the OS: • Integrated network controllers	None
Peripheral devices OS support	Support for peripheral devices, ensuring they are available to the operating system even if	None	All available peripheral devices must be described in Devicetree and advertised to the operating system through one or more configurations

	they are not required for booting but are intended to be used by the OS		All available peripherals must be provided with necessary drivers so that the operating system can access and utilise these devices after booting.
AB support	UEFI based support for AB firmware update methods	None	It is recommended that Firmware update using CapsuleUpdate() is supporting AB, also protecting against rollback and anti-brick

Table 4: SystemReady Devicetree band hardware functionality requirements

4 SystemReady Virtual Environment compliance

The Arm SystemReady Virtual Environment (VE) demonstrates the virtual environments providing similar user experience as SystemReady on bare metal.

4.1 SystemReady VE v3.0 requirements

The requirements for the SystemReady VE are the same as specified for SystemReady band and SystemReady Devicetree band. A virtual environment can be SystemReady VE or SystemReady VE-Devicetree compliant, depending on the virtualized hardware and firmware environment.

Note: The physical system on which the virtual environment is running does not need to be SystemReady compliant. For example, it is entirely valid to have a virtual environment that is SystemReady VE compliant running on a physical system that is not SystemReady compliant.