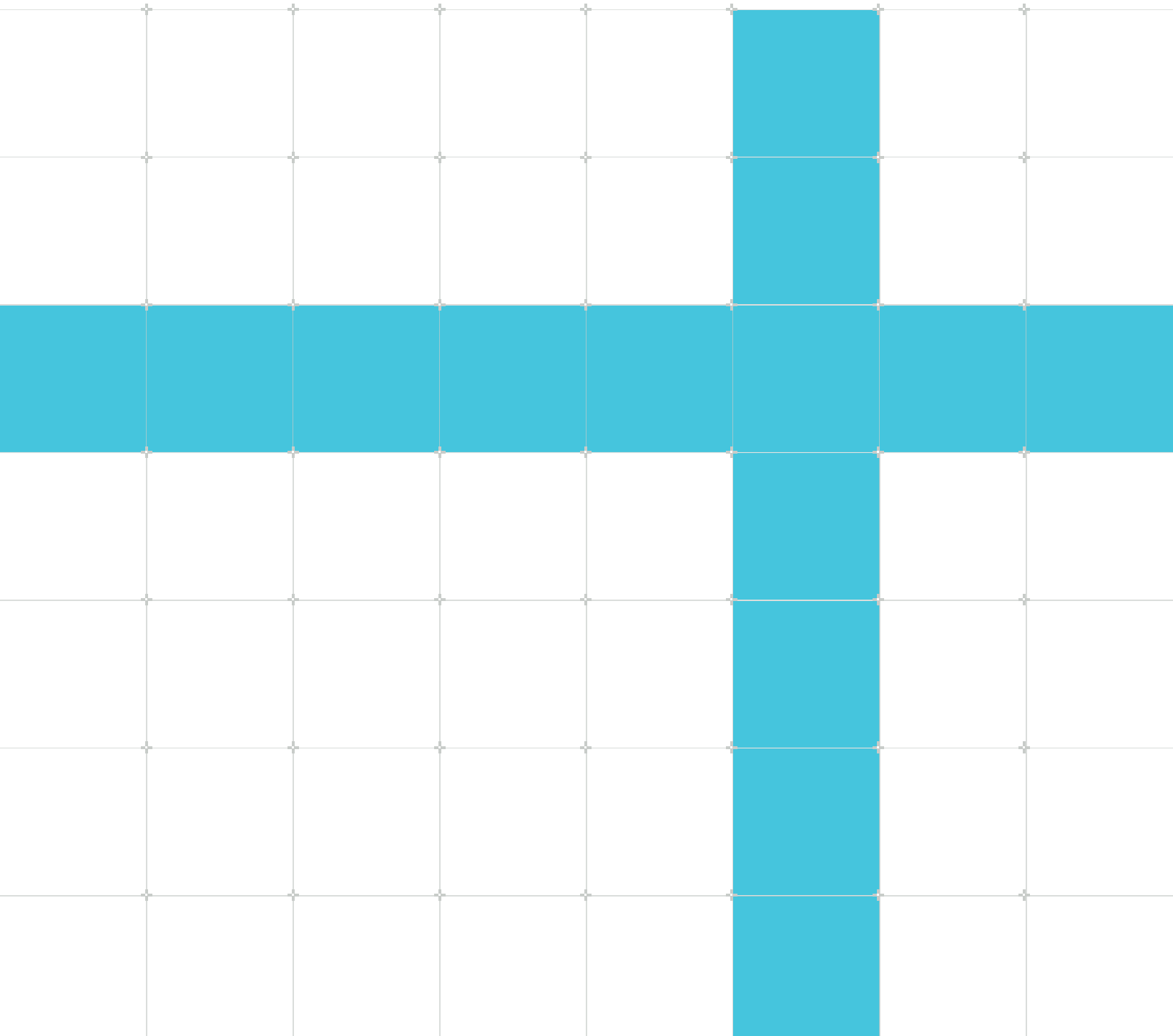
Arm SystemReady Devicetree Band Compliance Policy Guidelines

Version 1.0

Issue 01
110052_0100_01_en



Arm SystemReady Devicetree Band Compliance Policy Guidelines

Release information

Document history

Issue	Date	Confidentiality	Change
0100-01	21 November 2024	Non-Confidential	1.0 First release

Proprietary Notice

makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, any patents, copyrights, trade secrets, trademarks, or other rights.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Reference by Arm to any third party's products or services within this document is not an express or implied approval or endorsement of the use thereof.

This document consists solely of commercial items. You shall be responsible for ensuring that any permitted use, duplication, or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

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

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

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

PRE-1121-V1.0

Confidentiality Status

This document is Non-Confidential. The right to use, copy and disclose this document may be subject to license restrictions in accordance with the terms of the agreement entered into by Arm and the party that Arm delivered this document to.

Unrestricted Access is an Arm internal classification.

Product Status

The information in this document is Final, that is for a developed product.

Feedback

Arm welcomes feedback on this product and its documentation. To provide feedback on the product, create a ticket on https://support.developer.arm.com

To provide feedback on the document, fill the following survey: https://developer.arm.com/documentation-feedback-survey.

Inclusive language commitment

Arm values inclusive communities. Arm recognizes that we and our industry have used language that can be offensive. Arm strives to lead the industry and create change.

We believe that this document contains no offensive language. To report offensive language in this document, email terms@arm.com.

Contents

1. Arm SystemReady Devicetree Band Compliance Policy Guidelines

The purpose of the Arm SystemReady Devicetree Band Compliance Policy Guidelines is to outline the criteria and guidelines for declaring assisted compliance of third-party vendor products that possess the capability to function seamlessly with multiple OSs without requiring modification of the operating system of any kind.

This guide is intended for partners seeking to incorporate OS interoperability as a distinctive feature within their products.

From SRS 3.0 Arm Limited disclaims any responsibility for determining or assuring that any product passes the ACS or that representations of compliance by partners are true or accurate.

1.1 Arm SystemReady Devicetree band specification and tool versions

The SystemReady guided-compliance program recommends using the latest version of the Systems Requirement Specification (SRS) and the latest version of the Arm Compliance Suite (ACS). Note that the latest ACS version is backwards compatible with the specification.

From SRS 3.0 the SystemReady program exclusively supports 64-bit architectures. 32-bit architectures are completely excluded.

The ACS tool is governed as an open-source project. Partners are encouraged to contribute by submitting pull requests for coverage increases, bug fixes, and improvements. When submissions are accepted, a new ACS release is issued.

1.1.1 Pre-built OS distributions

Pre-built distributions used in testing should be generic and actively supported versions from the OS vendor of choice, as specified in the SRS. OS versions that are nearing end-of-life should be upgraded to more recent versions. In certain cases, and only when deemed appropriate, daily builds or live distributions may be accepted as proof of fixes that have not yet been propagated to the distribution's official releases.

1.1.2 Custom-built OS distributions

Custom-built distributions, such as Yocto and OpenWrt, are allowed for SystemReady Devicetree band. However, generic pre-built images should be used for compliance testing. To maintain compliance and ensure that custom-built distributions remain functional, alterations to the default baseline layers should occur in the mainline. Modifying default layers of downstream custom builds

is prohibited. Customization is allowed only in layers outside the generic baseline layer used for compliance, to ensure that interoperability is not compromised.

1.2 Guided-compliance process policy

While declarations of compliance are issued by vendors, these must be guided and supported by a qualified entity.

A qualified entity is one of the following:

- A qualified test lab.

  Vendors can engage independent and qualified test labs and service providers to perform compliance testing and declaration without requiring Arm's involvement. It is ultimately the vendor who claims compliance with guidance from the test lab.

- Arm.

  Arm may at its own discretion conduct compliance testing in its lab using hardware provided by the partner. This is expected to be a relatively rare case. Even when Arm is directly involved in the testing and inspection, the declaration of conformance is made by the vendor. This arrangement will be very limited.

- A qualified vendor.

  Arm may, at its discretion, permit qualified partners to perform compliance testing in their own labs.

1.2.1 Target SUT

Any product that considers the capability to boot various operating systems as an added value qualifies as a candidate for Arm SystemReady compliance.

SUTs are not restricted to:

- specific supply chain entities, such as SiPs, OEMs, ODMs, ISVs, OSVs, and so on
- particular phases of the end-product lifecycle, including reference designs, compute systems, or end-products

A viable SUT is any intentionally designed system meant to interoperate with multiple operating systems.

It is important to acknowledge the differences in the nature of products, the markets they address, and their lifecycle stages. For instance, while both compute systems and end-products can benefit from Arm SystemReady as a value-add, the methods for achieving Arm SystemReady compliance may not be equally suitable for all products. Arm SystemReady ACS is continually evolving to recognize these differences and processes, ensuring flexibility to accommodate various products and markets.

Hardware

Hardware to be claimed as compliant should be GA level hardware, available for consumers to access. Platforms still under development or any other non-ready-for-production level are not suitable for final compliance declaration.


Note

This is not limited to end-products. Evaluation boards or development kits meant to be used by developers meeting the GA level criteria are target SUTs.

Firmware

Firmware should be GA or similar level, with the only exception being the need to use unsigned versions to maintain the ability to flash revisions up or down as needed. Firmware should be available publicly or through other partner means such as registered customer portals. Private builds that are only available internally to the partner are not suitable for final compliance declaration.

It is unacceptable to use firmware for compliance that is specifically designed or configured to pass the tests, but not available for GA conditions.

System configuration

When conducting tests on an SUT able to accommodate and serve multiple configurations, partners are encouraged to run the test suite over as many configurations as possible, however just one is used for compliance purposes. The configuration of your choice must be a valid configuration, and it is recommended to be the one anticipated as the most common, or the most comprehensive one requiring the largest number of peripheral devices enabled.

For the minimum configuration, SRS 3.0 or later lists the minimum required hardware functionality for SystemReady Devicetree band guided-compliance.

1.3 Compliance of product updates

The following guidelines apply to compliance of product updates:

ACS updates and regression testing

The support team conducts regression testing on a set of approved hardware to consistently enhance the quality of test suite releases. This regression testing occurs at the compliance lab at Arm and has no impact on current compliant systems.

Arm recommends that partners integrate a regression testing element into their integration and development flows. This approach ensures that upcoming minor releases from partners remain in alignment with the SystemReady specifications.

As soon as tested OS versions become obsolete, newer and actively supported OS versions should be added to the regression tests.

Continuous compliance

Arm recommends that device releases are kept up-to-date with the latest version of the Systems Requirement Specification (SRS) using continuous integration and continuous deployment methods.

New compliance declarations or updates to existing declarations are only required for devices being introduced to the program for the first time, that is those not previously declared as compliant, or when significant changes are made to a previously compliant device. Major changes that necessitate a new declaration of compliance include any modifications that fundamentally alter the System-Under-Test profile. This may include, but is not limited to the following:

- CPU family updates, for example Cortex-A53 to Cortex-A72.
- Memory technology updates, for example DDR3 to DDR4.
- Changing an on-board device which is soldered to the main or daughter board, requiring a driver update, new functionality inclusion, or functionality updates. For example, changing out a PCIe or TPM device.
- Changes in the firmware related to major or substantial functional or structural changes
- A relatively large number of minor changes, as judged by the vendor, that could pose a risk for the SystemReady value delivery.

Minor changes do not require a new compliance declaration. The following are examples of system changes that do not require a declaration of compliance refresh:

- CPU speed changes, for example Cortex-A72 1.6GHz to Cortex-A72 2.4GHz.
- Memory size changes, for example 4 GiB to 16 GiB, unless the change increases the number of memory slots physically on the board. Whenever a question of re-compliance comes up, the compliance team will investigate the situation and make a decision on a case-by-case basis.
- Firmware bug fixes or minor changes do not require compliance, although Arm recommends that these are included within the vendor's regression tests.

1.4 SystemReady compliance list

For a certified system using SRS 2.1 and below, Arm expects that a SystemReady certification remains listed in the catalog until the end of the support life for that product. However, Arm reserves the right to remove an entry when deemed appropriate.

Compliant systems using SRS 3.0 and above are not listed in the SystemReady catalog.

1.5 SystemReady Devicetree band branding and co-marketing policy

Partners seeking to use the SystemReady Devicetree band logo must submit their results using the Devicetree template format for Arm to capture and store but not publish.

Partners interested in co-marketing with Arm must submit their results using the Devicetree template format for Arm's review, as well as comply with the policy guidelines. On validation, partners will be approved to engage in co-marketing with Arm.

SystemReady Devicetree band compliance is declared for a specific device or system, with a specific version of its system firmware. Please note that "compliant partner", "compliant SoC", and "compliant SOM" are not valid terms.

The Arm SystemReady usage rules are as follows:

- Arm SystemReady must be referred to as "Arm SystemReady" the first time it is referenced. After this, "SystemReady" or "Arm SystemReady" can be used interchangeably.
- The correct format is Arm SystemReady + base. For example, SystemReady Devicetree band or Arm SystemReady Devicetree band.
- Capital letters must be used for "S" and "R" in SystemReady.
- Capital letters must be used for "D" in Devicetree. "DeviceTree" is an incorrect use.
- SystemReady is one word with no spaces.
- Abbreviations, simplifications, and acronyms are not allowed. For example, "SystemReady DT", "SR Devicetree", and "SR DT" are incorrect uses.
- You may not insert additional words or characters within "SystemReady Devicetree band vx.x". For example, "SystemReady-Devicetree band" and "SystemReady IoTReady v3.0" are incorrect uses.

For more information about Arm SystemReady Devicetree band, please refer to the latest Arm Systems Requirement Specification (SRS). Any explanation of SystemReady Devicetree band in older versions of the SRS specification should not be used for declaring compliance.

1.6 Policy compliance

Partners must meet the guidelines outlined in this policy guide to be eligible for Arm SystemReady compliance declaration. Failure to adhere to these guidelines may result in rejection of joint marketing activities with Arm, or logo-usage revocation.

1.7 Policy effective date

This policy is effective as of the date of publication and applies to all compliance applications submitted thereafter.

1.8 Changes and compliance policy review

This policy will be periodically reviewed and updated to ensure its relevance and alignment with industry standards. Partners will be notified of any changes that may impact their compliance process.