



SystemReady Certification Guide

Version 1.0

Non-Confidential

Copyright © 2023–2024 Arm Limited (or its affiliates).
All rights reserved.

Issue 01

109506_0100_01_en



SystemReady Certification Guide

Copyright © 2023–2024 Arm Limited (or its affiliates). All rights reserved.

Release information

Document history

Issue	Date	Confidentiality	Change
0100-01	10 April 2024	Non-Confidential	Minor updates
0100	27 November 2023	Non-Confidential	First release version 1.0

Proprietary Notice

This document is protected by copyright and other related rights and the use or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm Limited ("Arm"). No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether the subject matter of this document infringes any third party patents.

The content of this document is informational only. Any solutions presented herein are subject to changing conditions, information, scope, and data. This document was produced using reasonable efforts based on information available as of the date of issue of this document. The scope of information in this document may exceed that which Arm is required to provide, and such additional information is merely intended to further assist the recipient and does not represent Arm's view of the scope of its obligations. You acknowledge and agree that you possess the necessary expertise in system security and functional safety and that you shall be solely responsible for compliance with all legal, regulatory, safety and security related requirements concerning your products, notwithstanding any information or support that may be provided by Arm herein. conjunction with any Arm technology described in this document, and to minimize risks, adequate design and operating safeguards should be provided for by you.

This document may include technical inaccuracies or typographical errors. THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm

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.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its affiliates) in the US and/or elsewhere. Please follow Arm's trademark usage guidelines at <https://www.arm.com/company/policies/trademarks>. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners.

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. SystemReady Overview.....6
- 2. What is SystemReady certification?.....7
 - 2.1 How the SystemReady certification process works.....8
- 3. Certification bands..... 9
- 4. Optional components..... 12
- 5. Information required for certification..... 14
- 6. Related information..... 16
- 7. Next steps..... 17

1. SystemReady Overview

This guide describes the Arm SystemReady certification process. By the end of this guide, you will understand the steps required to certify your system within the Arm SystemReady program in one of the defined certification bands. The SystemReady program replaces the successful ServerReady compliance program and extends it to a broader set of certification bands. Certification bands describe particular types of devices, usually associated with a specific market segment. See Chapter 3 for details.



The SystemReady program also includes pre-silicon compliance testing aimed at reducing future risk by verifying pre-tapeout designs. Pre-silicon certification is not included in this guide, but you can find relevant documents [here](#).

The Arm SystemReady Program is a set of standards and a compliance certification program that enables interoperability with generic, off-the-shelf operating systems and hypervisors. The Arm SystemReady certification program encompasses a broad set of devices from enterprise, through cloud devices, to IoT edge. Systems that comply with the Arm SystemReady terms and conditions are issued with a certificate and can use the Arm SystemReady certified stamp logo.

The Arm SystemReady specifications include a generic [Arm Base System Architecture \(BSA\) specification](#), which contains the minimum requirements to deploy an operating system. SystemReady also contains band-specific supplementary specifications, such as the Arm Server BSA (SBSA) for the server market.

The [Arm Base Boot Requirements \(BBR\)](#) specification provides boot recipes that accommodate the different standards. The specification also provides the boot firmware implementations that are used by a broader range of operating systems and hypervisors. Similar to the BSA, the BBR specification is extended with band-specific requirements for some SystemReady bands.

The [Arm Architecture Compliance Suite \(ACS\)](#) is a test framework that is used to systematically validate platform compliance with large parts of the SystemReady specification.

Full requirements for the SystemReady certification for a given platform is best examined in the given certification band. For example, a server platform needs to satisfy the Server band requirements, but it does not need to comply with any requirements from the other bands.

This guide provides reference information. Consult the latest [SystemReady Requirements Specification](#) for specific details.

For more information about the Arm SystemReady certification program, see [Arm SystemReady Certification Program](#).

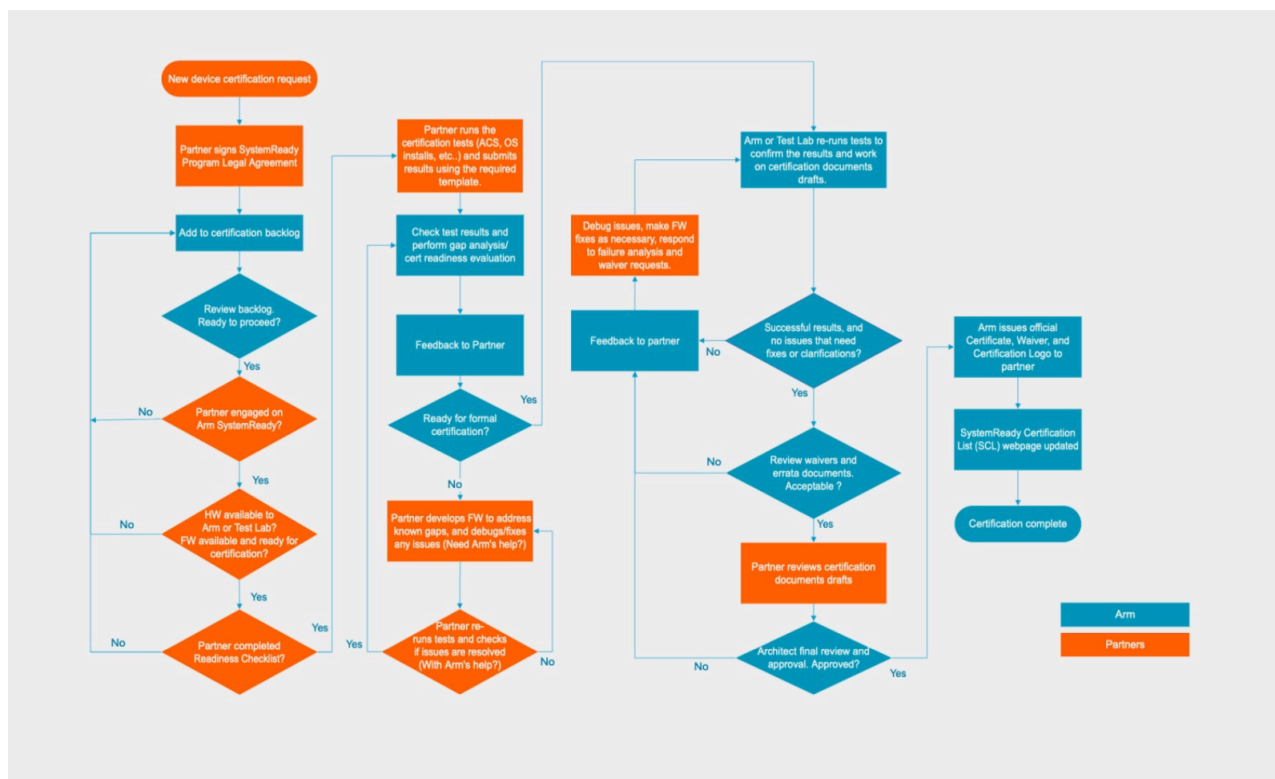
2. What is SystemReady certification?

The SystemReady certification program ensures the highest possible standards for systems supporting off-the-shelf operating systems and hypervisors. To help you navigate the process, Arm provides the following support.

- This guide, which explains how to get SystemReady certification in a requested band.
- The [Arm SystemReady Portal](#) with links to certification bands, guides, videos and more information.
- The Arm SystemReady Compliance team helps evaluate your system for certification, and provides feedback and guidance.
- Arm provides checklists, forms, and report templates to ensure the necessary information is submitted with your certification request.
- The Arm SystemArchAC mailing list. Contact the [Arm SystemReady Certification Program](#) for further information.

Figure 2-1 shows the process flow chart for Arm SystemReady Requirements Specification v2.1. For the latest process information, see the latest Arm SystemReady Requirements Specification.

Figure 2-1: SystemReady v2.1 Certification Process



2.1 How the SystemReady certification process works

The following steps describe the SystemReady certification process.

1. Partner submits a certification request and sign SystemReady Program Legal agreement through [this form](#).
2. Partner submits a [SystemReady firmware readiness checklist](#) to the SystemReady compliance team. When you provide the system hardware and firmware, the compliance team performs a certification readiness evaluation.
3. Arm provides feedback, including an estimate of the effort to achieve certification, and asks you to fix any readiness issues. This step is repeated until all issues have been addressed in the firmware and the formal certification process begins.
4. Partner (certification requester) runs pre-certification testing (ACS and OS tests) and submits test results to Arm for review, when the compliance team indicates the system is ready for formal certification.
5. Arm reviews the submission and provides feedback on any issues that prevent certification. You then debug issues, make firmware fixes as necessary, respond to the failure analysis, and prepare any additional waiver requests.
6. Partner (certification requester) runs the pre-certification testing again and submit the forms, logs, waiver requests, and errata to the compliance team for review. This step is repeated until all issues have been addressed.
7. Partner (certification requester) sets up or ships the system under test for Arm. Arm then re-runs the certification testing and confirms the test result.
8. Partner submits the certification test results and document drafts to the Arm Architects for final review and approval. Currently, Arm sends drafts of the certification documents to you for review.
9. Arm issues the official certificate, waivers, and certification logo when the Arm architects approve the certification.
10. Arm adds the system to the SystemReady Certification List (SCL) on the Arm website.

3. Certification bands

The SystemReady certification is requested in one certification band that is appropriate for the platform being certified. The available bands are: SR, ES, IR, and LS.

All bands target different standard operating systems and hypervisors based on different software stacks. They provide a solution so software “just works”, allowing partners to deploy Arm hardware with confidence. The same platform or device can be certified with different bands. Such certified Arm-based hardware works out-of-the-box, offering seamless interoperability with standard operating systems, hypervisors, and software. Commonly, standard firmware interfaces are used, reducing the cost of supporting multiple software versions.

Band versions

The SystemReady bands are versioned semantically with a major and minor version number.

- A major version of a SystemReady band signifies a substantial evolution of certification requirements. It will include significant changes, enhancements, or expansions to the criteria that govern the certification processes.
- Minor versions within the SystemReady bands occur more frequently and denote smaller, yet valuable, steps forward in development. They typically involve incremental changes, refinements, or additions to existing certification requirements.

While Arm strongly prefers certification in the latest version, it might be permissible to certify in a second-to-latest version of a given SystemReady band. For example, see Appendix C of the [SystemReady Requirements Specification](#).

The current versions of SystemReady bands are described in the [SystemReady Requirements Specification](#) or at the [SystemReady Portal](#).

SR certification band

The SR certification band encompasses much of the older ServerReady specification. It provides a solution for servers, workstations, and similar platforms or devices targetting generic off-the-shelf operating systems.

The [SystemReady SR](#) is designed for the Windows, Linux, VMware, and BSD environments on systems typically based on server or workstation Arm SoCs. It also aims to support old operating systems to run on new hardware and vice versa.

SystemReady SR-compliant systems must conform to the:

- Base System Architecture (BSA) specification
- Server Base System Architecture (SBSA) supplement specification
- SBBR recipe of the Base Boot Requirements (BBR) specification

The minimal hardware requirements are:

- One input and one output console

- Two OS media source devices
- Two OS installation destination devices
- One network device in OS

ES certification band

The ES certification band provides a solution for embedded devices, SmartNICs and similar platforms targetting generic off-the-shelf operating systems. The aim is so that software “just works”, ensuring that Arm-based embedded devices work out-of-the-box, offering seamless interoperability with standard operating systems, hypervisors, and software.

The [SystemReady ES](#) meets the needs of the Windows, Linux, VMware, and BSD ecosystems for systems based on Arm SoCs. It also aims to be both backward and forward compatible, supporting old operating systems on new hardware and vice versa.

SystemReady ES-certified platforms implement a minimum set of hardware and firmware features that an operating system can depend on to deploy the operating system image within a platform.

Compliant systems must conform to the:

- Base System Architecture (BSA) specification
- SBRR recipe of the Base Boot Requirements (BBR) specification

The minimal hardware requirements are:

- One input and one output console
- One OS media source device
- One OS installation destination device

IR certification band

The IR certification band meets the needs of embedded Linux/BSD ecosystem on systems based on embedded Arm SoCs. It assumes a SoC supported by mainline Linux/BSD. It targets both custom images and pre-built images on IoT platforms. Some examples are Yocto, OpenWRT, buildroot for custom and Debian, Fedora, SUSE for pre-built images. Forward compatibility, that is running old OS on new hardware, is not usually expected of these platforms.

The [SystemReady IR](#) certified platforms implement a minimum set of hardware and firmware features that an operating system can depend on to deploy the operating system image.

The IR band version 1.x supports 32-bit devices, while the 2.x version of the band supports 64-bit devices.

Compliant systems must conform to the:

- [Base Boot Requirements v1.0](#) (BBR) specification
 - The [EBBR Recipe v2.0.1](#)
- [Devicetree v0.3](#) specification

The 2.1 version of the band also requires:

- [Base Boot Requirements v2.0](#) (BBR) specification
- Ethernet ports present in the platform must be functional in Linux
- One of the following two options:
 - [Security Interface Extension](#) compliance, see Chapter 4
 - Compliance with the following [BBSR](#) rules:
 - 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

LS certification band

The LS certification band provides a framework for LinuxBoot, an alternative firmware stack using the Linux kernel as the normal world firmware component. SystemReady LS enables Arm-based servers that offer highly customizable firmware, while still providing a “just works” software experience.

The [SystemReady LS](#) meets the needs of many hyperscalers on systems based on Server Arm SoCs. It targets the hyperscaler’s Linux environment.

SystemReady LS-compliant systems must conform to the:

- Base System Architecture (BSA) specification
- Server Base System Architecture (SBSA) supplement specification
- LBBR recipe of the Base Boot Requirements (BBR) specification

4. Optional components

The SystemReady certification process describes recommended, but not mandatory, specifications.

Security Interface Extension

The [Security Interface Extension \(SIE\)](#) is a recommended, optional extension to the SystemReady certification in the SR, ES and IR bands. It certifies that a device complies with industry-standard security interfaces.

The [Base Boot Security Requirements \(BBSR\)](#) specification describes these security requirements and covers the following areas:

- UEFI authenticated variables
- UEFI secure boot
- UEFI capsule updates
- TPM 2.0 and measured boot

An SIE certification provides assurance that the security interfaces covered by BBSR are implemented according to standards. However, interface compliance does not provide assurance that the underlying platform is secure. When architecting a system, system-level threat modeling should be performed to evaluate threats, risks, and mitigations. For example, in the embedded IoT market, the [Platform Security Architecture \(PSA\)](#) and the [PSA Certified](#) framework provides a comprehensive approach to platform security that is based on a defined set of security goals. PSA provides architecture and requirements specifications for building secure platforms. An SIE certification complements PSA. PSA Certified shows the robustness of an implementation, through an assessment process that is performed by a security certification laboratory.

Virtual Environments

The Virtual Environment (VE) extension to SystemReady provides a solution for virtual environments, such as cloud instances or virtual platforms. Virtual environments certified with SystemReady VE demonstrate the same software user experience as other SystemReady bands. This way they allow partners to deploy OSes on these environments with confidence that they will “just work”. SystemReady VE ensures that Arm-based virtual environments work with seamless interoperability with standard operating systems and software.

SystemReady VE is designed for Windows, Linux, and BSD operating systems on Arm-based virtualization environments. SystemReady VE ensures standard firmware interfaces and virtual hardware to deploy and maintain the OSs in virtual machines, reducing the cost of supporting multiple software versions. It also aims to support old operating systems to run on new virtual environments and vice versa. Like the SR & ER certification bands, the VE extension targets generic off-the-shelf OSs.

SystemReady VE-compliant systems must conform to the same requirements as the corresponding SystemReady bands (SR, ES, IR, LS), depending on the virtualized hardware and firmware environment. A virtual environment can also be certified without any corresponding SystemReady band in cases where the UEFI preboot environment is not sufficient to run ACS tests. Also, the real

hardware which provides the virtual environment does not require SystemReady certification for the virtual environment to be certified using the VE extension. See [SystemReady Requirements Specification](#) for more details.

5. Information required for certification

When you submit a request for SystemReady Certification, you must provide forms, reports, and logs to ensure that the request can be evaluated. This section describes the information required for a certification request.

Arm provides a readiness checklist, forms, and report templates to ensure that all required inputs are provided throughout the certification process. Different information needs to be submitted at three points during the process: before the initial evaluation, formal request, and after certification has been granted.

1. Submit the firmware readiness checklist

You should submit the SystemReady firmware [readiness checklist](#) by email before the initial certification evaluation. This checklist ensures that you supply the following information:

- Company, system, and SoC information
- The SystemReady band for which you are requesting certification
- Hardware and firmware availability
- UEFI (U-Boot or EDK) information
- Arm Base System Architecture (BSA) compliance state
- OS boot, ACS compliance and security compliance sniff test information

2. Submit the readiness evaluation report

Submit the SystemReady readiness evaluation report when you request formal certification. You must complete the following information in the report:

- General, company, and system information
- An area for pictures of the system, setup, and any relevant screenshots such as the firmware boot and menus
- An overall SystemReady evaluation summary

3. Submit the pre-certification test results using the template

You can get the report templates for all certification bands from the [SystemReady GitLab repository](#). For details about the required testing results, please check the README.md file in the template repository. The report and the test results should be submitted by email or linked in an email if size is an issue.

Requesting waivers

Sometimes, waivers to the SystemReady standards are granted by the Arm architects and the Arm SystemReady compliance team. You must request and justify waivers when you submit the certification request.

Arm can consult with Independent Software Vendors (ISVs) if necessary. Arm provides feedback if it cannot grant a waiver. To help develop fixes or workarounds, consult the silicon partner (SiP)

or independent BIOS vendor (IBV). The certification request can then be resubmitted for further evaluation.

6. Related information

The following resources are related to material in this guide.

Specifications:

- [Base System Architecture \(BSA\) specification](#)
- [Arm Base Boot Requirements \(BBR\) specification](#)
- [Arm SystemReady Requirements Specification](#)

Repositories:

- [Arm SystemReady ACS Repository](#)
- [BSA ACS Repository](#)
- [SystemReady Gitlab Repository](#)

User Guides:

- [SystemReady SR and ES Test and Integration Guide](#)
- [SystemReady IR IoT Integration, Test, and Certification Guide](#)
- [SystemReady Pre-Silicon Reference Guide BSA integration and compliance](#)
- [SystemReady FAQ](#)

SystemReady Pages:

- [Arm SystemReady Certification Program](#)
- [Arm Community - SystemReady Forum](#)

7. Next steps

In this guide, you learned how to prepare for SystemReady certification and perform the tasks needed for the compliance program.

You are now ready to follow the process to certify your system as compliant with the Arm SystemReady specification. Continue by selecting an appropriate certification band for your hardware and following the band-specific guide.

For more information about certification registration, go to [Arm SystemReady Certification Program](#).

For support, send an email to [support](#) or raise a query on the [forum](#).