Arm SystemReady Certification
System Requirements Specification v2.2

Document number: DEN0109G

Arm SystemReady Certification System Requirements Specification

Release information

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

Table 1-1 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

CONTENTS

Arm Non-Confidential Document Licence ("Licence")

This Licence is a legal agreement between you and Arm Limited ("**Arm**") for the use of Arm's intellectual property (including, without limitation, any copyright) embodied in the document accompanying this Licence ("**Document**"). Arm licenses its intellectual property in the Document to you on condition that you agree to the terms of this Licence. By using or copying the Document you indicate that you agree to be bound by the terms of this Licence.

"**Subsidiary**" means any company the majority of whose voting shares is now or hereafter owner or controlled, directly or indirectly, by you. A company shall be a Subsidiary only for the period during which such control exists.

This Document is **NON-CONFIDENTIAL** and any use by you and your Subsidiaries ("Licensee") is subject to the terms of this Licence between you and Arm.

Subject to the terms and conditions of this Licence, Arm hereby grants to Licensee under the intellectual property in the Document owned or controlled by Arm, a non-exclusive, non-transferable, non-sub-licensable, royalty-free, worldwide licence to:

(i) use and copy the Document for the purpose of designing and having designed products that comply with the Document;

(ii) manufacture and have manufactured products which have been created under the licence granted in (i) above; and

(iii) sell, supply and distribute products which have been created under the licence granted in (i) above.

Licensee hereby agrees that the licences granted above shall not extend to any portion or function of a product that is not itself compliant with part of the Document.

Except as expressly licensed above, Licensee acquires no right, title or interest in any Arm technology or any intellectual property embodied therein.

THE 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. Arm may make changes to the Document at any time and without notice. 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, third party patents, copyrights, trade secrets, or other rights.

NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS LICENCE, 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 LICENCE (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 LICENCE). 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 Licence 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 Licence then Arm may terminate this Licence immediately upon giving written notice to Licensee. Licensee may terminate this Licence at any time. Upon termination of this Licence 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 Licence, all terms shall survive except for the licence grants.

Any breach of this Licence by a Subsidiary shall entitle Arm to terminate this Licence as if you were the party in breach. Any termination of this Licence 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 Licence may be translated into other languages for convenience, and Licensee agrees that if there is any conflict between the English version of this Licence and any translation, the terms of the English version of this Licence shall prevail.

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

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

Arm document reference: LES-PRE-21585 version 4.0

1 Introduction

Systems that are designed to “just work” for the end user (with the ability to install and run generic off-the-shelf operating systems out-of-the-box) need to follow a set of minimum hardware and firmware requirements to ensure forward and backward compatibility. This means that old operating systems can install and run on new hardware and vice versa without modifications. For these systems, the Base System Architecture (BSA) specification and the SBBR recipe (UEFI, ACPI and SMBIOS) defined in the Base Boot Requirements (BBR) specification are required. In addition, there may be additional market-specific requirements necessary foroperating 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.

Systems that are built to only support embedded Linux and BSD environments can still benefit from using the reduced set of common UEFI interfaces to support standard boot loader and standard secure boot and firmware update features. These interfaces are defined in the EBBR recipe described in the Base Boot Requirements (BBR) specification. BSA compliance is recommended but not required for these systems. These systems typically do not expect forward compatibility. That is, there is no expectation that old operating systems can install and run on new hardware without modifications. Therefore, Devicetree (descriptive) rather than ACPI (abstractive) can be used, along with the upstream of the SoC support in the mainline Linux and BSD.

Systems that are built to only support Linux in the cloud environment can use LinuxBoot in firmware along with ACPI and SMBIOS. This is the LBBR recipe described in the Base Boot Requirements (BBR) specification. BSA and SBSA compliances are required for these systems.

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

2 Arm SystemReady program

For the Arm SystemReady program, each market segment may target a different set of operating systems and hypervisors with different hardware and firmware requirements. We use the term band to identify these differences.

Table 1 summarizes the specifications that the devices need to comply with.

Certification	Specifications		
SystemReady SR	BSA	SBSA	SBBR Recipe in BBR
SystemReady LS	BSA	SBSA	LBBR Recipe in BBR
SystemReady ES	BSA	-	SBBR Recipe in BBR
SystemReady IR	-	-	EBBR Recipe in BBR and Devicetree

Table 1: Arm SystemReady bands

SystemReady SR and ES bands are for systems that are designed to “just work” for the end user, providing the ability to install and run generic off-the-shelf operating systems out-of-the-box with forward and backward compatibility. They both require BSA and SBBR compliance for the minimum hardware and firmware requirements. In addition, SystemReady SR requires SBSA compliance to support software standardization of server hardware features.

SystemReady IR band is for systems that are built to only support embedded Linux and BSD environments. It requires EBBR compliance and Devicetree support. BSA compliance is recommended for 64-bit devices but not required. BSA does not address 32-bit devices.

SystemReady LS has the same hardware requirements as SystemReady SR, but supports the alternative firmware stack LinuxBoot, that uses Linux kernel as the Normal world firmware component.

We define these bands in consultation with our partners, and we expect that all operating system distributions will find a band that adequately captures their basic requirements for a standards-based Arm platform.

SystemReady SR, ES, and IR bands are supported by a common Architectural Compliance Suite (ACS) that is modular, to support testing against different combinations of specifications required by a SystemReady band.

Systems that are certified as SystemReady SR meet the requirements for SystemReady ES. There is no need for these systems to be certified as SystemReady ES. Systems that are certified as SystemReady ES can also support many operating systems that SystemReady IR supports. There is no need for these systems to be certified as SystemReady IR unless they need to support an operating system that can only support Devicetree.

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

A 32-bit system can be certified as SystemReady IR v1.2 if it supports Devicetree and the EBBR specification. We list the 32-bit systems separately from the 64-bit systems on the Arm SystemReady System Compatibility List (SCL).

2.1 SystemReady band major and minor versions

A major version of a SystemReady band signifies a substantial advancement in the evolution of certification requirements for that iteration. It is characterized by the introduction of significant changes, enhancements, or expansions to the criteria that govern certification processes. An example is the capability to test new technologies required by SystemReady.

Minor versions within the SystemReady bands occur more frequently and are encompassed 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 certification requirements.

2.2 SystemReady SR certification

2.2.1 SystemReady SR v2.5 requirements, Oct 2023 update

SystemReady SR v2.5 requires the certified devices to be compliant to the following specifications:

- BSA v1.0c and Level 3-7 as defined in SBSA Supplement v7.1.
- SBBR recipe in BBR v1.0.

SystemReady SR v2.5 recommends the certified devices to obtain the Security Interface Extension certification as secure boot and secure firmware update features are critical to the server deployment and maintenance.

To certify a device for SystemReady SR v2.5, results from running the SystemReady SR ACS v2.0.0 must be submitted.

In addition, OS installation and boot logs are required:

- WinPE boot log, from a GPT partitioned disk, is required.
- Installation and boot logs from RHEL and SLES are required.
- VMware ESXi-Arm installation and boot logs are recommended.
- Installation and boot logs from other Linux distros or BSDs are recommended. For example, Fedora, CentOS, AlmaLinux, Rocky Linux, Oracle Linux, Anolis OS, openSUSE, Ubuntu, Debian, CBL-Mariner, NetBSD, OpenBSD, or FreeBSD.

All logs must be submitted using the ES/SR template.

SystemReady SR v2.5 requires the following hardware functionality:

Hardware / Peripheral	Functionality	Minimum Required	Recommended / Aspirational
Console in/out	Console for the user to interact with the system to install and boot the OS	At least one input and one output console should be functional: • Local USB keyboard and video graphics, or • BMC/remote keyboard and video graphics, or • UART console (local), or • Remote UART (such as IPMI SOL)	All of the following should be functional: • Local USB keyboard and video graphics, and • UART console (local) Servers that support BMC (SBMR compliance) should also have either: • BMC/remote keyboard and video graphics, or • Remote UART (such as IPMI SOL)
OS installation media	Media used for OS installation source	At least two separate media sources from the following groups: • USB (local), or USB (BMC remote/virtual media) • NVMe drive, or SATA drive, or SAS drive • Network (PXE, HTTP(s) , iSCSI, or FCoE)	All of the following should be functional: • USB (local) • NVMe drive (if present) • SATA drive (if present) • SAS drive (if present) • Network (PXE, HTTP(s) or iSCSI) Servers that support BMC (SBMR compliance) should also have: • USB (BMC remote/virtual media)
OS boot media	Media used for installing and booting the target OS	At least two separate media destinations: • USB (local), or • NVMe drive, or • SATA drive, or • SAS drive, or • Network (iSCSI or FCoE)	All of the following should be functional: • USB (local) • NVMe drive (if present) • SATA drive (if present) • SAS drive (if present)
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, or • HTTP or HTTPs Boot, or • iSCSI Boot
OS Network support	Network device for OS usage	At least one network device should be functional: • Integrated Network controller, or • PCIe network card, or • USB network device	OS support for network access to at least one network device, other than USB network devices.

Table 2: SystemReady SR hardware functionality requirements

2.2.2 Future SystemReady SR requirements

In the future, requirements based on newer versions of the BSA, SBSA, and BBR specifications may be added. In addition, installation and boot logs from VMware ESXi-Arm might be required. Security Interface Extension might be required as an integral part of SystemReady SR because secure boot, secure firmware update, and TPM support are critical to server deployment and maintenance.

2.3 SystemReady ES certification

2.3.1 SystemReady ES v1.5 requirements, Oct 2023 update

SystemReady ES v1.5 requires the certified devices to be compliant to the following specifications:

- BSA v1.0c.
- SBBR recipe in BBR v1.0.

SystemReady ES v1.5 recommends the certified devices to obtain the Security Interface Extension certification as secure boot and secure firmware update features are critical to edge and IoT deployment and maintenance.

Waiver Levels 0-2 as defined in Appendix A are available.

To certify a device for SystemReady ES v1.5, results from running the SystemReady ES ACS v1.3.0 must be submitted. In addition, OS installation and boot logs are required:

- Either the WinPE boot log, from a GPT partitioned disk, or VMware ESXi-Arm installation and boot logs, are required. Having both is recommended.
- Installation and boot logs from two of the Linux distros or BSDs are required.

All logs must be submitted using the ES/SR template.

When choosing the Linux distros or BSDs, maximize coverage by using a diverse range of distro heritages. For example, the following shows the recommended distros grouped by heritage:

- RHEL, Fedora, CentOS, Alma Linux, Rocky Linux, Oracle Linux, or Anolis OS
- SLES, or openSUSE
- Ubuntu, or Debian
- CBL-Mariner
- NetBSD, OpenBSD, or FreeBSD

Note: some classes of devices, such as DPUs and IPUs, may require special methods for deploying operating systems. This may include reformatting off-the-shelf OS distros in a device-specific format, or using non-standard deployment frameworks. These exceptions are allowed on such devices, as reviewed on a case by case basis.

For those certified platforms shipped with a different firmware image than the one used for the certification, vendors must make the certified firmware image (binary) available to users, either through their own means or through Arm SystemReady Certification List (SCL) portal. In addition, vendors must provide instructions on how to flash the firmware image binary into the certified board. This will allow users to retrieve the exact version the platform was certified for and deliver the 'it works' promise.

SystemReady ES v1.5 requires the following hardware functionality:

Hardware / Peripheral	Functionality	Minimum Required
Console in/out	Console for the user to interact with the system to install and boot the OS	At least one input and one output console should be functional • Local USB keyboard and video graphics, or • BMC/remote keyboard and video graphics, or • UART console (local), or • Remote UART (such as IPMI SOL)

OS installation media	Media used for OS installation source	At least one media source: • USB (local), or • USB (BMC remote/virtual media), • NVMe drive, or • SATA drive, or • SAS drive, or • Network (PXE, HTTP(s) , iSCSI, or FCoE)
OS boot media	Media used for installing and booting the target OS	At least one media destination: • USB (local), or • NVMe drive, or • SATA drive, or • SAS drive, or • Network (iSCSI or FCoE)
Network boot	Network device for OS boot	None
OS Network support	Network device for OS usage	One functioning network interface is recommended to be able to complete VMware ESXi-Arm installation

Table 3: SystemReady ES hardware functionality requirements

2.3.2 Future SystemReady ES requirements

In the future, requirements based on newer versions of the BSA and BBR specifications may be added. In addition, Security Interface Extension might be required as an integral part of SystemReady ES because secure boot and secure firmware update are critical to edge and IoT deployment and maintenance. Installation and boot logs from RHEL and SLES may be required.

2.4 SystemReady IR certification

In accordance to Appendix C.4.2 and the firmware general availability policy, for those certified platforms shipped with a different firmware image than the one used for the certification, vendors must make the certified firmware image (binary) available to users, either through their own means or through the Arm SystemReady Certification List (SCL) portal. In addition, vendors must provide instructions on how to flash the firmware image binary into the certified board. This will allow users to retrieve the exact version the platform was certified for and deliver the SystemReady IR promise. This is applicable for all active SystemReady IR certifications .

2.4.1 SystemReady IR v1.2 requirements, Oct 2023 update

SystemReady IR v1.2 has been updated to only support certifications for 32-bit devices. SystemReady IR v1.2 requires the certified devices to be compliant to the following specifications:

- There are no BSA requirements for 32-bit devices.
- EBBR recipe in BBR v1.0 (**Note:** the EBBR recipe is based on the EBBR Specification 2.0.1.).
- Devicetree v0.3.

Waiver levels 0-2 as defined in Appendix A are available.

To certify a 32-bit device for SystemReady IR v1.2, results from running the SystemReady IR ACS for 32-bit Arm Platforms must be submitted. In addition, installation and boot logs from one Linux or BSD distro are required. Refer to Appendix C.3 for more information.

All logs must be submitted using the IR template.

2.4.2 SystemReady IR v2.1 requirements, Oct 2023 update

SystemReady IR v2.1 requires the certified devices to be compliant to the following specifications:

- BSA v1.0c recommended for 64-bit devices (only test reporting, no enforcement).
- EBBR recipe in BBR v2.0 (**Note:** the EBBR recipe is based on the EBBR Specification 2.1.0.)
- SystemReady IR v2.1 recommends that certified devices obtain the Security Interface Extension certification because secure boot and secure firmware update features are critical to edge and IoT deployment and maintenance. But if that is not possible, the following BBSR rules are still required:
    - 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
- Devicetree v0.3 with additional clarifications defined in 2.4.2.1
- Ethernet port requirements as stated in 2.4.2.2

Waiver levels 0-2 as defined in Appendix A are available.

To certify a 64-bit device for SystemReady IR v2.1, results from running the SystemReady IR ACS v2.1.0 must be submitted. In addition, installation, boot, and storage medium test logs from three of the actively supported versions of Linux or BSD are required. The recommended distros are Fedora, Debian, Ubuntu, RHEL, Rocky Linux, SLES, openSUSE, and OpenWRT.

When choosing the Linux distros or BSDs, maximize coverage by using diverse range of distro heritages. For example, the following shows the recommended distros groups by heritage:

- RHEL, Fedora, or Rocky Linux
- SLES or openSUSE
- Ubuntu or Debian
- OpenWRT

Refer to Appendix C.2 for more information.

Note: Both SystemReady IR v2.0 and v2.1 are available for 64-bit device certification only. Refer to Appendix C.3 for more information..

All logs must be submitted using the IR template.

2.4.2.1 Devicetree clarifications

Ideally, 100% of nodes meant to be used by the OS must have a json-schema in the Linux kernel. However, it is acceptable for the majority of nodes to have a json-schema, and the remaining nodes pending acceptance and acknowledged by devicetree maintainers. Warnings from schemas are allowed in the test report.

Note: Non-OS nodes, that is, nodes not meant to be used by the OS, may be checked but are not required by the certification. 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

2.4.2.2 Ethernet port requirements

Ethernet ports present in the system directly as RJ45 connectors and stated by the vendor as expected to be used as such by users must be functional in Linux. Refer to Appendix C.4.2 (System Configuration) for more information.

Ethernet ports that are not part of the system won't be tested. Examples are:

- Ethernet ports available through a PCI daughter board not part of the system
- USB to ethernet converters
- External switch connected to any RJ45 connector

Note: ACS does not validate Ethernet ports against the IEEE standard, it only tests for availability and accessibility of the port from Linux.

2.4.3 Future SystemReady IR requirements

In the future, requirements based on newer versions of the BSA/BBR specifications might be added. Security Interface Extension is planned to be required. Warnings from Devicetree schemas might not be allowed. Waiver levels 0-1 might be deprecated.

2.5 SystemReady LS certification

2.5.1 SystemReady LS v1.0 ALPHA requirements, Oct 2022 update

SystemReady LS v1.0 ALPHA requires the certified devices to be compliant to the following specifications:

- BSA v1.0c and Level 3-6 as defined in SBSA Supplement v6.1.
- LBBR-v1 recipe in BBR v2.0.

To certify a device for SystemReady LS v1.0 ALPHA, results from running the SystemReady LS testing (see instructions) must be submitted. In addition, boot logs from two of the Linux distros are required. The recommended distros are CentOS, Debian, Ubuntu, openSUSE, and Fedora.

All logs must be submitted using the LS template.

2.6 SystemReady Virtual Environment (VE) certification

The Arm SystemReady Virtual Environment (VE) is designed for the certification of virtual environments that can demonstrate the same software "just works" user experience as other SystemReady certifications.

2.6.1 SystemReady Virtual Environment (VE) v1.0 requirements, Oct 2022 update

The requirements for the SystemReady VE certification are the same as specified in Section 2 for other SystemReady bands, with the exceptions specified in this section. A virtual environment may be certified with SystemReady VE to correspond to an equivalent SR, LS, ES and IR band, depending on the virtualized hardware and firmware environment.

The following are exceptions for SystemReady VE certifications:

- The virtual environment may not present sufficient UEFI preboot environment to run the full ACS test suite, including BSA and SBSA compliance tests. As a result, it may not be possible to determine which corresponding SystemReady band to use for the certification. In this case, the virtual environment may be certified without any corresponding SystemReady band. The following testing is still required:
  - FirmwareTestSuite (FWTS) must still be used.
  - Installation and boot logs from the supported OSes.
- Some virtual environments may not allow nested virtualization. Hypervisors such as VMware ESXi may not run. In such cases, the installation and boot logs from one more OS, if possible, may be used instead.

Note: The physical system on which the virtual environment is running does not need to be SystemReady certified, whether using the same band as the virtual environment or with any band. For example, it is entirely valid to have a virtual environment that is SystemReady VE certified (with corresponding SystemReady ES band) running on a physical system that is not SystemReady certified.

3 SystemReady opt-in extensions

3.1 Security Interface Extension

The Arm SystemReady program provides a Security Interface Extension for devices that are compliant to the UEFI Secure Boot and Secure Firmware Update through Capsule Update services, as well as Trusted Platform Module (TPM) Support. The requirements are specified in the Base Boot Security Requirements (BBSR) specification.

3.1.1 SystemReady Security Interface Extension v1.2 requirements, Oct 2023 update

The Arm SystemReady Security Interface Extension requires the certified devices to be compliant to the BBSR Specification v1.2.

SystemReady IR v2.1 recommends the certified devices to obtain the Security Interface Extension certification.

SystemReady ES v1.5 recommends the certified devices to obtain the Security Interface Extension certification.

SystemReady SR v2.5 recommends the certified devices to obtain the Security Interface Extension certification.

For SystemReady SR devices to be certified with the Security Interface Extension, TPM must be used and the related requirements in BBSR are required.

The ACS for Security Interface Extension has now been integrated into the ACS for the SystemReady IR, ES and SR bands.

Note: ACS for Security Interface Extension v1.1.0 is deprecated.

Appendix A SystemReady ES and IR waiver levels

Currently, most of the Arm SoCs targeting the embedded server and IoT markets are not BSA compliant. For existing SoCs targeting the embedded server and IoT markets, there are three possibilities for SystemReady ES and IR certification:

- **Level 2 - Waiver**: Like with any certification programs, some failures are expected. Waivers are granted, as long as the user experience of software "just works" is not impacted.
- **Level 1 – Waiver and Workaround**: Major failures may exist. However, the user experience of software "just works" (OS installation and boot from basic media) can still be mostly achieved using hardware or firmware workarounds. Significant investments may be needed to provide the workaround.
- **Level 0 – Waiver and OS Change**: Major failures may exist, and hardware or firmware workarounds are not sufficient. OS changes or workarounds are needed. The user experience of software "just works" is impacted until the OS changes are contained in the future OS releases.

Level 0 waivers put the system at risk of compromising the SystemReady vision of software "just works". However, it is still important at this stage to fully understand the existing SoCs in their journey to be fully BSA compliant in future generations. Devices with this class of failures can be certified at Level 0, if the required OS change or fix is available and meets the following requirements:

Linux/BSD:

- Fix is up-streamed. For example, Linux kernel.org, or linux-next, or equivalent for BSDs.
- Fix is available and tested in a public distro build like:
    - Alpha / beta /development distro release
    - Non-release build, for example Fedora Rawhide, OpenSUSE Tumbleweed, Ubuntu Daily Build, and Arch Linux kernel build

Windows and VMware ESXi, for SystemReady ES:

- Fix applied by a driver, for example OSV, OEM, or community, that can be injected in the OS image during deployment or installation. The driver could be available as open-source or public binary.
- Fix confirmed by OSV and is available and tested in a public beta or pre-release build, for example Windows Insider Preview or VMware ESXi-Arm Fling

Table 4 describes some of the details of the SystemReady ES and IR waiver levels. These levels do not apply to SystemReady SR or LS:

Criteria	Level 0 – Waiver + OS Change	Level 1 – Waiver + Workaround	Level 2 – Waiver
Hardware BSA compliant?	No. Major failures exist, resolved with OS change.	No. Major failures exist, resolved with workarounds.	Mostly yes. Some failures exist.
Firmware BBR compliant?	Mostly yes. Some or no failures exist.	Mostly yes. Some or no failures exist.	Mostly yes. Some or no failures exist.
Hardware or firmware workarounds?	Not possible, or inadequate solution. An OS change is required instead.	Required, provide good solution.	Not needed.
Impacts "just works" goal?	Yes. Must be resolved with an OS change.	With workaround, no impacts.	No.
Impacts user experience?	Yes. Must be contained with an OS change.	With workaround, impacts are minimal or contained.	Minimal or contained.
OS changes needed?	Yes, required to enable "just works" goal and resolve user experience issues. Based on upstream or public OS builds.	Optional. OS changes can be used, for example, to remove the need for the workaround, add missing drivers or SoC support.	No.
Existing OS distros work?	None, or one.	Yes, two or more work with workaround.	Yes, two or more work, typically more.
Future OS distros work?	Yes, some, two or more work with OS changes.	Yes, most work with or without workaround.	Yes, most.
Future hardware resolves issue?	Possible, not required. Partner committed to BSA.	Possible, not required. Partner committed to BSA.	Possible, not required. Partner committed to BSA.
Waiver type	Waiver issued to partner. Public errata describing issues and future path published on Arm SystemReady Certification List.	Waiver issued to partner. Partner documentation of workarounds, public or NDA to end customers, are required.	Waiver issued to partner.

Table 4: SystemReady ES and IR waiver levels

A.1 Time limit

The use of these levels will be time limited, with a requirement that any new certification submissions after these dates must be certified at a higher Level. The exact cutoff dates for Level 0 and Level 1 are to be determined.

Appendix B SystemReady certification process

The following flow chart illustrates the Arm SystemReady certification process from the initial certification request to the completion of the certification. This chart identifies the tasks and responsibilities that Arm and partners have throughout the process. Arm may use third-party engineering services and test labs to strategically enable firmware development with partners, or to assist in the final certification phase. Arm is responsible for the architect final review and approval, as well as the final certificate issuance and publication.

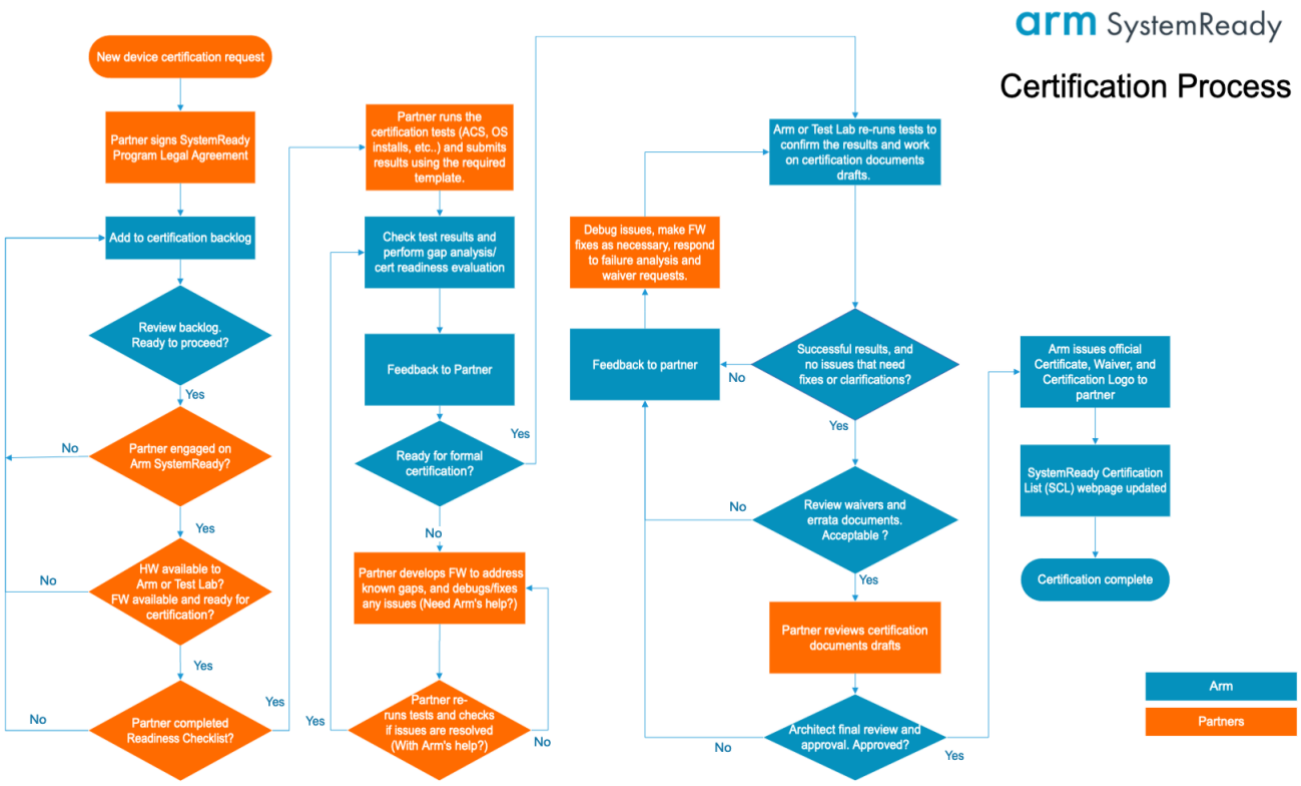

Figure 1: Arm SystemReady certification process

Appendix C SystemReady IR certification policy guide (ALPHA)

The purpose of this policy guide is to outline the criteria and guidelines for certifying third-party vendor products with SystemReady IR.

Note: This policy guide may cover other SystemReady bands in the future.

C.1 Band versions and ACS releases

Band version refers to a specific iteration of a specific SystemReady band. ACS release refers to a specific instance of ACS.

ACS follows a MAJOR.MINOR.PATCH semantic versioning format, where MAJOR and MINOR releases track SystemReady's band version as illustrated in Figure 2, and PATCH releases are used to accommodate smaller changes, as bug fixes.

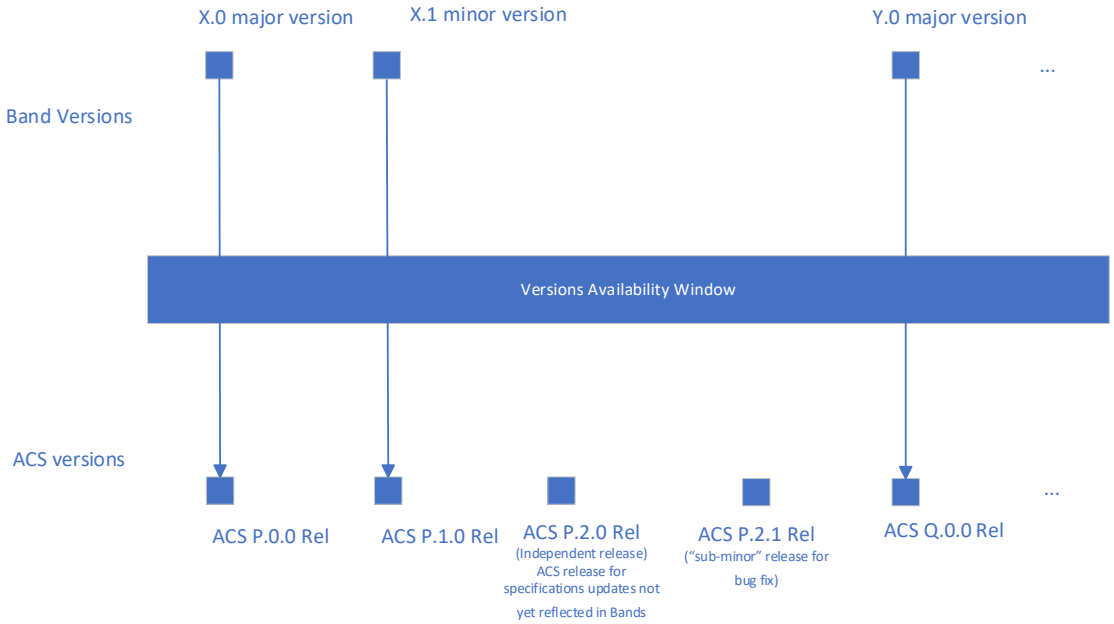

Figure 2: Arm SystemReady band versions and ACS releases Evolution

ACS is constantly evolving as new testing methods are employed, as technology changes, and as bugs are discovered and resolved. Test changes in each ACS release do not change the test requirements. They likely only change the method used to test.

Even though bug fixes in the ACS do not change the test requirements, they will eventually appear in a new ACS release. The certification team may ask for results from both the latest official ACS release, as well as the latest dev build that has the fixes but is not yet officially released.

Newly introduced tests in accordance with new band versions requirements constitute an ACS change and do not affect current certifications but may become required for future versions. For example, the inclusion of measured boot capabilities tests in ACS does not affect existing certifications, however, may affect new SystemReady versions.

C.2 Usage of OS distributions

Pre-built distributions usedfor testing should be any of the actively supported versions from the OS vendor of your choice as per this specification. A no longer supported OS version must be replaced by a more recent version. A soon-to-be discontinued OS version should also be replaced.

On occasions, and only when deemed appropriate by the certification team, daily builds or live distributions will be accepted as a proof of fixes, when those fixes are yet to be propagated to the distribution's releases.

Custom-built distributions, like OpenWRT and Yocto, are allowed for the SystemReady IR band. Nonetheless, to maintain compliance and guarantee that permitted custom-built distributions are functional foundations, alterations to the default baseline layers for certification purposes can only occur in the mainline. Modifying default layers of downstream custom builds is prohibited. Customization is permitted in layers situated above the default baseline layer.

C.3 Active band versions

Arm is open to accepting test results produced using the two latest band versions, N (last version) and N-1 (second-to-last) version.

Systems should aim for certification using the most recent band version, employing the latest test suite release.

Partners have the option to certify products using the N-1 band version. Throughout this time frame, if the SystemReady certification team deems it more appropriate for a particular certification, they may request the submitter to execute the tests using the most recent ACS version or the previous version.

For products registered under the N-1 band version, a transition period of 6 months is provided upon the release of a new band version. If the product's certification is not finalized within this 6-month window, it will be required to undergo certification under any of the two active band versions, N or N-1, as shown in Figure 3.

Granted certifications are never depreciated, however Arm encourages devices to stay up-to-date with the latest ACS available. See the certified products update policy in this document for more information.

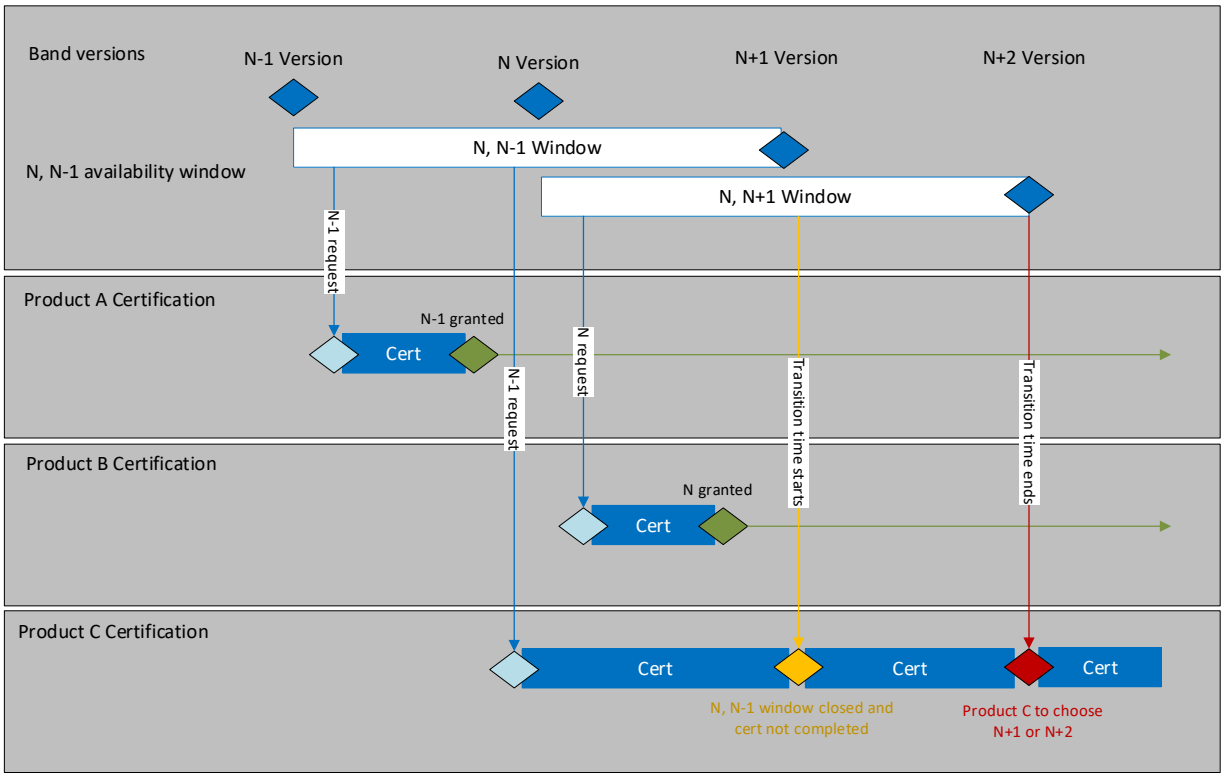

Figure 3: Active Arm SystemReady band versions

The following table shows the SystemReady band-versions available for certification against 32-bit and 64-bit architectures.

Active SR band versions	**SRS version**	**Architecture**
SR 2.4	2.1	64 bits
SR 2.5	2.2	64 bits
Active ES band versions	**SRS version**	**Architecture**
ES 1.4	2.1	64 bits
ES 1.5	2.2	64 bits
Active IR band versions	**SRS version**	**Architectures**
IR 1.1 IR 1.2	1.3 2.2	32 bit
IR 2.0 IR 2.1	2.1 2.2	64 bit

Table 5: Active Arm SystemReady versions

C.4 Certification process policy

C.4.1 Testing and test services

Test lab: Certification testing is performed in independent and certified test labs on hardware sent from the partner to the test lab.

In house: Arm will, when deemed necessary by Arm, perform certification testing in our lab on hardware sent from the partner to our lab.

Remote: Arm will, at the request of the partner, perform testing remotely. This service is not common and requires the partner to perform lab setup prior to Arm accessing the network and performing tests.

C.4.2 Target system

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

Target systems are not limited to specific supply chain entities (such as SiPs, OEMs, ODMs, ISVs, OSVs, and so on) or phase relative to the end-product lifecycle (including reference designs, compute systems, or end products). A viable system is any intentionally designed system meant to interoperate with multiple operating systems.

However, it is important to acknowledge the differences between the nature of products, markets they address, and stage within the lifecycle. For example, although compute systems and end products can equally see SystemReady as a value-add, the methods on which SystemReady certification is performed for these products may not be equally suited. SystemReady ACS is constantly changing in acknowledgement of these differences and processes, to be flexible to accommodate different products and markets.

Hardware

Hardware to be certified should be general availability level hardware, not development level hardware. Development or verification level hardware, or any other non-ready-for-production level is not suitable for final certification. The hardware should be the same hardware that customers are able to purchase.

Firmware

Firmware should be general availability or a 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 official partner means, such as registered customer portals. It cannot be private builds that are only available internally to the partner.

By no means will Arm allow the firmware used for certifications to be firmware specifically designed or configured to pass the certification but not general available.

System configuration

When conducting certification tests on a system able to accommodate and serve multiple configurations, the partner is encouraged to run the test suite over as many configurations as possible, however just one will be used for certification purposes. The configuration of your choice must be a valid configuration. It is advisable to be the one anticipated as the most common, or the most comprehensive one requiring the largest number of peripheral devices enabled.

System identification

Data in firmware must contain valid and correct identifiers for the make, model and version being tested, as defined in the BBR specification. This includes, for example, identifiers obtained from SMBIOS tables or SMCCC interfaces.

If the system is sold by a partner OEM/ODM, then the data must include the correct make and model for the system. If the system is intended for resale by a different brand or under a different mark, then the firmware data must include a verifiable identifier that shows the system is in fact the model being tested. In cases where one OEM/ODM is performing testing on behalf of another OEM/ODM who resells hardware from the primary OEM/ODM, that hardware must be identifiable in firmware as belonging to the reseller OEM/ODM.

C.4.3 Certified product updates

The following flow chart illustrates the Arm SystemReady certification process for updated or derivative systems. This flow refers to certification refresh for existing certified devices with new firmware, however, there is not always an obligation to re-certificate for firmware or hardware updates.

The certification team conducts regression testing on a set of approved hardware to consistently enhance the quality of ACS releases. This regression testing occurs inside Arm and has no impact on current certifications.

It is recommended 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 included to the regression tests.

Granted certifications do not expire. However, it is encouraged for devices to be kept up to date with no older than N-1 versions of the band-specific certifications.

There are circumstances on which re-certification is necessary. Changes that fundamentally alter a system's profile or are visible to the OS require a certification refresh. This includes, 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 driver updates, new functionality inclusion, or functionality updates. For example, changing 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, to be judged by the vendor, that could pose a risk for the SystemReady value delivery.

The following is a non-exhaustive list of examples of changes that do not require re-certification:

- CPU speed increases, for example Cortex-A72 1.6GHz to Cortex-A72 2.4GHz
- Memory increases or decreases, for example 4 GiB to 16 GiB, unless that includes an increase in the number of memory slots physically on the board. Whenever a question of re-certification comes up, the certification team will investigate the situation and make a decision on a case-by-case basis.
- Firmware bug fixes or minor changes do not require certification although it is encouraged to include these within the vendor's regression tests.

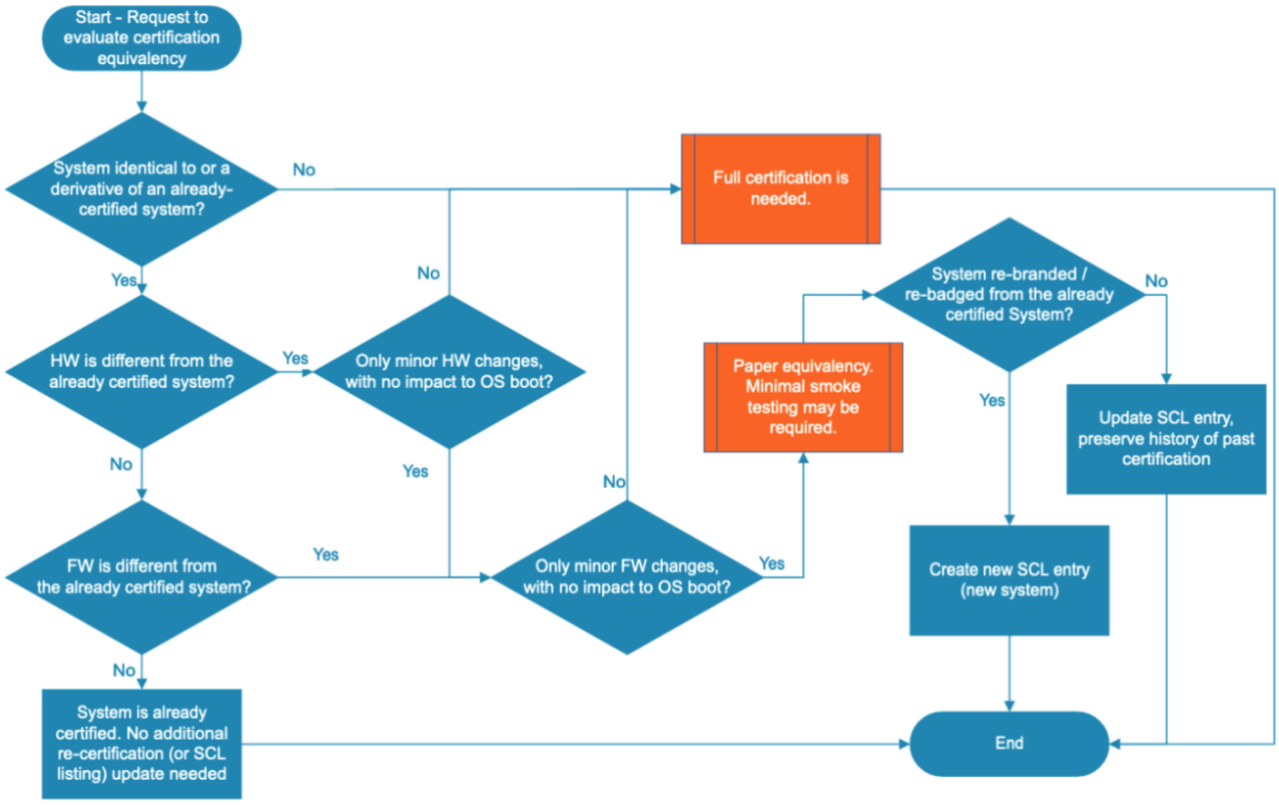

Figure 4: Arm SystemReady certification process for updated or derivative systems

C.4.4 SystemReady certification list

Arm expects that a SystemReady certification remains listed in the catalog until the end of the support life for the product. However, Arm reserves the right to remove an entry when deemed appropriate.

C.5 Certification policy compliance

Partners must comply with the guidelines outlined in this policy to be eligible for SystemReady certification. Failure to adhere to these guidelines may result in delayed certification, rejection of the application, or later certification revocation.

C.6 Policy effective date

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

C.7 Changes and certification 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 certification process.