



# Arm<sup>®</sup> RME System Architecture Compliance Suite

Version 0.7

## User Guide

### Non-Confidential

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

### Issue 01

108005\_0007\_01\_en



# Arm® RME System Architecture Compliance Suite

## User Guide

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

## Release Information

### Document history

Issue	Date	Confidentiality	Change
0005-01	24 April 2023	Confidential	First internal release for v0.5
0006-01	25 August 2023	Confidential	First internal release for v0.6
0007-01	6 November 2023	Non-Confidential	First release for v0.7

## Proprietary Notice

This document is protected by copyright and other related rights and the practice 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. 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 implementations infringe any third party patents.

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, patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

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.

This document consists solely of commercial items. You shall be responsible for ensuring that any 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 the Agreement shall prevail.

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. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow Arm’s trademark usage guidelines at <https://www.arm.com/company/policies/trademarks>.

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

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

(LES-PRE-20349|version 21.0)

## 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 for a Beta product, that is a product under development.

## Feedback on content

Information about how to give feedback on the content.

If you have comments on content then send an e-mail to [support-systemready-accs@arm.com](mailto:support-systemready-accs@arm.com). Give:

- The title Arm® RME System Architecture Compliance Suite User Guide.
- The number 108005\_0007\_01\_en.
- If applicable, the page number(s) to which your comments refer.
- A concise explanation of your comments.

Arm also welcomes general suggestions for additions and improvements.



Arm tests the PDF only in Adobe Acrobat and Acrobat Reader, and cannot guarantee the quality of the represented document when used with any other PDF reader.

---

## 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.

This document includes language that can be offensive. We will replace this language in a future issue of this document.

To report offensive language in this document, email [terms@arm.com](mailto:terms@arm.com).

# Contents

<b>1. Introduction.....</b>	<b>6</b>
1.1 Conventions.....	6
1.2 Useful resources.....	7
1.3 Other information.....	8
<b>2. Overview of the RME tests.....</b>	<b>9</b>
2.1 Abbreviations.....	9
2.2 Overview of RME tests.....	10
2.3 Test IDs.....	10
<b>3. UEFI shell application.....</b>	<b>11</b>
3.1 UEFI application arguments.....	11
3.2 UEFI implementation of PAL APIs.....	12
3.2.1 Infrastructure APIs.....	12
3.2.2 Module-specific APIs.....	13
<b>A. Revisions.....</b>	<b>14</b>
A.1 Revisions.....	14

# 1. Introduction

## 1.1 Conventions

The following subsections describe conventions used in Arm documents.

### Glossary

The Arm® Glossary is a list of terms used in Arm documentation, together with definitions for those terms. The Arm Glossary does not contain terms that are industry standard unless the Arm meaning differs from the generally accepted meaning.

See the Arm Glossary for more information: [developer.arm.com/glossary](https://developer.arm.com/glossary).

Convention	Use
<i>italic</i>	Citations.
<b>bold</b>	Terms in descriptive lists, where appropriate.
monospace	Text that you can enter at the keyboard, such as commands, file and program names, and source code.
monospace <u>underline</u>	A permitted abbreviation for a command or option. You can enter the underlined text instead of the full command or option name.
<and>	Encloses replaceable terms for assembler syntax where they appear in code or code fragments.  For example:  <pre>MRC p15, 0, &lt;Rd&gt;, &lt;CRn&gt;, &lt;CRm&gt;, &lt;Opcode_2&gt;</pre>
SMALL CAPITALS	Terms that have specific technical meanings as defined in the Arm® Glossary. For example, <b>IMPLEMENTATION DEFINED</b> , <b>IMPLEMENTATION SPECIFIC</b> , <b>UNKNOWN</b> , and <b>UNPREDICTABLE</b> .



Caution

Recommendations. Not following these recommendations might lead to system failure or damage.



Warning

Requirements for the system. Not following these requirements might result in system failure or damage.



Danger

Requirements for the system. Not following these requirements will result in system failure or damage.



An important piece of information that needs your attention.



A useful tip that might make it easier, better or faster to perform a task.



A reminder of something important that relates to the information you are reading.

## 1.2 Useful resources

This document contains information that is specific to this product. See the following resources for other useful information.

Access to Arm documents depends on their confidentiality:

- Non-Confidential documents are available at [developer.arm.com/documentation](https://developer.arm.com/documentation). Each document link in the following tables goes to the online version of the document.
- Confidential documents are available to licensees only through the product package.

Arm product resources	Document ID	Confidentiality
<a href="#">Arm® Realm Management Extension (RME) System Architecture</a>	DEN0129H	Non-Confidential
<a href="#">Arm® System Memory Management Unit Architecture Specification</a>	IHI0070	Non-Confidential

Arm architecture and specifications	Document ID	Confidentiality
<a href="#">Arm® Architecture Reference Manual for A-profile architecture</a>	DDI0487I.a	Non-Confidential
<a href="#">Arm® Generic Interrupt Controller Architecture Specification for GIC architecture version 3.0 and version 4.0</a>	IHI0069C	Non-Confidential



Arm tests its PDFs only in Adobe Acrobat and Acrobat Reader. Arm cannot guarantee the quality of its documents when used with any other PDF reader.

Adobe PDF reader products can be downloaded at <http://www.adobe.com>.

## 1.3 Other information

See the Arm® website for other relevant information.

- [Arm® Developer](#).
- [Arm® Documentation](#).
- [Technical Support](#).
- [Arm® Glossary](#).



## 2. Overview of the RME tests

This chapter provides an overview of the Realm Management Extension (RME) tests and the test IDs.

### 2.1 Abbreviations

The following table lists the abbreviations used in this document.

**Table 2-1: Abbreviations and expansions**

Abbreviation	Expansion
ACPI	Advanced Configuration and Power Interface
ACS	Architecture Compliance Suite
AEST	Arm Error Source Table
BDF	Bus, Device, and Function
CATU	CoreSight Address Translation Unit
ELx	Exception Level x (where x can be 0 to 3)
ETR	Embedded Trace Router
GIC	Generic Interrupt Controller
GCD	Grand Central Dispatch
HMAT	Heterogeneous Memory Attribute Table
HVC	Hyper Visor Call
IOMMU	Input-Output Memory Management Unit
ITS	Interrupt Translation Service
LPI	Locality-specific Peripheral Interrupt
MPAM	Memory System Resource Partitioning and Monitoring
MSI	Message-Signaled Interrupt
MTE	Memory Tagging Extension
NUMA	Non-Uniform Memory Access
PAL	Platform Abstraction Layer
PCIe	Peripheral Component Interconnect express
PCCT	Platform Communications Channel Table
PE	Processing Element
PMU	Performance Monitor Unit
PPTT	Processor Properties Topology Table
PSCI	Power State Coordination Interface
RAS	Reliability, Availability, and Serviceability
RAS2	Reliability, Availability, and Serviceability 2
RCiEP	Root Complex integrated End Point

Abbreviation	Expansion
RME	Realm Management Extension
SATA	Serial Advanced Technology Attachment
SBSA	Server Base System Architecture
SMC	Secure Monitor Call
SMMU	System Memory Management Unit
SRAT	System Resource Affinity Table
STS	Statistical Test Suite
SoC	System on Chip
UEFI	Unified Extensible Firmware Interface
UART	Universal Asynchronous Receiver and Transmitter
VAL	Validation Abstraction Layer

## 2.2 Overview of RME tests

The following table describes the general divisions of Arm Realm Management Extension System Architecture compliance tests between Unified Extensible Firmware Interface (UEFI) shell application and Bare-metal.

**Table 2-2: Test environment and modules**

Test environment	Modules
UEFI shell	RME, GIC, SMMU, Legacy System
Bare-metal	RME, GIC, SMMU, Legacy System

## 2.3 Test IDs

Each test ID is generated in addition to module ID and unit test ID. For a given module, unit test ID begins from 1.

The following table lists the module names and their IDs.

**Table 2-3: Module names and module IDs**

Module name	Module ID
RME	0
Exerciser	100
GIC	200
PCIe	300
SMMU	400
Legacy System	500

# 3. UEFI shell application

This chapter provides information on executing tests from the UEFI Shell application and its PAL API implementation.

## 3.1 UEFI application arguments

Run the UEFI Shell application with the following set of arguments:

```
uefi shell> rme.efi [-v <n>] [-skip <x,y,z>] [-t <test id>] [-m <module id>]
```

The following table provides descriptions to the arguments.

Table 3-1: Descriptions of UEFI application arguments

Argument	Description
-v	Print level  1 INFO and above. 2 DEBUG and above. 3 TEST and above. 4 WARN and ERROR. 5 ERROR.
-skip	Overrides the suite to skip the execution of a particular test. It allows a maximum of three values (comma-separated).  For example, 300 skips test case with ID = 300.  400 skips all tests in module with ID = 400.  For more information on module IDs, see, <a href="#">2.3 Test IDs</a> on page 10.
-t	To run only a single selected test.  <b>Note:</b> -m will override -t if used on the same module.
-m	To run only single selected module.



The UEFI session becomes unusable after the RME tests are run and the test results are printed on the UEFI console.

## Examples of UEFI application arguments

### Example 1

```
shell> rme.efi -v 2 -skip 200,2
```

The set of parameters shown in the code block:

- Prints messages with verbosity of 2 and above.
- Skips execution of all tests belonging to GIC module and test number 2.

### Example 2

```
shell > rme.efi -m 0 -skip 1
```

The set of parameters shown in the code block:

- Runs only the RME module.
- Skips the RME test 1.

## 3.2 UEFI implementation of PAL APIs

This section provides information on infrastructure APIs and module-specific APIs.

### 3.2.1 Infrastructure APIs

The following table describes the Platform Abstraction Layer (PAL) APIs and UEFI interfaces.

**Table 3-2: PAL APIs and UEFI interfaces**

PAL APIs	UEFI interfaces
pal_print	AsciiPrint
mem_alloc	gBS->AllocatePool
mem_free	gBS->FreePool
mem_alloc_shared	gBS->AllocatePool
mem_free_shared	gBS->FreePool
mem_get_shared_addr	None
mem_alloc_cacheable	gBS->AllocatePages
mem_free_cacheable	gBS->FreePages
time_delay_ms	gBS->Stall
mem_alloc_pages	gBS->AllocatePages
mem_free_pages	gBS->FreePages
mmio_read	None
mmio_write	None

## 3.2.2 Module-specific APIs

The following table represents the mapping of PAL API to Advanced Configuration and Power Interface (ACPI), if the system firmware presents platform configuration through ACPI tables.

**Table 3-3: PAL APIs, UEFI interfaces, and ACPI tables consumed**

PAL API	UEFI interfaces consumed	ACPI table consumed
pe_create_info_table	<ul style="list-style-type: none"> <li>gST-&gt;ConfigurationTable</li> <li>CompareGuid</li> <li>IndustryStandard/Acpi.h</li> </ul>	MADT Table
pe_execute_payload	-	-
pe_install_esr	<ul style="list-style-type: none"> <li>gEfiCpuArchProtocolGuid</li> <li>Cpu-&gt;RegisterInterruptHandler</li> </ul>	-
gic_create_info_table	<ul style="list-style-type: none"> <li>gST-&gt;ConfigurationTable</li> <li>CompareGuid</li> <li>IndustryStandard/Acpi.h</li> </ul>	MADT table
pcie_create_info_table	<ul style="list-style-type: none"> <li>gST-&gt;ConfigurationTable</li> <li>CompareGuid</li> <li>IndustryStandard/Acpi.h</li> </ul>	MCFG table
peripheral_create_info_table	<ul style="list-style-type: none"> <li>gEfiPciIoProtocolGuid</li> <li>Pci-&gt;GetLocation</li> <li>Pci-&gt;Pci.Read</li> </ul>	-
memory_create_info_table	gBS->GetMemoryMap	-

# Appendix A Revisions

This appendix describes the technical changes between released issues of this book.

## A.1 Revisions

The following tables describe the changes between different issues of this document.

**Table A-1: Issue 0005-01**

Change	Location
First release	-

**Table A-2: Differences between Issue 0005-01 and Issue 0006-01**

Change	Location
Information about legacy system is added.	See <a href="#">2.3 Test IDs</a> on page 10

**Table A-3: Differences between Issue 0006-01 and Issue 0007-01**

Change	Location
Module list has been updated.	See <a href="#">2.2 Overview of RME tests</a> on page 10