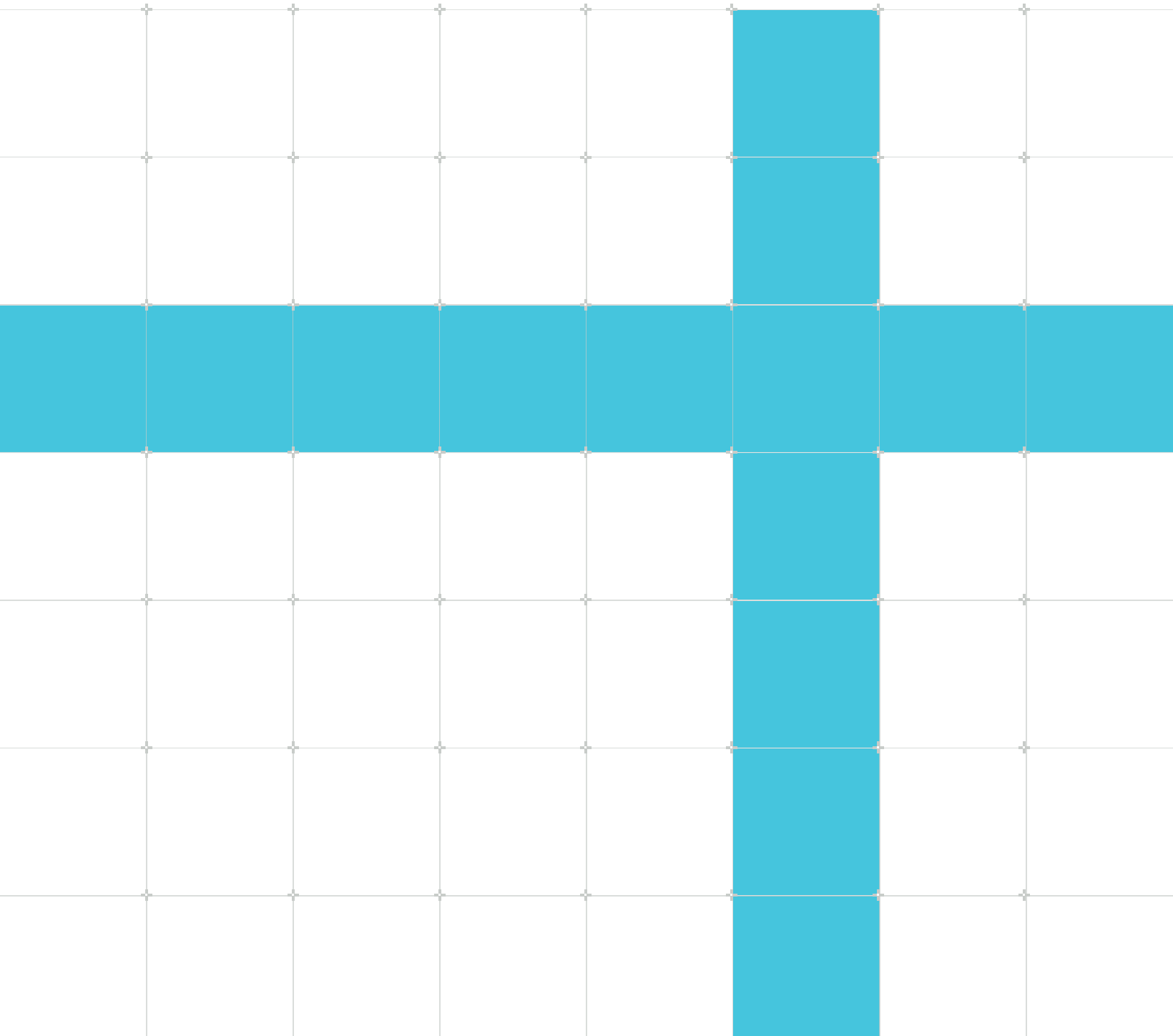
Arm® RME System Architecture Compliance Suite

Version 2.0

User Guide

Non-Confidential

Issue 01
108005_0200_01_en



Arm® RME System Architecture Compliance Suite

User Guide

Release Information

Document history

Issue	Date	Confidentiality	Change
0200-01	15 November 2024	Non-Confidential	Beta release for issue B
0100-02	9 August 2024	Non-Confidential	First internal release
0100-01	13 December 2023	Non-Confidential	First release for v1.0
0007-01	6 November 2023	Non-Confidential	First release for v0.7
0006-01	25 August 2023	Confidential	First internal release for v0.6
0005-01	24 April 2023	Confidential	First internal release for v0.5

Proprietary Notice

Arm herein. In addition, you are responsible for any applications which are used in 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.

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 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-rme-acs@arm.com. Give:

- The title Arm® RME System Architecture Compliance Suite User Guide.
- The number 108005_0200_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.


Note

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.

Contents

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.

Convention	Use
italic	Citations.
bold	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 underline`	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: `MRC p15, 0, <Rd>, <CRn>, <CRm>, <Opcode_2>`
SMALL CAPITALS	Terms that have specific technical meanings as defined in the *Arm® Glossary*. For example, **IMPLEMENTATION DEFINED**, **IMPLEMENTATION SPECIFIC**, **UNKNOWN**, and **UNPREDICTABLE**.

We recommend the following. If you do not follow these recommendations your system might not work.

Your system requires the following. If you do not follow these requirements your system will not work.

You are at risk of causing permanent damage to your system or your equipment, or of harming yourself.


Note

This information is important and needs your attention.


Tip

This information might help you perform a task in an easier, better, or faster way.


Remember

This information reminds you of something important relating to the current content.

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. 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
Arm® Realm Management Extension (RME) System Architecture	DEN0129	Non-Confidential
Arm® System Memory Management Unit Architecture Specification	IHI0070	Non-Confidential

Arm architecture and specifications	Document ID	Confidentiality
Arm® Architecture Reference Manual for A-profile architecture	DDI0487	Non-Confidential
Arm® Generic Interrupt Controller Architecture Specification for GIC architecture version 3.0 and version 4.0	IHI0069C	Non-Confidential


Note

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
BDF	Bus, Device, and Function
CATU	CoreSight Address Translation Unit
DA	Device Assignment
DPT	Device Permission Table
ELx	Exception Level x (where x can be 0 to 3)
ETR	Embedded Trace Router
GIC	Generic Interrupt Controller
HVC	Hyper Visor Call
IOMMU	Input-Output Memory Management Unit
ITS	Interrupt Translation Service
IDE	Integrity and Data Encryption
KM	Key Management
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
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
RMM	Realm Management Monitor
RMSD	Realm Management Security Domain
SBSA	Server Base System Architecture
SMC	Secure Monitor Call
SMMU	System Memory Management Unit
SoC	System on Chip
TDI	TEE Device Interface
TDISP	TEE Device Interface Security Protocol
TEE	Trusted Execution Environment
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 test suites

Test environment	Test suites
UEFI shell	RME, GIC, SMMU, Legacy System, and DA.
Bare-metal	RME, GIC, SMMU, Legacy System, and DA.

2.3 Test IDs

Each test ID is generated in addition to module ID and testcase ID. For a given module, testcase 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

Module name	Module ID
Legacy System	500
DA	600

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, 2.3 Test IDs on page 10.
`-t`	To run only a single selected test. **Note:** `-m` will override `-t` if used on the same module.
`-m`	To run only single selected module.


Note

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_cachebale	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`	• gST->ConfigurationTable • CompareGuid • IndustryStandard/Acpi.h	MADT Table
`pe_execute_payload`	-	-
`pe_install_esr`	• gEfiCpuArchProtocolGuid • Cpu->RegisterInterruptHandler	-
`gic_create_info_table`	• gST->ConfigurationTable • CompareGuid • IndustryStandard/Acpi.h	MADT table
`pcie_create_info_table`	• gST->ConfigurationTable • CompareGuid • IndustryStandard/Acpi.h	MCFG table
`peripheral_create_info_table`	• gEfiPciIoProtocolGuid • Pci->GetLocation • Pci->Pci.Read	-
`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 2.3 Test IDs on page 10

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

Change	Location
Module list has been updated.	See 2.2 Overview of RME tests on page 10

Table A-4: Differences between Issue 0007-01 and Issue 0100-01

Change	Location
No technical changes	-

Table A-5: Differences between Issue 0100-01 and Issue 0100-02

Change	Location
Added new abbreviations.	See 2.1 Abbreviations on page 9
Updated the test environment and test suites table.	See 2.2 Overview of RME tests on page 10
Updated the description of test IDs.	See 2.3 Test IDs on page 10

Table A-6: Differences between Issue 0100-02 and Issue 0200-01

Change	Location
Added new abbreviation.	See 2.1 Abbreviations on page 9.