



# Realm Management Monitor specification

Document number	DEN0137
Document quality	EAC
Document version	1.0-eac3
Document confidentiality	Non-confidential
Document build information	1b76d699 doctool 0.53.0

*Copyright © 2022-2023 Arm Limited or its affiliates. All rights reserved.*

# Realm Management Monitor specification

## Release information

### 1.0-eac3 (20-07-2023)

#### Clarifications

- Clarify which bits of command input / output values should / must be zero (FENIMORE-674)
- Explain distinction between concrete and abstract types (FENIMORE-693)
- Clarify return value from RSI\_IPA\_STATE\_SET when stopping at first DESTROYED entry (FENIMORE-699) [IGXDDX]

#### Defects

- PSCI\_SYSTEM\_{OFF,RESET}: change Realm state to SYSTEM\_OFF (FENIMORE-694)
- RMI\_REC\_CREATE: update RIM only if runnable flag is set (FENIMORE-697)
- RMI\_REALM\_CREATE: fix list of measured parameters (FENIMORE-695)
- Remove members from RmmSystemRegisters (FENIMORE-700)
  - State saved / restored depends on architecture features supported by the platform, so defining this type as an empty placeholder
- Avoid use of reserved ASL v1 keyword “entry” in MRS (FENIMORE-702)
  - RmiRecEntry -> RmiRecEnter
  - RmiRecEntryFlags -> RmiRecEnterFlags
  - RmiRecRun::entry -> RmiRecRun::enter
  - RmmRttWalkResult::entry -> RmmRttWalkResult::rtte
- RSI\_IPA\_STATE\_SET: prohibit RSI\_DESTROYED input value (FENIMORE-705)
- RMI\_PSCI\_COMPLETE: PSCI\_CPU\_ON: fix copy of context\_id to target CPU X0 (FENIMORE-703)
- Allow Host to reject request to change RIPAS to RAM (FENIMORE-661)
- Allow Host to reject PSCI\_CPU\_ON request via RMI\_PSCI\_COMPLETE (FENIMORE-706)

#### Relaxations

- Permit folding of level 2 RTT to create level 1 block mapping (FENIMORE-608)
- Remove restriction that attestation token size must not exceed 4KB (FENIMORE-691)

### 1.0-eac2 (07-06-2023)

#### Clarifications

- Remove reference to triggering ERROR\_INPUT by setting MBZ bit to 1 (FENIMORE-675)
- Clarify constraints on output values in case of command failure [R\_TFZMS] (FENIMORE-676)
- Clarify encoding of RmiRealmParams::sve\_sz (FENIMORE-684)
- Clarify set of SMCCC interfaces available to a Realm [R\_NPLKX] (FENIMORE-685)

#### Defects

- Replace PMU fields in RmiRecExit with single bit indicating the PMU overflow status [R\_WXTZF] (FENIMORE-679)
- RMI\_PSCI\_COMPLETE: failure condition should compare against MPIDR, not RD address (FENIMORE-681)
- RMI\_REC\_CREATE: remove params\_valid failure condition (FENIMORE-686)
- RMI\_RTT\_{INIT,SET}\_RIPAS: check alignment of “top” input value (FENIMORE-687)
- Reduce coupling between HIPAS and RIPAS (FENIMORE-680)
  - Replace HIPAS=DESTROYED with RIPAS=DESTROYED
  - Remove RmiRttEntryState::RMI\_DESTROYED
  - Change encoding of RmiRttEntryState::RMI\_TABLE

- Add RmiRipas::RMI\_DESTROYED
- Add RsiRipas::RSI\_DESTROYED
- RMI\_DATA\_CREATE\_UNKNOWN: remove pre-condition that RIPAS=RAM
- RMI\_DATA\_DESTROY:
  - \* In all cases, post-condition now states that HIPAS=UNASSIGNED
  - \* If pre-condition was RIPAS=RAM, post-condition states that RIPAS=DESTROYED
- RMI\_RTT\_DESTROY:
  - \* Remove post-condition that HIPAS=DESTROYED
  - \* Add post-condition that state of parent RTTE is UNASSIGNED
  - \* Add post-condition that RIPAS=DESTROYED
- RMI\_RTT\_SET\_IPA\_STATE: stop at first DESTROYED entry if “destroyed” flag is set
- RSI\_IPA\_STATE\_SET: add “destroyed” flag
- Clarify distinction between “RTT folding” [D<sub>QPXCP</sub>] and “RTT destruction” [D<sub>VXRZW</sub>]
- RMI\_RTT\_INIT\_RIPAS: success conditions should be bounded by walk\_top, not top

#### **Relaxations**

- RSI\_REALM\_CONFIG: provide Realm hash algorithm (FENIMORE-678)

### **1.0-eac1 (31-03-2023)**

#### **Clarifications**

- Unused bits of RmiRecEntry::gicv3\_hcr are SBZ [I<sub>SMHXB</sub>] (FENIMORE-666)
- RMI\_REC\_ENTER: all RMI\_ERROR\_INPUT failure conditions precede all RMI\_ERROR\_REC failure conditions (FENIMORE-668)
- Avoid use of raw Xn values in command conditions where possible (FENIMORE-671)
- Clarify definition of REC exit due to (Non-)emulatable Data Abort [D<sub>CYRMT</sub>, D<sub>MTZMC</sub>] (FENIMORE-673)

#### **Defects**

- RMI\_RTT\_INIT\_RIPAS: take account of “top” IPA value when calculating RIM contribution (FENIMORE-662)
- RttSkipEntriesWithRipas: fix inverted logic (FENIMORE-663)
- RMI\_RTT\_SET\_RIPAS: on success, modify IPA range [base, walk\_top) (FENIMORE-669)
- RMI\_RTT\_{INIT,SET}\_RIPAS: remove redundant failure conditions (FENIMORE-670)
- Clarify HIPAS=DESTROYED implies RIPAS=UNDEFINED [R<sub>JYDRL</sub>] (FENIMORE-672)

#### **Relaxations**

- RSI\_HOST\_CALL: relax alignment requirement from 4KB to 256B

### **1.0-eac0 (31-01-2023)**

#### **Clarifications**

None

#### **Defects**

- RmiRealmParams: reduce width of integer attributes (FENIMORE-647)
- RSI\_IPA\_STATE\_SET: replace (base, size) with (base, top) (FENIMORE-656)
- RMI\_RTT\_INIT\_RIPAS, RMI\_RTT\_SET\_RIPAS: allow single command to modify multiple RTT entries (FENIMORE-656)

#### **Relaxations**

- RMI\_RTT\_SET\_RIPAS: remove “ripas” input value (FENIMORE-659)

## 1.0-bet2 (16-12-2022)

### Clarifications

- Flows: update RMI\_REC\_ENTRY to take a single 'run' input value
- Clarify meaning of "TTD" [I<sub>YMNSR</sub>] (FENIMORE-641)
- Fix typo in reference to "CCA platform token claim map" [I<sub>FJKFY</sub>] (FENIMORE-647)
- Fix reference to "RME system architecture spec" (FENIMORE-648)
- Flows: remove stale reference to parameters passed to RMI\_DATA\_CREATE (FENIMORE-649)
- Improve definition and consistency of usage of the term "REC" (FENIMORE-650)
  - Where referring to the RMM data structure "REC object" is now used
- Clarify description of properties of Realm IPA space [I<sub>TPGKW</sub>] (FENIMORE-639)
  - Replace "permitted, under control of host" with statements which refer to particular HIPAS values.
  - Add "Protected IPA, HIPAS=DESTROYED" row, thereby removing contradictory statements regarding SEA taken to Realm, previously in "Protected IPA, RIPAS=EMPTY".
- On assertion of an EL1 timer, the RMM guarantees a *REC exit*, not only a *Realm exit* (FENIMORE-651)
- RMI\_RTT\_FOLD: preserve RIPAS value if IPA is Protected (FENIMORE-638)

### Defects

- Attestation: wrap sub-tokens in byte stream (FENIMORE-643)
- RMI\_DATA\_DESTROY, RMI\_RTT\_{DESTROY,FOLD}: return PA of destroyed object (FENIMORE-563)
- RMI\_REALM\_DESTROY, RMI\_REC\_DESTROY, RMI\_REC\_ENTER, RMI\_RTT\_DESTROY, RMI\_RTT\_FOLD, RMI\_RTT\_SET\_RIPAS: Remove RMI\_ERROR\_IN\_USE (FENIMORE-588)
- RMI\_DATA\_CREATE, RMI\_DATA\_CREATE\_UNKNOWN, RMI\_REC\_CREATE, RMI\_RTT\_CREATE: pass RD pointer in X1 (FENIMORE-655)
- Replace RmiRealmParams::features\_0 with discrete fields (FENIMORE-655)
- RMI\_DATA\_CREATE(\_UNKNOWN): require RIPAS=RAM (FENIMORE-645)
- Apply "must / should be zero" consistently (FENIMORE-619)
  - In command inputs, unused bits are SBZ
  - In command outputs, unused bits are MBZ

### Relaxations

- RSI\_HOST\_CALL: expand set of GPRs to X0-X30 (FENIMORE-607)
  - This enables the RMM to support any calling convention.
- RMI\_DATA\_DESTROY, RMI\_RTT\_DESTROY, RMI\_RTT\_UNMAP\_UNPROTECTED: return IPA of next live RTT entry (FENIMORE-563)

## 1.0-bet1 (31-10-2022)

### Clarifications

- Rename HIPAS\_VALID\_NS -> UNASSIGNED (FENIMORE-631)
- SEA injection is independent of whether Host emulates MMIO (FENIMORE-632)
- In RIPAS change flow, permit Host to apply the change to zero or more pages of the target IPA region (FENIMORE-633)
- Flows: replace HVC with Host call (FENIMORE-611)
- Clarify behavior of VmidIsValid() function (FENIMORE-630)
- Qualify "all other exit fields are zero" statements [R<sub>GTJRP</sub>, R<sub>LRCFP</sub>] (FENIMORE-634)
  - GIC, timer and PMU fields are valid on every REC exit.

### Defects

- Change size of RsiHostCall type to 256 bytes (FENIMORE-629)
- Correct the set of ESR\_EL2 fields which are returned to the Host on REC exit due to Data abort [R<sub>RYVFL</sub>]
  - On all Data Aborts, add FnV.
  - On Emulatable Data Aborts, add SF.
  - On Non-emulatable Data Abort at an Unprotected IPA, add IL.

***Relaxations***

None

## 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 Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its subsidiaries) 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. No licence, express, implied or otherwise, is granted to Licensee under this Licence, to use the Arm trade marks in connection with the Document or any products based thereon. Visit Arm's website at <http://www.arm.com/company/policies/trademarks> for more information about Arm's trademarks.

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

Copyright © 2022-2023 Arm Limited (or its affiliates). All rights reserved.

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

LES-PRE-21585 version 4.0

## Contents

# Realm Management Monitor specification

Realm Management Monitor specification . . . . .	ii
Release information . . . . .	ii
Arm Non-Confidential Document Licence ("Licence") . . . . .	vi

## Preface

Conventions . . . . .	xvii
Typographical conventions . . . . .	xvii
Numbers . . . . .	xvii
Pseudocode descriptions . . . . .	xvii
Addresses . . . . .	xvii
Rules-based writing . . . . .	xviii
Content item identifiers . . . . .	xviii
Content item rendering . . . . .	xviii
Content item classes . . . . .	xviii
Additional reading . . . . .	xx
Feedback . . . . .	xxi
Feedback on this book . . . . .	xxi
Open issues . . . . .	xxii

## Part A Architecture

### Chapter A1

#### Overview

A1.1 Confidential computing . . . . .	24
A1.2 System software components . . . . .	25
A1.3 Realm Management Monitor . . . . .	25

### Chapter A2

#### Concepts

A2.1 Realm . . . . .	28
A2.1.1 Overview . . . . .	28
A2.1.2 Realm execution environment . . . . .	28
A2.1.3 Realm attributes . . . . .	29
A2.1.4 Realm liveness . . . . .	30
A2.1.5 Realm lifecycle . . . . .	31
A2.1.6 Realm parameters . . . . .	32
A2.1.7 Realm Descriptor . . . . .	32
A2.2 Granule . . . . .	33
A2.2.1 Granule attributes . . . . .	33
A2.2.2 Granule ownership . . . . .	34
A2.2.3 Granule lifecycle . . . . .	34
A2.2.4 Granule wiping . . . . .	36
A2.3 Realm Execution Context . . . . .	38
A2.3.1 Overview . . . . .	38
A2.3.2 REC attributes . . . . .	38
A2.3.3 REC index and MPIDR value . . . . .	39
A2.3.4 REC lifecycle . . . . .	40

### Chapter A3

#### Realm creation

A3.1 Realm feature discovery and selection . . . . .	43
--	----



A3.1.1	Realm hash algorithm . . . . .	43
A3.1.2	Realm LPA2 and IPA width . . . . .	43
A3.1.3	Realm support for Scalable Vector Extension . . . . .	44
A3.1.4	Realm support for self-hosted debug . . . . .	44
A3.1.5	Realm support for Performance Monitors Extension . . . . .	44
A3.1.6	Realm support for Activity Monitors Extension . . . . .	45
A3.1.7	Realm support for Statistical Profiling Extension . . . . .	45
A3.1.8	Realm support for Trace Buffer Extension . . . . .	45

## Chapter A4

### Realm exception model

A4.1	Exception model overview . . . . .	47
A4.2	REC entry . . . . .	49
A4.2.1	RecEnter object . . . . .	49
A4.2.2	General purpose registers restored on REC entry . . . . .	51
A4.2.3	REC entry following REC exit due to Data Abort . . . . .	51
A4.3	REC exit . . . . .	52
A4.3.1	RecExit object . . . . .	52
A4.3.2	Realm exit reason . . . . .	54
A4.3.3	General purpose registers saved on REC exit . . . . .	54
A4.3.4	REC exit due to synchronous exception . . . . .	55
A4.3.5	REC exit due to IRQ . . . . .	57
A4.3.6	REC exit due to FIQ . . . . .	57
A4.3.7	REC exit due to PSCI . . . . .	58
A4.3.8	REC exit due to RIPAS change pending . . . . .	59
A4.3.9	REC exit due to Host call . . . . .	59
A4.3.10	REC exit due to SError . . . . .	59
A4.4	Emulated Data Aborts . . . . .	61
A4.5	Host call . . . . .	61

## Chapter A5

### Realm memory management

A5.1	Realm memory management overview . . . . .	63
A5.2	Realm view of memory management . . . . .	63
A5.2.1	Realm IPA space . . . . .	63
A5.2.2	Realm IPA state . . . . .	63
A5.2.3	Realm access to a Protected IPA . . . . .	64
A5.2.4	Changes to RIPAS while Realm state is NEW . . . . .	64
A5.2.5	Changes to RIPAS while Realm state is ACTIVE . . . . .	64
A5.2.6	Realm access to an Unprotected IPA . . . . .	66
A5.2.7	Synchronous External Aborts . . . . .	66
A5.2.8	Realm access outside IPA space . . . . .	66
A5.2.9	Summary of Realm IPA space properties . . . . .	67
A5.3	Host view of memory management . . . . .	68
A5.3.1	Host IPA state . . . . .	68
A5.3.2	Changes to HIPAS while Realm state is NEW . . . . .	69
A5.3.3	Changes to HIPAS while Realm state is ACTIVE . . . . .	70
A5.3.4	Summary of changes to HIPAS and RIPAS of a Protected IPA . . . . .	71
A5.3.5	Dependency of RMI command execution on RIPAS and HIPAS values . . . . .	73
A5.3.6	Changes to HIPAS of an Unprotected IPA . . . . .	73
A5.4	RIPAS change . . . . .	75
A5.5	Realm Translation Table . . . . .	77
A5.5.1	RTT overview . . . . .	77
A5.5.2	RTT structure and configuration . . . . .	77
A5.5.3	RTT starting level . . . . .	77
A5.5.4	RTT entry . . . . .	78
A5.5.5	RTT reading . . . . .	78

	A5.5.6	RTT folding . . . . .	79
	A5.5.7	RTT unfolding . . . . .	79
	A5.5.8	RTTE liveness and RTT liveness . . . . .	80
	A5.5.9	RTT destruction . . . . .	80
	A5.5.10	RTT walk . . . . .	81
	A5.5.11	RTT entry attributes . . . . .	81
<b>Chapter A6</b>	<b>Realm interrupts and timers</b>		
	A6.1	Realm interrupts . . . . .	85
	A6.2	Realm timers . . . . .	87
<b>Chapter A7</b>	<b>Realm measurement and attestation</b>		
	A7.1	Realm measurements . . . . .	89
	A7.1.1	Realm Initial Measurement . . . . .	89
	A7.1.2	Realm Extensible Measurement . . . . .	90
	A7.2	Realm attestation . . . . .	91
	A7.2.1	Attestation token . . . . .	91
	A7.2.2	Attestation token generation . . . . .	91
	A7.2.3	Attestation token format . . . . .	93
<b>Chapter A8</b>	<b>Realm debug and performance monitoring</b>		
	A8.1	Realm PMU . . . . .	112
<b>Part B</b>	<b>Interface</b>		
<b>Chapter B1</b>	<b>Commands</b>		
	B1.1	Overview . . . . .	115
	B1.2	Command definition . . . . .	116
	B1.2.1	Example command . . . . .	116
	B1.3	Command registers . . . . .	117
	B1.4	Command condition expressions . . . . .	117
	B1.5	Command context values . . . . .	118
	B1.6	Command failure conditions . . . . .	119
	B1.7	Command success conditions . . . . .	120
	B1.8	Concrete and abstract types . . . . .	120
	B1.9	Command footprint . . . . .	120
<b>Chapter B2</b>	<b>Command condition functions</b>		
	B2.1	AddrInRange function . . . . .	122
	B2.2	AddrIsAligned function . . . . .	122
	B2.3	AddrIsGranuleAligned function . . . . .	123
	B2.4	AddrIsProtected function . . . . .	123
	B2.5	AddrIsRttLevelAligned function . . . . .	123
	B2.6	AddrRangelsProtected function . . . . .	123
	B2.7	AlignDownToRttLevel function . . . . .	123
	B2.8	AlignUpToRttLevel function . . . . .	124
	B2.9	CurrentRealm function . . . . .	124
	B2.10	CurrentRec function . . . . .	124
	B2.11	Equal function . . . . .	124
	B2.12	Gicv3ConfigIsValid function . . . . .	125
	B2.13	Granule function . . . . .	125
	B2.14	MinAddress function . . . . .	125
	B2.15	MpidrEqual function . . . . .	126
	B2.16	MpidrUsed function . . . . .	126
	B2.17	PalsDelegable function . . . . .	126

B2.18	PsciReturnCodeEncode function . . . . .	126
B2.19	PsciReturnCodePermitted function . . . . .	126
B2.20	ReadMemory function . . . . .	127
B2.21	Realm function . . . . .	127
B2.22	RealmConfig function . . . . .	127
B2.23	RealmHostCall function . . . . .	127
B2.24	RealmsLive function . . . . .	127
B2.25	RealmParams function . . . . .	128
B2.26	RealmParamsSupported function . . . . .	128
B2.27	Rec function . . . . .	128
B2.28	RecAuxAlias function . . . . .	128
B2.29	RecAuxAligned function . . . . .	129
B2.30	RecAuxCount function . . . . .	129
B2.31	RecAuxEqual function . . . . .	129
B2.32	RecAuxSort function . . . . .	129
B2.33	RecAuxStateEqual function . . . . .	130
B2.34	RecAuxStates function . . . . .	130
B2.35	RecFromMpidr function . . . . .	130
B2.36	RecIndex function . . . . .	130
B2.37	RecParams function . . . . .	131
B2.38	RecRipasChangeResponse function . . . . .	131
B2.39	RecRun function . . . . .	131
B2.40	RemExtend function . . . . .	131
B2.41	ResultEqual function . . . . .	132
B2.42	RimExtendData function . . . . .	132
B2.43	RimExtendRec function . . . . .	132
B2.44	RimExtendRipas function . . . . .	132
B2.45	RimExtendRipasForEntry function . . . . .	133
B2.46	RimInit function . . . . .	133
B2.47	RmiRealmParamsIsValid function . . . . .	133
B2.48	Rtt function . . . . .	133
B2.49	RttAllEntriesContiguous function . . . . .	133
B2.50	RttAllEntriesRipas function . . . . .	134
B2.51	RttAllEntriesState function . . . . .	134
B2.52	RttConfigsValid function . . . . .	134
B2.53	RttDescriptorIsValidForUnprotected function . . . . .	134
B2.54	RttEntriesInRangeRipas function . . . . .	134
B2.55	RttEntry function . . . . .	135
B2.56	RttEntryFromDescriptor function . . . . .	135
B2.57	RttEntryIndex function . . . . .	135
B2.58	RttEntryState function . . . . .	135
B2.59	RttFold function . . . . .	136
B2.60	RttIsHomogeneous function . . . . .	136
B2.61	RttIsLive function . . . . .	136
B2.62	RttLevellsBlockOrPage function . . . . .	136
B2.63	RttLevellsStarting function . . . . .	136
B2.64	RttLevellsValid function . . . . .	137
B2.65	RttLevelSize function . . . . .	137
B2.66	RttsAllProtectedEntriesRipas function . . . . .	137
B2.67	RttsAllProtectedEntriesState function . . . . .	137
B2.68	RttsAllUnprotectedEntriesState function . . . . .	137
B2.69	RttsGranuleState function . . . . .	138
B2.70	RttSkipEntriesUnlessRipas function . . . . .	138
B2.71	RttSkipEntriesUnlessState function . . . . .	138
B2.72	RttSkipEntriesWithRipas function . . . . .	138

B2.73	RttSkipNonLiveEntries function . . . . .	139
B2.74	RttsStateEqual function . . . . .	139
B2.75	RttWalk function . . . . .	140
B2.76	ToAddress function . . . . .	140
B2.77	ToBits64 function . . . . .	140
B2.78	VmidIsFree function . . . . .	140
B2.79	VmidIsValid function . . . . .	141

## Chapter B3

### Realm Management Interface

B3.1	RMI version . . . . .	143
B3.2	RMI command return codes . . . . .	143
B3.3	RMI commands . . . . .	144
B3.3.1	RMI_DATA_CREATE command . . . . .	145
B3.3.2	RMI_DATA_CREATE_UNKNOWN command . . . . .	148
B3.3.3	RMI_DATA_DESTROY command . . . . .	151
B3.3.4	RMI_FEATURES command . . . . .	154
B3.3.5	RMI_GRANULE_DELEGATE command . . . . .	155
B3.3.6	RMI_GRANULE_UNDELEGATE command . . . . .	157
B3.3.7	RMI_PSCI_COMPLETE command . . . . .	159
B3.3.8	RMI_REALM_ACTIVATE command . . . . .	163
B3.3.9	RMI_REALM_CREATE command . . . . .	165
B3.3.10	RMI_REALM_DESTROY command . . . . .	170
B3.3.11	RMI_REC_AUX_COUNT command . . . . .	172
B3.3.12	RMI_REC_CREATE command . . . . .	174
B3.3.13	RMI_REC_DESTROY command . . . . .	179
B3.3.14	RMI_REC_ENTER command . . . . .	181
B3.3.15	RMI_RTT_CREATE command . . . . .	184
B3.3.16	RMI_RTT_DESTROY command . . . . .	187
B3.3.17	RMI_RTT_FOLD command . . . . .	191
B3.3.18	RMI_RTT_INIT_RIPAS command . . . . .	194
B3.3.19	RMI_RTT_MAP_UNPROTECTED command . . . . .	197
B3.3.20	RMI_RTT_READ_ENTRY command . . . . .	200
B3.3.21	RMI_RTT_SET_RIPAS command . . . . .	203
B3.3.22	RMI_RTT_UNMAP_UNPROTECTED command . . . . .	206
B3.3.23	RMI_VERSION command . . . . .	209
B3.4	RMI types . . . . .	210
B3.4.1	RmiCommandReturnCode type . . . . .	210
B3.4.2	RmiDataFlags type . . . . .	210
B3.4.3	RmiDataMeasureContent type . . . . .	211
B3.4.4	RmiEmulatedMmio type . . . . .	211
B3.4.5	RmiFeature type . . . . .	211
B3.4.6	RmiFeatureRegister0 type . . . . .	212
B3.4.7	RmiHashAlgorithm type . . . . .	213
B3.4.8	RmiInjectSea type . . . . .	213
B3.4.9	RmiInterfaceVersion type . . . . .	213
B3.4.10	RmiPmuOverflowStatus type . . . . .	214
B3.4.11	RmiRealmFlags type . . . . .	214
B3.4.12	RmiRealmParams type . . . . .	215
B3.4.13	RmiRecCreateFlags type . . . . .	216
B3.4.14	RmiRecEnter type . . . . .	216
B3.4.15	RmiRecEnterFlags type . . . . .	218
B3.4.16	RmiRecExit type . . . . .	218
B3.4.17	RmiRecExitReason type . . . . .	221
B3.4.18	RmiRecMpidr type . . . . .	221
B3.4.19	RmiRecParams type . . . . .	222

B3.4.20	RmiRecRun type	223
B3.4.21	RmiRecRunnable type	223
B3.4.22	RmiResponse type	224
B3.4.23	RmiRipas type	224
B3.4.24	RmiRttEntryState type	224
B3.4.25	RmiStatusCode type	225
B3.4.26	RmiTrap type	225

## Chapter B4

### Realm Services Interface

B4.1	RSI version	228
B4.2	RSI command return codes	228
B4.3	RSI commands	229
B4.3.1	RSI_ATTESTATION_TOKEN_CONTINUE command	230
B4.3.2	RSI_ATTESTATION_TOKEN_INIT command	232
B4.3.3	RSI_HOST_CALL command	234
B4.3.4	RSI_IPA_STATE_GET command	236
B4.3.5	RSI_IPA_STATE_SET command	238
B4.3.6	RSI_MEASUREMENT_EXTEND command	240
B4.3.7	RSI_MEASUREMENT_READ command	242
B4.3.8	RSI_REALM_CONFIG command	244
B4.3.9	RSI_VERSION command	246
B4.4	RSI types	247
B4.4.1	RsiCommandReturnCode type	247
B4.4.2	RsiHashAlgorithm type	247
B4.4.3	RsiHostCall type	248
B4.4.4	RsiInterfaceVersion type	249
B4.4.5	RsiRealmConfig type	249
B4.4.6	RsiResponse type	250
B4.4.7	RsiRipas type	250
B4.4.8	RsiRipasChangeDestroyed type	251
B4.4.9	RsiRipasChangeFlags type	251

## Chapter B5

### Power State Control Interface

B5.1	PSCI overview	253
B5.2	PSCI version	253
B5.3	PSCI commands	254
B5.3.1	PSCI_AFFINITY_INFO command	255
B5.3.2	PSCI_CPU_OFF command	257
B5.3.3	PSCI_CPU_ON command	258
B5.3.4	PSCI_CPU_SUSPEND command	260
B5.3.5	PSCI_FEATURES command	261
B5.3.6	PSCI_SYSTEM_OFF command	263
B5.3.7	PSCI_SYSTEM_RESET command	264
B5.3.8	PSCI_VERSION command	265
B5.4	PSCI types	266
B5.4.1	PsciInterfaceVersion type	266
B5.4.2	PsciReturnCode type	266

## Part C Types

### Chapter C1

#### RMM types

C1.1	RmmGranule type	269
C1.2	RmmGranuleState type	269
C1.3	RmmHashAlgorithm type	270

C1.4	RmmHostCallPending type	270
C1.5	RmmMeasurementDescriptorData type	270
C1.6	RmmMeasurementDescriptorRec type	271
C1.7	RmmMeasurementDescriptorRipas type	271
C1.8	RmmPhysicalAddressSpace type	272
C1.9	RmmPsciPending type	272
C1.10	RmmRealm type	273
C1.11	RmmRealmMeasurement type	273
C1.12	RmmRealmState type	273
C1.13	RmmRec type	274
C1.14	RmmRecAttestState type	274
C1.15	RmmRecEmulatableAbort type	275
C1.16	RmmRecFlags type	275
C1.17	RmmRecResponse type	275
C1.18	RmmRecRunnable type	276
C1.19	RmmRecState type	276
C1.20	RmmRipas type	276
C1.21	RmmRipasChangeDestroyed type	276
C1.22	RmmRtt type	277
C1.23	RmmRttEntry type	277
C1.24	RmmRttEntryState type	277
C1.25	RmmRttWalkResult type	278
C1.26	RmmSystemRegisters type	278

## Chapter C2

### Generic types

C2.1	Address type	279
C2.2	BitsN type	279
C2.3	IntN type	280
C2.4	UIntN type	280

## Part D Usage

### Chapter D1

#### Flows

D1.1	Granule delegation flows	283
D1.1.1	Granule delegation flow	283
D1.1.2	Granule undelegation flow	283
D1.2	Realm lifecycle flows	285
D1.2.1	Realm creation flow	285
D1.2.2	Realm Translation Table creation flow	285
D1.2.3	Initialize memory of New Realm flow	286
D1.2.4	REC creation flow	288
D1.2.5	Realm destruction flow	290
D1.3	Realm exception model flows	292
D1.3.1	Realm entry and exit flow	292
D1.3.2	Host call flow	292
D1.3.3	REC exit due to Data Abort fault flow	293
D1.3.4	MMIO emulation flow	294
D1.4	PSCI flows	296
D1.4.1	PSCI_CPU_ON flow	296
D1.5	Realm memory management flows	299
D1.5.1	Add memory to Active Realm flow	299
D1.5.2	NS memory flow	299
D1.5.3	RIPAS change flow	300
D1.6	Realm interrupts and timers flows	302

D1.6.1	Interrupt flow . . . . .	302
D1.6.2	Timer interrupt delivery flow . . . . .	302
D1.7	Realm attestation flows . . . . .	304
D1.7.1	Attestation token generation flow . . . . .	304
D1.7.2	Handling interrupts during attestation token generation flow . . . . .	304

## Chapter D2

### Realm shared memory protocol

D2.1	Realm shared memory protocol description . . . . .	307
D2.2	Realm shared memory protocol flow . . . . .	307

## Glossary

## **Preface**



# Conventions

## Typographical conventions

The typographical conventions are:

*italic*

Introduces special terminology, and denotes citations.

`monospace`

Used for pseudocode and source code examples.

Also used in the main text for instruction mnemonics and for references to other items appearing in pseudocode and source code examples.

**SMALL CAPITALS**

Used for some common terms such as IMPLEMENTATION DEFINED.

Used for a few terms that have specific technical meanings, and are included in the Glossary.

Red text

Indicates an open issue.

Blue text

Indicates a link. This can be

- A cross-reference to another location within the document
- A URL, for example <http://developer.arm.com>

## Numbers

Numbers are normally written in decimal. Binary numbers are preceded by 0b, and hexadecimal numbers by 0x. In both cases, the prefix and the associated value are written in a monospace font, for example 0xFFFF0000. To improve readability, long numbers can be written with an underscore separator between every four characters, for example 0xFFFF\_0000\_0000\_0000. Ignore any underscores when interpreting the value of a number.

## Pseudocode descriptions

This book uses a form of pseudocode to provide precise descriptions of the specified functionality. This pseudocode is written in a monospace font. The pseudocode language is described in the Arm Architecture Reference Manual.

## Addresses

Unless otherwise stated, the term *address* in this specification refers to a physical address.

## Rules-based writing

This specification consists of a set of individual *content items*. A content item is classified as one of the following:

- Declaration
- Rule
- Goal
- Information
- Rationale
- Implementation note
- Software usage

Declarations and Rules are normative statements. An implementation that is compliant with this specification must conform to all Declarations and Rules in this specification that apply to that implementation.

Declarations and Rules must not be read in isolation. Where a particular feature is specified by multiple Declarations and Rules, these are generally grouped into sections and subsections that provide context. Where appropriate, these sections begin with a short introduction.

Arm strongly recommends that implementers read *all* chapters and sections of this document to ensure that an implementation is compliant.

Content items other than Declarations and Rules are informative statements. These are provided as an aid to understanding this specification.

### Content item identifiers

A content item may have an associated identifier which is unique among content items in this specification.

After this specification reaches beta status, a given content item has the same identifier across subsequent versions of the specification.

### Content item rendering

In this document, a content item is rendered with a token of the following format in the left margin: *Liiii*

- *L* is a label that indicates the content class of the content item.
- *iiii* is the identifier of the content item.

### Content item classes

#### Declaration

A Declaration is a statement that does one or more of the following:

- Introduces a concept
- Introduces a term
- Describes the structure of data
- Describes the encoding of data

A Declaration does not describe behaviour.

A Declaration is rendered with the label *D*.

## Rule

A Rule is a statement that describes the behaviour of a compliant implementation.

A Rule explains what happens in a particular situation.

A Rule does not define concepts or terminology.

A Rule is rendered with the label *R*.

## Goal

A Goal is a statement about the purpose of a set of rules.

A Goal explains why a particular feature has been included in the specification.

A Goal is comparable to a “business requirement” or an “emergent property.”

A Goal is intended to be upheld by the logical conjunction of a set of rules.

A Goal is rendered with the label *G*.

## Information

An Information statement provides information and guidance as an aid to understanding the specification.

An Information statement is rendered with the label *I*.

## Rationale

A Rationale statement explains why the specification was specified in the way it was.

A Rationale statement is rendered with the label *X*.

## Implementation note

An Implementation note provides guidance on implementation of the specification.

An Implementation note is rendered with the label *U*.

## Software usage

A Software usage statement provides guidance on how software can make use of the features defined by the specification.

A Software usage statement is rendered with the label *S*.

## Additional reading

This section lists publications by Arm and by third parties.

See Arm Developer (<http://developer.arm.com>) for access to Arm documentation.

- [1] *Introducing Arm CCA*. (ARM DEN 0125) Arm Limited.
- [2] *Arm Architecture Reference Manual Supplement, The Realm Management Extension (RME), for Armv9-A*. (ARM DDI 0615 A.d) Arm Ltd.
- [3] *Arm Architecture Reference Manual for A-Profile architecture*. (ARM DDI 0487 I.a) Arm Ltd.
- [4] *Arm CCA Security model*. (ARM DEN 0096) Arm Limited.
- [5] *Arm Generic Interrupt Controller (GIC) Architecture Specification version 3 and version 4*. (ARM IHI 0069 G) Arm Ltd.
- [6] *Concise Binary Object Representation (CBOR)*.
- [7] *CBOR Object Signing and Encryption (COSE)*.
- [8] *Entity Attestation Token (EAT)*.
- [9] *Concise Data Definition Language (CDDL)*.
- [10] *IANA Hash Function Textual Names*.
- [11] *SEC 1: Elliptic Curve Cryptography, version 2.0*.
- [12] *RME system architecture spec*. (ARM DEN 0129) Arm Ltd.
- [13] *Arm SMC Calling Convention*. (ARM DEN 0028 D) Arm Ltd.
- [14] *Arm Specification Language Reference Manual*. (ARM DDI 0612) Arm Ltd.
- [15] *Secure Hash Standard (SHS)*.
- [16] *Arm Power State Coordination Interface (PSCI)*. (ARM DEN 0022 D.b) Arm Ltd.

# Feedback

Arm welcomes feedback on its documentation.

## Feedback on this book

If you have any comments or suggestions for additions and improvements, create a ticket at <https://support.developer.arm.com>.  
As part of the ticket, include:

- The title (Realm Management Monitor specification).
- The number (DEN0137 1.0-eac3).
- The section name(s) to which your comments refer.
- The page number(s) to which your comments apply.
- The rule identifier(s) to which your comments apply, if applicable.
- A concise explanation of your comments.

Arm also welcomes general suggestions for additions and improvements.

---

### Note

Arm tests PDFs only in Adobe Acrobat and Acrobat Reader, and cannot guarantee the appearance or behavior of any document when viewed with any other PDF reader.

---

## Open issues

The following table lists known open issues in this version of the document.

Key	Description
-----	-------------

## **Part A**

### **Architecture**

## Chapter A1

### Overview

The RMM is a software component which forms part of a system which implements the Arm Confidential Compute Architecture (Arm CCA). Arm CCA is an architecture which provides protected execution environments called *Realms*.

The threat model which Arm CCA is designed to address is described in *Introducing Arm CCA* [1].

The hardware architecture of Arm CCA is called the Realm Management Extension (RME), and is described in *Arm Architecture Reference Manual Supplement, The Realm Management Extension (RME), for Armv9-A* [2].

#### A1.1 Confidential computing

The Armv8-A architecture (*Arm Architecture Reference Manual for A-Profile architecture* [3]) includes mechanisms that establish a privilege hierarchy. Software operating at higher privilege levels is responsible for managing the resources (principally memory and processor cycles) that are used by entities at lower privilege levels.

Prior to Arm CCA, resource management was coupled with a right of access. That is, a resource that is managed by a higher-privileged entity is also accessible by it. A *Realm* is a protected execution environment for which this coupling is broken, so that the right to manage resources is separated from the right to access those resources.

The purpose of a Realm is to provide to the Realm owner an environment for confidential computing, without requiring the Realm owner to trust the software components that manage the resources used by the Realm.

Construction of a Realm, and allocation of resources to a Realm at runtime, are the responsibility of the Virtual Machine Monitor (VMM). In this specification, the term *Host* is used to refer to the VMM.

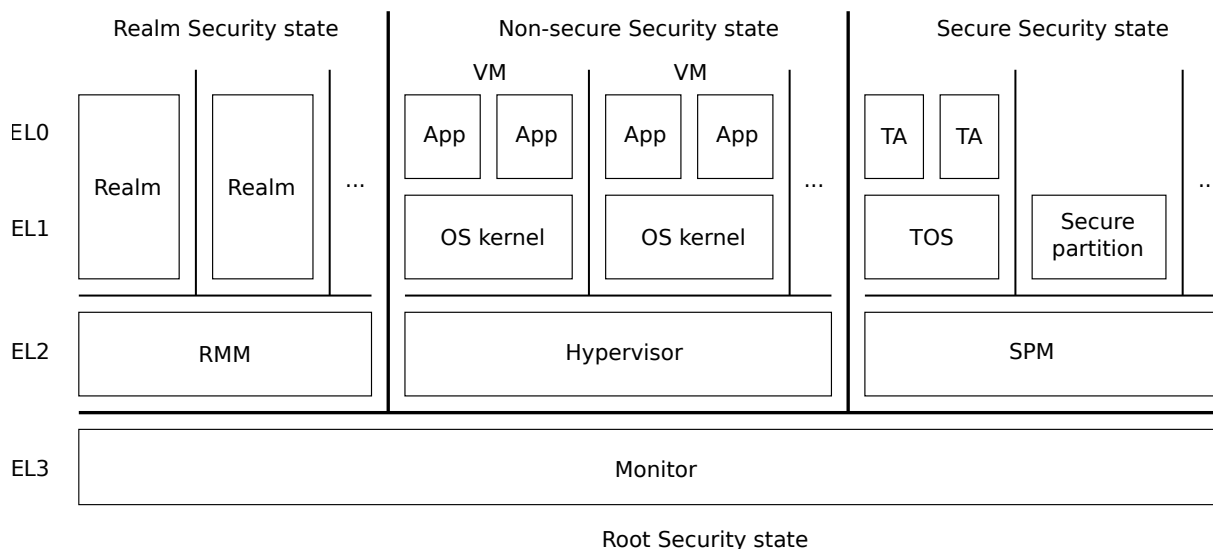
See also:

- [A2.1 Realm](#)



## A1.2 System software components

The system software architecture of Arm CCA is summarised in the following figure.



**Figure A1.1: System software architecture**

The components shown in the diagram are listed below.

Component	Description
Monitor	The most privileged software component, which is responsible for switching between the Security states used at EL2, EL1 and EL0.
Realm	A protected execution environment.
Realm Management Monitor (RMM)	The software component which is responsible for the management of Realms.
Virtual Machine (VM)	An execution environment within which an operating system can run. Note that a Realm is a VM which executes in the Realm security state.
Hypervisor	The software component which is responsible for the management of VMs.
Secure Partition Manager (SPM)	The software component which is responsible for the management of Secure Partitions.
Trusted OS (TOS)	An operating system which runs in a Secure Partition.
Trusted Application (TA)	An application hosted by a TOS.

## A1.3 Realm Management Monitor

The Realm Management Monitor (RMM) is the system component that is responsible for the management of Realms.

The responsibilities of the RMM are to:

- Provide services that allow the Host to create, populate, execute and destroy Realms.
- Provide services that allow the initial configuration and contents of a Realm to be attested.
- Protect the confidentiality and integrity of Realm state during the lifetime of the Realm.
- Protect the confidentiality of Realm state during and following destruction of the Realm.

The RMM exposes the following interfaces, which are accessed via SMC instructions, to the Host:

- The *Realm Management Interface* (RMI), which provides services for the creation, population, execution and destruction of Realms.

The RMM exposes the following interfaces, which are accessed via SMC instructions, to Realms:

- The *Realm Services Interface* (RSI), which provides services used to manage resources allocated to the Realm, and to request an attestation report.
- The *Power State Coordination Interface* (PSCI), which provides services used to control power states of VPEs within a Realm. Note that the HVC conduit for PSCI is not supported for Realms.

The RMM operates by manipulating data structures which are stored in memory accessible only to the RMM.

See also:

- [Chapter B3 Realm Management Interface](#)
- [Chapter B4 Realm Services Interface](#)
- [Chapter B5 Power State Control Interface](#)

## Chapter A2

# Concepts

This chapter introduces the following concepts which are central to the RMM architecture:

- [A2.1 \*Realm\*](#)
- [A2.2 \*Granule\*](#)
- [A2.3 \*Realm Execution Context\*](#)

## A2.1 Realm

This section describes the concept of a Realm.

### A2.1.1 Overview

**D<sub>DLRSR</sub>** A *Realm* is an execution environment which is protected from agents in the Non-secure and Secure Security states, and from other Realms.

### A2.1.2 Realm execution environment

**I<sub>LQYLY</sub>** The execution environment of a Realm is an EL0 + EL1 environment, as described in *Arm Architecture Reference Manual for A-Profile architecture* [3].

#### A2.1.2.1 Realm registers

**R<sub>NJHQK</sub>** On first entry to a Realm VPE, PE state is initialized according to “PE state on reset to AArch64 state” in *Arm Architecture Reference Manual for A-Profile architecture* [3], except for GPR and PC values which are specified by the Host during Realm creation.

**G<sub>ZFCQX</sub>** Confidentiality is guaranteed for a Realm VPE’s general purpose and SIMD / floating point registers.

**G<sub>QHZCS</sub>** Confidentiality is guaranteed for other Realm VPE register state (including stack pointer, program counter and EL0 / EL1 system registers).

**G<sub>XRMHP</sub>** Integrity is guaranteed for a Realm VPE’s general purpose and SIMD / floating point registers.

**G<sub>YKRWG</sub>** Integrity is guaranteed for other Realm VPE register state (including stack pointer, program counter and EL0 / EL1 system registers).

**I<sub>GPGFB</sub>** A Realm can use a Host call to pass arguments to the Host and receive results from the Host.

See also:

- [A2.3 Realm Execution Context](#)
- [A4.5 Host call](#)
- [B3.3.9 RMI\\_REALM\\_CREATE command](#)

#### A2.1.2.2 Realm memory

**I<sub>TQMMZ</sub>** A Realm is able to determine whether a given IPA is *protected* or *unprotected*.

**G<sub>LQFQH</sub>** Confidentiality is guaranteed for memory contents accessed via a protected address. Informally, this means that a change to the contents of such a memory location is not observable by any agent outside the *CCA platform*.

**G<sub>QMLCJ</sub>** Integrity is guaranteed for memory contents accessed via a protected address. Informally, this means that the Realm does not observe the contents of the location to change unless the Realm itself has either written a different value to the location, or provided consent to the RMM for integrity of the location to be violated.

See also:

- [A5.2.1 Realm IPA space](#)

### A2.1.2.3 Realm processor features

**R<sub>JGHHYJ</sub>** The value returned to a Realm from reading a feature register is architecturally valid and describes the set of features which are present in the Realm's execution environment.

**I<sub>KKBDP</sub>** The RMM may suppress a feature which is supported by the underlying hardware platform, if exposing that feature to a Realm could lead to a security vulnerability.

See also:

- [A3.1 Realm feature discovery and selection](#)

### A2.1.2.4 IMPDEF system registers

**R<sub>FQCKH</sub>** A Realm read from or write to an IMPLEMENTATION DEFINED system register causes an Unknown exception taken to the Realm.

## A2.1.3 Realm attributes

This section describes the attributes of a Realm.

**D<sub>JSGFY</sub>** A *Realm attribute* is a property of a Realm whose value can be observed or modified either by the Host or by the Realm.

**I<sub>TTDVX</sub>** An example of a way in which a Realm attribute may be observable is the outcome of an RMM command.

**D<sub>MHJCK</sub>** The attributes of a Realm are summarized in the following table.

Name	Type	Description
ipa_width	UInt8	IPA width in bits
measurements	RmmRealmMeasurement[5]	Realm measurements
hash_algo	RmmHashAlgorithm	Algorithm used to compute Realm measurements
rec_index	UInt64	Index of next REC to be created
rtt_base	Address	Realm Translation Table base address
rtt_level_start	Int64	RTT starting level
rtt_num_start	UInt64	Number of physically contiguous starting level RTTs
state	RmmRealmState	Lifecycle state
vmid	Bits16	Virtual Machine Identifier
rpv	Bits512	Realm Personalization Value

**D<sub>MGGPT</sub>** A *Realm Initial Measurement* (RIM) is a measurement of the configuration and contents of a Realm at the time of activation.

**D<sub>GRFCS</sub>** A *Realm Extensible Measurement* (REM) is a measurement value which can be extended during the lifetime of a Realm.

**I<sub>FMPYL</sub>** Attributes of a Realm include an array of measurement values. The first entry in this array is a RIM. The remaining entries in this array are REMs.

**X<sub>DNDKV</sub>** During Realm creation, the Host provides ipa\_width, rtt\_level\_start and rtt\_num\_start values as Realm parameters. According to the VMSA, the rtt\_num\_start value is architecturally defined as a function of the ipa\_width and rtt\_level\_start values. It would therefore have been possible to design the Realm creation interface such that the

Host provided only the `ipa_width` and `rtt_level_start` values. However, this would potentially allow a Realm to be successfully created, but with a configuration which did not match the Host's intent. For this reason, it was decided that the Host should specify all three values explicitly, and that Realm creation should fail if the values are not consistent. See *Arm Architecture Reference Manual for A-Profile architecture* [3] for further details.

`I_QRVTT` The VMID of a Realm is chosen by the Host. The VMID must be within the range supported by the hardware platform. The RMM ensures that every Realm on the system has a unique VMID.

`D_FTWBK` A *Realm Personalization Value* (RPV) is provided by the Host, to distinguish between Realms which have the same Realm Initial Measurement, but different behavior.

`S_FCNBF` Possible uses of the RPV include:

- A GUID
- Hash of Realm Owner public key
- Hash of a “personalisation document” which is provided to the Realm via a side-band (for example, via NS memory) and contains configuration information used by Realm software.

`I_ZFSWC` The RMM treats the RPV as an opaque value.

`I_BFSRK` The RPV is included in the Realm attestation report as a separate claim.

See also:

- [A2.1.5 Realm lifecycle](#)
- [A2.3 Realm Execution Context](#)
- [A3.1.2 Realm LPA2 and IPA width](#)
- [A5.2.1 Realm IPA space](#)
- [A5.5 Realm Translation Table](#)
- [A7.1 Realm measurements](#)
- [A7.2.3.1.2 Realm Personalization Value claim](#)
- [C1.10 RmmRealm type](#)

## A2.1.4 Realm liveness

`D_WTXTJ` *Realm liveness* is a property which means that there exists one or more Granules, other than the RD and the starting level RTTs, which are owned by the Realm.

`I_PVPQB` If a Realm is live, it cannot be destroyed.

`D_PCKRN` A Realm is *live* if any of the following is true:

- The number of RECs owned by the Realm is not zero
- A starting level RTT of the Realm is live

`I_VKKPJ` If a Realm owns a non-zero number of Data Granules, this implies that it has a starting level RTT which is live, and therefore that the Realm itself is live.

See also:

- [A2.1.5 Realm lifecycle](#)
- [A2.2.2 Granule ownership](#)
- [A2.2.3 Granule lifecycle](#)
- [A2.3 Realm Execution Context](#)
- [A5.5.8 RTTE liveness and RTT liveness](#)
- [B2.24 RealmIsLive function](#)
- [B3.3.10 RMI\\_REALM\\_DESTROY command](#)

## A2.1.5 Realm lifecycle

See also:

- [Chapter A3 Realm creation](#)
- [D1.2 Realm lifecycle flows](#)

### A2.1.5.1 States

D<sub>GDQPJ</sub>

The states of a Realm are listed below.

State	Description
NEW	Under construction. Not eligible for execution.
ACTIVE	Eligible for execution.
SYSTEM_OFF	System has been turned off. Not eligible for execution.

### A2.1.5.2 State transitions

I<sub>RRHFG</sub>

Permitted Realm state transitions are shown in the following table. The rightmost column lists the events which can cause the corresponding state transition.

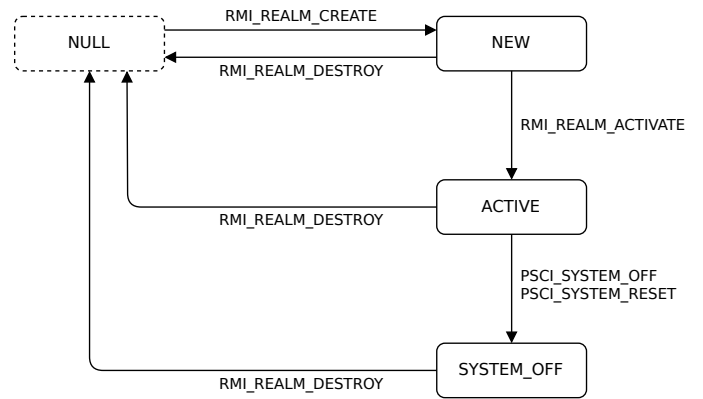
A transition from the pseudo-state *NULL* represents creation of a Realm object. A transition to the pseudo-state *NULL* represents destruction of a Realm object.

From state	To state	Events
<i>NULL</i>	NEW	<a href="#">RMI_REALM_CREATE</a>
NEW	<i>NULL</i>	<a href="#">RMI_REALM_DESTROY</a>
ACTIVE	<i>NULL</i>	<a href="#">RMI_REALM_DESTROY</a>
SYSTEM_OFF	<i>NULL</i>	<a href="#">RMI_REALM_DESTROY</a>
NEW	ACTIVE	<a href="#">RMI_REALM_ACTIVATE</a>
ACTIVE	SYSTEM_OFF	<a href="#">PSCI_SYSTEM_OFF</a> <a href="#">PSCI_SYSTEM_RESET</a>

I<sub>YCPWW</sub>

Permitted Realm state transitions are shown in the following figure. Each arc is labeled with the events which can cause the corresponding state transition.

A transition from the pseudo-state *NULL* represents creation of an RD. A transition to the pseudo-state *NULL* represents destruction of an RD.



**Figure A2.1: Realm state transitions**

See also:

- [B3.3.8 RMI\\_REALM\\_ACTIVATE command](#)
- [B3.3.9 RMI\\_REALM\\_CREATE command](#)
- [B3.3.10 RMI\\_REALM\\_DESTROY command](#)
- [B5.3.6 PSCI\\_SYSTEM\\_OFF command](#)
- [B5.3.7 PSCI\\_SYSTEM\\_RESET command](#)

## A2.1.6 Realm parameters

D<sub>TGMVZ</sub>

A *Realm parameter* is a value which is provided by the Host during Realm creation.

See also:

- [A2.1.3 Realm attributes](#)
- [A3.1 Realm feature discovery and selection](#)
- [B2.25 RealmParams function](#)
- [B3.3.9 RMI\\_REALM\\_CREATE command](#)
- [B3.4.12 RmiRealmParams type](#)

## A2.1.7 Realm Descriptor

D<sub>TNSBY</sub>

A *Realm Descriptor* (RD) is an RMM data structure which stores attributes of a Realm.

D<sub>GKWX</sub>

The size of an RD is one Granule.

See also:

- [A2.1.3 Realm attributes](#)
- [A2.2.3 Granule lifecycle](#)



## A2.2 Granule

This section describes the concept of a Granule.

**D<sub>NBXXX</sub>** A *Granule* is a unit of physical memory whose size is 4KB.

**I<sub>DJGZW</sub>** A Granule may be used to store one of the following:

- Code or data used by the Host
- Code or data used by software in the Secure Security state
- Code or data used by a Realm
- Data used by the RMM to manage a Realm

The use of a Granule is reflected in its lifecycle state.

**D<sub>ZVRXC</sub>** A Granule is *delegable* if it can be delegated by the Host for use by the RMM or by a Realm.

**U<sub>KHKLP</sub>** In a typical implementation, all memory which is presented to the Host as RAM is delegable. Examples of non-delegable memory may include the following:

- Memory which is carved out for use by the Root world, the RMM or the Secure world
- Device memory

See also:

- [A2.2.1 Granule attributes](#)
- [A2.2.3 Granule lifecycle](#)

### A2.2.1 Granule attributes

This section describes the attributes of a Granule.

**D<sub>JPBBC</sub>** A *Granule attribute* is a property of a Granule whose value can be observed or modified either by the Host or by a Realm.

**I<sub>WVXGK</sub>** Examples of ways in which a Granule attribute may be observable include the outcome of an RMM command, and whether a memory access generates a fault.

**D<sub>DVMRF</sub>** The attributes of a Granule are summarized in the following table.

Name	Type	Description
pas	<a href="#">RmmPhysicalAddressSpace</a>	Physical Address Space
state	<a href="#">RmmGranuleState</a>	Lifecycle state

**D<sub>QZNGW</sub>** The set of Physical Address Spaces is:

- NS
- REALM
- OTHER

**X<sub>LQZFB</sub>** The RMM cannot distinguish whether a Granule is in the Secure or Root PAS, so these two values are combined as OTHER.

**I<sub>YYVSN</sub>** If the state of a Granule is not UNDELEGATED then the PAS of the Granule is REALM.

**I<sub>BQDWY</sub>** If the state of a Granule is UNDELEGATED then the PAS of the Granule is not REALM.

**I<sub>MPGJV</sub>** If the state of a Granule is UNDELEGATED then the RMM does not prevent the PAS of the Granule from being changed by another agent to any value except REALM.

**D<sub>VRSKZ</sub>** An NS Granule is a Granule whose PAS is NS.

See also:

- [A2.1 Realm](#)
- [A2.1.7 Realm Descriptor](#)
- [A2.2.3 Granule lifecycle](#)
- [C1.1 RmmGranule type](#)

## A2.2.2 Granule ownership

**I<sub>DMVQM</sub>** A Granule whose state is neither UNDELEGATED nor DELEGATED is owned by a Realm.

**I<sub>PRNTM</sub>** The owner of a Granule is identified by the address of a Realm Descriptor (RD).

**I<sub>ZXBZM</sub>** For a Granule whose state is RD, the ownership relation is recursive: the owning Realm is identified by the address of the RD itself.

**I<sub>TYHTD</sub>** A Granule whose state is RTT is one of the following:

- A starting level RTT. The address of this RTT is stored in the RD of the owning Realm.
- A non-starting level RTT. The address of this RTT is stored in its parent RTT, in an RTT entry whose state is TABLE. Recursively following the parent relationship leads to the RD of the owning Realm.

**I<sub>QCNRM</sub>** A Granule whose state is DATA is mapped at a Protected IPA, in an RTT entry whose state is ASSIGNED. The Realm which owns the RTT is the owner of the DATA Granule.

**I<sub>HHPVB</sub>** A REC has an “owner” attribute which points to the RD of the owning Realm.

**X<sub>NDNHG</sub>** A REC is not mapped at a Protected IPA. Its ownership therefore needs to be recorded explicitly.

See also:

- [A2.1 Realm](#)
- [A2.1.7 Realm Descriptor](#)
- [A2.3 Realm Execution Context](#)
- [A5.2.1 Realm IPA space](#)
- [A5.5 Realm Translation Table](#)
- [B3.3.1 RMI\\_DATA\\_CREATE command](#)
- [B3.3.2 RMI\\_DATA\\_CREATE\\_UNKNOWN command](#)
- [B3.3.12 RMI\\_REC\\_CREATE command](#)
- [B3.3.15 RMI\\_RTT\\_CREATE command](#)

## A2.2.3 Granule lifecycle

### A2.2.3.1 States

**D<sub>MPLGT</sub>** The states of a Granule are listed below.

State	Description
UNDELEGATED	Not delegated for use by the RMM.
DELEGATED	Delegated for use by the RMM.
RD	Realm Descriptor.
REC	Realm Execution Context.
REC_AUX	Realm Execution Context auxiliary Granule.

State	Description
DATA	Realm code or data.
RTT	Realm Translation Table.

### A2.2.3.2 State transitions

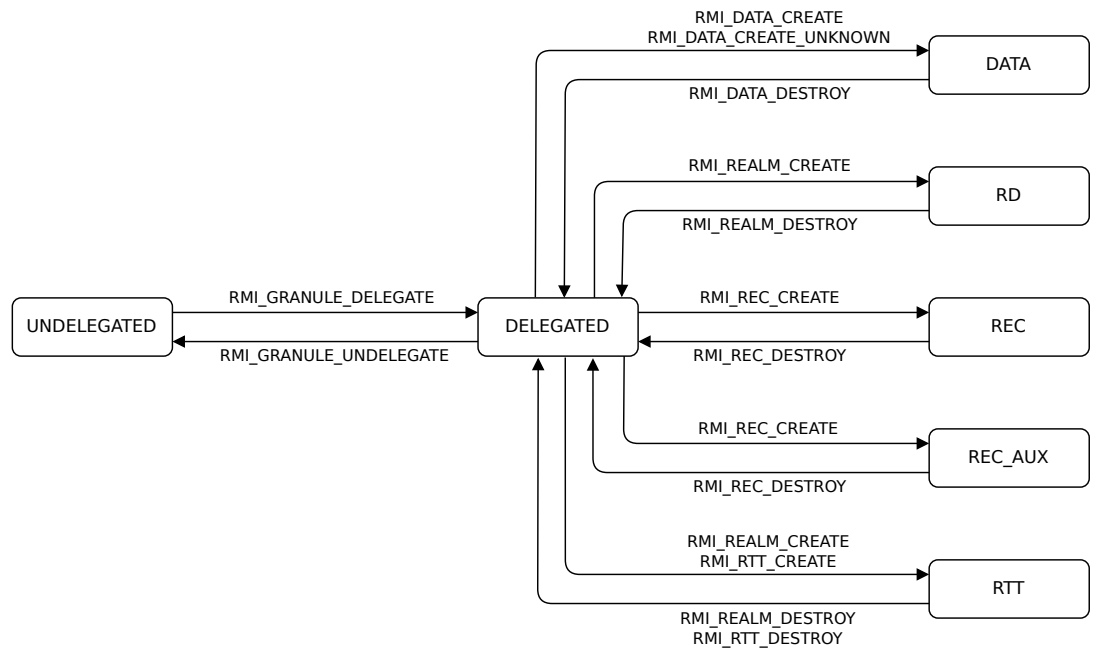
I\_ZJBTT

Permitted Granule state transitions are shown in the following table. The rightmost column lists the events which can cause the corresponding state transition.

From state	To state	Events
UNDELEGATED	DELEGATED	<a href="#">RMI_GRANULE_DELEGATE</a>
DELEGATED	UNDELEGATED	<a href="#">RMI_GRANULE_UNDELEGATE</a>
DELEGATED	RD	<a href="#">RMI_REALM_CREATE</a>
RD	DELEGATED	<a href="#">RMI_REALM_DESTROY</a>
DELEGATED	DATA	<a href="#">RMI_DATA_CREATE</a> <a href="#">RMI_DATA_CREATE_UNKNOWN</a>
DATA	DELEGATED	<a href="#">RMI_DATA_DESTROY</a>
DELEGATED	REC	<a href="#">RMI_REC_CREATE</a>
REC	DELEGATED	<a href="#">RMI_REC_DESTROY</a>
DELEGATED	REC_AUX	<a href="#">RMI_REC_CREATE</a>
REC_AUX	DELEGATED	<a href="#">RMI_REC_DESTROY</a>
DELEGATED	RTT	<a href="#">RMI_REALM_CREATE</a> <a href="#">RMI_RTT_CREATE</a>
RTT	DELEGATED	<a href="#">RMI_REALM_DESTROY</a> <a href="#">RMI_RTT_DESTROY</a>

I\_VVGVM

Permitted Granule state transitions are shown in the following figure. Each arc is labeled with the events which can cause the corresponding state transition.



**Figure A2.2: Granule state transitions**

See also:

- [B3.3.1 RMI\\_DATA\\_CREATE command](#)
- [B3.3.2 RMI\\_DATA\\_CREATE\\_UNKNOWN command](#)
- [B3.3.3 RMI\\_DATA\\_DESTROY command](#)
- [B3.3.5 RMI\\_GRANULE\\_DELEGATE command](#)
- [B3.3.6 RMI\\_GRANULE\\_UNDELEGATE command](#)
- [B3.3.9 RMI\\_REALM\\_CREATE command](#)
- [B3.3.10 RMI\\_REALM\\_DESTROY command](#)
- [B3.3.12 RMI\\_REC\\_CREATE command](#)
- [B3.3.13 RMI\\_REC\\_DESTROY command](#)
- [B3.3.15 RMI\\_RTT\\_CREATE command](#)
- [B3.3.16 RMI\\_RTT\\_DESTROY command](#)

## A2.2.4 Granule wiping

$R_{TMGSL}$	When the state of a Granule has transitioned from $P$ to DELEGATED and then to any other state, any content associated with $P$ has been <i>wiped</i> .
$X_{CTGQZ}$	Any sequence of Granule state transitions which passes through the DELEGATED state causes the Granule contents to be wiped. This is necessary to ensure that information does not leak from one Realm to another, or from a Realm to the Host. Note that no agent can observe the contents of a Granule while its state is DELEGATED.
$D_{WTWJR}$	<i>Wiping</i> is an operation which changes the observable value of a memory location from $X$ to $Y$ , such that the value $X$ cannot be determined from the value $Y$ .
$R_{BSXXV}$	Wiping of a memory location does not reveal, directly or indirectly, any confidential Realm data.
$I_{MRPCQ}$	Wiping is not guaranteed to be implemented as zero filling.
$S_{VJWYH}$	Realm software should not assume that the initial contents of uninitialized memory (that is, Realm IPA space which is backed by DATA Granules created using RMI_DATA_CREATE_UNKNOWN) are zero.

See also:

- *Arm CCA Security model* [4]
- *B3.3.2 RMI\_DATA\_CREATE\_UNKNOWN command*
- *B3.3.6 RMI\_GRANULE\_UNDELEGATE command*

## A2.3 Realm Execution Context

This section describes the concept of a Realm Execution Context (REC).

### A2.3.1 Overview

D<sub>L</sub>RFCP

A *Realm Execution Context* (REC) is an R-EL0&1 execution context which is associated with a Realm VPE.

A *REC object* is an RMM data structure which is used to store the register state of a REC.

See also:

- [A2.1.2 Realm execution environment](#)
- [Chapter A4 Realm exception model](#)

### A2.3.2 REC attributes

This section describes the attributes of a REC.

D<sub>Z</sub>LGLT

A *REC attribute* is a property of a REC whose value can be observed or modified either by the Host or by the Realm which owns the REC.

I<sub>C</sub>SGGT

Examples of ways in which a REC attribute may be observable include the outcome of an RMM command, and the PE state following Realm entry.

D<sub>L</sub>QSFT

The attributes of a REC are summarized in the following table.

Name	Type	Description
attest_state	<a href="#">RmmRecAttestState</a>	Attestation token generation state
attest_challenge	<a href="#">Bits512</a>	Challenge for under-construction attestation token
aux	<a href="#">Address[16]</a>	Addresses of auxiliary Granules
emulatable_abort	<a href="#">RmmRecEmulatableAbort</a>	Whether the most recent exit from this REC was due to an Emulatable Data Abort
flags	<a href="#">RmmRecFlags</a>	Flags which control REC behavior
gprs	<a href="#">Bits64[32]</a>	General-purpose register values
mpidr	<a href="#">Bits64</a>	MPIDR value
owner	<a href="#">Address</a>	PA of RD of Realm which owns this REC
pc	<a href="#">Bits64</a>	Program counter value
psci_pending	<a href="#">RmmPsciPending</a>	Whether a PSCI request is pending
state	<a href="#">RmmRecState</a>	Lifecycle state
sysregs	<a href="#">RmmSystemRegisters</a>	EL1 and EL0 system register values
ripas_addr	<a href="#">Address</a>	Next address to be processed in RIPAS change
ripas_top	<a href="#">Address</a>	Top address of pending RIPAS change
ripas_value	<a href="#">RmmRipas</a>	RIPAS value of pending RIPAS change
ripas_destroyed	<a href="#">RmmRipasChangeDestroyed</a>	Whether a RIPAS change from DESTROYED should be permitted

Name	Type	Description
ripas_response	<a href="#">RmmRecResponse</a>	Host response to RIPAS change request
host_call_pending	<a href="#">RmmHostCallPending</a>	Whether a Host call is pending

I <sub>PVMTY</sub>	The <i>aux</i> attribute of a REC is a list of <i>auxiliary Granules</i> .
I <sub>RWFZF</sub>	The number of auxiliary Granules required for a REC is returned by the RMI_REC_AUX_COUNT command.
X <sub>LRWHB</sub>	Depending on the configuration of the CCA platform and of the Realm, the amount of storage space required for a REC may exceed a single Granule.
I <sub>TGLBK</sub>	The number of auxiliary Granules required for a REC can vary between Realms on a CCA platform.
R <sub>MMBNR</sub>	The number of auxiliary Granules required for a REC is a constant for the lifetime of a given Realm.
I <sub>BGVRT</sub>	The <i>gprs</i> attribute of a REC is the set of general-purpose register values which are saved by the RMM on exit from the REC and restored by the RMM on entry to the REC.
I <sub>FPJDL</sub>	The <i>mpidr</i> attribute of a REC is a value which can be used to identify the VPE associated with the REC.
I <sub>BLVKZ</sub>	The <i>pc</i> attribute of a REC is the program counter which is saved by the RMM on exit from the REC and restored by the RMM on entry to the REC.
I <sub>GHFNQ</sub>	The <i>runnable</i> flag of a REC determines whether the REC is eligible for execution. The RMI_REC_ENTER command results in a REC entry only if the value of the flag is RUNNABLE.
I <sub>SCCMH</sub>	The runnable flag of a REC is controlled by the Realm. Its initial value is reflected in the Realm Initial Measurement, and during Realm execution its value can be changed by execution of the PSCI_CPU_ON and PSCI_CPU_OFF commands.
I <sub>PMYBG</sub>	The <i>state</i> attribute of a REC is controlled by the Host, by execution of the RMI_REC_ENTER command.
D <sub>CDXDZ</sub>	The <i>sysregs</i> attribute of a REC is the set of system register values which are saved by the RMM on exit from the REC and restored by the RMM on entry to the REC.

See also:

- [A2.3.3 REC index and MPIDR value](#)
- [A2.3.4 REC lifecycle](#)
- [A4.3.4.3 REC exit due to Data Abort](#)
- [B3.3.14 RMI\\_REC\\_ENTER command](#)
- [B5.3.2 PSCI\\_CPU\\_OFF command](#)
- [B5.3.3 PSCI\\_CPU\\_ON command](#)
- [C1.13 RmmRec type](#)

### A2.3.3 REC index and MPIDR value

D <sub>KQVHN</sub>	The <i>REC index</i> is the unsigned integer value generated by concatenation of MPIDR fields:
--------------------	--

`index = Aff3:Aff2:Aff1:Aff0[3:0]`

This is illustrated by the following table.

REC index	Aff3	Aff2	Aff1	Aff0[3:0]
0	0	0	0	0
1	0	0	0	1

REC index	Aff3	Aff2	Aff1	Aff0[3:0]
...	...	...	...	...
16	0	0	1	0
...	...	...	...	...
4096	0	1	0	0
...	...	...	...	...
1048576	1	0	0	0
...	...	...	...	...

$I_{PVLZY}$  The Aff0[7:4] field of a REC MPIDR value is RES0 for compatibility with GICv3.

$I_{TTWVM}$  When creating the  $n$ th REC in a Realm, the Host is required to use the MPIDR corresponding to REC index  $n$ .  
See also:

- [B2.36 RecIndex function](#)
- [B3.3.12 RMI\\_REC\\_CREATE command](#)
- [B3.4.18 RmiRecMpidr type](#)

## A2.3.4 REC lifecycle

### A2.3.4.1 States

$D_{HTXQY}$  The states of a REC are listed below.

State	Description
READY	REC is not currently running.
RUNNING	REC is currently running.

### A2.3.4.2 State transitions

$I_{PHMWT}$  Permitted REC state transitions are shown in the following table. The rightmost column lists the events which can cause the corresponding state transition.

A transition from the pseudo-state *NULL* represents creation of a REC object. A transition to the pseudo-state *NULL* represents destruction of a REC object.

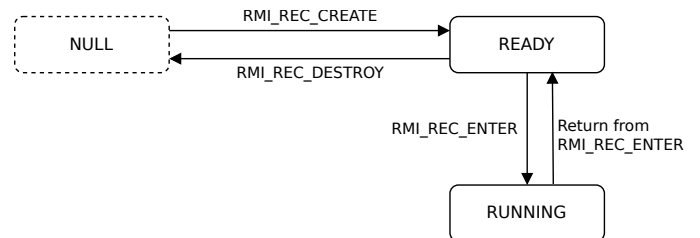
From state	To state	Events
<i>NULL</i>	READY	<a href="#">RMI_REC_CREATE</a>
READY	<i>NULL</i>	<a href="#">RMI_REC_DESTROY</a>
READY	RUNNING	<a href="#">RMI_REC_ENTER</a>
RUNNING	READY	Return from <a href="#">RMI_REC_ENTER</a>



I<sub>FNSTJ</sub>

Permitted REC state transitions are shown in the following figure. Each arc is labeled with the events which can cause the corresponding state transition.

A transition from the pseudo-state *NULL* represents creation of a REC. A transition to the pseudo-state *NULL* represents destruction of a REC.



**Figure A2.3: REC state transitions**

See also:

- [B3.3.12 \*RMI\\_REC\\_CREATE\* command](#)
- [B3.3.13 \*RMI\\_REC\\_DESTROY\* command](#)
- [B3.3.14 \*RMI\\_REC\\_ENTER\* command](#)

## Chapter A3

# Realm creation

This section describes the process of creating a Realm.

See also:

- [A2.1 Realm](#)
- [D1.2 Realm lifecycle flows](#)

## A3.1 Realm feature discovery and selection

I <sub>GJSMC</sub>	RMM implementations across different CCA platforms may support disparate features and may offer disparate configuration options for Realms.
I <sub>YRSDX</sub>	The features supported by an RMM implementation are discovered by reading feature pseudo-register values using the RMI_FEATURES command.
X <sub>WPHWG</sub>	The term <i>pseudo-register</i> is used because, although these values are stored in memory, their usage model is similar to feature registers specified in the Arm A-profile architecture.
I <sub>QNJTQ</sub>	On Realm creation, the Host specifies a set of desired features in a Realm parameters structure to the RMI_REALM_CREATE command. The RMM checks that the features specified by the Host are supported by the implementation.
I <sub>RRHJJ</sub>	The features specified at Realm creation time are included in the Realm Initial Measurement. See also: <ul style="list-style-type: none"> <li>• <a href="#">A2.1.6 Realm parameters</a></li> <li>• <a href="#">A7.1.1 Realm Initial Measurement</a></li> <li>• <a href="#">B3.3.4 RMI_FEATURES command</a></li> <li>• <a href="#">B3.3.9 RMI_REALM_CREATE command</a></li> </ul>

### A3.1.1 Realm hash algorithm

I <sub>WMKGX</sub>	The set of hash algorithms supported by the implementation is reported by the RMI_FEATURES command in RmiFeatureRegister0.
R <sub>KPBQM</sub>	Requesting an unsupported hash algorithm causes execution of RMI_REALM_CREATE to fail. See also: <ul style="list-style-type: none"> <li>• <a href="#">A7.1 Realm measurements</a></li> <li>• <a href="#">B3.3.9 RMI_REALM_CREATE command</a></li> <li>• <a href="#">B3.4.6 RmiFeatureRegister0 type</a></li> </ul>

### A3.1.2 Realm LPA2 and IPA width

I <sub>GVJMZ</sub>	Support by the implementation for LPA2 is reported by the RMI_FEATURES command in RmiFeatureRegister0.
I <sub>NKLXQ</sub>	Usage of LPA2 for Realm Translation Tables is an attribute which is set by the Host during Realm creation.
I <sub>LKJGN</sub>	Realm IPA width is an attribute which is set by the Host during Realm creation.
R <sub>SZVDK</sub>	Requesting an unsupported IPA width (for example, smaller than the minimum supported, or larger than the maximum supported) causes execution of RMI_REALM_CREATE to fail.
I <sub>GKCCS</sub>	The Host can choose a smaller IPA width than the maximum supported IPA width reported by RMI_FEATURES. This is true regardless of whether LPA2 is enabled for the Realm.
X <sub>FTVXQ</sub>	The Host may want to enable LPA2 for a Realm due to either or both of the following reasons: <ul style="list-style-type: none"> <li>• to allow the Realm to be configured with a larger IPA width</li> <li>• to allow access from mappings in the Realm's stage 2 translation to a larger PA space</li> </ul>
I <sub>XDBQB</sub>	A Realm can query its IPA width using the RSI_REALM_CONFIG command. See also: <ul style="list-style-type: none"> <li>• <a href="#">A5.2.1 Realm IPA space</a></li> </ul>

- [B3.3.9 RMI\\_REALM\\_CREATE command](#)
- [B3.4.6 RmiFeatureRegister0 type](#)
- [B4.3.8 RSI\\_REALM\\_CONFIG command](#)

### A3.1.3 Realm support for Scalable Vector Extension

I <sub>KJVLJ</sub>	Support by the implementation for the Scalable Vector Extension (FEAT_SVE) is reported by the RMI_FEATURES command in RmiFeatureRegister0.
I <sub>ZJSMJ</sub>	Availability of SVE to a Realm is set by the Host during Realm creation.
I <sub>VNLNH</sub>	SVE vector length for a Realm is set by the Host during Realm creation.
R <sub>FZZDS</sub>	Requesting a larger-than-supported SVE vector length causes execution of RMI_REALM_CREATE to fail. This is different from the behaviour of the hardware architecture, in which a larger-than-supported SVE vector length value is silently truncated.
X <sub>YGWTK</sub>	The RMI ABI provides a natural mechanism to signal an invalid feature selection, via the return code of RMI_REALM_CREATE. The analog in the hardware architecture would be to generate an illegal exception return, which would cause undesirable coupling between two disparate parts of the architecture, namely the exception model and the SVE feature.
R <sub>NBYKC</sub>	If SVE is supported by the platform but is disabled for the Realm via the RMI_REALM_CREATE command then a read of ID_AA64PFR0_EL1.SVE indicates that SVE is not supported.
U <sub>ZRJXL</sub>	The RMM should trap and emulate reads of ID_AA64PFR0_EL1.SVE.
S <sub>VXRNN</sub>	A Realm should discover SVE support by reading ID_AA64PFR0_EL1.SVE rather than based on the platform identity read from MIDR_EL1.
	See also:
	<ul style="list-style-type: none"> <li>• <a href="#">B3.3.9 RMI_REALM_CREATE command</a></li> <li>• <a href="#">B3.4.6 RmiFeatureRegister0 type</a></li> </ul>

### A3.1.4 Realm support for self-hosted debug

I <sub>SSTJD</sub>	Self-hosted debug is always available in Armv8-A.
I <sub>LVMFG</sub>	The number of breakpoints and watchpoints are attributes which are set by the Host during Realm creation.
R <sub>CJQTB</sub>	Requesting a number of breakpoints which is different from the number of breakpoints available causes execution of RMI_REALM_CREATE to fail.
R <sub>PLMDH</sub>	Requesting a number of watchpoints which is different from the number of watchpoints available causes execution of RMI_REALM_CREATE to fail.
	See also:
	<ul style="list-style-type: none"> <li>• <a href="#">B3.3.9 RMI_REALM_CREATE command</a></li> </ul>

### A3.1.5 Realm support for Performance Monitors Extension

I <sub>RVCQD</sub>	Support by the implementation for the Performance Monitors Extension (FEAT_PMU) is reported by the RMI_FEATURES command in RmiFeatureRegister0.
I <sub>NHCFC</sub>	Availability of PMU to a Realm is set by the Host during Realm creation.
I <sub>XZMKC</sub>	The number of PMU counters available to a Realm is set by the Host during Realm creation.

$R_{XVRGD}$  Requesting a number of PMU counters which is different from the number of PMU counters available causes `RMI_REALM_CREATE` to fail.

See also:

- [A8.1 Realm PMU](#)
- [B3.3.9 RMI\\_REALM\\_CREATE command](#)
- [B3.4.6 RmiFeatureRegister0 type](#)

### A3.1.6 Realm support for Activity Monitors Extension

$R_{JJVZS}$  The Activity Monitors Extension (FEAT\_AMUv1) is not available to a Realm.

### A3.1.7 Realm support for Statistical Profiling Extension

$R_{DCBNL}$  The Statistical Profiling Extension (FEAT\_SPE) is not available to a Realm.

### A3.1.8 Realm support for Trace Buffer Extension

$R_{NXDXG}$  The Trace Buffer Extension (FEAT\_TRBE) is not available to a Realm.

## Chapter A4

# Realm exception model

This section describes how Realms are executed, and how exceptions which cause exit from a Realm are handled.

See also:

- [A2.1.2 Realm execution environment](#)

## A4.1 Exception model overview

$D_{HCGWL}$	A <i>Realm entry</i> is a transfer of control to a Realm.
$D_{RMGWJ}$	A <i>Realm exit</i> is a transition of control from a Realm.
$I_{SMPWB}$	When executing in a Realm, an exception taken to R-EL2 or EL3 results in a Realm exit.
$D_{XSNZP}$	A <i>REC entry</i> is a Realm entry due to execution of RMI_REC_ENTER.
$I_{FQZJG}$	The Host provides the address of a REC as an input to the RMI_REC_ENTER command.
$I_{MDQWG}$	In this chapter, both <i>rec</i> and “the target REC” refer to the REC object which is provided to the RMI_REC_ENTER command.
$D_{BLJGY}$	A <i>RecRun object</i> is a data structure used to pass values between the RMM and the Host on REC entry and on REC exit.
$I_{VCCFV}$	A RecRun object is stored in Non-secure memory.
$I_{WBHYZ}$	The Host provides the address of a RecRun object as an input to the RMI_REC_ENTER command.
$I_{HMSQM}$	An implementation is permitted to return RMI_SUCCESS from RMI_REC_ENTER without performing a REC entry. For example, on observing a pending interrupt, the implementation can generate a REC exit due to IRQ without entering the target REC.
$D_{TJCGH}$	A <i>REC exit</i> is return from an execution of RMI_REC_ENTER which caused a REC entry.
$I_{HPWVY}$	The following diagram summarises the possible control flows that result from a Realm exit.

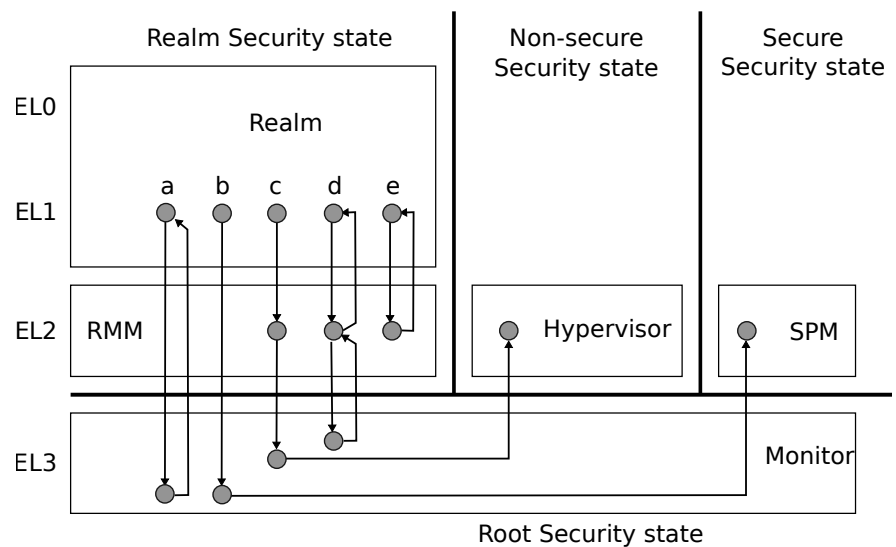


Figure A4.1: Realm exit paths

- The exception is taken to EL3. The Monitor handles the exception and returns control to the Realm.
- The exception is taken to EL3. The Monitor pre-empted Realm Security state and passes control to the Secure Security state. This may be for example due to an FIQ.
- The exception is taken to EL2. The RMM decides to perform a REC exit. The RMM executes an SMC instruction, requesting the Monitor to pass control to the Non-secure Security state.
- The exception is taken to EL2. The RMM executes an SMC instruction, requesting the Monitor to perform an operation, then returns control to the Realm.

- e. The exception is taken to EL2. The RMM handles the exception and returns control to the Realm.

See also:

- [A4.2 REC entry](#)
- [A4.3 REC exit](#)
- [B3.3.14 RMI\\_REC\\_ENTER command](#)
- [B3.4.20 RmiRecRun type](#)



## A4.2 REC entry

This section describes REC entry.

See also:

- [A4.3 REC exit](#)
- [B3.3.14 RMI\\_REC\\_ENTER command](#)

### A4.2.1 RecEnter object

D <sub>SVSJM</sub>	A <i>RecEnter</i> object is a data structure used to pass values from the Host to the RMM on REC entry.
I <sub>YSKDN</sub>	A RecEnter object is stored in the RecRun object which is passed by the Host as an input to the RMI_REC_ENTER command.
I <sub>TRKKX</sub>	On REC entry, execution state is restored from the REC object and from the RecEnter object to the PE.
I <sub>GHDLM</sub>	A RecEnter object contains attributes which are used to manage Realm virtual interrupts.
D <sub>CLNLW</sub>	The attributes of a RecEnter object are summarized in the following table.

Name	Byte offset	Type	Description
flags	0x0	<a href="#">RmiRecEnterFlags</a>	Flags
gprs[0]	0x200	<a href="#">Bits64</a>	Registers
gprs[1]	0x208	<a href="#">Bits64</a>	Registers
gprs[2]	0x210	<a href="#">Bits64</a>	Registers
gprs[3]	0x218	<a href="#">Bits64</a>	Registers
gprs[4]	0x220	<a href="#">Bits64</a>	Registers
gprs[5]	0x228	<a href="#">Bits64</a>	Registers
gprs[6]	0x230	<a href="#">Bits64</a>	Registers
gprs[7]	0x238	<a href="#">Bits64</a>	Registers
gprs[8]	0x240	<a href="#">Bits64</a>	Registers
gprs[9]	0x248	<a href="#">Bits64</a>	Registers
gprs[10]	0x250	<a href="#">Bits64</a>	Registers
gprs[11]	0x258	<a href="#">Bits64</a>	Registers
gprs[12]	0x260	<a href="#">Bits64</a>	Registers
gprs[13]	0x268	<a href="#">Bits64</a>	Registers
gprs[14]	0x270	<a href="#">Bits64</a>	Registers
gprs[15]	0x278	<a href="#">Bits64</a>	Registers
gprs[16]	0x280	<a href="#">Bits64</a>	Registers
gprs[17]	0x288	<a href="#">Bits64</a>	Registers
gprs[18]	0x290	<a href="#">Bits64</a>	Registers
gprs[19]	0x298	<a href="#">Bits64</a>	Registers

Name	Byte offset	Type	Description
gprs[20]	0x2a0	Bits64	Registers
gprs[21]	0x2a8	Bits64	Registers
gprs[22]	0x2b0	Bits64	Registers
gprs[23]	0x2b8	Bits64	Registers
gprs[24]	0x2c0	Bits64	Registers
gprs[25]	0x2c8	Bits64	Registers
gprs[26]	0x2d0	Bits64	Registers
gprs[27]	0x2d8	Bits64	Registers
gprs[28]	0x2e0	Bits64	Registers
gprs[29]	0x2e8	Bits64	Registers
gprs[30]	0x2f0	Bits64	Registers
gicv3_hcr	0x300	Bits64	GICv3 Hypervisor Control Register value
gicv3_lrs[0]	0x308	Bits64	GICv3 List Register values
gicv3_lrs[1]	0x310	Bits64	GICv3 List Register values
gicv3_lrs[2]	0x318	Bits64	GICv3 List Register values
gicv3_lrs[3]	0x320	Bits64	GICv3 List Register values
gicv3_lrs[4]	0x328	Bits64	GICv3 List Register values
gicv3_lrs[5]	0x330	Bits64	GICv3 List Register values
gicv3_lrs[6]	0x338	Bits64	GICv3 List Register values
gicv3_lrs[7]	0x340	Bits64	GICv3 List Register values
gicv3_lrs[8]	0x348	Bits64	GICv3 List Register values
gicv3_lrs[9]	0x350	Bits64	GICv3 List Register values
gicv3_lrs[10]	0x358	Bits64	GICv3 List Register values
gicv3_lrs[11]	0x360	Bits64	GICv3 List Register values
gicv3_lrs[12]	0x368	Bits64	GICv3 List Register values
gicv3_lrs[13]	0x370	Bits64	GICv3 List Register values
gicv3_lrs[14]	0x378	Bits64	GICv3 List Register values
gicv3_lrs[15]	0x380	Bits64	GICv3 List Register values

**I<sub>ZWRQP</sub>** In this chapter, both `enter` and “the `RecEnter` object” refer to the `RecEnter` object which is provided to the `RMI_REC_ENTER` command.

**I<sub>LFYDV</sub>** On REC exit, all `enter` fields are ignored unless specified otherwise.

See also:

- [A2.3 Realm Execution Context](#)
- [A4.3.1 RecExit object](#)
- [Chapter A6 Realm interrupts and timers](#)

- [B3.4.14 RmiRecEnter type](#)

### A4.2.2 General purpose registers restored on REC entry

<code>R<sub>NMSFT</sub></code>	On REC entry, if the most recent exit from the target REC was a REC exit due to PSCI, then all of the following occur: <ul style="list-style-type: none"> <li>• X0 to X6 contain the PSCI return code and PSCI output values.</li> <li>• GPR values X7 to X30 are restored from the REC object to the PE.</li> </ul>
<code>R<sub>RZRRM</sub></code>	On REC entry, if either this is the first entry to this REC, or the most recent exit from the target REC was not a REC exit due to PSCI, then GPR values X0 to X30 are restored from the REC object to the PE.
<code>R<sub>YSNYQ</sub></code>	On REC entry, if <code>rec.host_call_pending</code> is <code>HOST_CALL_PENDING</code> , then GPR values X0 to X30 are copied from <code>enter.gprs[0..30]</code> to the <code>RsiHostCall</code> data structure.
<code>R<sub>YWHKC</sub></code>	On REC entry, if writing to the <code>RsiHostCall</code> data structure fails due to the target IPA not being mapped then a REC exit to Data Abort results.
<code>R<sub>TZVNK</sub></code>	On REC entry, if writing to the <code>RsiHostCall</code> data structure succeeds then <code>rec.host_call_pending</code> is <code>NO_HOST_CALL_PENDING</code> .
<code>R<sub>NLVXB</sub></code>	On REC entry, if RMM access to <code>enter</code> causes a GPF then the <code>RMI_REC_ENTER</code> command fails with <code>RMI_ERROR_INPUT</code> .

See also:

- [A4.3.3 General purpose registers saved on REC exit](#)
- [A4.3.4.3 REC exit due to Data Abort](#)
- [A4.3.7 REC exit due to PSCI](#)
- [A4.3.9 REC exit due to Host call](#)
- [A4.5 Host call](#)

### A4.2.3 REC entry following REC exit due to Data Abort

<code>R<sub>BWZKH</sub></code>	On REC entry, if the most recent exit from the target REC was a REC exit due to Emulatable Data Abort and <code>enter.flags.emul_mmio == RMI_EMULATED_MMIO</code> , then the return address is the next instruction following the faulting instruction.
<code>R<sub>SCJWG</sub></code>	On REC entry, if the most recent exit from the target REC was a REC exit due to Emulatable Data Abort and the Realm memory access was a read and <code>enter.flags.emul_mmio == RMI_EMULATED_MMIO</code> , then the register indicated by <code>ESR_EL2.ISS.SRT</code> is set to <code>enter.gprs[0]</code> .
<code>R<sub>LJWRK</sub></code>	On REC entry, if the most recent exit from the target REC was a REC exit due to Data Abort at an Unprotected IPA and <code>enter.flags.inject_sea == RMI_INJECT_SEA</code> , then a Synchronous External Abort is taken to the Realm.

See also:

- [A4.3.4.3 REC exit due to Data Abort](#)
- [A4.4 Emulated Data Aborts](#)
- [A5.2.6 Realm access to an Unprotected IPA](#)
- [A5.2.7 Synchronous External Aborts](#)

## A4.3 REC exit

This section describes REC exit.

See also:

- [A4.2 REC entry](#)
- [B3.3.14 RMI\\_REC\\_ENTER command](#)

### A4.3.1 RecExit object

D <sub>PBDCB</sub>	A <i>RecExit</i> object is a data structure used to pass values from the RMM to the Host on REC exit.
I <sub>VHJTL</sub>	A RecExit object is stored in the RecRun object which is passed by the Host as an input to the RMI_REC_ENTER command.
I <sub>JKWPB</sub>	On REC exit, execution state is saved from the PE to the REC object and to the RecExit object.
I <sub>ZSCNM</sub>	A RecExit object contains attributes which are used to manage Realm virtual interrupts and Realm timers.
D <sub>FFCMN</sub>	The attributes of a RecExit object are summarized in the following table.

Name	Byte offset	Type	Description
exit_reason	0x0	<a href="#">RmiRecExitReason</a>	Exit reason
esr	0x100	<a href="#">Bits64</a>	Exception Syndrome Register
far	0x108	<a href="#">Bits64</a>	Fault Address Register
hpfar	0x110	<a href="#">Bits64</a>	Hypervisor IPA Fault Address register
gprs[0]	0x200	<a href="#">Bits64</a>	Registers
gprs[1]	0x208	<a href="#">Bits64</a>	Registers
gprs[2]	0x210	<a href="#">Bits64</a>	Registers
gprs[3]	0x218	<a href="#">Bits64</a>	Registers
gprs[4]	0x220	<a href="#">Bits64</a>	Registers
gprs[5]	0x228	<a href="#">Bits64</a>	Registers
gprs[6]	0x230	<a href="#">Bits64</a>	Registers
gprs[7]	0x238	<a href="#">Bits64</a>	Registers
gprs[8]	0x240	<a href="#">Bits64</a>	Registers
gprs[9]	0x248	<a href="#">Bits64</a>	Registers
gprs[10]	0x250	<a href="#">Bits64</a>	Registers
gprs[11]	0x258	<a href="#">Bits64</a>	Registers
gprs[12]	0x260	<a href="#">Bits64</a>	Registers
gprs[13]	0x268	<a href="#">Bits64</a>	Registers
gprs[14]	0x270	<a href="#">Bits64</a>	Registers
gprs[15]	0x278	<a href="#">Bits64</a>	Registers
gprs[16]	0x280	<a href="#">Bits64</a>	Registers

Name	Byte offset	Type	Description
gprs[17]	0x288	Bits64	Registers
gprs[18]	0x290	Bits64	Registers
gprs[19]	0x298	Bits64	Registers
gprs[20]	0x2a0	Bits64	Registers
gprs[21]	0x2a8	Bits64	Registers
gprs[22]	0x2b0	Bits64	Registers
gprs[23]	0x2b8	Bits64	Registers
gprs[24]	0x2c0	Bits64	Registers
gprs[25]	0x2c8	Bits64	Registers
gprs[26]	0x2d0	Bits64	Registers
gprs[27]	0x2d8	Bits64	Registers
gprs[28]	0x2e0	Bits64	Registers
gprs[29]	0x2e8	Bits64	Registers
gprs[30]	0x2f0	Bits64	Registers
gicv3_hcr	0x300	Bits64	GICv3 Hypervisor Control Register value
gicv3_lrs[0]	0x308	Bits64	GICv3 List Register values
gicv3_lrs[1]	0x310	Bits64	GICv3 List Register values
gicv3_lrs[2]	0x318	Bits64	GICv3 List Register values
gicv3_lrs[3]	0x320	Bits64	GICv3 List Register values
gicv3_lrs[4]	0x328	Bits64	GICv3 List Register values
gicv3_lrs[5]	0x330	Bits64	GICv3 List Register values
gicv3_lrs[6]	0x338	Bits64	GICv3 List Register values
gicv3_lrs[7]	0x340	Bits64	GICv3 List Register values
gicv3_lrs[8]	0x348	Bits64	GICv3 List Register values
gicv3_lrs[9]	0x350	Bits64	GICv3 List Register values
gicv3_lrs[10]	0x358	Bits64	GICv3 List Register values
gicv3_lrs[11]	0x360	Bits64	GICv3 List Register values
gicv3_lrs[12]	0x368	Bits64	GICv3 List Register values
gicv3_lrs[13]	0x370	Bits64	GICv3 List Register values
gicv3_lrs[14]	0x378	Bits64	GICv3 List Register values
gicv3_lrs[15]	0x380	Bits64	GICv3 List Register values
gicv3_misr	0x388	Bits64	GICv3 Maintenance Interrupt State Register value
gicv3_vmcr	0x390	Bits64	GICv3 Virtual Machine Control Register value

Name	Byte offset	Type	Description
cntp_ctl	0x400	Bits64	Counter-timer Physical Timer Control Register value
cntp_cval	0x408	Bits64	Counter-timer Physical Timer CompareValue Register value
cntv_ctl	0x410	Bits64	Counter-timer Virtual Timer Control Register value
cntv_cval	0x418	Bits64	Counter-timer Virtual Timer CompareValue Register value
ripas_base	0x500	Bits64	Base address of target region for pending RIPAS change
ripas_top	0x508	Bits64	Top address of target region for pending RIPAS change
ripas_value	0x510	RmiRipas	RIPAS value of pending RIPAS change
imm	0x600	Bits16	Host call immediate value
pmu_ovf_status	0x700	RmiPmuOverflowStatus	PMU overflow status

**I<sub>FQZXZ</sub>** In this chapter, both `exit` and “the RecExit object” refer to the RecExit object which is provided to the `RMI_REC_ENTER` command.

**R<sub>PNWZV</sub>** On REC exit, all `exit` fields are zero unless specified otherwise.  
See also:

- [A2.3 Realm Execution Context](#)
- [A4.2.1 RecEnter object](#)
- [A4.5 Host call](#)
- [Chapter A6 Realm interrupts and timers](#)
- [Chapter A8 Realm debug and performance monitoring](#)
- [B3.4.16 RmiRecExit type](#)

### A4.3.2 Realm exit reason

**I<sub>DYWHJ</sub>** On return from the `RMI_REC_ENTER` command, the reason for the REC exit is indicated by `exit.exit_reason` and `exit.esr`.

See also:

- [B3.4.17 RmiRecExitReason type](#)

### A4.3.3 General purpose registers saved on REC exit

**R<sub>PBKV B</sub>** On REC exit due to PSCI, all of the following are true:

- `exit.gprs[0]` contains the PSCI FID.
- `exit.gprs[1..3]` contain the corresponding PSCI arguments. If the PSCI command has fewer than 3 arguments, the remaining values contain zero.
- GPR values X7 to X30 are saved from the PE to the REC object.

**R<sub>FNZKM</sub>** On REC exit for any reason which is not REC exit due to PSCI, GPR values X0 to X30 are saved from the PE to the REC.

**R<sub>MZGPT</sub>** On REC exit for any reason which is neither REC exit due to Host call nor REC exit due to PSCI, `exit.gprs` is zero.

**R<sub>FRGVT</sub>** On REC exit, if RMM access to `exit` causes a GPF then the `RMI_REC_ENTER` command fails with `RMI_ERROR_INPUT`.

See also:

- [A4.2.2 General purpose registers restored on REC entry](#)
- [A4.3.7 REC exit due to PSCI](#)
- [A4.3.9 REC exit due to Host call](#)

### A4.3.4 REC exit due to synchronous exception

**I<sub>SNDHF</sub>** A synchronous exception taken to R-EL2 can cause a REC exit.

**I<sub>RPSNC</sub>** The following table summarises the behavior of synchronous exceptions taken to R-EL2.

Exception class	Behavior
Trapped WFI or WFE instruction execution	<a href="#">REC exit due to WFI or WFE</a>
HVC instruction execution in AArch64 state	Unknown exception taken to Realm
SMC instruction execution in AArch64 state	One of: <ul style="list-style-type: none"> <li>• <a href="#">REC exit due to PSCI</a></li> <li>• RSI command handled by RMM, followed by return to Realm</li> </ul>
Trapped MSR, MRS or System instruction execution in AArch64 state	Emulated by RMM, followed by return to Realm
Instruction Abort from a lower Exception level	<a href="#">REC exit due to Instruction Abort</a>
Data Abort from a lower Exception level	<a href="#">REC exit due to Data Abort</a>

**R<sub>YLFMD</sub>** Realm execution of an SMC which is not part of one of the following ABIs results in a return value of `SMCCC_NOT_SUPPORTED`:

- PSCI
- RSI

See also:

- [A4.5 Host call](#)
- [Chapter B4 Realm Services Interface](#)
- [Chapter B5 Power State Control Interface](#)

#### A4.3.4.1 REC exit due to WFI or WFE

**D<sub>GLHPX</sub>** A *REC exit due to WFI or WFE* is a REC exit due to WFI, WFIT, WFE or WFET instruction execution in a Realm.

**R<sub>VTJQF</sub>** On WFI or WFIT instruction execution in a Realm, a REC exit due to WFI or WFE is caused if `enter.trap_wfi` is `RMI_TRAP`.

**R<sub>GBNGW</sub>** On WFE or WFET instruction execution in a Realm, a REC exit due to WFI or WFE is caused if `enter.trap_wfe` is `RMI_TRAP`.

R<sub>YQWST</sub>

On REC exit due to WFI or WFE, all of the following are true:

- `exit.exit_reason` is `RMI_EXIT_SYNC`.
- `exit.esr.EC` contains the value of `ESR_EL2.EC` at the time of the Realm exit.
- `exit.esr.ISS.TI` contains the value of `ESR_EL2.ISS.TI` at the time of the Realm exit.
- All other `exit` fields are zero.

R<sub>BPYBC</sub>

On REC exit due to WFI or WFE, if the exit was caused by `WFET` or `WFIT` instruction execution then `exit.gprs[0]` contains the timeout value.

#### A4.3.4.2 REC exit due to Instruction Abort

D<sub>GYQXK</sub>

A *REC exit due to Instruction Abort* is a REC exit due to a Realm instruction fetch from a Protected IPA for which either of the following is true:

- HIPAS is `UNASSIGNED` and RIPAS is `RAM`
- RIPAS is `DESTROYED`

R<sub>MGWRC</sub>

On REC exit due to Instruction Abort, all of the following are true:

- `exit.exit_reason` is `RMI_EXIT_SYNC`.
- `exit.esr.EC` contains the value of `ESR_EL2.EC` at the time of the Realm exit.
- `exit.esr.ISS.SET` contains the value of `ESR_EL2.ISS.SET` at the time of the Realm exit.
- `exit.esr.ISS.EA` contains the value of `ESR_EL2.ISS.EA` at the time of the Realm exit.
- `exit.esr.ISS.IFSC` contains the value of `ESR_EL2.ISS.IFSC` at the time of the Realm exit.
- `exit.hpfar` contains the value of `HPFAR_EL2` at the time of the Realm exit.
- All other `exit` fields are zero.

See also:

- [A5.2.2 Realm IPA state](#)
- [A5.2.3 Realm access to a Protected IPA](#)

#### A4.3.4.3 REC exit due to Data Abort

D<sub>CYRMT</sub>

A *REC exit due to Emulatable Data Abort* is a REC exit due to a Realm data access to one of the following:

- an Unprotected IPA whose HIPAS is `UNASSIGNED_NS`, where the access caused `ESR_EL2.ISS.ISV` to be set to `'1'`
- an Unprotected IPA whose HIPAS is `ASSIGNED_NS`, where the access caused a stage 2 permission fault and caused `ESR_EL2.ISS.ISV` to be set to `'1'`

D<sub>MTZMC</sub>

A *REC exit due to Non-emulatable Data Abort* is a REC exit due to a Realm data access to one of the following:

- an Unprotected IPA whose HIPAS is `UNASSIGNED_NS`, where the access caused `ESR_EL2.ISS.ISV` to be set to `'0'`
- an Unprotected IPA whose HIPAS is `ASSIGNED_NS`, where the access caused a stage 2 permission fault and caused `ESR_EL2.ISS.ISV` to be set to `'0'`
- a Protected IPA whose HIPAS is `UNASSIGNED` and whose RIPAS is `RAM`
- a Protected IPA whose RIPAS is `DESTROYED`.

R<sub>RYVFL</sub>

On REC exit due to Data Abort, all of the following are true:

- `exit.exit_reason` is `RMI_EXIT_SYNC`.
- `exit.esr.EC` contains the value of `ESR_EL2.EC` at the time of the Realm exit.
- `exit.esr.ISS.SET` contains the value of `ESR_EL2.ISS.SET` at the time of the Realm exit.
- `exit.esr.ISS.FnV` contains the value of `ESR_EL2.ISS.FnV` at the time of the Realm exit.
- `exit.esr.ISS.EA` contains the value of `ESR_EL2.ISS.EA` at the time of the Realm exit.
- `exit.esr.ISS.DFSC` contains the value of `ESR_EL2.ISS.DFSC` at the time of the Realm exit.
- `exit.hpfar` contains the value of `HPFAR_EL2` at the time of the Realm exit.



On REC exit due to Emulatable Data Abort, all of the following are true:

- `rec.emulatable_abort` is `EMULATABLE_ABORT`.
- `exit.esr.ISS.ISV` contains the value of `ESR_EL2.ISS.ISV` at the time of the Realm exit.
- `exit.esr.ISS.SAS` contains the value of `ESR_EL2.ISS.SAS` at the time of the Realm exit.
- `exit.esr.ISS.SF` contains the value of `ESR_EL2.ISS.SF` at the time of the Realm exit.
- `exit.esr.ISS.WnR` contains the value of `ESR_EL2.ISS.WnR` at the time of the Realm exit.
- `exit.far` contains the value of `FAR_EL2` at the time of the Realm exit, with bits more significant than the size of a Granule masked to zero.

On REC exit due to Non-emulatable Data Abort at an Unprotected IPA, all of the following are true:

- `exit.esr.II` contains the value of `ESR_EL2.II` at the time of the Realm exit.

On REC exit due to Data Abort, all of the other `exit` fields are zero.

`XHHXJC` On REC exit due to Emulatable Data Abort, `ESR_EL2.ISS.SSE` is not propagated to the Host. This is because this field is used to emulate sign extension on loads, which must be performed by the RMM so that the Realm can rely on architecturally correct behavior of the virtual execution environment.

`XHSWFR` On REC exit due to Emulatable Data Abort, the Host can calculate the faulting IPA from the `exit.hpfar` and `exit.far` values.

`RFFNHW` On REC exit due to Emulatable Data Abort, if the Realm memory access was a write, `exit.gprs[0]` contains the value of the register indicated by `ESR_EL2.ISS.SRT` at the time of the Realm exit.

`RQBTPR` On REC exit not due to Emulatable Data Abort, `rec.emulatable_abort` is `NOT_EMULATABLE_ABORT`.

See also:

- [A4.2.3 REC entry following REC exit due to Data Abort](#)
- [A4.4 Emulated Data Aborts](#)
- [A5.2.1 Realm IPA space](#)
- [A5.2.3 Realm access to a Protected IPA](#)
- [A5.2.6 Realm access to an Unprotected IPA](#)

### A4.3.5 REC exit due to IRQ

`DYLWKK` A REC exit due to IRQ is a REC exit due to an IRQ exception which should be handled by the Host.

`RTYJSX` On REC exit due to IRQ, `exit.exit_reason` is `RMI_EXIT_IRQ`.

`RCSQXV` On REC exit due to IRQ, `exit.esr` is zero.

See also:

- [Chapter A6 Realm interrupts and timers](#)

### A4.3.6 REC exit due to FIQ

`DZTYMM` A REC exit due to FIQ is a REC exit due to an FIQ exception which should be handled by the Host.

`RPDSBD` On REC exit due to FIQ, `exit.exit_reason` is `RMI_EXIT_FIQ`.

`RGXZRF` On REC exit due to FIQ, `exit.esr` is zero.

See also:

- [Chapter A6 Realm interrupts and timers](#)

### A4.3.7 REC exit due to PSCI

I\_ZSGFP

A PSCI function executed by a Realm is either:

- handled by the RMM, returning to the Realm, or
- forwarded by the RMM to the Host via a *REC exit due to PSCI*.

D\_RFTQD

A *REC exit due to PSCI* is a REC exit due to Realm PSCI function execution by SMC instruction which was forwarded by the RMM to the Host.

I\_VBJXY

The following table summarises the behavior of PSCI function execution by a Realm.

PSCI functions not listed in this table are not supported. Calling a non-supported PSCI function results in a return value of PSCI\_NOT\_SUPPORTED.

PSCI function	Can result in REC exit due to PSCI	Requires Host to call RMI_PSCI_COMPLETE
PSCI_VERSION	No	-
PSCI_FEATURES	No	-
PSCI_CPU_SUSPEND	Yes	No
PSCI_CPU_OFF	Yes	No
PSCI_CPU_ON	Yes	Yes
PSCI_AFFINITY_INFO	Yes	Yes
PSCI_SYSTEM_OFF	Yes	No
PSCI_SYSTEM_RESET	Yes	No

R\_NTZNJ

On REC exit due to PSCI, `exit.exit_reason` is RMI\_EXIT\_PSCI.

R\_SXGJK

On REC exit due to PSCI, `exit.gprs` contains sanitised parameters from the PSCI call.

R\_YTDGT

On REC exit due to PSCI, if the command arguments include an MPIDR value, `rec.psci_pending` is set to PSCI\_REQUEST\_PENDING. Otherwise, `rec.psci_pending` is set to NO\_PSCI\_REQUEST\_PENDING.

I\_KKFMQ

Following REC exit due to PSCI, if `rec.psci_pending` is PSCI\_REQUEST\_PENDING, the Host must complete the request by calling the RMI\_PSCI\_COMPLETE command, prior to re-entering the REC.

In the call to RMI\_PSCI\_COMPLETE, the Host provides the target REC, which corresponds to the MPIDR value provided by the Realm. This is necessary because the RMM does not maintain a mapping from MPIDR values to REC addresses. The RMM validates that the REC provided by the Host matches the MPIDR value.

In the call to RMI\_PSCI\_COMPLETE, the Host provides a PSCI status value, which the RMM handles as follows:

- If the Host provides PSCI\_SUCCESS, the RMM performs the PSCI operation requested by the Realm. The result of the PSCI operation is recorded in the REC and returned to the Realm on the next entry to the calling REC.
- If the Host provides a status value other than PSCI\_SUCCESS, the RMM validates that the status code is permitted for the PSCI operation requested by the Realm. If the status code is permitted, it is recorded in the REC and returned to the Realm on the next entry to the calling REC.

See also:

- [A4.3.3 General purpose registers saved on REC exit](#)
- [B2.19 PsciReturnCodePermitted function](#)
- [B3.3.7 RMI\\_PSCI\\_COMPLETE command](#)
- [Chapter B5 Power State Control Interface](#)

- [D1.4 PSCI flows](#)

### A4.3.8 REC exit due to RIPAS change pending

D <sub>JGCVY</sub>	A REC exit due to RIPAS change pending is a REC exit due to the Realm issuing a RIPAS change request.
R <sub>QSSKK</sub>	On REC exit due to RIPAS change pending, all of the following are true: <ul style="list-style-type: none"> <li>• <code>exit.exit_reason</code> is <code>RMI_EXIT_RIPAS_CHANGE</code>.</li> <li>• <code>exit.ripas_base</code> is the base address of the region on which a RIPAS change is pending.</li> <li>• <code>exit.ripas_top</code> is the top address of the region on which a RIPAS change is pending.</li> <li>• <code>exit.ripas_value</code> is the requested RIPAS value.</li> <li>• <code>rec.ripas_addr</code> is the base address of the region on which a RIPAS change is pending.</li> <li>• <code>rec.ripas_top</code> is the top address of the region on which a RIPAS change is pending.</li> <li>• <code>rec.ripas_value</code> is the requested RIPAS value.</li> </ul>
I <sub>MCKKH</sub>	On REC exit due to RIPAS change pending: <ul style="list-style-type: none"> <li>• <code>exit</code> holds the base address and the size of the region on which a RIPAS change is pending. These values inform the Host of the bounds of the RIPAS change request.</li> <li>• <code>rec</code> holds the next address to be processed in a RIPAS change, and the top of the requested RIPAS change region. These values are used by the RMM to enforce that the <code>RMI_RTT_SET_RIPAS</code> command can only apply RIPAS change within the bounds of the RIPAS change request, and to report the progress of the RIPAS change to the Realm on the next REC entry.</li> </ul>
R <sub>QRMNM</sub>	On REC exit not due to RIPAS change pending, all of the following are true: <ul style="list-style-type: none"> <li>• <code>rec.ripas_addr</code> is 0</li> <li>• <code>rec.ripas_top</code> is 0</li> </ul> <p>See also:</p> <ul style="list-style-type: none"> <li>• <a href="#">A2.3.2 REC attributes</a></li> <li>• <a href="#">A5.4 RIPAS change</a></li> </ul>

### A4.3.9 REC exit due to Host call

D <sub>WFZXK</sub>	A REC exit due to Host call is a REC exit due to <code>RSI_HOST_CALL</code> execution in a Realm.
R <sub>GTJRP</sub>	On REC exit due to Host call, all of the following are true: <ul style="list-style-type: none"> <li>• <code>rec.host_call_pending</code> is <code>HOST_CALL_PENDING</code>.</li> <li>• <code>exit.exit_reason</code> is <code>RMI_EXIT_HOST_CALL</code>.</li> <li>• <code>exit.imm</code> contains the immediate value passed to the <code>RSI_HOST_CALL</code> command.</li> <li>• <code>exit.gprs[0..30]</code> contain the register values passed to the <code>RSI_HOST_CALL</code> command.</li> <li>• All other <code>exit</code> fields except for <code>exit.givc3_*</code>, <code>exit_cnt*</code> and <code>exit.pmu_ovf_status</code> are zero.</li> </ul> <p>See also:</p> <ul style="list-style-type: none"> <li>• <a href="#">A4.5 Host call</a></li> <li>• <a href="#">B4.3.3 RSI_HOST_CALL command</a></li> </ul>

### A4.3.10 REC exit due to SError

D <sub>PGMH</sub>	A REC exit due to SError is a REC exit due to an SError interrupt during Realm execution.
-------------------	---

R<sub>LRCFP</sub>

On REC exit due to SError, all of the following occur:

- `exit.exit_reason` is `RMI_EXIT_SERROR`.
- `exit.esr.EC` contains the value of `ESR_EL2.EC` at the time of the Realm exit.
- `exit.esr.ISS.IDS` contains the value of `ESR_EL2.ISS.IDS` at the time of the Realm exit.
- `exit.esr.ISS.AET` contains the value of `ESR_EL2.ISS.AET` at the time of the Realm exit.
- `exit.esr.ISS.EA` contains the value of `ESR_EL2.ISS.EA` at the time of the Realm exit.
- `exit.esr.ISS.DFSC` contains the value of `ESR_EL2.ISS.DFSC` at the time of the Realm exit.
- All other `exit` fields except for `exit.givc3_*`, `exit_cnt*` and `exit.pmu_ovf_status` are zero.

## A4.4 Emulated Data Aborts

I<sub>SVYDC</sub>

On REC exit due to Emulatable Data Abort, sufficient information is provided to the Host to enable it to emulate the access, for example to emulate a virtual peripheral.

On taking the REC exit, the Host can either

- Establish a mapping in the RTT, in which case it would want the Realm to re-attempt the access. In this case, on the next REC entry the Host sets `enter.flags.emul_mmio = RMI_NOT_EMULATED_MMIO`, which indicates that instruction emulation was not performed. This causes the return address to be the faulting instruction.
- Emulate the access. For an emulated write, the data is provided in `exit.gprs[0]`. For an emulated read, the data is provided in `enter.gprs[0]`. In this case, on the next REC entry the Host sets `enter.flags.emul_mmio = RMI_EMULATED_MMIO`, which indicates that the instruction was emulated. This causes the return address to be the address of the instruction which generated the Data Abort plus 4 bytes.

See also:

- [A4.2.3 REC entry following REC exit due to Data Abort](#)
- [A4.3.4.3 REC exit due to Data Abort](#)
- [A5.2.1 Realm IPA space](#)

## A4.5 Host call

This section describes the programming model for Realm communication with the Host.

D<sub>YDJWT</sub>

A *Host call* is a call made by the Realm to the Host, by execution of the `RSI_HOST_CALL` command.

I<sub>XNFKZ</sub>

A Host call can be used by a Realm to make a hypercall.

R<sub>DNBQF</sub>

On Realm execution of HVC, an Unknown exception is taken to the Realm.

See also:

- [A4.2.2 General purpose registers restored on REC entry](#)
- [A4.3.9 REC exit due to Host call](#)
- [B4.3.3 RSI\\_HOST\\_CALL command](#)
- [D1.3.2 Host call flow](#)

## Chapter A5

# Realm memory management

This section describes how Realm memory is managed. This includes:

- How the translation tables which describe the Realm's address space are managed by the Host.
- Properties of the Realm's address space, and of the memory which can be mapped into it.
- How faults caused by Realm memory accesses are handled.

See also:

- [A2.1.2 Realm execution environment](#)
- [D1.5 Realm memory management flows](#)
- [Chapter D2 Realm shared memory protocol](#)

## A5.1 Realm memory management overview

Realm memory management can be viewed from one of two standpoints: the Realm and the Host.

From the Realm's point of view, the RMM provides security guarantees regarding the IPA space of the Realm and the memory which is mapped into it. These security guarantees are upheld via RSI commands which the Realm can execute in order to query the initial configuration and contents of its address space, and to modify properties of the address space at runtime.

From the Host's point of view, Realm memory management involves manipulating the stage 2 translation tables which describe the Realm's address space, and handling faults which are caused by Realm memory accesses. These operations are similar to those involved in managing the memory of a normal VM, but in the case of a Realm they are performed via execution of RMI commands.

See also:

- [A5.2 Realm view of memory management](#)
- [A5.3 Host view of memory management](#)

## A5.2 Realm view of memory management

This section describes memory management from the Realm's point of view.

### A5.2.1 Realm IPA space

I <sub>DLRZF</sub>	The IPA space of a Realm is divided into two halves: Protected IPA space and Unprotected IPA space.
S <sub>LZHXC</sub>	Software in a Realm should treat the most significant bit of an IPA as a protection attribute.
D <sub>KXGDV</sub>	A <i>Protected IPA</i> is an address in the lower half of a Realm's IPA space. The most significant bit of a Protected IPA is 0.
D <sub>MRWGM</sub>	An <i>Unprotected IPA</i> is an address in the upper half of a Realm's IPA space. The most significant bit of an Unprotected IPA is 1.

See also:

- [A2.1.3 Realm attributes](#)
- [A3.1.2 Realm LPA2 and IPA width](#)

### A5.2.2 Realm IPA state

D <sub>WWCBD</sub>	A Protected IPA has an associated <i>Realm IPA state</i> (RIPAS).
--------------------	---

The RIPAS values are shown in the following table.

RIPAS	Description
EMPTY	Address where no Realm resources are mapped
RAM	Address where private code or data owned by the Realm is mapped
DESTROYED	Address which is inaccessible to the Realm due to an action taken by the Host

I <sub>VZCZV</sub>	RIPAS values are stored in an RTT.
--------------------	------------------------------------

See also:

- [A5.5 Realm Translation Table](#)

### A5.2.3 Realm access to a Protected IPA

<code>R_JVQQR</code>	Realm data access to a Protected IPA whose RIPAS is EMPTY causes a Synchronous External Abort taken to the Realm.
<code>R_MKLS D</code>	Realm instruction fetch from a Protected IPA whose RIPAS is EMPTY causes a Synchronous External Abort taken to the Realm.
<code>R_QSQLF</code>	Realm data access to a Protected IPA whose RIPAS is RAM does not cause a Synchronous External Abort taken to the Realm.
<code>I_PG HBT</code>	Realm data access to a Protected IPA can cause an REC exit due to Data Abort.
<code>R_FCJCP</code>	Realm instruction fetch from a Protected IPA whose RIPAS is RAM does not cause a Synchronous External Abort taken to the Realm.
<code>I_XHKQY</code>	Realm instruction fetch from a Protected IPA whose RIPAS is RAM can cause a REC exit due to Instruction Abort.
<code>R_CLVKF</code>	Realm data access to a Protected IPA whose RIPAS is DESTROYED causes a REC exit due to Data Abort.
<code>R_MZYQT</code>	Realm instruction fetch from a Protected IPA whose RIPAS is DESTROYED causes a REC exit due to Instruction Abort.

See also:

- [A4.3.4.2 REC exit due to Instruction Abort](#)
- [A4.3.4.3 REC exit due to Data Abort](#)
- [A5.2.7 Synchronous External Aborts](#)

### A5.2.4 Changes to RIPAS while Realm state is NEW

This section describes how the RIPAS of a Protected IPA can change while the Realm state is NEW.

<code>I_BSBHN</code>	For a Realm in the NEW state, the RIPAS of a Protected IPA can change to RAM due to Host execution of <code>RMI_RTT_INIT_RIPAS</code> .
<code>I_BSGSW</code>	For a Realm in the NEW state, changing the RIPAS of a Protected IPA to RAM causes the RIM to be updated.
<code>I_YCPNY</code>	For a Realm in the NEW state, the RIPAS of a Protected IPA can change to DESTROYED due to Host execution of <code>RMI_DATA_DESTROY</code> or <code>RMI_RTT_DESTROY</code> .
<code>I_YXLCP</code>	For a Realm in the NEW state, changing the RIPAS of a Protected IPA to DESTROYED does not cause the RIM to be updated.

See also:

- [A5.4 RIPAS change](#)
- [A7.1.1 Realm Initial Measurement](#)
- [B3.3.3 RMI\\_DATA\\_DESTROY command](#)
- [B3.3.16 RMI\\_RTT\\_DESTROY command](#)
- [B3.3.18 RMI\\_RTT\\_INIT\\_RIPAS command](#)

### A5.2.5 Changes to RIPAS while Realm state is ACTIVE

This section describes how the RIPAS of a Protected IPA can change while the Realm state is ACTIVE.

<code>I_NZXPG</code>	A Realm in the ACTIVE state can request the RIPAS of a region of Protected IPA space to be changed to either EMPTY or RAM.
----------------------	--



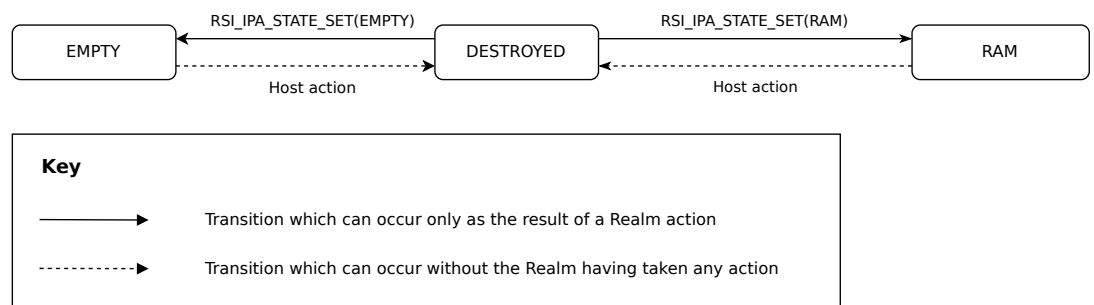
I <sub>RXHXF</sub>	A Realm in the ACTIVE state cannot request the RIPAS of a region of Protected IPA space to be changed to DESTROYED.
I <sub>FRJJH</sub>	For a Realm in the ACTIVE state, the RIPAS of a Protected IPA can change to EMPTY only in response to Realm execution of RSI_IPA_STATE_SET.
X <sub>HQLVY</sub>	The fact that the Host cannot change the RIPAS of a Protected IPA to EMPTY without the Realm having consented to this change prevents the Host from injecting an SEA at a Protected IPA which has been configured to have a RIPAS of RAM, which could potentially trigger unexpected behavior in the Realm.
I <sub>HNFYR</sub>	For a Realm in the ACTIVE state, the RIPAS of a Protected IPA can change to RAM only in response to Realm execution of RSI_IPA_STATE_SET.
I <sub>VVFMX</sub>	On execution of RSI_IPA_STATE_SET, a Realm can optionally specify that the RIPAS change should only succeed if the current RIPAS is not DESTROYED.
X <sub>VXHBV</sub>	An expected pattern for Realm creation is as follows:

1. Host populates an “initial image” range of Realm IPA space with measured content:
  - a. Host executes RMI\_RTT\_INIT\_RIPAS, causing a RIPAS change to RAM.
  - b. Host executes RMI\_DATA\_CREATE, establishing a mapping to physical memory and updating the RIM.
2. Host informs the Realm of the range of IPA space which should be considered by the Realm as DRAM. This is a superset of the IPA range populated in step 1. For unpopulated parts of this IPA range, the RIPAS is EMPTY.
3. Realm executes RSI\_IPA\_STATE\_SET(ripas=RAM) for the DRAM IPA range described to it in step 2. Following this command, the desired state is:
  - a. For the initial image IPA range, the contents match those described by the RIM.
  - b. For the entire DRAM IPA range, RIPAS is RAM.

If at step 2, the Host were to execute RMI\_DATA\_DESTROY on a page within the initial image IPA range, its RIPAS would change to DESTROYED. The Host could then execute RMI\_DATA\_CREATE\_UNKNOWN, with the result that contents of the initial image IPA range no longer match those described by the RIM.

By specifying at step 3 that the RIPAS change should only succeed if the current RIPAS is not DESTROYED, the Realm is able to prevent loss of integrity within the initial image IPA range.

I <sub>KZVDC</sub>	For a Realm in the ACTIVE state, the RIPAS of a Protected IPA can change to DESTROYED due to Host execution of RMI_DATA_DESTROY or RMI_RTT_DESTROY.
X <sub>JJPHJ</sub>	The result of changing the RIPAS of a Protected IPA to DESTROYED is that subsequent Realm accesses to that address do not make forward progress. This is consistent with the principle that the RMM does not provide an availability guarantee to a Realm.
I <sub>NMMSG</sub>	The following diagram summarizes RIPAS changes which can occur when the Realm state is ACTIVE.



See also:

- [A5.4 RIPAS change](#)
- [B3.3.1 RMI\\_DATA\\_CREATE command](#)
- [B3.3.2 RMI\\_DATA\\_CREATE\\_UNKNOWN command](#)
- [B3.3.3 RMI\\_DATA\\_DESTROY command](#)
- [B3.3.16 RMI\\_RTT\\_DESTROY command](#)
- [B3.3.18 RMI\\_RTT\\_INIT\\_RIPAS command](#)
- [B4.3.5 RSI\\_IPA\\_STATE\\_SET command](#)

## A5.2.6 Realm access to an Unprotected IPA

I_KQJML	An access by a Realm to an Unprotected IPA can result in a <i>Granule Protection Fault</i> (GPF). The RMM does not ensure that the PAS of a Granule mapped at an Unprotected IPA is NS.
S_ZZBQF	Realm software must be able to handle taking a GPF during access to an Unprotected IPA.
I_WCVBZ	Realm data access to an Unprotected IPA can cause a REC exit due to Data Abort.
I_RNDTJ	On taking a REC exit due to Data Abort at an Unprotected IPA, the Host can inject a Synchronous External Abort to the Realm.
X_MGBDH	The Host can inject an SEA in response to an unexpected Realm data access to an Unprotected IPA.
I_FVYCM	Realm data access to an Unprotected IPA which caused <code>ESR_EL2.ISS.ISV</code> to be set to '1' can be emulated by the Host.
R_XLSKP	Realm instruction fetch from an Unprotected IPA causes a Synchronous External Abort taken to the Realm. See also: <ul style="list-style-type: none"> <li>• <a href="#">A4.2.3 REC entry following REC exit due to Data Abort</a></li> <li>• <a href="#">A4.3.4.3 REC exit due to Data Abort</a></li> <li>• <a href="#">A4.4 Emulated Data Aborts</a></li> <li>• <a href="#">A5.2.7 Synchronous External Aborts</a></li> </ul>

## A5.2.7 Synchronous External Aborts

R_VKNJW	When a Synchronous External Abort is taken to a Realm, <code>ESR_EL1.EA == '1'</code> .
---------	---

## A5.2.8 Realm access outside IPA space

R_GYVZQ	If stage 1 translation is enabled, Realm access to an IPA which is greater than the IPA space of the Realm causes a stage 1 Address Size Fault taken to the Realm, with the fault status code indicating the level at which the fault occurred.
R_LSJJR	If stage 1 translation is disabled, Realm access to an IPA which is greater than the IPA space of the Realm causes a stage 1 level 0 Address Size Fault taken to the Realm.

## A5.2.9 Summary of Realm IPA space properties

└TPGKW

The following table summarizes the properties of Realm IPA space.

Realm IPA	Data access causes abort to Realm?	Data access causes REC exit due to Data Abort?	Instruction fetch causes abort to Realm?	Instruction fetch causes REC exit due to Instruction Abort?
Protected, RIPAS=EMPTY	Always (SEA)	Never	Always (SEA)	Never
Protected, RIPAS=RAM	Never	When HIPAS=UNASSIGNED	Never	When HIPAS=UNASSIGNED
Protected, RIPAS=DESTROYED	Never	Always	Never	Always
Unprotected	Host can inject SEA following REC exit due to Data Abort	When HIPAS=UNASSIGNED_NS	Always (SEA)	Never
Outside Realm IPA space	Always (Address Size Fault)	Never	Always (Address Size Fault)	Never

See also:

- [A4.2.3 REC entry following REC exit due to Data Abort](#)

## A5.3 Host view of memory management

This section describes memory management from the Host's point of view.

### A5.3.1 Host IPA state

D<sub>YZTZJ</sub>

A Realm IPA has an associated *Host IPA state* (HIPAS).

The HIPAS values for a Protected IPA are shown in the following table.

HIPAS	Description
UNASSIGNED	Address is not associated with any Granule.
ASSIGNED	Address is associated with a DATA Granule.

The HIPAS values for an Unprotected IPA are shown in the following table.

HIPAS	Description
UNASSIGNED_NS	Address is not associated with any Granule.
ASSIGNED_NS	Host-owned memory is mapped at this address.

I<sub>TRSKJ</sub>

HIPAS values are stored in a Realm Translation Table (RTT).

I<sub>GZMKQ</sub>

HIPAS transitions are caused by execution of RMI commands.

I<sub>NQCGS</sub>

A mapping at a Protected IPA is valid if the HIPAS is ASSIGNED and the RIPAS is RAM.

I<sub>YMNSR</sub>

The following table summarizes, for each combination of RIPAS and HIPAS for a Protected IPA:

- the translation table entry attributes, and
- the behavior which results from Realm access to that IPA.

Each TTD.X column refers to the value of the corresponding “X” field in the architecturally-defined Stage 2 translation table descriptor which is written by the RMM.

RIPAS	HIPAS	TTD.ADDR	TTD.NS	TTD.VALID	Data access	Instruction fetch
EMPTY	UNASSIGNED			0	SEA to Realm	SEA to Realm
EMPTY	ASSIGNED	DATA		0	SEA to Realm	SEA to Realm
RAM	UNASSIGNED			0	REC exit due to Data Abort	REC exit due to Instruction Abort
RAM	ASSIGNED	DATA	0	1	Data access	Instruction fetch
DESTROYED	UNASSIGNED			0	REC exit due to Data Abort	REC exit due to Instruction Abort
DESTROYED	ASSIGNED	DATA		0	REC exit due to Data Abort	REC exit due to Instruction Abort

See also:

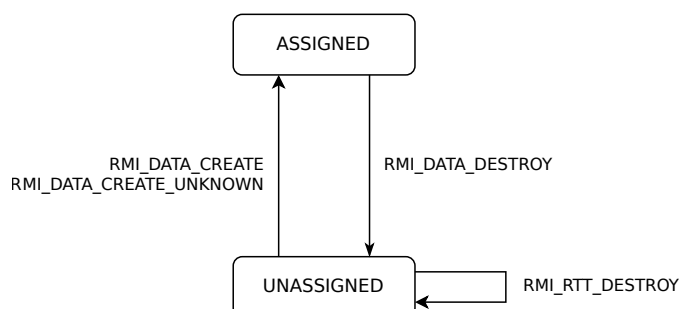
- [A5.5 Realm Translation Table](#)

### A5.3.2 Changes to HIPAS while Realm state is NEW

This section describes how the HIPAS of a Protected IPA can change while the Realm state is NEW.

I<sub>YNFGD</sub>

The following diagram summarizes HIPAS changes at a Protected IPA which can occur when the Realm state is NEW.



See also:

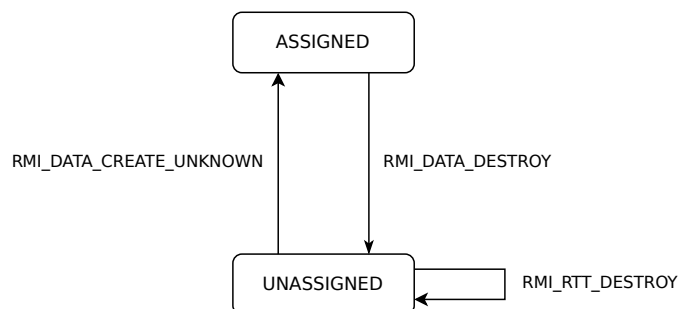
- [B3.3.1 RMI\\_DATA\\_CREATE command](#)
- [B3.3.2 RMI\\_DATA\\_CREATE\\_UNKNOWN command](#)
- [B3.3.3 RMI\\_DATA\\_DESTROY command](#)
- [B3.3.16 RMI\\_RTT\\_DESTROY command](#)

### A5.3.3 Changes to HIPAS while Realm state is ACTIVE

This section describes how the HIPAS of a Protected IPA can change while the Realm state is ACTIVE.

I<sub>WKZXY</sub>

The following diagram summarizes HIPAS changes at a Protected IPA which can occur when the Realm state is ACTIVE.



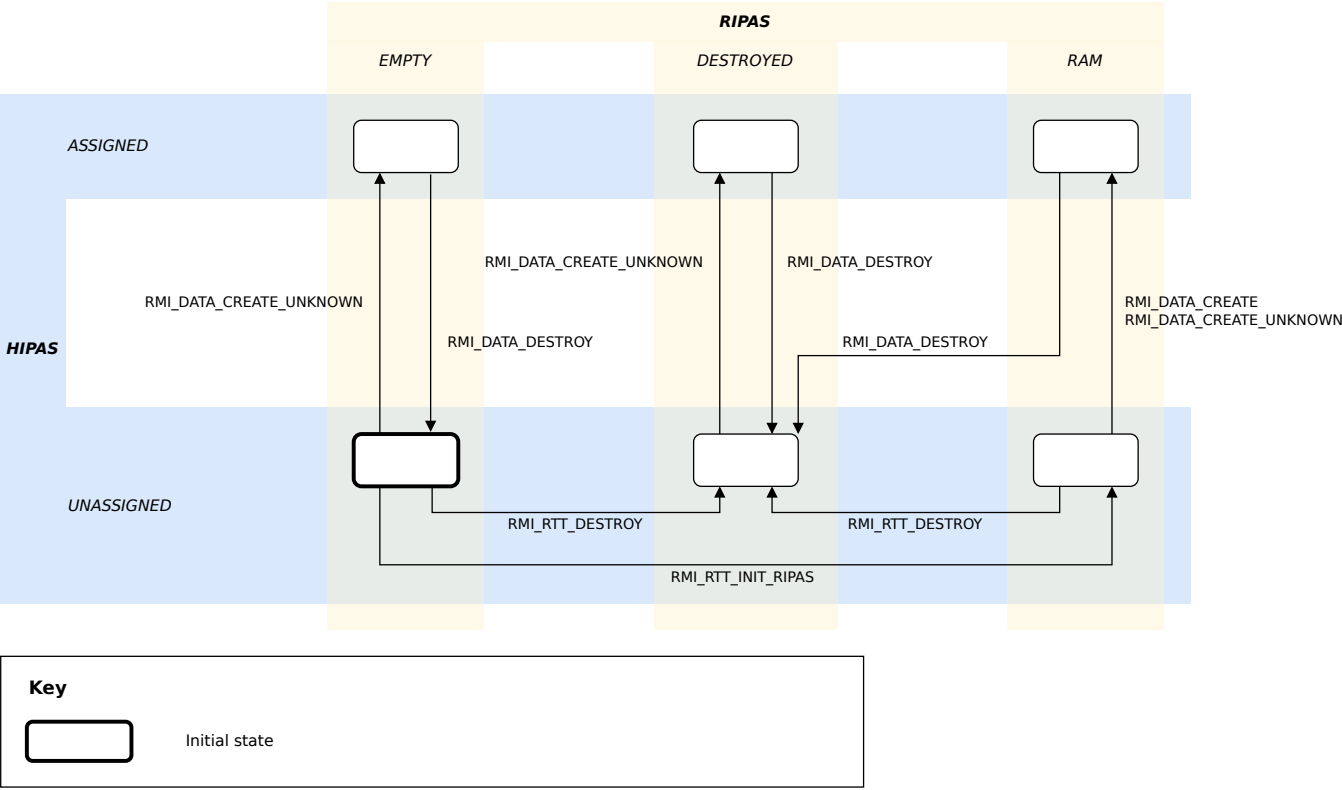
See also:

- [B3.3.2 `RMI\_DATA\_CREATE\_UNKNOWN` command](#)
- [B3.3.3 `RMI\_DATA\_DESTROY` command](#)
- [B3.3.16 `RMI\_RTT\_DESTROY` command](#)

A5.3.4 Summary of changes to HIPAS and RIPAS of a Protected IPA

└─TJ MCP

The following diagram summarizes HIPAS and RIPAS changes at a Protected IPA which can occur when the Realm state is NEW.



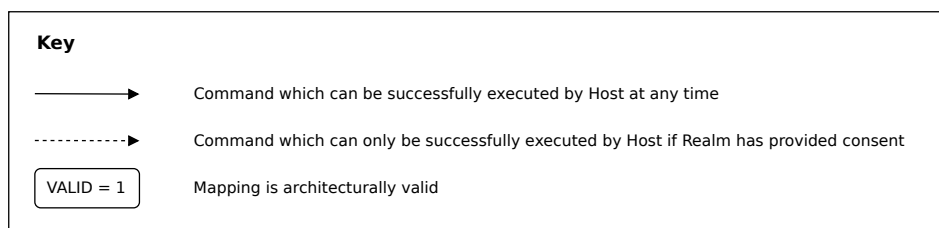
The diagram illustrates the state transitions for the RIPAS scheme across three memory regions: EMPTY, DESTROYED, and RAM. The states are represented by rounded rectangles, and the transitions are labeled with RMI commands.

**States:**

- EMPTY:**
  - Top: VALID = 0
  - Bottom: VALID = 0
- DESTROYED:**
  - Top: VALID = 0
  - Bottom: VALID = 0
- RAM:**
  - Top: VALID = 1
  - Bottom: VALID = 0

**Transitions:**

- EMPTY (Top) to EMPTY (Bottom):** RMI\_DATA\_DESTROY
- EMPTY (Bottom) to EMPTY (Top):** RMI\_DATA\_CREATE\_UNKNOWN
- DESTROYED (Top) to DESTROYED (Bottom):** RMI\_DATA\_DESTROY
- DESTROYED (Bottom) to DESTROYED (Top):** RMI\_DATA\_CREATE\_UNKNOWN
- RAM (Top) to RAM (Bottom):** RMI\_DATA\_DESTROY
- RAM (Bottom) to RAM (Top):** RMI\_DATA\_CREATE\_UNKNOWN
- EMPTY (Top) to DESTROYED (Top):** RMI\_RTT\_SET\_RIPAS
- DESTROYED (Top) to EMPTY (Top):** RMI\_RTT\_DESTROY
- DESTROYED (Top) to RAM (Top):** RMI\_RTT\_DESTROY
- DESTROYED (Bottom) to EMPTY (Bottom):** RMI\_RTT\_DESTROY
- DESTROYED (Bottom) to RAM (Bottom):** RMI\_RTT\_DESTROY
- EMPTY (Bottom) to DESTROYED (Bottom):** RMI\_RTT\_DESTROY
- EMPTY (Bottom) to RAM (Bottom):** RMI\_RTT\_DESTROY
- DESTROYED (Bottom) to EMPTY (Bottom):** RMI\_RTT\_DESTROY
- DESTROYED (Bottom) to RAM (Bottom):** RMI\_RTT\_DESTROY
- RAM (Bottom) to DESTROYED (Bottom):** RMI\_RTT\_DESTROY
- RAM (Bottom) to EMPTY (Bottom):** RMI\_RTT\_DESTROY
- RAM (Bottom) to DESTROYED (Bottom):** RMI\_RTT\_DESTROY
- RAM (Bottom) to EMPTY (Bottom):** RMI\_RTT\_DESTROY
- EMPTY (Bottom) to DESTROYED (Bottom):** RMI\_RTT\_DESTROY
- EMPTY (Bottom) to RAM (Bottom):** RMI\_RTT\_DESTROY
- DESTROYED (Bottom) to EMPTY (Bottom):** RMI\_RTT\_DESTROY
- DESTROYED (Bottom) to RAM (Bottom):** RMI\_RTT\_DESTROY
- RAM (Bottom) to DESTROYED (Bottom):** RMI\_RTT\_DESTROY
- RAM (Bottom) to EMPTY (Bottom):** RMI\_RTT\_DESTROY
- RAM (Bottom) to DESTROYED (Bottom):** RMI\_RTT\_DESTROY
- RAM (Bottom) to EMPTY (Bottom):** RMI\_RTT\_DESTROY



- B3.3.1 *RMI\_DATA\_CREATE* command
- B3.3.2 *RMI\_DATA\_CREATE\_UNKNOWN* command
- B3.3.3 *RMI\_DATA\_DESTROY* command
- B3.3.16 *RMI\_RTT\_DESTROY* command
- B3.3.18 *RMI\_RTT\_INIT\_RIPAS* command
- B3.3.21 *RMI\_RTT\_SET\_RIPAS* command



### A5.3.5 Dependency of RMI command execution on RIPAS and HIPAS values

$\mathcal{I}_{HLHZS}$  The following table summarizes dependencies on RMI command execution on the current Protected IPA.

Command	Dependency on RIPAS	Dependency on HIPAS	New RIPAS	New HIPAS
RMI_DATA_CREATE	RIPAS is RAM	HIPAS is UNASSIGNED	Unchanged	ASSIGNED
RMI_DATA_CREATE_UNKNOWN	None	HIPAS is UNASSIGNED	Unchanged	ASSIGNED
RMI_DATA_DESTROY	If RIPAS is EMPTY	HIPAS is ASSIGNED	Unchanged	UNASSIGNED
RMI_DATA_DESTROY	If RIPAS is RAM	HIPAS is ASSIGNED	DESTROYED	UNASSIGNED
RMI_RTT_CREATE	None	None	Unchanged	Unchanged
RMI_RTT_DESTROY	None	HIPAS of all entries is UNASSIGNED	DESTROYED	Unchanged
RMI_RTT_FOLD	RIPAS of all entries is identical	HIPAS of all entries is identical	Unchanged	Unchanged
RMI_RTT_INIT_RIPAS	RIPAS is EMPTY	HIPAS is UNASSIGNED	RAM	Unchanged
RMI_RTT_SET_RIPAS	Optionally, Realm may specify that RIPAS is not DESTROYED	None	As specified by Realm	Unchanged

$\mathcal{I}_{WBR CN}$  Successful execution of RMI\_DATA\_CREATE\_UNKNOWN does not depend on the RIPAS value of the target IPA.

$\mathcal{I}_{LCSVH}$  Successful execution of RMI\_DATA\_DESTROY does not depend on the RIPAS value of the target IPA.

$\mathcal{I}_{MMSBL}$  Successful execution of RMI\_RTT\_DESTROY does not depend on the RIPAS values of entries in the target RTT.

$\mathcal{I}_{TJCGT}$  Successful execution of RMI\_RTT\_FOLD does depend on the RIPAS values of entries in the target RTT.

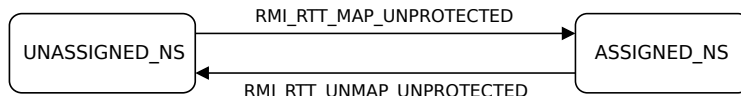
See also:

- [B3.3.1 RMI\\_DATA\\_CREATE command](#)
- [B3.3.2 RMI\\_DATA\\_CREATE\\_UNKNOWN command](#)
- [B3.3.3 RMI\\_DATA\\_DESTROY command](#)
- [B3.3.15 RMI\\_RTT\\_CREATE command](#)
- [B3.3.16 RMI\\_RTT\\_DESTROY command](#)
- [B3.3.17 RMI\\_RTT\\_FOLD command](#)
- [B3.3.18 RMI\\_RTT\\_INIT\\_RIPAS command](#)
- [B3.3.21 RMI\\_RTT\\_SET\\_RIPAS command](#)

### A5.3.6 Changes to HIPAS of an Unprotected IPA

I<sub>YNYBY</sub>

The following diagram summarises HIPAS transitions for an Unprotected IPA.



See also:

- [A5.4 RIPAS change](#)
- [A5.5 Realm Translation Table](#)
- [B3.3.1 RMI\\_DATA\\_CREATE command](#)
- [B3.3.2 RMI\\_DATA\\_CREATE\\_UNKNOWN command](#)
- [B3.3.3 RMI\\_DATA\\_DESTROY command](#)
- [B3.3.16 RMI\\_RTT\\_DESTROY command](#)
- [B3.3.18 RMI\\_RTT\\_INIT\\_RIPAS command](#)
- [B3.3.21 RMI\\_RTT\\_SET\\_RIPAS command](#)
- [B4.3.5 RSI\\_IPA\\_STATE\\_SET command](#)

## A5.4 RIPAS change

**D<sub>BTSQY</sub>** A *RIPAS change* is a process via which the RIPAS of a region of Protected IPA space is changed, for a Realm whose state is ACTIVE.

**I<sub>KXXBV</sub>** A RIPAS change consists of actions taken by first the Realm, and then the Host:

- The Realm issues a *RIPAS change request* by executing RSI\_IPA\_STATE\_SET.
  - The input values to this command include:
    - \* The requested IPA range: [base, top)
    - \* The requested RIPAS value (either EMPTY or RAM)
    - \* A flag which indicates whether a change from DESTROYED should be permitted
  - The RMM records these values in the REC, and then performs a REC exit due to RIPAS change pending.
- In response, the Host executes zero or more RMI\_RTT\_SET\_RIPAS commands.
- If the requested RIPAS value was RAM, at the next RMI\_REC\_ENTER the Host can optionally indicate that it rejects the RIPAS change request.

Output values from RSI\_IPA\_STATE\_SET indicate:

- The top of the IPA range which has been modified by the command (new\_base).
- If the requested RIPAS value was RAM, whether the Host rejected the Realm request.

**S<sub>CTTQV</sub>** Output values from RSI\_IPA\_STATE\_SET are expected to be handled by the Realm as follows:

new_base	response	Meaning	Expected Realm action
new_base == base	RSI_ACCEPT	RIPAS change incomplete.	Call RSI_IPA_STATE_SET again, with base = new_base.
base < new_base < top	RSI_ACCEPT	RIPAS change incomplete.	Call RSI_IPA_STATE_SET again, with base = new_base.
new_base == top	RSI_ACCEPT	RIPAS change complete.	No further Realm action required.
new_base == base	RSI_REJECT	RIPAS change request rejected.	Depends on protocol agreed between Realm and Host, out of scope of this specification.
base < new_base < top	RSI_REJECT	RIPAS change to partial region [base, new_base). Host rejected request to change RIPAS for region [new_base, top).	Depends on protocol agreed between Realm and Host, out of scope of this specification.

**I<sub>RFVTG</sub>** The RIPAS change process, together with the Realm Initial Measurement ensures that a Realm can always reliably determine the RIPAS of any Protected IPA.

**I<sub>LPZWK</sub>** A RIPAS change is applied by one or more calls to the RMI\_RTT\_SET\_RIPAS command.

**I<sub>MMHMZ</sub>** Successful execution of RMI\_RTT\_SET\_RIPAS targets an RTTE at address `rec.ripas_addr`.

**I<sub>JHJGZ</sub>** On successful execution of RMI\_RTT\_SET\_RIPAS, both of the following are set to the address of the next page whose RIPAS is to be modified:

- `rec.ripas_addr`

- The command output value

I<sub>GXDDX</sub>

If both of the following are true on successful execution of RMI\_RTT\_SET\_RIPAS

- The RIPAS change request indicated that a change from DESTROYED should not be permitted
- A page *P* within the target IPA range has RIPAS value DESTROYED

then `rec.ripas_addr` and the command output value are both set to *P*.

I<sub>HXKPB</sub>

On REC entry following a REC exit due to RIPAS change, GPR values are updated to indicate for how much of the target IPA range the RIPAS change has been applied.

S<sub>TZYZV</sub>

To complete a RIPAS change for a given target IPA range, a Realm should execute RSI\_IPA\_STATE\_SET in a loop, until the value of X1 reaches the top of the target IPA range.

R<sub>LDMLC</sub>

On REC entry following a REC exit due to RIPAS change, `rec.ripas_response` is set to the value of `enter.flags.ripas_response`.

I<sub>DRPPK</sub>

If all of the following are true then the output value of RSI\_IPA\_STATE\_SET indicates “Host rejected the request”:

- `rec.ripas_value` is RAM.
- `rec.ripas_addr` is not equal to `rec.ripas_top`.
- `rec.ripas_response` is REJECT.

Otherwise, the output value of RSI\_IPA\_STATE\_SET indicates “Host accepted the request”.

See also:

- [A2.3.2 REC attributes](#)
- [A4.2 REC entry](#)
- [A4.3.8 REC exit due to RIPAS change pending](#)
- [A5.2.2 Realm IPA state](#)
- [A7.1.1 Realm Initial Measurement](#)
- [B2.38 RecRipasChangeResponse function](#)
- [B3.3.14 RMI\\_REC\\_ENTER command](#)
- [B3.3.21 RMI\\_RTT\\_SET\\_RIPAS command](#)
- [B4.3.5 RSI\\_IPA\\_STATE\\_SET command](#)
- [D1.5.3 RIPAS change flow](#)

## A5.5 Realm Translation Table

This section introduces the stage 2 translation table used by a Realm.

### A5.5.1 RTT overview

D <sub>FRNCX</sub>	A <i>Realm Translation Table</i> (RTT) is an abstraction over an Armv8-A stage 2 translation table used by a Realm.
I <sub>MBCVZ</sub>	The attributes and format of an Armv8-A stage 2 translation table are defined by the Armv8-A Virtual Memory System Architecture (VMSA) <i>Arm Architecture Reference Manual for A-Profile architecture</i> [3].
R <sub>PXNHQ</sub>	The translation granule size of an RTT is 4KB.
I <sub>TQVTP</sub>	The RMM architecture can only be deployed on a hardware platform which implements a translation granule size of 4KB.
I <sub>PHGQQ</sub>	The contents of an RTT are not directly accessible to the Host.
I <sub>FPLRL</sub>	The contents of an RTT are manipulated using RMM commands. These commands allow the Host to manipulate the contents of the RTT used by a Realm, subject to constraints imposed by the RMM.
D <sub>QTZDW</sub>	An <i>RTT entry</i> (RTTE) is an abstraction over an Armv8-A stage 2 translation table descriptor.
I <sub>VYLTT</sub>	An RTTE contains an output address which can point to one of the following: <ul style="list-style-type: none"><li>• Another RTT</li><li>• A DATA Granule which is owned by the Realm</li><li>• Non-secure memory which is accessible to both the Realm and the Host</li></ul>

### A5.5.2 RTT structure and configuration

D <sub>VHLWF</sub>	An <i>RTT tree</i> is a hierarchical data structure composed of RTTs, connected via Table Descriptors.
I <sub>KNPNX</sub>	An RTT contains an array of RTTEs.
D <sub>HYTCJ</sub>	An <i>RTT level</i> is the depth of an RTT within an RTT tree.
I <sub>KKMSX</sub>	An RTT does not have an intrinsic “level” attribute. The level of an RTT is determined by its position within an RTT tree.
D <sub>QSYBS</sub>	The RTT level of the root of an RTT tree is called the <i>starting level</i> .
I <sub>SSDBT</sub>	The maximum depth of an RTT tree depends on all of the following: <ul style="list-style-type: none"><li>• whether LPA2 is selected when the Realm is created</li><li>• the <code>rtt_level_start</code> attribute of the Realm</li><li>• the <code>ipa_width</code> attribute of the Realm.</li></ul> See also: <ul style="list-style-type: none"><li>• <a href="#">A2.1.3 Realm attributes</a></li><li>• <a href="#">A3.1.2 Realm LPA2 and IPA width</a></li></ul>

### A5.5.3 RTT starting level

I <sub>FDWZF</sub>	The RTT starting level is set when a Realm is created.
I <sub>YCPMF</sub>	The number of starting level RTTs is architecturally defined as a function of the Realm IPA width and the RTT starting level. See <i>Arm Architecture Reference Manual for A-Profile architecture</i> [3] for further details.

$I_{RYNXB}$  The address of the first starting level RTT is stored in the RTT base attribute of the owning Realm.

$I_{XXWQW}$  The RTT base attribute is set when a Realm is created.

See also:

- [A2.1.3 Realm attributes](#)

#### A5.5.4 RTT entry

$I_{ZBGGZ}$  An RTT entry (RTTE) is an abstraction over an Armv8-A stage 2 translation table descriptor. The attributes and format of an Armv8-A stage 2 translation table descriptor are defined by the Armv8-A Virtual Memory System Architecture (VMSA) *Arm Architecture Reference Manual for A-Profile architecture* [3].

$D_{BNHQQ}$  An RTTE has a *state*.

The values of *RTTE state* are:

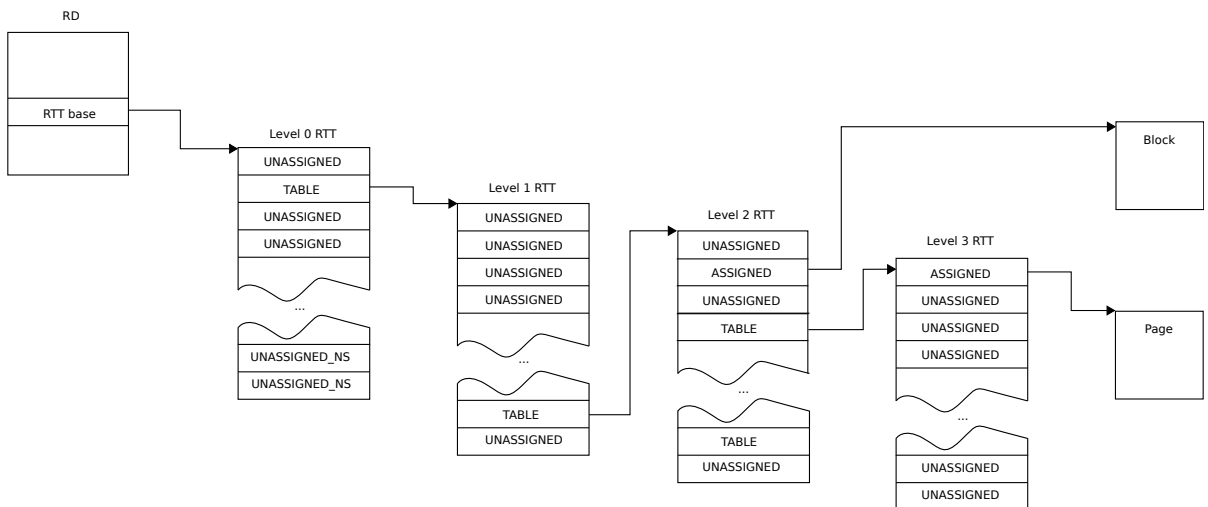
- TABLE: the output address of the RTTE points to another RTT
- A HIPAS value

$I_{QWQSB}$  The state of an RTTE in a RTT which is not level 2 or level 3 is UNASSIGNED, UNASSIGNED\_NS or TABLE.

$D_{NSHSL}$  The output address of an RTTE whose state is TABLE and which is in a level  $n$  RTT is the physical address of a level  $n+1$  RTT.

$I_{DJZTM}$  An RTT whose level  $n$  is not the starting RTT level is pointed-to by exactly one TABLE RTTE in a level  $n-1$  RTT.

$I_{DXQWZ}$  The following diagram shows an example RTT tree, annotated with RTTE states.



$I_{FGWQS}$  The function `AddrIsRttLevelAligned()` is used to evaluate whether an address is aligned to the address range described by an RTTE at a specified RTT level.

See also:

- [A5.3.1 Host IPA state](#)
- [B1.4 Command condition expressions](#)

#### A5.5.5 RTT reading

$I_{KJWQO}$  Attributes of an RTTE, including the RTTE state, can be read by calling the `RMI_RTT_READ_ENTRY` command. The set of RTTE attributes which are returned depends on the state of the RTTE.

See also:

- [B3.3.20 RMI\\_RTT\\_READ\\_ENTRY command](#)

## A5.5.6 RTT folding

D<sub>RMCLC</sub>

An RTT is *homogeneous* if its entries satisfy one of the conditions in the following table. If an RTT is homogeneous, the following table specifies the state to which the parent RTTE is set.

Conditions on child RTT contents	Parent RTTE state
All of the following are true: <ul style="list-style-type: none"> <li>• State of all entries is UNASSIGNED</li> <li>• RIPAS of all entries is the same</li> </ul>	UNASSIGNED
State of all entries is UNASSIGNED_NS	UNASSIGNED_NS
All of the following are true: <ul style="list-style-type: none"> <li>• Level is 2 or 3</li> <li>• State of all entries is ASSIGNED</li> <li>• Output address of first entry is aligned to size of the address range described by an entry in the parent RTT</li> <li>• Output addresses of all entries are contiguous</li> <li>• RIPAS of all entries is the same</li> </ul>	ASSIGNED
All of the following are true: <ul style="list-style-type: none"> <li>• Level is 2 or 3</li> <li>• State of all entries is ASSIGNED_NS</li> <li>• Output address of first entry is aligned to size of the address range described by an entry in the parent RTT</li> <li>• Output addresses of all entries are contiguous</li> <li>• Attributes of all entries are identical</li> </ul>	ASSIGNED_NS

I<sub>KDXLT</sub>

The function `RttIsHomogeneous()` is used to evaluate whether an RTT is homogeneous.

D<sub>QPCXP</sub>

*RTT folding* is the operation of destroying a homogeneous child RTT, and moving information which was stored in the child RTT into the parent RTTE.

I<sub>QMGWK</sub>

On RTT folding, the state of the parent RTTE is determined from the contents of the child RTTEs.

I<sub>LLWGH</sub>

The function `RttFold()` is used to evaluate the parent RTTE state which results from an RTT folding operation.

I<sub>TPMGT</sub>

On RTT folding, if the state of the parent RTTE is ASSIGNED or ASSIGNED\_NS then the attributes of the parent RTTE are copied from the child RTTEs.

See also:

- [A5.5.9 RTT destruction](#)
- [B2.59 RttFold function](#)
- [B2.60 RttIsHomogeneous function](#)
- [B3.3.17 RMI\\_RTT\\_FOLD command](#)

## A5.5.7 RTT unfolding

D<sub>HQQMG</sub>

*RTT unfolding* is the operation of creating a child RTT, and populating it based on the contents of the parent RTTE.

<code>I_KWZXN</code>	On RTT unfolding, the state of all RTTEs in the child RTT are set to the state of the parent RTTE.
<code>I_HMYSW</code>	On RTT unfolding, if the state of the parent RTTE is ASSIGNED or ASSIGNED_NS, then the output addresses of RTTEs in the child RTT are set to a contiguous range which starts from the address of the parent RTTE.

See also:

- [B3.3.15 RMI\\_RTT\\_CREATE command](#)

### A5.5.8 RTTE liveness and RTT liveness

<code>D_KCMLN</code>	<i>RTTE liveness</i> is a property which means that a physical address is stored in the RTTE.
<code>D_HGYJZ</code>	An RTTE is <i>live</i> if the RTTE state is ASSIGNED, ASSIGNED_NS or TABLE.
<code>I_RHLYZ</code>	The function <code>RttSkipNonLiveEntries()</code> is used to scan an RTT to find the next live RTTE. The resulting IPA is returned to the Host from commands whose successful execution causes a live RTTE to become non-live.
<code>X_GQPSF</code>	Identifying the next live RTTE allows the Host to avoid calls to <code>RMI_RTT_READ_ENTRY</code> when unmapping ranges of a Realm's IPA space, for example during Realm destruction.
<code>D_MPWLR</code>	<i>RTT liveness</i> is a property which means that there exists another RMM data structure which is referenced by the RTT.
<code>D_YPSLW</code>	An RTT is <i>live</i> if, for any of its entries, either of the following is true: <ul style="list-style-type: none"> <li>• The RTTE state is ASSIGNED</li> <li>• The RTTE state is TABLE.</li> </ul>
<code>I_MXJNY</code>	Note that an RTT can be non-live, even if one of its entries is live. This would be the case for example if the RTT corresponds to an Unprotected IPA range and the state of one of its entries is ASSIGNED_NS.
<code>I_YPLKM</code>	The function <code>RttIsLive()</code> is used to evaluate whether an RTT is live.

See also:

- [A5.5.9 RTT destruction](#)
- [B2.61 RttIsLive function](#)
- [B2.73 RttSkipNonLiveEntries function](#)
- [B3.3.3 RMI\\_DATA\\_DESTROY command](#)
- [B3.3.16 RMI\\_RTT\\_DESTROY command](#)
- [B3.3.22 RMI\\_RTT\\_UNMAP\\_UNPROTECTED command](#)

### A5.5.9 RTT destruction

<code>D_VXRZW</code>	<i>RTT destruction</i> is the operation of destroying a child RTT, and discarding information which was stored in the child RTT.
<code>I_PRMFR</code>	An RTT cannot be destroyed if it is live.
<code>I_MDFQN</code>	An RTT can be destroyed regardless of whether it is homogeneous.
<code>I_MCKSK</code>	Following RTT destruction, all of the following are true for the parent RTTE: <ul style="list-style-type: none"> <li>• RIPAS is DESTROYED</li> <li>• RTTE state is UNASSIGNED</li> </ul>

See also:

- [A5.2 Realm view of memory management](#)
- [A5.5.6 RTT folding](#)
- [A5.5.8 RTTE liveness and RTT liveness](#)



- [B3.3.16 RMI\\_RTT\\_DESTROY command](#)

### A5.5.10 RTT walk

I <sub>CBWSX</sub>	An IPA is translated to a PA by walking an RTT tree, starting at the RTT base.
I <sub>FDWYV</sub>	The behaviour of an RTT walk is defined by the Armv8-A Virtual Memory System Architecture (VMSA) <i>Arm Architecture Reference Manual for A-Profile architecture</i> [3].
I <sub>TVGQD</sub>	<p>The inputs to an RTT walk are:</p> <ul style="list-style-type: none"><li>• a Realm Descriptor, which contains the address of the initial RTT</li><li>• a target IPA</li><li>• a target RTT level.</li></ul> <p>The RTT walk terminates when either:</p> <ul style="list-style-type: none"><li>• it reaches the target RTT level, or</li><li>• it reaches an RTTE whose state is not TABLE.</li></ul>
D <sub>RBHVQ</sub>	<p>The result of an RTT walk performed by the RMM is a data structure of type <code>RmmRttWalkResult</code>.</p> <p>The attributes of an <code>RmmRttWalkResult</code> are summarized in the following table.</p>

Name	Type	Description
level	<a href="#">Int8</a>	RTT level reached by the walk
rtt_addr	<a href="#">Address</a>	Address of RTT reached by the walk
rtte	<a href="#">RmmRttEntry</a>	RTTE reached by the walk

I <sub>ZSRCD</sub>	The function <code>RmmRttWalkResult RttWalk(rd, addr, level)</code> is used to represent an RTT walk.
I <sub>FBZPQ</sub>	<p>The input address to an RTT walk is always less than <math>2^w</math>, where <math>w</math> is the IPA width of the target Realm.</p> <p>See also:</p>

- [A2.1.3 Realm attributes](#)
- [B1.4 Command condition expressions](#)
- [B2.75 RttWalk function](#)
- [B3.3.1 RMI\\_DATA\\_CREATE command](#)
- [B3.3.2 RMI\\_DATA\\_CREATE\\_UNKNOWN command](#)
- [B3.3.3 RMI\\_DATA\\_DESTROY command](#)
- [B3.3.15 RMI\\_RTT\\_CREATE command](#)
- [B3.3.16 RMI\\_RTT\\_DESTROY command](#)
- [B3.3.19 RMI\\_RTT\\_MAP\\_UNPROTECTED command](#)
- [B3.3.22 RMI\\_RTT\\_UNMAP\\_UNPROTECTED command](#)
- [C1.25 RmmRttWalkResult type](#)

### A5.5.11 RTT entry attributes

R <sub>KCFCT</sub>	The cacheability attributes of an RTT entry which corresponds to a Protected IPA and whose state is ASSIGNED are independent of any stage 1 descriptors and of the state of the stage 1 MMU.
U <sub>NPVGN</sub>	The RMM uses FEAT_S2FWB to ensure that the cacheability attributes of an RTT entry which corresponds to a Protected IPA and whose state is ASSIGNED are independent of stage 1 translation.

R <sub>JZKMH</sub>	<p>The attributes of an RTT entry which corresponds to a Protected IPA and whose state is ASSIGNED include the following:</p> <ul style="list-style-type: none"> <li>• Normal memory</li> <li>• Inner Write-Back Cacheable</li> <li>• Inner Shareable</li> </ul>
D <sub>FJTME</sub>	<p>The following attributes of an RTT entry which corresponds to an Unprotected IPA and whose state is ASSIGNED_NS are <i>Host-controlled RTT attributes</i>:</p> <ul style="list-style-type: none"> <li>• ADDR</li> <li>• MemAttr[2:0]</li> <li>• S2AP</li> <li>• SH</li> </ul>
X <sub>QHLLKB</sub>	<p>In an RTT entry which corresponds to an Unprotected IPA and whose state is ASSIGNED_NS, MemAttr[3] is RES0 because the RMM uses FEAT_S2FWB.</p>
R <sub>JRZTL</sub>	<p>Hardware access flag and dirty bit management is disabled for the stage 2 translation used by a Realm.</p>
I <sub>QFGJC</sub>	<p>Hardware access flag and dirty bit management may be enabled by software executing within the Realm, for its own stage 1 translation.</p> <p>See also:</p> <ul style="list-style-type: none"> <li>• <a href="#">A5.2.1 Realm IPA space</a></li> <li>• <a href="#">B2.53 RttDescriptorIsValidForUnprotected function</a></li> <li>• <a href="#">B3.3.19 RMI_RTT_MAP_UNPROTECTED command</a></li> <li>• <a href="#">B3.3.20 RMI_RTT_READ_ENTRY command</a></li> </ul>

## Chapter A6

### Realm interrupts and timers

This specification requires that a virtual Generic Interrupt Controller (vGIC) is presented to a Realm. This vGIC should be architecturally compliant with respect to GICv3 with no legacy operation.

The Host is able to inject virtual interrupts using the GIC virtual CPU interface.

The vGIC presented to a Realm is expected to be implemented via a combination of Host emulation and RMM mediation, as follows:

- Management of Non-secure physical interrupts is performed by the Host, via the GIC Interrupt Routing Infrastructure (IRI).
- The Host is responsible for emulating a GICv3 distributor MMIO interface.
- The Host is responsible for emulating a GICv3 redistributor MMIO interface for each REC.
- The GIC MMIO interfaces emulated by the Host must be presented to the Realm via its Unprotected IPA space.
- The Host may optionally provide a virtual Interrupt Translation Service (ITS). The Realm must allocate ITS tables within its Unprotected IPA space.
- The RMM allows the Host to control some of the GIC virtual CPU interface state which is observed by the Realm. This state is designed to be the minimum required to allow the Host to correctly manage interrupts for the Realm, with integrity guaranteed by the RMM for the remainder of the GIC CPU interface state.
- On REC exit, the RMM exposes some of the GIC virtual CPU interface state to the Host. This state is designed to be the minimum required to allow the Host to correctly manage interrupts for the Realm, with confidentiality guaranteed by the RMM for the remainder of the GIC virtual CPU interface state.

On every REC exit, the EL1 timer state is exposed to the Host. The RMM guarantees that a REC exit occurs whenever a Realm EL1 timer asserts or de-asserts its output.

See also:

- *Arm Generic Interrupt Controller (GIC) Architecture Specification version 3 and version 4* [\[5\]](#)
- [A5.2.1 Realm IPA space](#)
- [D1.6 Realm interrupts and timers flows](#)

## A6.1 Realm interrupts

This section describes the programming model for a REC's GIC CPU interface.

D <sub>XZVGB</sub>	<p>The value of <code>enter.gicv3_lrs[n]</code> is valid if all of the following are true:</p> <ul style="list-style-type: none"> <li>• The value is an architecturally valid encoding of <code>ICH_LR&lt;n&gt;_EL2</code> according to <i>Arm Generic Interrupt Controller (GIC) Architecture Specification version 3 and version 4</i> [5].</li> <li>• <code>HW == '0'</code>.</li> </ul>
X <sub>DMSDZ</sub>	<p>The GICv3 architecture states that, if <code>HW == '1'</code> then the virtual interrupt must be linked to a physical interrupt whose state is Active, otherwise behavior is undefined. The RMM is unable to validate that invariant, so it imposes the constraint that <code>HW == '0'</code>.</p>
D <sub>CPLDX</sub>	<p>The value of <code>enter.gicv3_hcr</code> is valid if the value is an architecturally valid encoding of <code>ICH_HCR_EL2</code> according to <i>Arm Generic Interrupt Controller (GIC) Architecture Specification version 3 and version 4</i> [5].</p>
R <sub>HLEFRY</sub>	<p>REC entry fails if the value of any <code>enter.gicv3_*</code> attribute is invalid.</p>
R <sub>WNFRW</sub>	<p>On REC entry, <code>ICH_LR&lt;n&gt;_EL2</code> is set to <code>enter.gicv3_lrs[n]</code>, for all values of <code>n</code> supported by the PE.</p>
R <sub>WVGFIJ</sub>	<p>On REC entry, the following fields in <code>ICH_HCR_EL2</code> are set to the corresponding values in <code>enter.gicv3_hcr</code>:</p> <ul style="list-style-type: none"> <li>• <code>UIE</code></li> <li>• <code>LRENPIE</code></li> <li>• <code>NPIE</code></li> <li>• <code>VGrp0EIE</code></li> <li>• <code>VGrp0DIE</code></li> <li>• <code>VGrp1EIE</code></li> <li>• <code>VGrp1DIE</code></li> <li>• <code>TDIR</code></li> </ul>
I <sub>SMHXB</sub>	<p>On REC entry, fields in <code>enter.gicv3_hcr</code> must be set to '0' except for the following:</p> <ul style="list-style-type: none"> <li>• <code>UIE</code></li> <li>• <code>LRENPIE</code></li> <li>• <code>NPIE</code></li> <li>• <code>VGrp0EIE</code></li> <li>• <code>VGrp0DIE</code></li> <li>• <code>VGrp1EIE</code></li> <li>• <code>VGrp1DIE</code></li> <li>• <code>TDIR</code></li> </ul> <p>If any other field in <code>enter.gicv3_hcr</code> is set to '1', then <code>RMI_REC_ENTER</code> fails.</p>
X <sub>LMXCX</sub>	<p>The RMM provides access to the GIC virtual CPU interface to the Realm and therefore controls the enable bit and most trap bits in <code>ICH_HCR_EL2</code>. The maintenance interrupt control bits are controlled by the Host, because the maintenance interrupts are provided as hints to the hypervisor to allocate List Registers optimally and to correctly emulate GICv3 behavior. The <code>TDIR</code> bit is also controlled by the Host because it is used when supporting <code>EOImode == '1'</code> in the Realm. This mode is used to allow deactivation of virtual interrupts across RECs. This deactivation must be handled by the Host because the RMM can only operate on a single REC during execution of <code>RMI_REC_ENTER</code>.</p>
R <sub>LNQRL</sub>	<p>A REC exit due to IRQ is not generated for an interrupt which is masked by the value of <code>ICC_PMR_EL1</code> at the time of REC entry.</p>
U <sub>GXCHC</sub>	<p>The RMM should preserve the value of <code>ICC_PMR_EL1</code> during REC entry.</p>
R <sub>NKPNC</sub>	<p>On REC exit, <code>exit.gicv3_vmcr</code> contains the value of <code>ICH_VMCR_EL2</code> at the time of the Realm exit.</p>
R <sub>SKQNF</sub>	<p>On REC exit, <code>exit.gicv3_misr</code> contains the value of <code>ICH_MISR_EL2</code> at the time of the Realm exit.</p>

X <sub>DBGXB</sub>	The Host could in principle infer the value of ICH_MISR_EL2 at the time of the Realm exit from the combination of <code>exit.gicv3_lrs[n]</code> and <code>exit.gicv3_hcr</code> . However, this would be cumbersome, error-prone, and diverge from the design of existing hypervisor software.
R <sub>QKZXD</sub>	On REC exit, <code>exit.gicv3_lrs[n]</code> contains the value of ICH_LR<n>_EL2 at the time of the Realm exit, for all values of n supported by the PE.
R <sub>SNVZH</sub>	On REC exit, the following fields in <code>exit.gicv3_hcr</code> contains the value of the corresponding field in ICH_HCR_EL2 at the time of the Realm exit: <ul style="list-style-type: none"> <li>• EOICount</li> <li>• UIE</li> <li>• LRENPIE</li> <li>• NPIE</li> <li>• VGrp0EIE</li> <li>• VGrp0DIE</li> <li>• VGrp1EIE</li> <li>• VGrp1DIE</li> <li>• TDIR</li> </ul> <p>All other fields contain zero.</p>
R <sub>FGQXT</sub>	On REC exit, the values of the following registers may have changed: <ul style="list-style-type: none"> <li>• ICH_AP0R&lt;n&gt;_EL2</li> <li>• ICH_AP1R&lt;n&gt;_EL2</li> <li>• ICH_LR&lt;n&gt;_EL2</li> <li>• ICH_VMCR_EL2</li> <li>• ICH_HCR_EL2</li> </ul>
S <sub>QMJVJ</sub>	It is the responsibility of the caller to save and restore GIC virtualization system control registers if their value needs to be preserved following execution of RMI_REC_ENTER.
X <sub>KDGHF</sub>	On REC entry, the values of the GIC virtualization control system registers are overwritten. The Non-secure hypervisor runs at EL2 and therefore does not make direct use of the virtual GIC CPU interface for its own execution. This means that saving / restoring the caller's GIC virtualization control system registers would typically not be required and would add additional runtime overhead for each execution of RMI_REC_ENTER.
R <sub>VSBBS</sub>	On REC exit, <code>ICH_HCR_EL2.En == '0'</code> .
X <sub>WLTBX</sub>	Disabling the virtual GIC CPU interface ensures that the caller does not receive unexpected GIC maintenance interrupts. A stronger constraint, for example stating that all GIC virtualization control system registers are zero on REC exit, was considered. However, this was rejected on the basis that it may preclude future optimisations, such as returning early from execution of RMI_REC_ENTER, without needing to first write zero to all GIC virtualization control system registers, if an interrupt is pending.

See also:

- *Arm Generic Interrupt Controller (GIC) Architecture Specification version 3 and version 4* [5]
- [A4.2 REC entry](#)
- [A4.3 REC exit](#)
- [B3.3.14 RMI\\_REC\\_ENTER command](#)
- [B3.4.14 RmiRecEnter type](#)
- [B3.4.16 RmiRecExit type](#)
- [D1.6.1 Interrupt flow](#)

## A6.2 Realm timers

This section describes the programming model for Realm EL1 timers.

R <sub>LKNDV</sub>	Architectural timers are available to a Realm and behave according to their architectural specification.
R <sub>YWXTJ</sub>	During Realm execution, if a Realm EL1 timer asserts its output, a Realm exit occurs.
I <sub>VFYJV</sub>	If the Host has programmed an EL1 timer to assert its output during Realm execution, that timer output is not guaranteed to assert.
R <sub>FKCHX</sub>	If the Host has programmed an EL2 timer to assert its output during Realm execution, that timer output is guaranteed to assert.
R <sub>RJZRP</sub>	Both the virtual and physical counter values are guaranteed to be monotonically increasing when read by a Realm, in accordance with the architectural counter behavior.
R <sub>JSMQP</sub>	When read by a Realm, either the virtual or physical counter returns the same value at a given point in time on a given PE.
X <sub>YCDMW</sub>	In order to ensure that the Realm has a consistent view of time, the virtual timer offset must be fixed for the lifetime of the Realm. The absolute value of the virtual timer offset is not important, so the value zero has been chosen for simplicity of both the specification and the implementation.
I <sub>FKMGZ</sub>	The rule that virtual and physical counter values are identical may need to be amended if a future version of the specification supports migration and / or virtualization of time based on the virtual counter differing from the physical counter.
R <sub>VWQDH</sub>	<p>On REC exit, Realm EL1 timer state is exposed via the RecExit object:</p> <ul style="list-style-type: none"><li>• <code>exit.cntv_ctl</code> contains the value of <code>CNTV_CTL_EL0</code> at the time of the Realm exit.</li><li>• <code>exit.cntv_cval</code> contains the value of <code>CNTV_CVAL_EL0</code> at the time of the Realm exit, expressed as if the virtual counter offset was zero.</li><li>• <code>exit.cntp_ctl</code> contains the value of <code>CNTP_CTL_EL0</code> at the time of the Realm exit.</li><li>• <code>exit.cntp_cval</code> contains the value of <code>CNTP_CVAL_EL0</code> at the time of the Realm exit, expressed as if the physical counter offset was zero.</li></ul>
S <sub>PYWWE</sub>	<p>The Host should check the Realm EL1 timer state on every return from <code>RMI_REC_ENTER</code>, and if a timer condition is met, the Host should inject a virtual interrupt. This is true regardless of the value of <code>exit.exit_reason</code>: even if the return occurred for a reason unrelated to timer state (for example, a REC exit due to Data Abort), the timer condition should be checked.</p> <p>This is to ensure that the Realm does not miss a timer interrupt if, for example, there is no other event causing a return from <code>RMI_REC_ENTER</code>. In other words, the RMM only guarantees that the Host can observe a change in timer output state during return from <code>RMI_REC_ENTER</code>, but does not guarantee a REC exit specifically indicating an asserted timer output change.</p> <p>See also:</p> <ul style="list-style-type: none"><li>• <a href="#">A4.3 REC exit</a></li><li>• <a href="#">B3.4.16 RmiRecExit type</a></li><li>• <a href="#">D1.6.2 Timer interrupt delivery flow</a></li></ul>

## Chapter A7

### **Realm measurement and attestation**

This section describes how the initial state of a Realm is measured and can be attested.



## A7.1 Realm measurements

This section describes how Realm measurement values are calculated.

$D_{SJWWS}$	A Realm measurement value is a rolling hash.
$D_{YKDBY}$	A <i>Realm Hash Algorithm</i> (RHA) is an algorithm which is used to extend a Realm measurement value.
$I_{NRKWB}$	The RHA used by a Realm is selected via the <code>hash_algo</code> attribute.

See also:

- [A2.1.3 Realm attributes](#)
- [A3.1.1 Realm hash algorithm](#)
- [A7.2.3.1.3 Realm Initial Measurement claim](#)
- [A7.2.3.1.4 Realm Extensible Measurements claim](#)

### A7.1.1 Realm Initial Measurement

This section describes how the Realm Initial Measurement (RIM) is calculated.

$I_{XKSBZ}$	The initial RIM value for a Realm is calculated from a subset of the Realm parameters.
$I_{NCNDK}$	A RIM is extended by applying the RHA to the inputs of RMM operations which are executed during Realm construction.
$I_{NQQTF}$	The following operations cause a RIM to be extended: <ul style="list-style-type: none"> <li>• Creation of a DATA Granule during Realm construction</li> <li>• Creation of a runnable REC</li> <li>• Changes to RIPAS of Protected IPA during Realm construction</li> </ul>
$R_{VMPZG}$	On execution of an operation which requires extension of a RIM, the RMM first constructs a <i>measurement descriptor</i> structure. The measurement descriptor contents include the current RIM value. The new RIM value is computed by applying the RHA to the measurement descriptor.

$$desc = MeasurementDescriptor(M_{i-1}, \dots)$$

$$M_i = RHA(desc)$$

$I_{FQHFC}$	A RIM is immutable while the state of the Realm is ACTIVE. This implies that a RIM reflects the configuration and contents of the Realm at the moment when it transitioned from the NEW to the ACTIVE state.
$I_{DQGP}$	A RIM depends upon the order of the RMM operations which are executed during Realm construction.
$S_{VZNCW}$	The order in which RMM operations are executed during Realm construction must be agreed between the Realm owner (or a delegate of the Realm owner which will receive and validate the RIM) and the Host which executes the RMM commands. This ensures that a correctly-constructed Realm will have the expected measurement.
$I_{LTWBL}$	The value of a RIM can be read using the <code>RSI_MEASUREMENT_READ</code> command.

See also:

- [B3.3.1.4 RMI\\_DATA\\_CREATE extension of RIM](#)
- [B3.3.9.4 RMI\\_REALM\\_CREATE initialization of RIM](#)
- [B3.3.12.4 RMI\\_REC\\_CREATE extension of RIM](#)
- [B3.3.18.4 RMI\\_RTT\\_INIT\\_RIPAS extension of RIM](#)
- [B4.3.7 RSI\\_MEASUREMENT\\_READ command](#)

## A7.1.2 Realm Extensible Measurement

This section describes the behavior of a Realm Extensible Measurement (REM).

$I_{QJ\text{DWM}}$

A REM is extended using the `RSI_MEASUREMENT_EXTEND` command.

$I_{CT\text{MBT}}$

The value of a REM can be read using the `RSI_MEASUREMENT_READ` command.

$I_{MD\text{QRP}}$

The initial value of a REM is zero.

See also:

- [B4.3.6 `RSI\_MEASUREMENT\_EXTEND` command](#)
- [B4.3.7 `RSI\_MEASUREMENT\_READ` command](#)

## A7.2 Realm attestation

This section describes the primitives which are used to support remote Realm attestation.

### A7.2.1 Attestation token

$\mathcal{D}_{VRRLN}$  A CCA attestation token is a collection of claims about the state of a Realm and of the CCA platform on which the Realm is running.

$\mathcal{I}_{BXBSD}$  A CCA attestation token consists of two parts:

- Realm token
  - Contains attributes of the Realm, including:
    - Realm Initial Measurement
    - Realm Extensible Measurements
- CCA platform token
  - Contains attributes of the CCA platform on which the Realm is running, including:
    - CCA platform identity
    - CCA platform lifecycle state
    - CCA platform software component measurements

$\mathcal{I}_{JKJCQ}$  The size of a CCA attestation token may be greater than 4KB.

See also:

- [A7.1.1 Realm Initial Measurement](#)
- [A7.1.2 Realm Extensible Measurement](#)

### A7.2.2 Attestation token generation

$\mathcal{I}_{KRMRH}$  The process for a Realm to obtain an attestation token is:

- Call `RSI_ATTESTATION_TOKEN_INIT` once
- Call `RSI_ATTESTATION_TOKEN_CONTINUE` in a loop, until the result is not `RSI_INCOMPLETE`

Each call to `RSI_ATTESTATION_TOKEN_CONTINUE` retrieves up to one Granule of the attestation token.

S<sub>XMLMF</sub>

The following pseudocode illustrates the process of a Realm obtaining an attestation token.

---

```

int get_attestation_token(...)
{
    int ret;

    ret = RSI_ATTESTATION_TOKEN_INIT(challenge);
    if (ret) {
        return ret;
    }

    do { // Retrieve one Granule of data per loop iteration
        uint64_t granule = alloc_granule();
        uint64_t offset = 0;

        do { // Retrieve sub-Granule chunk of data per loop iteration
            uint64_t size = GRANULE_SIZE - offset;
            (status, len) = RSI_ATTESTATION_TOKEN_CONTINUE(Granule, offset, size);
            offset += len;
        } while (ret == RSI_INCOMPLETE && offset < GRANULE_SIZE);

        // "offset" bytes of data are now ready for consumption from "granule"
    } while (ret == RSI_INCOMPLETE);

    return ret;
}

```

---

I<sub>ZWQCB</sub>

Up to one attestation token generation operation may be ongoing on a REC.

I<sub>TMJVG</sub>

On execution of RSI\_ATTESTATION\_TOKEN\_INIT, if an attestation token generation operation is ongoing on the calling REC, it is terminated.

I<sub>WTKDD</sub>

The challenge value provided to RSI\_ATTESTATION\_TOKEN\_INIT is included in the generated attestation token. This allows the relying party to establish freshness of the attestation token.

If the size of the challenge provided by the relying party is less than 64 bytes, it should be zero-padded prior to calling RSI\_ATTESTATION\_TOKEN\_INIT. Arm recommends that the challenge should contain at least 32 bytes of unique data.

I<sub>GKDJW</sub>

Generation of an attestation token can be a long-running operation, during which interrupts may need to be handled.

I<sub>CXSJP</sub>

If a physical interrupt becomes pending during execution of RSI\_ATTESTATION\_TOKEN\_CONTINUE, a REC exit due to IRQ can occur.

On the next entry to the REC:

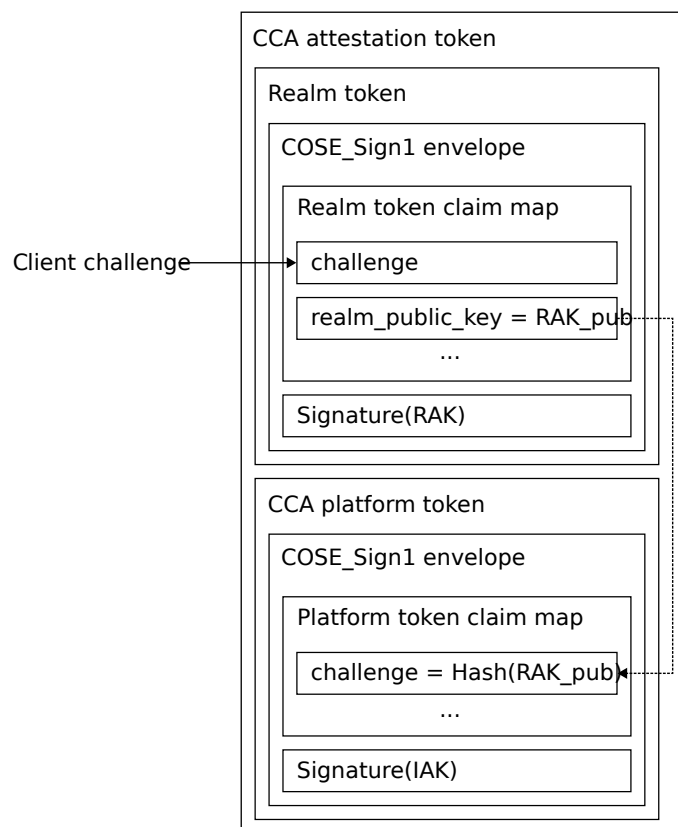
- If a virtual interrupt is pending on that REC, it is taken to the REC's exception handler
- RSI\_ATTESTATION\_TOKEN\_CONTINUE returns RSI\_INCOMPLETE
- The REC should call RSI\_ATTESTATION\_TOKEN\_CONTINUE again

See also:

- [A4.3.5 REC exit due to IRQ](#)
- [A6.1 Realm interrupts](#)
- [A7.2.3.1.1 Realm challenge claim](#)
- [B4.3.1 RSI\\_ATTESTATION\\_TOKEN\\_CONTINUE command](#)
- [B4.3.2 RSI\\_ATTESTATION\\_TOKEN\\_INIT command](#)
- [D1.7.1 Attestation token generation flow](#)
- [D1.7.2 Handling interrupts during attestation token generation flow](#)

**A7.2.3 Attestation token format**

<code>I<sub>TFHGX</sub></code>	The CCA attestation token is a profiled IETF Entity Attestation Token (EAT).
<code>I<sub>LPTVH</sub></code>	The CCA attestation token is a Concise Binary Object Representation (CBOR) map, in which the map values are the Realm token and the CCA platform token.
<code>I<sub>YZPHG</sub></code>	The Realm token contains structured data in CBOR, wrapped with a COSE_Sign1 envelope according to the CBOR Object Signing and Encryption (COSE) standard.
<code>I<sub>MMQZG</sub></code>	The Realm token is signed by the Realm Attestation Key (RAK).
<code>I<sub>WBGNP</sub></code>	The CCA platform token contains structured data in CBOR, wrapped with a COSE_Sign1 envelope according to the COSE standard.
<code>I<sub>CGYKX</sub></code>	The CCA platform token is signed by the Initial Attestation Key (IAK).
<code>I<sub>CCGQH</sub></code>	The CCA platform token contains a hash of RAK <sub>pub</sub> . This establishes a cryptographic binding between the Realm token and the CCA platform token.
<code>I<sub>PTKYD</sub></code>	<p>The CCA attestation token is defined as follows:</p> <hr/> <pre>cca-token = #6.399(cca-token-collection) ; EAT token-collection extension  cca-platform-token = bstr .cbor COSE_Sign1_Tagged cca-realm-delegated-token = bstr .cbor COSE_Sign1_Tagged  cca-token-collection = {     44234 =&gt; cca-platform-token          ; 44234 = 0xACCA     44241 =&gt; cca-realm-delegated-token }  ; EAT standard definitions COSE_Sign1_Tagged = #6.18(COSE_Sign1)  ; Deliberately shortcut these definitions until EAT is finalised and able to ; pull in the full set of definitions COSE_Sign1 = "COSE-Sign1 placeholder"</pre> <hr/>
<code>I<sub>HZNNH</sub></code>	The composition of the CCA attestation token is summarised in the following figure.



**Figure A7.1: Attestation token format**

See also:

- *Arm CCA Security model* [4]
- *Concise Binary Object Representation (CBOR)* [6]
- *CBOR Object Signing and Encryption (COSE)* [7]
- *Entity Attestation Token (EAT)* [8]
- [A7.2.3.1 Realm claims](#)
- [A7.2.3.2 CCA platform claims](#)

### A7.2.3.1 Realm claims

This section defines the format of the Realm token claim map. The format is described using a combination of Concise Data Definition Language (CDDL) and text description.

I<sub>HKBHC</sub>

The Realm token claim map is defined as follows:

---

```
cca-realm-claims = (cca-realm-claim-map)
```

```
cca-realm-claim-map = {  
    cca-realm-challenge  
    cca-realm-personalization-value  
    cca-realm-initial-measurement  
    cca-realm-extensible-measurements  
    cca-realm-hash-algo-id  
    cca-realm-public-key  
    cca-realm-public-key-hash-algo-id  
}
```

---

See also:

- [Concise Data Definition Language \(CDDL\) \[9\]](#)
- [A7.2.3.1.1 Realm challenge claim](#)
- [A7.2.3.1.2 Realm Personalization Value claim](#)
- [A7.2.3.1.3 Realm Initial Measurement claim](#)
- [A7.2.3.1.4 Realm Extensible Measurements claim](#)
- [A7.2.3.1.5 Realm hash algorithm ID claim](#)
- [A7.2.3.1.6 Realm public key claim](#)
- [A7.2.3.1.7 Realm public key hash algorithm identifier claim](#)
- [A7.2.3.1.8 Collated CDDL for Realm claims](#)
- [A7.2.3.1.9 Example Realm claims](#)

#### A7.2.3.1.1 Realm challenge claim

I<sub>TFWXQ</sub>

The Realm challenge claim is used to carry the challenge provided by the caller to demonstrate freshness of the generated token.

I<sub>RVLZK</sub>

The Realm challenge claim is identified using the EAT<sub>nonce</sub> label (10).

I<sub>MNVNP</sub>

The length of the Realm challenge is 64 bytes.

I<sub>PXMXF</sub>

The Realm challenge claim must be present in a Realm token.

I<sub>BXGFN</sub>

The format of the Realm challenge claim is defined as follows:

---

```
cca-realm-challenge-label = 10  
cca-realm-challenge-type = bytes .size 64  
  
cca-realm-challenge = (  
    cca-realm-challenge-label => cca-realm-challenge-type  
)
```

---

See also:

- [A7.2.2 Attestation token generation](#)
- [B4.3.2 RSI\\_ATTESTATION\\_TOKEN\\_INIT command](#)

#### A7.2.3.1.2 Realm Personalization Value claim

I<sub>SCNXB</sub>

The Realm Personalization Value claim contains the RPV which was provided at Realm creation.

I<sub>BKZPD</sub>

The Realm Personalization Value claim must be present in a Realm token.

I<sub>QKNDV</sub>

The format of the Realm Personalization Value claim is defined as follows:

---

```
cca-realm-personalization-value-label = 44235
cca-realm-personalization-value-type = bytes .size 64

cca-realm-personalization-value = (
    cca-realm-personalization-value-label => cca-realm-personalization-value-type
)
```

---

See also:

- [A2.1.3 Realm attributes](#)

#### **A7.2.3.1.3 Realm Initial Measurement claim**

I<sub>BXKGD</sub>

The Realm Initial Measurement claim contains the values of the Realm Initial Measurement.

I<sub>FZQSM</sub>

The Realm Initial Measurement claim must be present in a Realm token.

I<sub>GGTNH</sub>

The format of the Realm Initial Measurement claim is defined as follows:

---

```
cca-realm-measurement-type = bytes .size 32 / bytes .size 48 / bytes .size 64

cca-realm-initial-measurement-label = 44238

cca-realm-initial-measurement = (
    cca-realm-initial-measurement-label => cca-realm-measurement-type
)
```

---

See also:

- [A7.1 Realm measurements](#)
- [A7.2.3.1.4 Realm Extensible Measurements claim](#)

#### **A7.2.3.1.4 Realm Extensible Measurements claim**

I<sub>KFNMV</sub>

The Realm Extensible Measurements claim contains the values of the Realm Extensible Measurements.

I<sub>DSNFB</sub>

The Realm Extensible Measurements claim must be present in a Realm token.

I<sub>ZKVMN</sub>

The format of the Realm measurements claim is defined as follows:

---

```
cca-realm-measurement-type = bytes .size 32 / bytes .size 48 / bytes .size 64

cca-realm-extensible-measurements-label = 44239

cca-realm-extensible-measurements = (
    cca-realm-extensible-measurements-label => [ 4*4 cca-realm-measurement-type ]
)
```

---

See also:

- [A7.1 Realm measurements](#)
- [A7.2.3.1.3 Realm Initial Measurement claim](#)

#### **A7.2.3.1.5 Realm hash algorithm ID claim**

I<sub>DGCGG</sub>

The Realm hash algorithm ID claim identifies the algorithm used to calculate all hash values which are present in the Realm token.

I<sub>PVLCJ</sub>

Arm recommends that the value of the Realm hash algorithm ID claim is an IANA Hash Function name *IANA Hash Function Textual Names* [10].



**I<sub>WKVCQ</sub>** The Realm hash algorithm ID claim must be present in a Realm token.

**I<sub>PWPLJ</sub>** The format of the Realm hash algorithm ID claim is defined as follows:

---

```
cca-realm-hash-algo-id-label = 44236

cca-realm-hash-algo-id = (
    cca-realm-hash-algo-id-label => text
)
```

---

#### **A7.2.3.1.6 Realm public key claim**

**I<sub>ZCFMQ</sub>** The Realm public key claim identifies the key which is used to sign the Realm token.

**I<sub>WBNHC</sub>** The value of the Realm public key claim is RAK\_pub, encoded according to *SEC 1: Elliptic Curve Cryptography, version 2.0* [11].

**I<sub>LSNPQ</sub>** The Realm public key claim must be present in a Realm token.

**I<sub>NNNDS</sub>** The format of the Realm public key claim is defined as follows:

---

```
cca-realm-public-key-label = 44237

; TODO: support public key sizes other than ECC-P384
cca-realm-public-key-type = bytes .size 97

cca-realm-public-key = (
    cca-realm-public-key-label => cca-realm-public-key-type
)
```

---

See also:

- *SEC 1: Elliptic Curve Cryptography, version 2.0* [11]
- [A7.2.3.1.7 Realm public key hash algorithm identifier claim](#)
- [A7.2.3.2.2 CCA platform challenge claim](#)

#### **A7.2.3.1.7 Realm public key hash algorithm identifier claim**

**I<sub>WWSLP</sub>** The Realm public key hash algorithm identifier claim identifies the algorithm used to calculate H(RAK\_pub).

**I<sub>TNRBN</sub>** The Realm public key hash algorithm identifier claim must be present in a Realm token.

**I<sub>NNPVX</sub>** The format of the Realm public key hash algorithm identifier claim is defined as follows:

---

```
cca-realm-public-key-hash-algo-id-label = 44240

cca-realm-public-key-hash-algo-id = (
    cca-realm-public-key-hash-algo-id-label => text
)
```

---

See also:

- *SEC 1: Elliptic Curve Cryptography, version 2.0* [11]
- [A7.2.3.1.6 Realm public key claim](#)
- [A7.2.3.2.2 CCA platform challenge claim](#)

### A7.2.3.1.8 Collated CDDL for Realm claims

D<sub>DCYXZ</sub>

The format of the Realm token claim map is defined as follows:

---

```
cca-realm-claims = (cca-realm-claim-map)

cca-realm-claim-map = {
    cca-realm-challenge
    cca-realm-personalization-value
    cca-realm-initial-measurement
    cca-realm-extensible-measurements
    cca-realm-hash-algo-id
    cca-realm-public-key
    cca-realm-public-key-hash-algo-id
}

cca-realm-challenge-label = 10
cca-realm-challenge-type = bytes .size 64

cca-realm-challenge = (
    cca-realm-challenge-label => cca-realm-challenge-type
)

cca-realm-personalization-value-label = 44235
cca-realm-personalization-value-type = bytes .size 64

cca-realm-personalization-value = (
    cca-realm-personalization-value-label => cca-realm-personalization-value-type
)

cca-realm-measurement-type = bytes .size 32 / bytes .size 48 / bytes .size 64

cca-realm-initial-measurement-label = 44238

cca-realm-initial-measurement = (
    cca-realm-initial-measurement-label => cca-realm-measurement-type
)

cca-realm-extensible-measurements-label = 44239

cca-realm-extensible-measurements = (
    cca-realm-extensible-measurements-label => [ 4*4 cca-realm-measurement-type ]
)

cca-realm-hash-algo-id-label = 44236

cca-realm-hash-algo-id = (
    cca-realm-hash-algo-id-label => text
)

cca-realm-public-key-label = 44237

; TODO: support public key sizes other than ECC-P384
cca-realm-public-key-type = bytes .size 97

cca-realm-public-key = (
    cca-realm-public-key-label => cca-realm-public-key-type
)

cca-realm-public-key-hash-algo-id-label = 44240
```

```
cca-realm-public-key-hash-algo-id = (  
    cca-realm-public-key-hash-algo-id-label => text  
)
```

---

#### A7.2.3.1.9 Example Realm claims

 $\mathbb{I}_{\text{CPTFR}}$ 

An example Realm claim map is shown below in COSE-DIAG format:

[illegible]

### A7.2.3.2 CCA platform claims

This section defines the format of the CCA platform token claim map. The format is described using a combination of Concise Data Definition Language (CDDL) and text description.

I\_FJKFY

The CCA platform token claim map is defined as follows:

---

```
cca-platform-claims = (cca-platform-claim-map)
```

```
cca-platform-claim-map = {  
    cca-platform-profile  
    cca-platform-challenge  
    cca-platform-implementation-id  
    cca-platform-instance-id  
    cca-platform-config  
    cca-platform-lifecycle  
    cca-platform-sw-components  
    ? cca-platform-verification-service  
    cca-platform-hash-algo-id  
}
```

---

See also:

- [Concise Data Definition Language \(CDDL\) \[9\]](#)
- [A7.2.3.2.1 CCA platform profile claim](#)
- [A7.2.3.2.2 CCA platform challenge claim](#)
- [A7.2.3.2.3 CCA platform Implementation ID claim](#)
- [A7.2.3.2.4 CCA platform Instance ID claim](#)
- [A7.2.3.2.5 CCA platform config claim](#)
- [A7.2.3.2.6 CCA platform lifecycle claim](#)
- [A7.2.3.2.7 CCA platform software components claim](#)
- [A7.2.3.2.8 CCA platform verification service claim](#)
- [A7.2.3.2.9 CCA platform hash algorithm ID claim](#)
- [A7.2.3.2.10 Collated CDDL for CCA platform claims](#)
- [A7.2.3.2.11 Example CCA platform claims](#)

#### A7.2.3.2.1 CCA platform profile claim

I\_FQYTP

The CCA platform profile claim identifies the EAT profile to which the CCA platform token conforms. Note that because the platform token is expected to be issued when bound to a Realm token, the profile document should include a description of the Realm claims.

I\_XMVFR

The CCA platform profile claim is identified using the EAT profile label (265).

I\_GMKNR

The CCA platform profile claim must be present in a CCA platform token.

I\_MHRTD

The format of the CCA platform profile claim is defined as follows:

---

```
cca-platform-profile-label = 265 ; EAT profile  
  
cca-profile-type = "http://arm.com/CCA-SSD/1.0.0"  
  
cca-platform-profile = (  
    cca-platform-profile-label => cca-profile-type  
)
```

---

#### A7.2.3.2.2 CCA platform challenge claim

I\_TKTWZ

The CCA platform challenge claim contains a hash of the public key used to sign the Realm token.

**I<sub>CLJKK</sub>** The CCA platform challenge claim is identified using the EAT<sub>nonce</sub> label (10).

**I<sub>XHLVJ</sub>** The length of the CCA platform challenge is either 32, 48 or 64 bytes.

**I<sub>GVHNV</sub>** The CCA platform challenge claim must be present in a CCA platform token.

**I<sub>LRWHR</sub>** The format of the CCA platform challenge claim is defined as follows:

---

```
cca-hash-type = bytes .size 32 / bytes .size 48 / bytes .size 64
```

```
cca-platform-challenge-label = 10
```

```
cca-platform-challenge = (
    cca-platform-challenge-label => cca-hash-type
)
```

---

See also:

- [A7.2.3.1.6 Realm public key claim](#)

### **A7.2.3.2.3 CCA platform Implementation ID claim**

**I<sub>SMWND</sub>** The CCA platform Implementation ID claim uniquely identifies the implementation of the CCA platform.

**I<sub>NDVFB</sub>** The value of the CCA platform Implementation ID claim can be used by a verification service to locate the details of the CCA platform implementation from an endorser or manufacturer. Such details are used by a verification service to determine the security properties or certification status of the CCA platform implementation.

**I<sub>RXPVW</sub>** The semantics of the CCA platform Implementation ID value are defined by the manufacturer or a particular certification scheme. For example, the ID could take the form of a product serial number, database ID, or other appropriate identifier.

**I<sub>SRPZY</sub>** The CCA platform Implementation ID claim does not identify a particular instance of the CCA implementation.

**I<sub>NTCFY</sub>** The CCA platform Implementation ID claim must be present in a CCA platform token.

**I<sub>DHYDG</sub>** The format of the CCA platform Implementation ID claim is defined as follows:

---

```
cca-platform-implementation-id-label = 2396 ; PSA implementation ID
```

```
cca-platform-implementation-id-type = bytes .size 32
```

```
cca-platform-implementation-id = (
    cca-platform-implementation-id-label => cca-platform-implementation-id-type
)
```

---

See also:

- [Arm CCA Security model \[4\]](#)
- [A7.2.3.2.4 CCA platform Instance ID claim](#)

### **A7.2.3.2.4 CCA platform Instance ID claim**

**I<sub>ZYRZB</sub>** The CCA platform Instance ID claim represents the unique identifier of the Initial Attestation Key (IAK) for the CCA platform.

**I<sub>XVLLN</sub>** The CCA platform Instance ID claim is identified using the EAT<sub>ueid</sub> label (256).

**R<sub>HVTNC</sub>** The first byte of the CCA platform Instance ID value must be 0x01.

**I<sub>ZNGDF</sub>** The CCA platform Instance ID claim must be present in a CCA platform token.

I_VPKJN	<p>The format of the CCA platform Instance ID claim is defined as follows:</p> <hr/> <pre>cca-platform-instance-id-label = 256 ; EAT uuid  ; TODO: require that the first byte of cca-platform-instance-id-type is 0x01 ; EAT UEIDs need to be 7 - 33 bytes cca-platform-instance-id-type = bytes .size 33  cca-platform-instance-id = (     cca-platform-instance-id-label =&gt; cca-platform-instance-id-type )</pre> <hr/> <p>See also:</p> <ul style="list-style-type: none"> <li>• <a href="#">Arm CCA Security model [4]</a></li> <li>• <a href="#">A7.2.3.2.3 CCA platform Implementation ID claim</a></li> </ul> <p><b>A7.2.3.2.5 CCA platform config claim</b></p>
I_WVQJT	<p>The CCA platform config claim describes the set of chosen implementation options of the CCA platform. As an example, these may include a description of the level of physical memory protection which is provided.</p>
U_GPXWX	<p>The CCA platform config claim is expected to contain the System Properties field which is present in the Root Non-volatile Storage (RNVS) public parameters.</p>
I_MJHQT	<p>The CCA platform config claim must be present in a CCA platform token.</p> <hr/> <pre>cca-platform-config-label = 2401 ; PSA platform range                                 ; TBD: add to IANA registration cca-platform-config-type = bytes  cca-platform-config = (     cca-platform-config-label =&gt; cca-platform-config-type )</pre> <hr/> <p>See also:</p> <ul style="list-style-type: none"> <li>• <a href="#">RME system architecture spec [12]</a></li> </ul> <p><b>A7.2.3.2.6 CCA platform lifecycle claim</b></p>
I_SYKFY	<p>The CCA platform lifecycle claim identifies the lifecycle state of the CCA platform.</p>
R_NBFVV	<p>The value of the CCA platform lifecycle claim is an integer which is divided as follows:</p> <ul style="list-style-type: none"> <li>• value[15:8]: CCA platform lifecycle state</li> <li>• value[7:0]: IMPLEMENTATION DEFINED</li> </ul>
I_WFZHV	<p>The CCA platform lifecycle claim must be present in a CCA platform token.</p>
I_QFYLF	<p>A non debugged CCA platform will be in psa-lifecycle-secured state. Realm Management Security Domain debug is always recoverable, and would therefore be represented by psa-lifecycle-non-psa-rot-debug state. Root world debug is recoverable on a HES system and would be represented by psa-lifecycle-recoverable-psa-rot state. On a non-HES system Root world debug is usually non-recoverable, and would be represented by psa-lifecycle-lifecycle-decommissioned state.</p>
I_HMZLL	<p>The format of the CCA platform lifecycle claim is defined as follows:</p> <hr/> <pre>cca-platform-lifecycle-label = 2395 ; PSA lifecycle  cca-platform-lifecycle-unknown-type = 0x0000..0x00ff cca-platform-lifecycle-assembly-and-test-type = 0x1000..0x10ff cca-platform-lifecycle-cca-platform-rot-provisioning-type = 0x2000..0x20ff</pre> <hr/>

```
cca-platform-lifecycle-secured-type = 0x3000..0x30ff
cca-platform-lifecycle-non-cca-platform-rot-debug-type = 0x4000..0x40ff
cca-platform-lifecycle-recoverable-cca-platform-rot-debug-type = 0x5000..0x50ff
cca-platform-lifecycle-decommissioned-type = 0x6000..0x60ff

cca-platform-lifecycle-type =
    cca-platform-lifecycle-unknown-type /
    cca-platform-lifecycle-assembly-and-test-type /
    cca-platform-lifecycle-cca-platform-rot-provisioning-type /
    cca-platform-lifecycle-secured-type /
    cca-platform-lifecycle-non-cca-platform-rot-debug-type /
    cca-platform-lifecycle-recoverable-cca-platform-rot-debug-type /
    cca-platform-lifecycle-decommissioned-type

cca-platform-lifecycle = (
    cca-platform-lifecycle-label => cca-platform-lifecycle-type
)
```

See also:

- *Arm CCA Security model* [4]

#### A7.2.3.2.7 CCA platform software components claim

$I_{PJCS}$	The CCA platform software components claim is a list of software components which can affect the behavior of the CCA platform. It is expected that an implementation will describe the expected software component values within the profile.
$I_{TJTXG}$	The CCA platform software components claim must be present in a CCA platform token.
$I_{DPSKT}$	The format of the CCA platform software components claim is defined as follows:

```
cca-platform-sw-components-label = 2399 ; PSA software components

cca-platform-sw-component = {
    ? 1 => text,          ; component type
    ? 2 => cca-hash-type, ; measurement value
    ? 4 => text,          ; version
    ? 5 => cca-hash-type, ; signer id
    ? 6 => text,          ; hash algorithm identifier
}

cca-platform-sw-components = (
    cca-platform-sw-components-label => [ + cca-platform-sw-component ]
)
```

#### CCA platform software component type

$I_{PDNCF}$	The CCA platform software component type is a string which represents the role of the software component.
$I_{TPSYF}$	The CCA platform software component type is intended for use as a hint to help the relying party understand how to evaluate the CCA platform software component measurement value.
$R_{RSNBH}$	The CCA platform software component type is optional in a CCA platform token.

#### CCA platform software component measurement value

$I_{RWDKD}$	The CCA platform software component measurement value represents a hash of the state of the software component in memory at the time it was initialized.
$R_{TVXRZ}$	The CCA platform software component measurement value must be a hash of 256 bits or stronger.



**R<sub>LGBCM</sub>** The CCA platform software component measurement value must be present in a CCA platform token.

#### **CCA platform software component version**

**I<sub>JVJFW</sub>** The CCA platform software component version is a text string whose meaning is defined by the software component vendor.

**R<sub>CZRXB</sub>** The CCA platform software component version is optional in a CCA platform token.

#### **CCA platform software component signer ID**

**I<sub>DCDMR</sub>** The CCA platform software component signer ID is the hash of a signing authority public key for the software component. It can be used by a verifier to ensure that the software component was signed by an expected trusted source.

**R<sub>PXRMC</sub>** The CCA platform software component signer ID value must be a hash of 256 bits or stronger.

**R<sub>XPHQC</sub>** The CCA platform software signer ID must be present in a CCA platform token.

#### **CCA platform software hash algorithm ID**

**I<sub>TQWZX</sub>** The CCA platform software hash algorithm ID identifies the way in which the hash algorithm used to measure the CCA platform software component.

**I<sub>HBBHG</sub>** Arm recommends that the value of the CCA platform software hash algorithm ID is an IANA Hash Function name *IANA Hash Function Textual Names* [10].

**I<sub>NJYCM</sub>** Arm recommends that the hash algorithm used to measure the CCA platform software component is one of the algorithms listed in the *Arm CCA Security model* [4].

**I<sub>HPHCD</sub>** The CCA platform software hash algorithm ID is optional in a CCA platform token.

#### **A7.2.3.2.8 CCA platform verification service claim**

**I<sub>NSTDP</sub>** The CCA platform verification service claim is a hint which can be used by a relying party to locate a verifier for the token.

**I<sub>RZJSQ</sub>** The value of the CCA platform verification service claim is a text string which can be used to locate the service or a URL specifying the address of the service.

**I<sub>MFYCX</sub>** The CCA platform verification service claim may be ignored by a relying party in favor of other information.

**I<sub>MRSXY</sub>** The CCA platform verification service claim is optional in a CCA platform token.

**I<sub>WRJSX</sub>** The format of the CCA platform verification service claim is defined as follows:

---

```
cca-platform-verification-service-label = 2400 ; PSA verification service
cca-platform-verification-service-type = text

cca-platform-verification-service = (
    cca-platform-verification-service-label =>
        cca-platform-verification-service-type
)
```

---

#### **A7.2.3.2.9 CCA platform hash algorithm ID claim**

**I<sub>VDZMF</sub>** The CCA platform hash algorithm ID claim identifies the algorithm used to calculate the extended measurements in the CCA platform token.

**I<sub>YRPPY</sub>** Arm recommends that the value of the CCA platform hash algorithm ID claim is an IANA Hash Function name *IANA Hash Function Textual Names* [10].

$I_{TQSTK}$

The CCA platform hash algorithm ID claim must be present in a CCA platform token.

$I_{RKZJT}$

The format of the CCA platform hash algorithm ID claim is defined as follows:

---

```
cca-platform-hash-algo-id-label = 2402 ; PSA platform range
                                   ; TBD: add to IANA registration

cca-platform-hash-algo-id = (
    cca-platform-hash-algo-id-label => text
)
```

---

#### A7.2.3.2.10 Collated CDDL for CCA platform claims

D<sub>DVMJZ</sub>

The format of the CCA platform token claim map is defined as follows:

---

```
cca-platform-claims = (cca-platform-claim-map)

cca-platform-claim-map = {
    cca-platform-profile
    cca-platform-challenge
    cca-platform-implementation-id
    cca-platform-instance-id
    cca-platform-config
    cca-platform-lifecycle
    cca-platform-sw-components
    ? cca-platform-verification-service
    cca-platform-hash-algo-id
}

cca-platform-profile-label = 265 ; EAT profile

cca-profile-type = "http://arm.com/CCA-SSD/1.0.0"

cca-platform-profile = (
    cca-platform-profile-label => cca-profile-type
)
cca-hash-type = bytes .size 32 / bytes .size 48 / bytes .size 64

cca-platform-challenge-label = 10

cca-platform-challenge = (
    cca-platform-challenge-label => cca-hash-type
)

cca-platform-implementation-id-label = 2396 ; PSA implementation ID
cca-platform-implementation-id-type = bytes .size 32

cca-platform-implementation-id = (
    cca-platform-implementation-id-label => cca-platform-implementation-id-type
)

cca-platform-instance-id-label = 256 ; EAT ueid

; TODO: require that the first byte of cca-platform-instance-id-type is 0x01
; EAT UEIDs need to be 7 - 33 bytes
cca-platform-instance-id-type = bytes .size 33

cca-platform-instance-id = (
    cca-platform-instance-id-label => cca-platform-instance-id-type
)

cca-platform-config-label = 2401 ; PSA platform range
                                ; TBD: add to IANA registration
cca-platform-config-type = bytes

cca-platform-config = (
    cca-platform-config-label => cca-platform-config-type
)

cca-platform-lifecycle-label = 2395 ; PSA lifecycle
```

```
cca-platform-lifecycle-unknown-type = 0x0000..0x00ff
cca-platform-lifecycle-assembly-and-test-type = 0x1000..0x10ff
cca-platform-lifecycle-cca-platform-rot-provisioning-type = 0x2000..0x20ff
cca-platform-lifecycle-secured-type = 0x3000..0x30ff
cca-platform-lifecycle-non-cca-platform-rot-debug-type = 0x4000..0x40ff
cca-platform-lifecycle-recoverable-cca-platform-rot-debug-type = 0x5000..0x50ff
cca-platform-lifecycle-decommissioned-type = 0x6000..0x60ff

cca-platform-lifecycle-type =
    cca-platform-lifecycle-unknown-type /
    cca-platform-lifecycle-assembly-and-test-type /
    cca-platform-lifecycle-cca-platform-rot-provisioning-type /
    cca-platform-lifecycle-secured-type /
    cca-platform-lifecycle-non-cca-platform-rot-debug-type /
    cca-platform-lifecycle-recoverable-cca-platform-rot-debug-type /
    cca-platform-lifecycle-decommissioned-type

cca-platform-lifecycle = (
    cca-platform-lifecycle-label => cca-platform-lifecycle-type
)

cca-platform-sw-components-label = 2399 ; PSA software components

cca-platform-sw-component = {
    ? 1 => text,          ; component type
    ? 2 => cca-hash-type, ; measurement value
    ? 4 => text,          ; version
    ? 5 => cca-hash-type, ; signer id
    ? 6 => text,          ; hash algorithm identifier
}

cca-platform-sw-components = (
    cca-platform-sw-components-label => [ + cca-platform-sw-component ]
)

cca-platform-verification-service-label = 2400 ; PSA verification service
cca-platform-verification-service-type = text

cca-platform-verification-service = (
    cca-platform-verification-service-label =>
        cca-platform-verification-service-type
)

cca-platform-hash-algo-id-label = 2402 ; PSA platform range
                                     ; TBD: add to IANA registration

cca-platform-hash-algo-id = (
    cca-platform-hash-algo-id-label => text
)
```

---

#### A7.2.3.2.11 Example CCA platform claims

I<sub>TVHKL</sub>

An example CCA platform claim map is shown below in COSE-DIAG format:

```
/ CCA platform claim map /
{
  / cca-platform-profile /
  265: "http://arm.com/CCA-SSD/1.0.0",

  / cca-platform-challenge /
  10: h'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA',

  / cca-platform-implementation-id /
  2396: h'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA',

  / cca-platform-instance-id /
  256: h'010BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
      BB',

  / cca-platform-config /
  2401: h'CFCFCFCF',

  / cca-platform-lifecycle /
  2395: 12288,

  / cca-platform-sw-components /
  2399: [
    {
      / measurement value /
      2: h'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
          AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA',

      / signer id /
      5: h'BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
          BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB',

      / version /
      4: "1.0.0",

      / hash algorithm identifier /
      6: "sha-256"
    },
    {
      / measurement value /
      2: h'CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
          CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC',

      / signer id /
      5: h'DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
          DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD',

      / version /
      4: "1.0.0",

      / hash algorithm identifier /
      6: "sha-256"
    }
  ],
}
```

## Chapter A7. Realm measurement and attestation

### A7.2. Realm attestation

```
    / cca-platform-verification-service /  
    2400: "https://cca_verifier.org",  
  
    / cca-platform-hash-algo-id /  
    2402: "sha-256"  
}
```

---

## Chapter A8

# Realm debug and performance monitoring

This section describes the debug and performance monitoring features which are available to a Realm.

## A8.1 Realm PMU

This section describes the programming model for usage of PMU by a Realm.

R<sub>DNNQQ</sub>

On REC entry, Realm PMU state is restored from the REC object.

R<sub>LHRYJ</sub>

On REC exit, all Realm PMU state is saved to the REC object.

R<sub>WXTZF</sub>

On REC exit, `exit.pmu_ovf_status` indicates the status of the PMU overflow at the time of the Realm exit.

See also:

- [A3.1.5 Realm support for Performance Monitors Extension](#)
- [A4.3 REC exit](#)
- [B3.4.16 RmiRecExit type](#)



## **Part B**

### **Interface**

## Chapter B1

# Commands

This chapter describes how RMM commands are defined in this specification.

## B1.1 Overview

R <sub>VZRKZ</sub>	<p>The RMM exposes the following interfaces to the Host:</p> <ul style="list-style-type: none"> <li>• The <i>Realm Management Interface</i> (RMI)</li> </ul>
R <sub>NPLKX</sub>	<p>The RMM exposes the following interfaces to a Realm:</p> <ul style="list-style-type: none"> <li>• The <i>Realm Services Interface</i> (RSI)</li> <li>• The <i>Power State Coordination Interface</i> (PSCI)</li> </ul> <p>Any other SMC executed by a Realm returns SMCCC_NOT_SUPPORTED.</p>
I <sub>TKQXF</sub>	An RMM interface consists of a set of RMM commands.
I <sub>RTRYT</sub>	An RMM interface is compliant with the SMC Calling Convention (SMCCC).
R <sub>NNFPH</sub>	SMCCC version $\geq 1.2$ is required.
X <sub>FDXJG</sub>	SMCCC version 1.2 increases the number of SMC64 arguments and return values from 4 to 17. Some RMM commands use more than 4 input or output values.
R <sub>VXJJQ</sub>	On a CCA platform which implements FEAT_SVE, SMCCC version $\geq 1.3$ is required.
X <sub>KCMSY</sub>	SMCCC version 1.3 introduces a bit in the FID which a caller can use to indicate that SVE state does not need to be preserved across the SMC call.
R <sub>JNVJQ</sub>	On a CCA platform which implements FEAT_SME, SMCCC version $\geq 1.4$ is required.
X <sub>QXMZL</sub>	SMCCC version 1.4 adds support for preservation of SME state across an SMC call.
R <sub>KWMVX</sub>	An RMM command uses the SMC64 calling convention.
S <sub>DFNMZ</sub>	<p>To determine whether an RMM interface is implemented, software should use the following flow:</p> <ol style="list-style-type: none"> <li>1. Determine whether the SMCCC_VERSION command is implemented, following the procedure described in <i>Arm SMC Calling Convention</i> [13].</li> <li>2. Check that the SMCCC version is <math>\geq 1.1</math>.</li> <li>3. Execute the &lt;Interface&gt;.Version command, which returns: <ul style="list-style-type: none"> <li>• SMCCC_NOT_SUPPORTED (-1) if &lt;Interface&gt; is not implemented.</li> <li>• A version number (<math>&gt;0</math>) if &lt;Interface&gt; is implemented.</li> </ul> </li> </ol>
R <sub>YBXKR</sub>	<p>All data types defined in this specification are little-endian.</p> <p>See also:</p> <ul style="list-style-type: none"> <li>• <a href="#">Chapter B3 Realm Management Interface</a></li> <li>• <a href="#">Chapter B4 Realm Services Interface</a></li> <li>• <a href="#">Chapter B5 Power State Control Interface</a></li> </ul>

## B1.2 Command definition

I<sub>WBMVP</sub>

The definition of an RMM command consists of:

- A *function identifier* (FID)
- A set of *input values* (referred to as “arguments” in SMCCC)
- A set of *output values* (referred to as “results” in SMCCC)
- A set of *context values*
- A partially-ordered set of *failure conditions*
- A set of *success conditions*
- A set of *footprint items*

I<sub>GCVWC</sub>

Each failure condition, success condition and footprint item has an associated identifier. Identifiers are unique within each of the above groups, within each command.

An identifier has no meaning. It is only a label by which a given condition or footprint item can be referred to.

See also:

- SMCCC *Arm SMC Calling Convention* [13]

### B1.2.1 Example command

I<sub>NFVGF</sub>

The following command, EXAMPLE\_ADD, is an example of how the components of an RMM command definition are presented in this document.

This command takes as an input value the address `params_ptr` of an NS Granule which contains two integer values `x` and `y`. On successful execution of the command:

- The output value `sum` contains the sum of `x` and `y`
- The output value `zero` indicates whether either of `x` or `y` is zero

EXAMPLE\_ADD is defined as follows:

#### Interface

##### FID

0x042

##### Input values

Name	Register	Field	Type	Description
<code>fid</code>	X0	[63:0]	<i>UInt64</i>	Command FID
<code>params_ptr</code>	X1	[63:0]	<i>Address</i>	PA of parameters

##### Context

The EXAMPLE\_ADD command operates on the following context.

Name	Type	Value	Before	Description
<code>params</code>	ExampleParams	Params( <code>params_ptr</code> )	false	Parameters

### Output values

Name	Register	Field	Type	Description
result	X0	[15:0]	CommandReturnCode	Command return status
sum	X1	[63:0]	UInt64	Sum of x and y
zero	X2	[63:0]	UInt64	Whether either x or y was zero

### Failure conditions

ID	Condition
params_align	pre: !AddrIsGranuleAligned(params_ptr) post: ResultEqual(result, ERROR_INPUT)
params_state	pre: Granule(params_ptr).state != NS post: ResultEqual(result, ERROR_MEMORY)

### Success conditions

ID	Post-condition
sum	sum == params.x + params.y
zero	zero == (params.x == 0)    (params.y == 0)

## B1.3 Command registers

D <sub>ZDGNM</sub>	An <i>FID</i> is a value which identifies a particular RMM command.
I <sub>MJQ GK</sub>	The FID of an RMM command is unique among the RMM commands in an RMM interface.
I <sub>RVPGY</sub>	An FID is read from general-purpose register X0.
D <sub>XL SFS</sub>	An <i>input value</i> is a value read by an RMM command from general-purpose registers.
D <sub>VCDCW</sub>	An <i>output value</i> is a value written by an RMM command to general-purpose registers.
D <sub>CZLVJ</sub>	A <i>command return code</i> is a value which specifies whether an RMM command succeeded or failed.
I <sub>FRZFT</sub>	A command return code is written to general-purpose register X0.

## B1.4 Command condition expressions

D <sub>CHRYB</sub>	A <i>condition expression</i> is an expression which evaluates to a boolean value.
I <sub>BNPKQ</sub>	Following expansion of macros, a <i>condition expression</i> is a valid expression in Arm Specification Language (ASL). See also:

- *Arm Specification Language Reference Manual* [14]

- [Chapter B2 Command condition functions](#)

## B1.5 Command context values

**D<sub>DLBYC</sub>** A *context value* is a value which is derived from the value of a command input register and which is used by a command condition expression.

**I<sub>VKKKY</sub>** A context value can be thought of as a local variable for use by command condition expressions.

For example, consider the following example command condition expression:

---

```
!AddrIsGranuleAligned(RealmParams(params_ptr).rtt_base)
```

---

By introducing a context value `params` with the value `RealmParams(params_ptr)`, this command condition expression can be re-written as:

---

```
!AddrIsGranuleAligned(params.rtt_base)
```

---

**D<sub>QDFNW</sub>** The *before* property of a context value indicates whether its expression is re-evaluated after the command has executed.

- `before = true`: the expression is not re-evaluated after the command has executed
- `before = false`: the expression is re-evaluated after the command has executed

**I<sub>LTLQN</sub>** Specifying `before = true` for a context value allows system state to be sampled before command execution, and then used after command execution in a command success condition.

For example, the `RMI_REALM_DESTROY` command takes as an input value the address `rd` of a Realm Descriptor. Successful execution of the command results observable effects including the following:

- The state of the RD Granule changes from RD to DELEGATED
- The state of the RTT base Granule, whose address was previously held in the RD, changes from RTT to DELEGATED

The address of the RTT base Granule is not included in the input values of the command.

A context value is defined as follows:

Name	Type	Value	Before	Description
<code>rtt_base</code>	<a href="#">Address</a>	<code>Realm(rd).rtt_base</code>	true	RTT base address

The state change of the RTT Granule can then be expressed as:

---

```
Granule(rtt_base).state == DELEGATED
```

---

**I<sub>YNDGD</sub>** The *before* property of a context value has no effect if the value is only used in command failure conditions.

**D<sub>XBHPB</sub>** An *in-memory value* is a value passed to a command via an in-memory data structure, the address of which is passed in an input register.

**I<sub>ZTYSS</sub>** An in-memory value is a context value.

See also:

- [B3.3.9 RMI\\_REALM\\_CREATE command](#)

## B1.6 Command failure conditions

$D_{DNQOC}$	An RMM command <i>failure condition</i> defines a way in which the command can fail.
$I_{GVBBZ}$	A failure condition consists of a <i>pre-condition</i> and a <i>post-condition</i> .
$I_{WTSZH}$	A failure pre-condition can be thought of as the “trigger” of the failure: if the pre-condition is true then the command fails.
$I_{KJHNX}$	A failure post-condition can be thought of as the “effect” of the failure: if the command failed due to a particular trigger, then the post-condition defines the error code which is returned.
$I_{CVTGY}$	A failure pre-condition is a condition expression whose terms can include input values and context values.
$I_{HNDNN}$	A failure post-condition is a condition expression whose terms can include input values and context values.
$I_{KHJDY}$	Observability of the checking of command failure conditions is subject to a partial order.

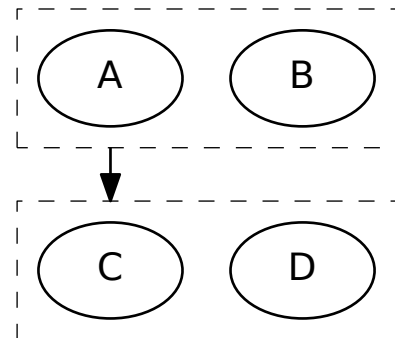
An ordering relation “*A* precedes *B*” means either of the following:

- The pre-condition of *B* is well-formed only if the pre-condition of *A* is false. This is referred to as a *well-formedness ordering*.
- If the pre-conditions of *A* and *B* are both true, then the post-condition of *A* is observed. This is referred to as a *behavioral ordering*.

The absence of an ordering relation “*A* precedes *B*” means that, if the pre-conditions of *A* and *B* are both true then either the post-condition of *A* is observed or the post-condition of *B* is observed.

Orderings are specified between groups of failure conditions. For example, the expression  $[A, B] < [C, D]$  means that both conditions *A* and *B* precede both conditions *C* and *D*.

The same information is also presented graphically, with failure conditions represented as nodes and ordering relations represented as edges.



The specification does not state whether an individual ordering relation is a well-formedness ordering or a behavioral ordering.

$I_{JMTTY}$	A given implementation of the RMM is expected to have deterministic behavior. That is, for a runtime instance of the RMM in a particular state, two executions of a command without an interleaving of other commands, with the same input values, results in the same outcome (either success, or the same failure condition.)
-------------	---

R <sub>WXZJJ</sub>	If a failure pre-condition evaluates to true then the corresponding failure post-condition evaluates to true.
R <sub>DDGDW</sub>	If a failure pre-condition evaluates to true then the command is aborted.
R <sub>TFZMS</sub>	If a command fails then all output values except for X0 are UNDEFINED, unless stated otherwise.
R <sub>VHFHD</sub>	If no failure pre-condition evaluates to true then the command succeeds.

## B1.7 Command success conditions

D <sub>SZGNZ</sub>	An RMM command <i>success condition</i> defines an observable effect of a successful execution of the command.
I <sub>LZXHB</sub>	A success condition is a condition expression whose terms can include input values, context values and output values.
I <sub>NMCSF</sub>	The order in which success conditions are listed has no architectural significance.
I <sub>NJQFG</sub>	If an RMM command succeeds then the return code is <Interface>_SUCCESS.
R <sub>MKRUV</sub>	If an RMM command succeeds then all of its success conditions evaluate to true.

## B1.8 Concrete and abstract types

D <sub>0001</sub>	<p>A <i>concrete type</i> is a type which has a defined encoding.</p> <p>Examples of concrete types include:</p> <ul style="list-style-type: none"> <li>• An integer which has a defined bit width.</li> <li>• An enumeration within which each label is associated with a unique binary value.</li> <li>• A struct which has a defined width, and within which each member has a defined position. The type of each member of a concrete struct is a concrete type.</li> </ul>
I <sub>0002</sub>	Concrete types are used to define command input values and output values.
D <sub>0003</sub>	<p>An <i>abstract type</i> is a type which does not have a defined encoding.</p> <p>Examples of concrete types include:</p> <ul style="list-style-type: none"> <li>• An integer which does not have a defined bit width.</li> <li>• An enumeration which has a set of labels, but which does not define a binary value for each label.</li> <li>• A struct which has a set of members, but which does not define a struct width nor a position for each member. The type of each member of an abstract struct is an abstract type.</li> </ul>
I <sub>0004</sub>	Abstract types are used to model the internal state of the RMM.
I <sub>0005</sub>	<p>A command failure condition or success condition may need to test for logical equality between a concrete type and a corresponding abstract type. For example, the command may set the value of an internal RMM variable to match the value of a command input. To enable such comparisons, the specification defines an <code>Equal()</code> function for each pair of corresponding concrete and abstract types.</p> <p>See also:</p> <ul style="list-style-type: none"> <li>• <a href="#">B2.11 Equal function</a></li> </ul>

## B1.9 Command footprint

D <sub>ZDJDB</sub>	The <i>footprint</i> of an RMM command defines the set of state items which successful execution of the command can modify.
--------------------	---



I <sub>XMZYS</sub>	The footprint of an RMM command may include state items which are not modified by successful execution of the command.
I <sub>RWQMJ</sub>	<p>If an RMM command changes the state of a Granule then the footprint typically does not include all attributes of the object which is created or destroyed.</p> <p>For example, the footprint of RMI_REALM_CREATE includes the state of the RD Granule, but does not include attributes of the newly-created Realm.</p>
R <sub>WZYBV</sub>	Except for items in the footprint of an RMM command and registers in the output values of the RMM command, execution of the command does not have any observable effects.

## Chapter B2

# Command condition functions

This chapter describes functions which are used in command condition expressions.

See also:

- [B1.4 Command condition expressions](#)

### B2.1 AddrInRange function

Returns TRUE if `addr` is within `[base, base+size]`.

---

```
func AddrInRange(  
    addr : Address,  
    base : Address,  
    size : integer) => boolean  
begin  
    return ((UInt(addr) >= UInt(base))  
        && (UInt(addr) <= UInt(base) + size));  
end
```

---

### B2.2 AddrIsAligned function

Returns TRUE if address `addr` is aligned to an `n` byte boundary.

---

```
func AddrIsAligned(  
    addr : Address,  
    n : integer) => boolean
```

---

## B2.3 AddrIsGranuleAligned function

Returns TRUE if address `addr` is aligned to the size of a Granule.

---

```
func AddrIsGranuleAligned(  
    addr : Address) => boolean
```

---

```
func AddrIsGranuleAligned(  
    addr : integer) => boolean
```

---

See also:

- [A2.2 Granule](#)

## B2.4 AddrIsProtected function

Returns TRUE if address `addr` is a Protected IPA for `realm`.

---

```
func AddrIsProtected(  
    addr : Address,  
    realm : RmmRealm) => boolean  
begin  
    return UInt(addr) < 2^(realm.ipa_width - 1);  
end
```

---

## B2.5 AddrIsRttLevelAligned function

Returns TRUE if Address `addr` is aligned to the size of the address range described by an RTTE in a level `level` RTT.

Returns FALSE if `level` is invalid.

---

```
func AddrIsRttLevelAligned(  
    addr : Address,  
    level : integer) => boolean
```

---

## B2.6 AddrRangeIsProtected function

Returns TRUE if all addresses in range `[base, top)` are Protected IPAs for `realm`.

---

```
func AddrRangeIsProtected(  
    base : Address,  
    top : Address,  
    realm : RmmRealm) => boolean  
begin  
    var size = UInt(top) - UInt(base);  
    return (AddrIsProtected(base, realm)  
        && size > 0  
        && size < 2^realm.ipa_width  
        && AddrIsProtected(ToAddress(UInt(top) - 1), realm));  
end
```

---

## B2.7 AlignDownToRttLevel function

Round down `addr` to align to the size of the address range described by an RTTE in a level `level` RTT.

---

```
func AlignDownToRttLevel(  
    addr : Address,  
    level : integer) => Address
```

---

## B2.8 AlignUpToRttLevel function

Round up `addr` to align to the size of the address range described by an RTTE in a level `level` RTT.

---

```
func AlignUpToRttLevel(  
    addr : Address,  
    level : integer) => Address
```

---

## B2.9 CurrentRealm function

Returns the current Realm.

---

```
func CurrentRealm() => RmmRealm
```

---

## B2.10 CurrentRec function

Returns the current REC.

---

```
func CurrentRec() => RmmRec
```

---

## B2.11 Equal function

Check whether concrete and abstract values are equal

---

```
func Equal(  
    abstract : RmmHashAlgorithm,  
    concrete : RmiHashAlgorithm) => boolean
```

---

---

```
func Equal(  
    concrete : RmiHashAlgorithm,  
    abstract : RmmHashAlgorithm) => boolean
```

---

---

```
func Equal(  
    abstract : RmmRecRunnable,  
    concrete : RmiRecRunnable) => boolean
```

---

---

```
func Equal(  
    concrete : RmiRecRunnable,  
    abstract : RmmRecRunnable) => boolean
```

---

---

```
func Equal(  
    abstract : RmmRipas,  
    concrete : RmiRipas) => boolean
```

---

---

```
func Equal(  
    concrete : RmiRipas,  
    abstract : RmmRipas) => boolean
```

---

---

```
func Equal(  
    abstract : RmmHashAlgorithm,  
    concrete : RsiHashAlgorithm) => boolean
```

---

---

```
func Equal(  
    concrete : RsiHashAlgorithm,  
    abstract : RmmHashAlgorithm) => boolean
```

---

```
func Equal(  
    abstract : RmmRipas,  
    concrete : RsiRipas) => boolean
```

---

```
func Equal(  
    concrete : RsiRipas,  
    abstract : RmmRipas) => boolean
```

---

```
func Equal(  
    abstract : RmmRipasChangeDestroyed,  
    concrete : RsiRipasChangeDestroyed) => boolean
```

---

```
func Equal(  
    concrete : RsiRipasChangeDestroyed,  
    abstract : RmmRipasChangeDestroyed) => boolean
```

---

See also:

- [B1.8 Concrete and abstract types](#)

## B2.12 Gicv3ConfigIsValid function

Returns TRUE if the values of all gicv3\_\* attributes are valid.

---

```
func Gicv3ConfigIsValid(  
    gicv3_hcr : bits(64),  
    gicv3_lrs : array [16] of bits(64)) => boolean
```

---

See also:

- [A6.1 Realm interrupts](#)
- [B3.4.14 RmiRecEnter type](#)

## B2.13 Granule function

Returns the Granule located at physical address addr.

---

```
func Granule(  
    addr : Address) => RmmGranule
```

---

See also:

- [A2.2 Granule](#)

## B2.14 MinAddress function

Returns the smaller of two addresses.

---

```
func MinAddress(  
    addr1 : Address,  
    addr2 : Address) => Address
```

begin

```
        return ToAddress (Min (UInt (addr1), UInt (addr2)));  
    end
```

---

## B2.15 MpidrEqual function

Returns TRUE if the specified MPIDR values are logically equivalent.

```
func MpidrEqual(  
    rmm_mpidr : bits(64),  
    rmi_mpidr : RmiRecMpidr) => boolean  
begin  
    return (rmm_mpidr[ 3: 0] == rmi_mpidr.aff0  
        && rmm_mpidr[15: 8] == rmi_mpidr.aff1  
        && rmm_mpidr[23:16] == rmi_mpidr.aff2  
        && rmm_mpidr[31:24] == rmi_mpidr.aff3);  
end
```

---

## B2.16 MpidrIsUsed function

Returns TRUE if the specified MPIDR value identifies a REC in the current Realm.

```
func MpidrIsUsed(  
    mpidr : bits(64)) => boolean
```

---

## B2.17 PalsDelegable function

Returns TRUE if the Granule located at physical address addr is delegable.

```
func PaIsDelegable(  
    addr : Address) => boolean
```

---

## B2.18 PsciReturnCodeEncode function

Return encoding for a PsciReturnCode value.

```
func PsciReturnCodeEncode(  
    value : PsciReturnCode) => bits(64)
```

---

## B2.19 PsciReturnCodePermitted function

Whether a PSCI return code is permitted.

```
func PsciReturnCodePermitted(  
    calling_rec : RmmRec,  
    target_rec : RmmRec,  
    value : PsciReturnCode) => boolean  
begin  
    if value == PSCI_SUCCESS then  
        return TRUE;  
    end  
  
    var fid : bits(64) = calling_rec.gprs[0];  
  
    // Host is permitted to deny a PSCI_CPU_ON request, if the target  
    // CPU is not already on.
```

```
    if (fid == FID_PSCI_CPU_ON
        && target_rec.flags.runnable != RUNNABLE
        && value == PSCI_DENIED) then
        return TRUE;
    end

    return FALSE;
end
```

---

See also:

- [A4.3.7 REC exit due to PSCI](#)
- [B3.3.7 RMI\\_PSCI\\_COMPLETE command](#)

## B2.20 ReadMemory function

Read contents of memory at address range [addr + offset, addr + offset + size)

offset and size are both numbers of bytes.

```
func ReadMemory(
    addr : bits(64),
    offset : integer,
    size : integer) => bits(size * 8)
```

---

## B2.21 Realm function

Returns the Realm whose RD is located at physical address addr.

```
func Realm(
    addr : Address) => RmmRealm
```

---

See also:

- [A2.1 Realm](#)

## B2.22 RealmConfig function

Returns Realm configuration stored at IPA addr, mapped in the current Realm.

```
func RealmConfig(
    addr : Address) => RsiRealmConfig
```

---

## B2.23 RealmHostCall function

Returns Host call data stored at IPA addr, mapped in the current Realm.

```
func RealmHostCall(
    addr : Address) => RsiHostCall
```

---

## B2.24 RealmlsLive function

Returns TRUE if the Realm whose RD is located at physical address addr is live.

---

```
func RealmIsLive(  
    addr : Address) => boolean
```

---

See also:

- [A2.1.4 Realm liveness](#)

## B2.25 RealmParams function

Returns Realm parameters stored at physical address `addr`.

If the PAS of `addr` is not NS, the return value is UNKNOWN.

---

```
func RealmParams(  
    addr : Address) => RmiRealmParams
```

---

See also:

- [A2.1.6 Realm parameters](#)

## B2.26 RealmParamsSupported function

Returns TRUE if the Realm parameters are supported by the implementation.

---

```
func RealmParamsSupported(  
    value : RmiRealmParams) => boolean
```

---

## B2.27 Rec function

Returns the REC object located at physical address `addr`.

---

```
func Rec(  
    addr : Address) => RmmRec
```

---

See also:

- [A2.3 Realm Execution Context](#)

## B2.28 RecAuxAlias function

Returns TRUE if any of the first `count` entries in a list of REC auxiliary Granule addresses are aliased - either among themselves, or with the REC address itself.

---

```
func RecAuxAlias(  
    rec : Address,  
    aux : array [16] of Address,  
    count : integer) => boolean  
begin  
    assert 0 <= count && count <= 16;  
    var sorted = RecAuxSort(aux, count);  
  
    for i = 0 to count - 1 do  
        if sorted[i] == rec then  
            return TRUE;  
        end
```



```
        if i >= 1 && sorted[i] == sorted[i - 1] then
            return TRUE;
        end
    end
    return FALSE;
end
```

---

## B2.29 RecAuxAligned function

Returns TRUE if the first `count` entries in a list of REC auxiliary Granule addresses are aligned to the size of a Granule.

```
func RecAuxAligned(
    aux : array [16] of Address,
    count : integer) => boolean
begin
    assert 0 <= count && count <= 16;
    for i = 0 to count - 1 do
        if !AddrIsGranuleAligned(aux[i]) then
            return FALSE;
        end
    end
    return TRUE;
end
```

---

## B2.30 RecAuxCount function

Returns the number of auxiliary Granules required for a REC in the Realm described by `rd`.

```
func RecAuxCount(
    rd : Address) => integer
```

---

## B2.31 RecAuxEqual function

Returns TRUE if the first `count` entries in two lists of REC auxiliary Granule addresses are equal.

```
func RecAuxEqual(
    aux1 : array [16] of Address,
    aux2 : array [16] of Address,
    count : integer) => boolean
begin
    assert 0 <= count && count <= 16;
    for i = 0 to count - 1 do
        if aux1[i] != aux2[i] then
            return FALSE;
        end
    end
    return TRUE;
end
```

---

## B2.32 RecAuxSort function

Sort first `count` entries in array of auxiliary Granule addresses.

```
func RecAuxSort(
    addrs : array [16] of Address,
```

---

---

```
count : integer) => array [16] of Address
```

---

## B2.33 RecAuxStateEqual function

Returns TRUE if the state of the first `count` entries in a list of REC auxiliary Granule addresses is equal to `state`.

---

```
func RecAuxStateEqual(  
    aux : array [16] of Address,  
    count : integer,  
    state : RmmGranuleState) => boolean  
begin  
    assert 0 <= count && count <= 16;  
    for i = 0 to count - 1 do  
        if (!PaIsDelegable(aux[i])  
            || Granule(aux[i]).state != state) then  
            return FALSE;  
        end  
    end  
    return TRUE;  
end
```

---

## B2.34 RecAuxStates function

Inductive function which identifies the states of the first `count` entries in a list of REC auxiliary Granules.

This function is used in the definition of command footprint.

---

```
func RecAuxStates(  
    aux : array [16] of Address,  
    count : integer)
```

---

## B2.35 RecFromMpidr function

Returns the REC object identified by the specified MPIDR value, in the current Realm.

---

```
func RecFromMpidr(  
    mpidr : bits(64)) => RmmRec
```

---

## B2.36 RecIndex function

Returns the REC index which corresponds to `mpidr`.

---

```
func RecIndex(  
    mpidr : RmiRecMpidr) => integer  
begin  
    return (UInt(mpidr.aff0)  
        + 16 * UInt(mpidr.aff1)  
        + 16 * 256 * UInt(mpidr.aff2)  
        + 16 * 256 * 256 * UInt(mpidr.aff3));  
end
```

---

See also:

- [A2.3.3 REC index and MPIDR value](#)

## B2.37 RecParams function

Returns REC parameters stored at physical address `addr`.

If the PAS of `addr` is not NS, the return value is UNKNOWN.

---

```
func RecParams(  
    addr : Address) => RmiRecParams
```

---

## B2.38 RecRipasChangeResponse function

Returns response to RIPAS change request.

---

```
func RecRipasChangeResponse(  
    rec : RmmRec) => RsiResponse  
begin  
    if ((rec.ripas_value == RAM)  
        && (rec.ripas_addr != rec.ripas_top)  
        && (rec.ripas_response == REJECT)) then  
        return RSI_REJECT;  
    end  
  
    return RSI_ACCEPT;  
end
```

---

See also:

- [A5.4 RIPAS change](#)

## B2.39 RecRun function

Returns the RecRun object stored at physical address `addr`.

---

```
func RecRun(  
    addr : Address) => RmiRecRun
```

---

See also:

- [A4.2 REC entry](#)
- [A4.3 REC exit](#)

## B2.40 RemExtend function

Extend REM, using `size` LSBs from `new_value`, with the remaining bits zero-padded to form a 512-bit value.

---

```
func RemExtend(  
    hash_algo : RmmHashAlgorithm,  
    old_value : RmmRealmMeasurement,  
    new_value : RmmRealmMeasurement,  
    size : integer) => RmmRealmMeasurement
```

---

See also:

- [A7.1.2 Realm Extensible Measurement](#)

## B2.41 ResultEqual function

Returns TRUE if command result matches the stated value.

---

```
func ResultEqual(  
    result : RmiCommandReturnCode,  
    status : RmiStatusCode) => boolean
```

---

```
func ResultEqual(  
    result : RmiCommandReturnCode,  
    status : RmiStatusCode,  
    index : integer) => boolean
```

---

## B2.42 RimExtendData function

Extend RIM with contribution from DATA creation.

---

```
func RimExtendData(  
    realm : RmmRealm,  
    ipa : Address,  
    data : Address,  
    flags : RmiDataFlags) => RmmRealmMeasurement
```

---

See also:

- [B3.3.1.4 RMI\\_DATA\\_CREATE extension of RIM](#)

## B2.43 RimExtendRec function

Extend RIM with contribution from REC creation.

---

```
func RimExtendRec(  
    realm : RmmRealm,  
    params : RmiRecParams) => RmmRealmMeasurement
```

---

See also:

- [B3.3.12.4 RMI\\_REC\\_CREATE extension of RIM](#)

## B2.44 RimExtendRipas function

Extend RIM with contribution from RIPAS change for an IPA range.

---

```
func RimExtendRipas(  
    realm : RmmRealm,  
    base : Address,  
    top : Address,  
    level : integer) => RmmRealmMeasurement  
begin  
    var rim = realm.measurements[0];  
    var size = RttLevelSize(level);  
    var addr = base;  
  
    while (UInt(addr) < UInt(top)) do  
        rim = RimExtendRipasForEntry(rim, addr, level);  
        addr = ToAddress(UInt(addr) + size);
```

```
    end  
  
    return rim;  
end
```

---

See also:

- [B3.3.18.4 RMI\\_RTT\\_INIT\\_RIPAS extension of RIM](#)

## B2.45 RimExtendRipasForEntry function

Extend RIM with contribution from RIPAS change for a single RTT entry.

```
func RimExtendRipasForEntry(  
    rim : RmmRealmMeasurement,  
    ipa : Address,  
    level : integer) => RmmRealmMeasurement
```

---

## B2.46 RimInit function

Initialize RIM.

```
func RimInit(  
    hash_algo : RmmHashAlgorithm,  
    params : RmiRealmParams) => RmmRealmMeasurement
```

---

See also:

- [B3.3.9.4 RMI\\_REALM\\_CREATE initialization of RIM](#)

## B2.47 RmiRealmParamsIsValid function

Returns TRUE if the memory location contains a valid encoding of the RmiRealmParams type.

```
func RmiRealmParamsIsValid(  
    addr : Address) => boolean
```

---

## B2.48 Rtt function

Returns the RTT at address rtt.

```
func Rtt(  
    addr : Address) => RmmRtt
```

---

## B2.49 RttAllEntriesContiguous function

Returns TRUE if all entries in the RTT at address rtt at level level have contiguous output addresses, starting with addr.

```
func RttAllEntriesContiguous(  
    rtt : RmmRtt,  
    addr : Address,  
    level : integer) => boolean
```

---

See also:

- [A5.5 Realm Translation Table](#)

## B2.50 RttAllEntriesRipas function

Returns TRUE if all entries in the RTT at address `rtt` have RIPAS `ripas`.

---

```
func RttAllEntriesRipas(  
    rtt : RmmRtt,  
    ripas : RmmRipas) => boolean
```

---

## B2.51 RttAllEntriesState function

Returns TRUE if all entries in the RTT at address `rtt` have state `state`.

---

```
func RttAllEntriesState(  
    rtt : RmmRtt,  
    state : RmmRttEntryState) => boolean
```

---

See also:

- [A5.5 Realm Translation Table](#)

## B2.52 RttConfigIsValid function

Returns TRUE if the RTT configuration values provided are self-consistent and are supported by the platform.

---

```
func RttConfigIsValid(  
    ipa_width : integer,  
    rtt_level_start : integer,  
    rtt_num_start : integer) => boolean
```

---

See also:

- [A5.5 Realm Translation Table](#)

## B2.53 RttDescriptorIsValidForUnprotected function

Returns TRUE if, within the descriptor `desc`, all of the following are true:

- All fields which are *Host-controlled RTT attributes* are set to architecturally valid values.
- All fields which are not *Host-controlled RTT attributes* are set to zero.

---

```
func RttDescriptorIsValidForUnprotected(  
    desc : bits(64)) => boolean
```

---

See also:

- [A5.5.11 RTT entry attributes](#)

## B2.54 RttEntriesInRangeRipas function

Returns TRUE if all entries in the RTT at address `rtt` at level `level`, within IPA range [base, top), have RIPAS

```
ripas.  
  
func RttEntriesInRangeRipas(  
    rtt : RmmRtt,  
    level : integer,  
    base : Address,  
    top : Address,  
    ripas : RmmRipas) => boolean
```

## B2.55 RttEntry function

Returns the *i*th entry in the RTT at address *rtt*.

```
func RttEntry(  
    addr : Address,  
    i : integer) => RmmRttEntry
```

See also:

- [A5.5 Realm Translation Table](#)

## B2.56 RttEntryFromDescriptor function

Converts a descriptor to an RmmRttEntry object.

```
func RttEntryFromDescriptor(  
    desc : bits(64)) => RmmRttEntry
```

## B2.57 RttEntryIndex function

Returns the index of the entry in a level *level* RTT which is identified by *addr*.

```
func RttEntryIndex(  
    addr : Address,  
    level : integer) => integer
```

See also:

- [A5.5 Realm Translation Table](#)

## B2.58 RttEntryState function

Encodes the state of an RTTE.

```
func RttEntryState(  
    state : RmmRttEntryState) => RmiRttEntryState  
begin  
    case state of  
        when UNASSIGNED => return RMI_UNASSIGNED;  
        when ASSIGNED => return RMI_ASSIGNED;  
        when UNASSIGNED_NS => return RMI_UNASSIGNED;  
        when ASSIGNED_NS => return RMI_ASSIGNED;  
        when TABLE => return RMI_TABLE;  
    end  
end
```

## B2.59 RttFold function

Returns the RTTE which results from folding the homogeneous RTT at address `rtt`.

---

```
func RttFold(  
    rtt : RmmRtt) => RmmRttEntry
```

---

See also:

- [A5.5.6 RTT folding](#)

## B2.60 RttIsHomogeneous function

Returns TRUE if the RTT at address `rtt` is homogeneous.

---

```
func RttIsHomogeneous(  
    rtt : RmmRtt) => boolean
```

---

See also:

- [A5.5.6 RTT folding](#)

## B2.61 RttIsLive function

Returns TRUE if the RTT at address `rtt` is live.

---

```
func RttIsLive(  
    rtt : RmmRtt) => boolean
```

---

See also:

- [A5.5.8 RTTE liveness and RTT liveness](#)
- [A5.5.9 RTT destruction](#)

## B2.62 RttLevelIsBlockOrPage function

Returns TRUE if `level` is either a block or page RTT level for the Realm described by `rd`.

---

```
func RttLevelIsBlockOrPage(  
    rd : Address,  
    level : integer) => boolean
```

---

See also:

- [A5.5 Realm Translation Table](#)

## B2.63 RttLevelIsStarting function

Returns TRUE if `level` is the starting level of the RTT for the Realm described by `rd`.

---

```
func RttLevelIsStarting(  
    rd : Address,  
    level : integer) => boolean
```

---



See also:

- [A5.5 Realm Translation Table](#)

## B2.64 RttLevellsValid function

Returns TRUE if `level` is a valid RTT level for the Realm described by `rd`.

---

```
func RttLevelIsValid(  
    rd : Address,  
    level : integer) => boolean
```

---

See also:

- [A5.5 Realm Translation Table](#)

## B2.65 RttLevelSize function

Returns the size of the address space described by each entry in an RTT at level.

If `level` is invalid, the return value is UNKNOWN.

---

```
func RttLevelSize(  
    level : integer) => integer
```

---

See also:

- [A5.5 Realm Translation Table](#)

## B2.66 RttsAllProtectedEntriesRipas function

Returns TRUE if the RIPAS of all entries identified by Protected IPAs in all of the starting-level RTT Granules is equal to `ripas`.

---

```
func RttsAllProtectedEntriesRipas(  
    rtt_base : Address,  
    rtt_num_start : integer,  
    ripas : RmmRipas) => boolean
```

---

## B2.67 RttsAllProtectedEntriesState function

Returns TRUE if the state of all entries identified by Protected IPAs in all of the starting-level RTT Granules is equal to `state`.

---

```
func RttsAllProtectedEntriesState(  
    rtt_base : Address,  
    rtt_num_start : integer,  
    state : RmmRttEntryState) => boolean
```

---

## B2.68 RttsAllUnprotectedEntriesState function

Returns TRUE if the state of all entries identified by Unprotected IPAs in all of the starting-level RTT Granules is equal to `state`.

---

```
func RttsAllUnprotectedEntriesState(  
    rtt_base : Address,  
    rtt_num_start : integer,  
    state : RmmRttEntryState) => boolean
```

---

## B2.69 RttsGranuleState function

Inductive function which identifies the states of the starting-level RTT Granules.

This function is used in the definition of command footprint.

---

```
func RttsGranuleState(  
    rtt_base : Address,  
    rtt_num_start : integer)
```

---

## B2.70 RttSkipEntriesUnlessRipas function

Scanning *rtt* starting from *ipa*, returns the IPA of the first entry whose RIPAS is *ripas*.

If no entry is found whose RIPAS is *ripas*, returns the next IPA after the last entry in *rtt*.

The return value is aligned to the size of the address range described by an entry at RTT level.

---

```
func RttSkipEntriesUnlessRipas(  
    rtt : RmmRtt,  
    level : integer,  
    ipa : Address,  
    ripas : RmmRipas) => Address
```

---

## B2.71 RttSkipEntriesUnlessState function

Scanning *rtt* starting from *ipa*, returns the IPA of the first entry whose state is *state*.

If no entry is found whose state is *state*, returns the next IPA after the last entry in *rtt*.

The return value is aligned to the size of the address range described by an entry at RTT level.

---

```
func RttSkipEntriesUnlessState(  
    rtt : RmmRtt,  
    level : integer,  
    ipa : Address,  
    state : RmmRttEntryState) => Address
```

---

## B2.72 RttSkipEntriesWithRipas function

Scan *rtt* starting from *base* and terminating at *top*.

- If *stop\_at\_destroyed* is FALSE then return IPA of the first entry whose state is TABLE.
- If *stop\_at\_destroyed* is TRUE then return IPA of the first entry whose state is TABLE or whose RIPAS is DESTROYED.

If no such entry is found, returns the smaller of:

- The next IPA after the last entry in *rtt*
- The *top* argument.

The return value is aligned to the size of the address range described by an entry at RTT level.

---

```
func RttSkipEntriesWithRipas(  
    rtt : RmmRtt,  
    level : integer,  
    base : Address,  
    top : Address,  
    stop_at_destroyed : boolean) => Address  
begin  
    var result : Address = RttSkipEntriesUnlessState(  
        rtt, level, base, TABLE);  
  
    if stop_at_destroyed then  
        result = MinAddress(result,  
            RttSkipEntriesUnlessRipas(  
                rtt, level, base, DESTROYED));  
    end  
  
    result = MinAddress(result, top);  
  
    return AlignDownToRttLevel(result, level);  
end
```

---

## B2.73 RttSkipNonLiveEntries function

Scanning rtt starting from ipa, returns the IPA of the first live entry.

If no live entry is found, returns the next IPA after the last entry in rtt.

The return value is aligned to the size of the address range described by an entry at RTT level.

---

```
func RttSkipNonLiveEntries(  
    rtt : RmmRtt,  
    level : integer,  
    ipa : Address) => Address  
begin  
    var result : Address = RttSkipEntriesUnlessState(  
        rtt, level, ipa, ASSIGNED);  
  
    result = MinAddress(result,  
        RttSkipEntriesUnlessState(  
            rtt, level, ipa, ASSIGNED_NS));  
  
    result = MinAddress(result,  
        RttSkipEntriesUnlessState(  
            rtt, level, ipa, TABLE));  
  
    return AlignDownToRttLevel(result, level);  
end
```

---

See also:

- [A5.5.8 RTTE liveness and RTT liveness](#)

## B2.74 RttStateEqual function

Returns TRUE if the state of all of the starting-level RTT Granules is equal to state.

---

```
func RttStateEqual(  
    rtt_base : Address,  
    rtt_num_start : integer,  
    state : RmmGranuleState) => boolean  
begin  
    for i = 0 to rtt_num_start - 1 do  
        var addr = (UInt(rtt_base) + i * RMM_GRANULE_SIZE) [(ADDRESS_WIDTH-1):0];  
        if (!PaIsDelegable(addr)  
            || Granule(addr).state != state) then  
            return FALSE;  
        end  
    end  
    return TRUE;  
end
```

---

## B2.75 RttWalk function

Returns the result of an RTT walk from the RTT base of `rd` to address `addr`.

If `level` is provided, the walk terminates at `level`.

```
func RttWalk(  
    rd : Address,  
    addr : Address) => RmmRttWalkResult  
  
func RttWalk(  
    rd : Address,  
    addr : Address,  
    level : integer) => RmmRttWalkResult
```

---

See also:

- [A5.5.10 RTT walk](#)

## B2.76 ToAddress function

Convert integer to Address.

```
func ToAddress(value : integer) => Address  
begin  
    return value[(ADDRESS_WIDTH-1):0];  
end
```

---

## B2.77 ToBits64 function

Convert integer to Bits64.

```
func ToBits64(value : integer) => bits(64)  
begin  
    return value[63:0];  
end
```

---

## B2.78 VmidIsFree function

Returns TRUE if `vmid` is unused.

---

```
func VmidIsFree(  
    vmid : bits(16)) => boolean
```

---

## B2.79 VmidIsValid function

Returns TRUE if `vmid` is valid on the platform.

---

```
func VmidIsValid(  
    vmid : bits(16)) => boolean
```

---

If the underlying hardware platform does not implement FEAT\_VMID16 then a VMID value with `vmid[15:8] != 0` is invalid.

See also:

- [A2.1.3 Realm attributes](#)
- [B3.3.9 RMI\\_REALM\\_CREATE command](#)

## Chapter B3

# Realm Management Interface

This chapter defines the interface used by the Host to manage Realms.

## B3.1 RMI version

**R<sub>NCFDX</sub>** This specification defines version 1.0 of the Realm Management Interface.

See also:

- [B3.3.23 RMI\\_VERSION command](#)

## B3.2 RMI command return codes

**I<sub>JQMBN</sub>** The return code of an RMI command is a tuple which contains *status* and *index* fields.

**I<sub>YCHQV</sub>** The *status* field of an RMI command return code indicates whether the command

- succeeded, or
- failed, and the reason for the failure.

**I<sub>PPNST</sub>** If an RMI command succeeds then the status of its return code is RMI\_SUCCESS.

**I<sub>MBVPG</sub>** The *index* field of an RMI command return code can provide additional information about the reason for a command failure. The meaning of the index field depends on the status, and is described by the following table.

Status	Description	Meaning of index
RMI_SUCCESS	Command completed successfully	None: index is zero.
RMI_ERROR_INPUT	The value of a command input value caused the command to fail	None: index is zero.
RMI_ERROR_REALM	An attribute of a Realm does not match the expected value	Varies between usages. See individual commands for details.
RMI_ERROR_REC	An attribute of a REC does not match the expected value	None: index is zero.
RMI_ERROR_RTT	An RTT walk terminated before reaching the target RTT level, or reached an RTTE with an unexpected value	RTT level at which the walk terminated.

**I<sub>QQQNB</sub>** Multiple failure conditions in an RMI command may return the same error code - that is, the same status and index values.

**R<sub>XRDYQ</sub>** If an input to an RMI command uses an invalid encoding then the command fails and returns RMI\_ERROR\_INPUT. Command inputs include registers and in-memory data structures.

Invalid encodings include:

- using a reserved encoding in an enumeration

See also:

- [B3.4.1 RmiCommandReturnCode type](#)

## B3.3 RMI commands

The following table summarizes the FIDs of commands in the RMI interface.

FID	Command
0xC4000153	<a href="#">RMI_DATA_CREATE</a>
0xC4000154	<a href="#">RMI_DATA_CREATE_UNKNOWN</a>
0xC4000155	<a href="#">RMI_DATA_DESTROY</a>
0xC4000165	<a href="#">RMI_FEATURES</a>
0xC4000151	<a href="#">RMI_GRANULE_DELEGATE</a>
0xC4000152	<a href="#">RMI_GRANULE_UNDELEGATE</a>
0xC4000164	<a href="#">RMI_PSCI_COMPLETE</a>
0xC4000157	<a href="#">RMI_REALM_ACTIVATE</a>
0xC4000158	<a href="#">RMI_REALM_CREATE</a>
0xC4000159	<a href="#">RMI_REALM_DESTROY</a>
0xC4000167	<a href="#">RMI_REC_AUX_COUNT</a>
0xC400015A	<a href="#">RMI_REC_CREATE</a>
0xC400015B	<a href="#">RMI_REC_DESTROY</a>
0xC400015C	<a href="#">RMI_REC_ENTER</a>
0xC400015D	<a href="#">RMI_RTT_CREATE</a>
0xC400015E	<a href="#">RMI_RTT_DESTROY</a>
0xC4000166	<a href="#">RMI_RTT_FOLD</a>
0xC4000168	<a href="#">RMI_RTT_INIT_RIPAS</a>
0xC400015F	<a href="#">RMI_RTT_MAP_UNPROTECTED</a>
0xC4000161	<a href="#">RMI_RTT_READ_ENTRY</a>
0xC4000169	<a href="#">RMI_RTT_SET_RIPAS</a>
0xC4000162	<a href="#">RMI_RTT_UNMAP_UNPROTECTED</a>
0xC4000150	<a href="#">RMI_VERSION</a>



### B3.3.1 RMI\_DATA\_CREATE command

Creates a Data Granule, copying contents from a Non-secure Granule provided by the caller.

See also:

- [Chapter A5 Realm memory management](#)
- [B3.3.3 RMI\\_DATA\\_DESTROY command](#)
- [D1.2.3 Initialize memory of New Realm flow](#)

#### B3.3.1.1 Interface

##### B3.3.1.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000153
rd	X1	63:0	Address	PA of the RD for the target Realm
data	X2	63:0	Address	PA of the target Data
ipa	X3	63:0	Address	IPA at which the Granule will be mapped in the target Realm
src	X4	63:0	Address	PA of the source Granule
flags	X5	63:0	RmiDataFlags	Flags

##### B3.3.1.1.2 Context

The RMI\_DATA\_CREATE command operates on the following context.

Name	Type	Value	Before	Description
realm	RmmRealm	Realm(rd)	true	Realm
walk	RmmRttWalkResult	RttWalk( rd, ipa, RMM_RTT_PAGE_LEVEL)	false	RTT walk result
entry_idx	UInt64	RttEntryIndex( ipa, walk.level)	false	RTTE index

##### B3.3.1.1.3 Output values

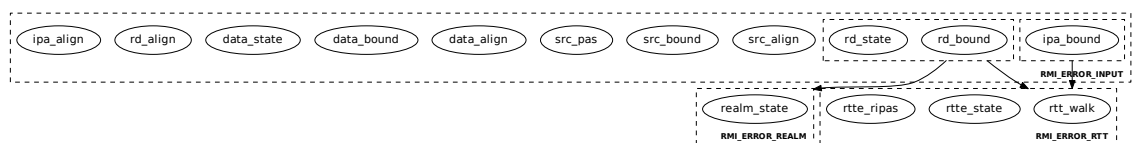
Name	Register	Bits	Type	Description
result	X0	63:0	RmiCommandReturnCode	Command return status

#### B3.3.1.2 Failure conditions

ID	Condition
src_align	pre: !AddrIsGranuleAligned(src) post: ResultEqual(result, RMI_ERROR_INPUT)
src_bound	pre: !PaIsDelegable(src) post: ResultEqual(result, RMI_ERROR_INPUT)
src_pas	pre: Granule(src).pas != NS post: ResultEqual(result, RMI_ERROR_INPUT)
data_align	pre: !AddrIsGranuleAligned(data) post: ResultEqual(result, RMI_ERROR_INPUT)
data_bound	pre: !PaIsDelegable(data) post: ResultEqual(result, RMI_ERROR_INPUT)
data_state	pre: Granule(data).state != DELEGATED post: ResultEqual(result, RMI_ERROR_INPUT)
rd_align	pre: !AddrIsGranuleAligned(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_bound	pre: !PaIsDelegable(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_state	pre: Granule(rd).state != RD post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_align	pre: !AddrIsGranuleAligned(ipa) post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_bound	pre: !AddrIsProtected(ipa, realm) post: ResultEqual(result, RMI_ERROR_INPUT)
realm_state	pre: realm.state != NEW post: ResultEqual(result, RMI_ERROR_REALM)
rtt_walk	pre: walk.level < RMM_RTT_PAGE_LEVEL post: ResultEqual(result, RMI_ERROR_RTT, walk.level)
rtte_state	pre: walk.rtte.state != UNASSIGNED post: ResultEqual(result, RMI_ERROR_RTT, walk.level)
rtte_ripas	pre: walk.rtte.ripas != RAM post: ResultEqual(result, RMI_ERROR_RTT, walk.level)

### B3.3.1.2.1 Failure condition ordering

```
[rd_bound, rd_state] < [realm_state]
[rd_bound, rd_state] < [rtt_walk, rtte_state, rtte_ripas]
[ipa_bound] < [rtt_walk, rtte_state, rtte_ripas]
```



### B3.3.1.3 Success conditions

ID	Condition
data_state	<code>Granule(data).state == DATA</code>
rtte_state	<code>walk.rtte.state == ASSIGNED</code>
rtte_addr	<code>walk.rtte.addr == data</code>
rim	<code>Realm(rd).measurements[0] == RimExtendData(     realm, ipa, data, flags)</code>

### B3.3.1.4 RMI\_DATA\_CREATE extension of RIM

On successful execution of RMI\_DATA\_CREATE, the new RIM value of the target Realm is calculated by the RMM as follows:

1. If `flags.measure == RMI_MEASURE_CONTENT` then using the RHA of the target Realm, compute the hash of the contents of the DATA Granule.
2. Allocate an [RmmMeasurementDescriptorData](#) data structure.
3. Populate the measurement descriptor:
  - Set the `desc_type` field to the descriptor type.
  - Set the `len` field to the descriptor length.
  - Set the `rim` field to the current RIM value of the target Realm.
  - Set the `ipa` field to the IPA at which the DATA Granule is mapped in the target Realm.
  - Set the `flags` field to the flags provided by the Host.
  - If `flags.measure == RMI_MEASURE_CONTENT` then set the `content` field to the hash of the contents of the DATA Granule. Otherwise, set the `content` field to zero.
4. Using the RHA of the target Realm, compute the hash of the measurement descriptor. Set the RIM of the target Realm to this value, zero filling upper bytes if the RHA output is smaller than the size of the RIM.

See also:

- [A7.1.1 Realm Initial Measurement](#)
- [B2.42 RimExtendData function](#)
- [C1.5 RmmMeasurementDescriptorData type](#)

### B3.3.1.5 Footprint

ID	Value
data_state	<code>Granule(data).state</code>
rim	<code>Realm(rd).measurements[0]</code>
rtte	<code>RttEntry(walk.rtt_addr, entry_idx)</code>

### B3.3.2 RMI\_DATA\_CREATE\_UNKNOWN command

Creates a Data Granule with unknown contents.

See also:

- [A2.2.4 Granule wiping](#)
- [Chapter A5 Realm memory management](#)
- [B3.3.3 RMI\\_DATA\\_DESTROY command](#)
- [D1.5.1 Add memory to Active Realm flow](#)

#### B3.3.2.1 Interface

##### B3.3.2.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000154
rd	X1	63:0	Address	PA of the RD for the target Realm
data	X2	63:0	Address	PA of the target Data
ipa	X3	63:0	Address	IPA at which the Granule will be mapped in the target Realm

##### B3.3.2.1.2 Context

The RMI\_DATA\_CREATE\_UNKNOWN command operates on the following context.

Name	Type	Value	Before	Description
walk	RmmRttWalkResult	RttWalk( rd, ipa, RMM_RTT_PAGE_LEVEL)	false	RTT walk result
entry_idx	UInt64	RttEntryIndex( ipa, walk.level)	false	RTTE index

##### B3.3.2.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	RmiCommandReturnCode	Command return status

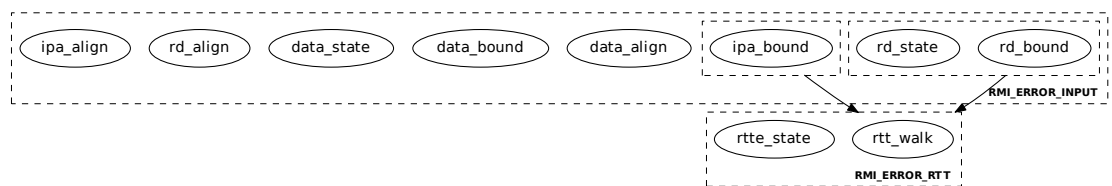
#### B3.3.2.2 Failure conditions

ID	Condition
data_align	pre: !AddrIsGranuleAligned(data) post: ResultEqual(result, RMI_ERROR_INPUT)

ID	Condition
data_bound	pre: <code>!PaIsDelegable(data)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
data_state	pre: <code>Granule(data).state != DELEGATED</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rd_align	pre: <code>!AddrIsGranuleAligned(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rd_bound	pre: <code>!PaIsDelegable(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rd_state	pre: <code>Granule(rd).state != RD</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
ipa_align	pre: <code>!AddrIsGranuleAligned(ipa)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
ipa_bound	pre: <code>!AddrIsProtected(ipa, Realm(rd))</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rtt_walk	pre: <code>walk.level &lt; RMM_RTT_PAGE_LEVEL</code> post: <code>ResultEqual(result, RMI_ERROR_RTT, walk.level)</code>
rtte_state	pre: <code>walk.rtte.state != UNASSIGNED</code> post: <code>ResultEqual(result, RMI_ERROR_RTT, walk.level)</code>

#### B3.3.2.2.1 Failure condition ordering

```
[rd_bound, rd_state] < [rtt_walk, rtte_state]
[ipa_bound] < [rtt_walk, rtte_state]
```



#### B3.3.2.3 Success conditions

ID	Condition
data_state	<code>Granule(data).state == DATA</code>
data_content	Contents of target Granule are wiped.
rtte_state	<code>walk.rtte.state == ASSIGNED</code>
rtte_addr	<code>walk.rtte.addr == data</code>

#### B3.3.2.4 Footprint

ID	Value
data_state	<code>Granule(data).state</code>
rtte	<code>RttEntry(walk.rtt_addr, entry_idx)</code>

### B3.3.3 RMI\_DATA\_DESTROY command

Destroys a Data Granule.

See also:

- [Chapter A5 Realm memory management](#)
- [B3.3.1 RMI\\_DATA\\_CREATE command](#)
- [B3.3.2 RMI\\_DATA\\_CREATE\\_UNKNOWN command](#)
- [D1.2.5 Realm destruction flow](#)

#### B3.3.3.1 Interface

##### B3.3.3.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000155
rd	X1	63:0	Address	PA of the RD which owns the target Data
ipa	X2	63:0	Address	IPA at which the Granule is mapped in the target Realm

##### B3.3.3.1.2 Context

The RMI\_DATA\_DESTROY command operates on the following context.

Name	Type	Value	Before	Description
walk	RmmRttWalkResult	RttWalk( rd, ipa, RMM_RTT_PAGE_LEVEL)	false	RTT walk result
entry_idx	UInt64	RttEntryIndex( ipa, walk.level)	false	RTTE index
walk_top	Address	RttSkipNonLiveEntries( Rtt(walk.rtt_addr), walk.level, ipa)	false	Top IPA of non-live RTT entries, from entry at which the RTT walk terminated

##### B3.3.3.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	RmiCommandReturnCode	Command return status
data	X1	63:0	Address	PA of the Data Granule which was destroyed

Name	Register	Bits	Type	Description
top	X2	63:0	Address	Top IPA of non-live RTT entries, from entry at which the RTT walk terminated

The `data` output value is valid only when the command result is `RMI_SUCCESS`.

The values of the `result` and `top` output values for different command outcomes are summarized in the following table.

Scenario	result	top	walk.rtte.state
ipa is mapped as a page	<code>RMI_SUCCESS</code>	<code>&gt; ipa</code>	Before execution: <code>ASSIGNED</code> After execution: <code>UNASSIGNED</code> and <code>RIPAS</code> is <code>DESTROYED</code>
ipa is not mapped	<code>(RMI_ERROR_RTT, &lt;= 3)</code>	<code>&gt; ipa</code>	<code>UNASSIGNED</code>
ipa is mapped as a block	<code>(RMI_ERROR_RTT, 2)</code>	<code>== ipa</code>	<code>ASSIGNED</code>
RTT walk was not performed, due to any other command failure	Another error code	<code>0</code>	Unknown

See also:

- [A5.5.8 RTTE liveness and RTT liveness](#)

### B3.3.3.2 Failure conditions

ID	Condition
rd_align	pre: <code>!AddrIsGranuleAligned(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rd_bound	pre: <code>!PaIsDelegable(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rd_state	pre: <code>Granule(rd).state != RD</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
ipa_align	pre: <code>!AddrIsGranuleAligned(ipa)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
ipa_bound	pre: <code>!AddrIsProtected(ipa, Realm(rd))</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rtt_walk	pre: <code>walk.level &lt; RMM_RTT_PAGE_LEVEL</code> post: <code>(ResultEqual(result, RMI_ERROR_RTT, walk.level) &amp;&amp; (top == walk_top))</code>
rtte_state	pre: <code>walk.rtte.state != ASSIGNED</code> post: <code>(ResultEqual(result, RMI_ERROR_RTT, walk.level) &amp;&amp; (top == walk_top))</code>

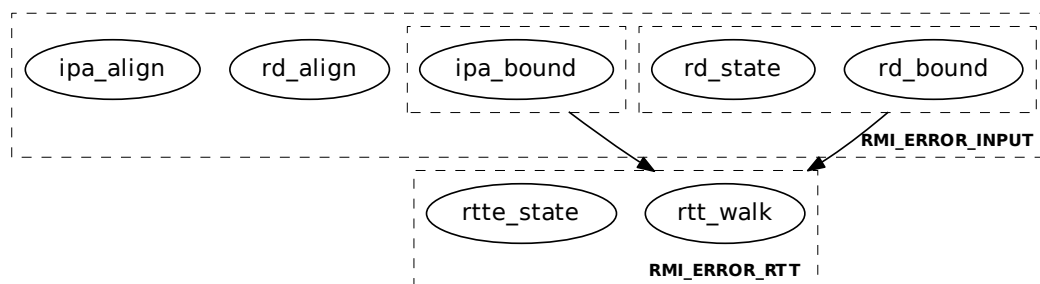


### B3.3.3.2.1 Failure condition ordering

---

```
[rd_bound, rd_state] < [rtt_walk, rtte_state]
[ipa_bound] < [rtt_walk, rtte_state]
```

---



### B3.3.3.3 Success conditions

ID	Condition
data_state	<code>Granule(walk.rtte.addr).state == DELEGATED</code>
rtte_state	<code>walk.rtte.state == UNASSIGNED</code>
ripas_ram	pre: <code>walk.rtte.ripas == RAM</code> post: <code>walk.rtte.ripas == DESTROYED</code>
data	<code>data == walk.rtte.addr</code>
top	<code>top == walk_top</code>

### B3.3.3.4 Footprint

ID	Value
data_state	<code>Granule(walk.rtte.addr).state</code>
rtte	<code>RttEntry(walk.rtt_addr, entry_idx)</code>

### B3.3.4 RMI\_FEATURES command

Read feature register.

The following table indicates which feature register is returned depending on the index provided.

Index	Feature register
0	<a href="#">Feature register 0</a>

See also:

- [A3.1 Realm feature discovery and selection](#)

#### B3.3.4.1 Interface

##### B3.3.4.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000165
index	X1	63:0	<a href="#">UInt64</a>	Feature register index

##### B3.3.4.1.2 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status
value	X1	63:0	<a href="#">Bits64</a>	Feature register value

#### B3.3.4.2 Failure conditions

The RMI\_FEATURES command does not have any failure conditions.

#### B3.3.4.3 Success conditions

ID	Condition
index	pre: index != 0 post: value == Zeros()

#### B3.3.4.4 Footprint

The RMI\_FEATURES command does not have any footprint.

### B3.3.5 RMI\_GRANULE\_DELEGATE command

Delegates a Granule.

See also:

- [A2.2 Granule](#)
- [B3.3.6 RMI\\_GRANULE\\_UNDELEGATE command](#)
- [D1.2.1 Realm creation flow](#)

#### B3.3.5.1 Interface

##### B3.3.5.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000151
addr	X1	63:0	<a href="#">Address</a>	PA of the target Granule

##### B3.3.5.1.2 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status

#### B3.3.5.2 Failure conditions

ID	Condition
gran_align	pre: <a href="#">!AddrIsGranuleAligned</a> (addr) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
gran_bound	pre: <a href="#">!PaIsDelegable</a> (addr) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
gran_state	pre: <a href="#">Granule</a> (addr).state != <a href="#">UNDELEGATED</a> post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
gran_pas	pre: <a href="#">Granule</a> (addr).pas != <a href="#">NS</a> post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )

##### B3.3.5.2.1 Failure condition ordering

The RMI\_GRANULE\_DELEGATE command does not have any failure condition orderings.

#### B3.3.5.3 Success conditions

ID	Condition
gran_state	<code>Granule(addr).state == DELEGATED</code>
gran_pas	<code>Granule(addr).pas == REALM</code>

#### B3.3.5.4 Footprint

ID	Value
gran_pas	<code>Granule(addr).pas</code>
gran_state	<code>Granule(addr).state</code>

### B3.3.6 RMI\_GRANULE\_UNDELEGATE command

Undelegates a Granule.

See also:

- [A2.2 Granule](#)
- [B3.3.5 RMI\\_GRANULE\\_DELEGATE command](#)
- [D1.2.5 Realm destruction flow](#)

#### B3.3.6.1 Interface

##### B3.3.6.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000152
addr	X1	63:0	<a href="#">Address</a>	PA of the target Granule

##### B3.3.6.1.2 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status

#### B3.3.6.2 Failure conditions

ID	Condition
gran_align	pre: <a href="#">!AddrIsGranuleAligned</a> (addr) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
gran_bound	pre: <a href="#">!PaIsDelegable</a> (addr) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
gran_state	pre: <a href="#">Granule</a> (addr).state != <a href="#">DELEGATED</a> post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )

##### B3.3.6.2.1 Failure condition ordering

The RMI\_GRANULE\_UNDELEGATE command does not have any failure condition orderings.

#### B3.3.6.3 Success conditions

ID	Condition
gran_pas	<a href="#">Granule</a> (addr).pas == <a href="#">NS</a>

ID	Condition
gran_state	<code>Granule(addr).state == UNDELEGATED</code>
gran_content	Contents of target Granule are wiped.

See also:

- [A2.2.4 Granule wiping](#)

#### B3.3.6.4 Footprint

ID	Value
gran_pas	<code>Granule(addr).pas</code>
gran_state	<code>Granule(addr).state</code>

### B3.3.7 RMI\_PSCI\_COMPLETE command

Completes a pending PSCI command which was called with an MPIDR argument, by providing the corresponding REC.

See also:

- [A4.3.7 REC exit due to PSCI](#)
- [B5.3.1 PSCI\\_AFFINITY\\_INFO command](#)
- [B5.3.3 PSCI\\_CPU\\_ON command](#)
- [D1.4 PSCI flows](#)

#### B3.3.7.1 Interface

##### B3.3.7.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000164
calling_rec	X1	63:0	<a href="#">Address</a>	PA of the calling REC
target_rec	X2	63:0	<a href="#">Address</a>	PA of the target REC
status	X3	31:0	<a href="#">PsciReturnCode</a>	Status of the PSCI request

The following unused bits of RMI\_PSCI\_COMPLETE input values should be zero: X3[63:32].

##### B3.3.7.1.2 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status

#### B3.3.7.2 Failure conditions

ID	Condition
alias	pre: <code>calling_rec == target_rec</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
calling_align	pre: <code>!AddrIsGranuleAligned(calling_rec)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
calling_bound	pre: <code>!PaIsDelegable(calling_rec)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
calling_state	pre: <code>Granule(calling_rec).state != REC</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
target_align	pre: <code>!AddrIsGranuleAligned(target_rec)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>

ID	Condition
target_bound	pre: <code>!PaIsDelegable(target_rec)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
target_state	pre: <code>Granule(target_rec).state != REC</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
pending	pre: <code>Rec(calling_rec).psci_pending != PSCI_REQUEST_PENDING</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
owner	pre: <code>Rec(target_rec).owner != Rec(calling_rec).owner</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
target	pre: <code>Rec(target_rec).mpidr != Rec(calling_rec).gpr[1]</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
status	pre: <code>!PsciReturnCodePermitted(Rec(calling_rec), Rec(target_rec), status)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>

#### B3.3.7.2.1 Failure condition ordering

The RMI\_PSCI\_COMPLETE command does not have any failure condition orderings.

#### B3.3.7.3 Success conditions

ID	Condition
pending	<code>Rec(calling_rec).psci_pending == NO_PSCI_REQUEST_PENDING</code>
on_already	pre: <code>(status == PSCI_SUCCESS</code> <code>&amp;&amp; Rec(calling_rec).gpr[0] == FID_PSCI_CPU_ON</code> <code>&amp;&amp; Rec(target_rec).flags.runnable == RUNNABLE)</code> post: <code>(Rec(calling_rec).gpr[0] ==</code> <code>PsciReturnCodeEncode(PSCI_ALREADY_ON))</code>



ID	Condition
on_success	<pre> pre: (status == PSCI_SUCCESS       &amp;&amp; Rec(calling_rec).gprs[0] == FID_PSCI_CPU_ON       &amp;&amp; Rec(target_rec).flags.runnable != RUNNABLE) post: (Rec(target_rec).gprs[0] == Rec(calling_rec).gprs[3]       &amp;&amp; Rec(target_rec).gprs[1] == Zeros()       &amp;&amp; Rec(target_rec).gprs[2] == Zeros()       &amp;&amp; Rec(target_rec).gprs[3] == Zeros()       &amp;&amp; Rec(target_rec).gprs[4] == Zeros()       &amp;&amp; Rec(target_rec).gprs[5] == Zeros()       &amp;&amp; Rec(target_rec).gprs[6] == Zeros()       &amp;&amp; Rec(target_rec).gprs[7] == Zeros()       &amp;&amp; Rec(target_rec).gprs[8] == Zeros()       &amp;&amp; Rec(target_rec).gprs[9] == Zeros()       &amp;&amp; Rec(target_rec).gprs[10] == Zeros()       &amp;&amp; Rec(target_rec).gprs[11] == Zeros()       &amp;&amp; Rec(target_rec).gprs[12] == Zeros()       &amp;&amp; Rec(target_rec).gprs[13] == Zeros()       &amp;&amp; Rec(target_rec).gprs[14] == Zeros()       &amp;&amp; Rec(target_rec).gprs[15] == Zeros()       &amp;&amp; Rec(target_rec).gprs[16] == Zeros()       &amp;&amp; Rec(target_rec).gprs[17] == Zeros()       &amp;&amp; Rec(target_rec).gprs[18] == Zeros()       &amp;&amp; Rec(target_rec).gprs[19] == Zeros()       &amp;&amp; Rec(target_rec).gprs[20] == Zeros()       &amp;&amp; Rec(target_rec).gprs[21] == Zeros()       &amp;&amp; Rec(target_rec).gprs[22] == Zeros()       &amp;&amp; Rec(target_rec).gprs[23] == Zeros()       &amp;&amp; Rec(target_rec).gprs[24] == Zeros()       &amp;&amp; Rec(target_rec).gprs[25] == Zeros()       &amp;&amp; Rec(target_rec).gprs[26] == Zeros()       &amp;&amp; Rec(target_rec).gprs[27] == Zeros()       &amp;&amp; Rec(target_rec).gprs[28] == Zeros()       &amp;&amp; Rec(target_rec).gprs[29] == Zeros()       &amp;&amp; Rec(target_rec).gprs[30] == Zeros()       &amp;&amp; Rec(target_rec).gprs[31] == Zeros()       &amp;&amp; Rec(target_rec).pc == Rec(calling_rec).gprs[2]       &amp;&amp; Rec(target_rec).flags.runnable == RUNNABLE       &amp;&amp; Rec(calling_rec).gprs[0] ==           PsciReturnCodeEncode(PSCI_SUCCESS)) </pre>
affinity_on	<pre> pre: (status == PSCI_SUCCESS       &amp;&amp; Rec(calling_rec).gprs[0] == FID_PSCI_AFFINITY_INFO       &amp;&amp; Rec(target_rec).flags.runnable == RUNNABLE) post: (Rec(calling_rec).gprs[0] ==       PsciReturnCodeEncode(PSCI_SUCCESS)) </pre>
affinity_off	<pre> pre: (status == PSCI_SUCCESS       &amp;&amp; Rec(calling_rec).gprs[0] == FID_PSCI_AFFINITY_INFO       &amp;&amp; Rec(target_rec).flags.runnable != RUNNABLE) post: (Rec(calling_rec).gprs[0] ==       PsciReturnCodeEncode(PSCI_OFF)) </pre>
status	<pre> pre: status != PSCI_SUCCESS post: (Rec(calling_rec).gprs[0] ==       PsciReturnCodeEncode(status)) </pre>

ID	Condition
args	<code>(Rec(calling_rec).gprs[1] == Zeros())</code> <code>&amp;&amp; Rec(calling_rec).gprs[2] == Zeros()</code> <code>&amp;&amp; Rec(calling_rec).gprs[3] == Zeros())</code>

#### B3.3.7.4 Footprint

ID	Value
target_flags	<code>Rec(target_rec).flags</code>
target_gprs	<code>Rec(target_rec).gprs</code>
target_pc	<code>Rec(target_rec).pc</code>
calling_pend	<code>Rec(calling_rec).psci_pending</code>
calling_gprs	<code>Rec(calling_rec).gprs</code>

### B3.3.8 RMI\_REALM\_ACTIVATE command

Activates a Realm.

See also:

- [A2.1 Realm](#)

#### B3.3.8.1 Interface

##### B3.3.8.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000157
rd	X1	63:0	<a href="#">Address</a>	PA of the RD

##### B3.3.8.1.2 Output values

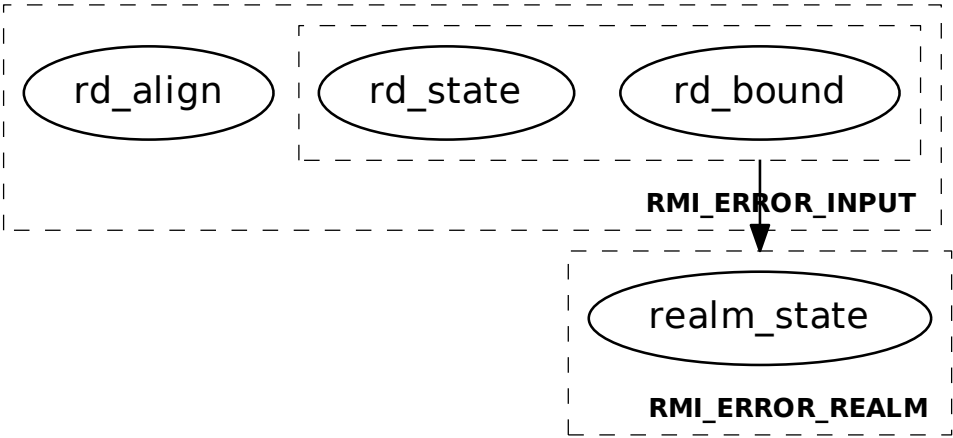
Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status

#### B3.3.8.2 Failure conditions

ID	Condition
rd_align	pre: <a href="#">!AddrIsGranuleAligned</a> (rd) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
rd_bound	pre: <a href="#">!PaIsDelegable</a> (rd) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
rd_state	pre: <a href="#">Granule</a> (rd).state != <a href="#">RD</a> post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
realm_state	pre: <a href="#">Realm</a> (rd).state != <a href="#">NEW</a> post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_REALM</a> )

##### B3.3.8.2.1 Failure condition ordering

```
[rd_bound, rd_state] < [realm_state]
```



**B3.3.8.3 Success conditions**

ID	Condition
realm_state	<code>Realm(rd).state == ACTIVE</code>

**B3.3.8.4 Footprint**

ID	Value
realm_state	<code>Realm(rd).state</code>

### B3.3.9 RMI\_REALM\_CREATE command

Creates a Realm.

See also:

- [A2.1 Realm](#)
- [A2.1.6 Realm parameters](#)
- [B3.3.10 RMI\\_REALM\\_DESTROY command](#)
- [D1.2.1 Realm creation flow](#)

#### B3.3.9.1 Interface

##### B3.3.9.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000158
rd	X1	63:0	<a href="#">Address</a>	PA of the RD
params_ptr	X2	63:0	<a href="#">Address</a>	PA of Realm parameters

##### B3.3.9.1.2 Context

The RMI\_REALM\_CREATE command operates on the following context.

Name	Type	Value	Before	Description
params	<a href="#">RmiRealmParams</a>	<a href="#">RealmParams</a> (params_ptr)	false	Realm parameters

##### B3.3.9.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status

#### B3.3.9.2 Failure conditions

ID	Condition
params_align	pre: <a href="#">!AddrIsGranuleAligned</a> (params_ptr) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
params_bound	pre: <a href="#">!PaIsDelegable</a> (params_ptr) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
params_pas	pre: <a href="#">Granule</a> (params_ptr).pas != NS post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )

ID	Condition
params_valid	pre: <code>!RmiRealmParamsIsValid(params_ptr)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
params_supp	pre: <code>!RealmParamsSupported(params)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
alias	pre: <code>AddrInRange(rd, params.rtt_base, (params.rtt_num_start - 1) * RMM_GRANULE_SIZE)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rd_align	pre: <code>!AddrIsGranuleAligned(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rd_bound	pre: <code>!PaIsDelegable(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rd_state	pre: <code>Granule(rd).state != DELEGATED</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rtt_align	pre: <code>!AddrIsAligned(params.rtt_base, params.rtt_num_start * RMM_GRANULE_SIZE)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rtt_num_level	pre: <code>!RttConfigIsValid(params.s2sz, params.rtt_level_start, params.rtt_num_start)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rtt_state	pre: <code>!RttsStateEqual(params.rtt_base, params.rtt_num_start, DELEGATED)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
vmid_valid	pre: <code>!VmidIsValid(params.vmid)    !VmidIsFree(params.vmid)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>

#### B3.3.9.2.1 Failure condition ordering

The RMI\_REALM\_CREATE command does not have any failure condition orderings.

#### B3.3.9.3 Success conditions

ID	Condition
rd_state	<code>Granule(rd).state == RD</code>
realm_state	<code>Realm(rd).state == NEW</code>
rec_index	<code>Realm(rd).rec_index == 0</code>
rtt_base	<code>Realm(rd).rtt_base == params.rtt_base</code>
rtt_state	<code>RttsStateEqual(Realm(rd).rtt_base, Realm(rd).rtt_num_start, RTT)</code>
rtte_p_states	<code>RttsAllProtectedEntriesState(Realm(rd).rtt_base, Realm(rd).rtt_num_start, UNASSIGNED)</code>

ID	Condition
rtte_up_states	<code>RttsAllUnprotectedEntriesState(Realm(rd).rtt_base, Realm(rd).rtt_num_start, UNASSIGNED_NS)</code>
rtte_ripas	<code>RttsAllProtectedEntriesRipas(Realm(rd).rtt_base, Realm(rd).rtt_num_start, EMPTY)</code>
ipa_width	<code>Realm(rd).ipa_width == params.s2sz</code>
hash_algo	<code>Equal(Realm(rd).hash_algo, params.hash_algo)</code>
rim	<code>Realm(rd).measurements[0] == RimInit(Realm(rd).hash_algo, params)</code>
rem	<code>(Realm(rd).measurements[1] == Zeros() &amp;&amp; Realm(rd).measurements[2] == Zeros() &amp;&amp; Realm(rd).measurements[3] == Zeros() &amp;&amp; Realm(rd).measurements[4] == Zeros())</code>
rtt_level	<code>Realm(rd).rtt_level_start == params.rtt_level_start</code>
rtt_num	<code>Realm(rd).rtt_num_start == params.rtt_num_start</code>
vmid	<code>Realm(rd).vmid == params.vmid</code>
rpv	<code>Realm(rd).rpv == params.rpv</code>

#### B3.3.9.4 RMI\_REALM\_CREATE initialization of RIM

On successful execution of RMI\_REALM\_CREATE, the initial RIM value of the target Realm is calculated by the RMM as follows:

1. Allocate a zero-filled [RmiRealmParams](#) data structure to hold the measured Realm parameters.
2. Copy the following attributes from the Host-provided [RmiRealmParams](#) data structure into the measured Realm parameters data structure:
  - flags
  - s2sz
  - sve\_vl
  - num\_bps
  - num\_wps
  - pmu\_num\_ctrs
  - hash\_algo
3. Using the RHA of the target Realm, compute the hash of the measured Realm parameters data structure. Set the RIM of the target Realm to this value, zero filling upper bytes if the RHA output is smaller than the size of the RIM.

See also:

- [A7.1.1 Realm Initial Measurement](#)
- [B2.46 RimInit function](#)
- [B3.4.12 RmiRealmParams type](#)

### **B3.3.9.5 Footprint**



ID	Value
rd_state	<code>Granule(rd).state</code>
rtt_state	<code>RttsGranuleState( Realm(rd).rtt_base, Realm(rd).rtt_num_start)</code>

### B3.3.10 RMI\_REALM\_DESTROY command

Destroys a Realm.

See also:

- [A2.1 Realm](#)
- [B3.3.9 RMI\\_REALM\\_CREATE command](#)
- [D1.2.5 Realm destruction flow](#)

#### B3.3.10.1 Interface

##### B3.3.10.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000159
rd	X1	63:0	<a href="#">Address</a>	PA of the RD

##### B3.3.10.1.2 Context

The RMI\_REALM\_DESTROY command operates on the following context.

Name	Type	Value	Before	Description
realm	<a href="#">RmmRealm</a>	<a href="#">Realm</a> (rd)	true	Realm

##### B3.3.10.1.3 Output values

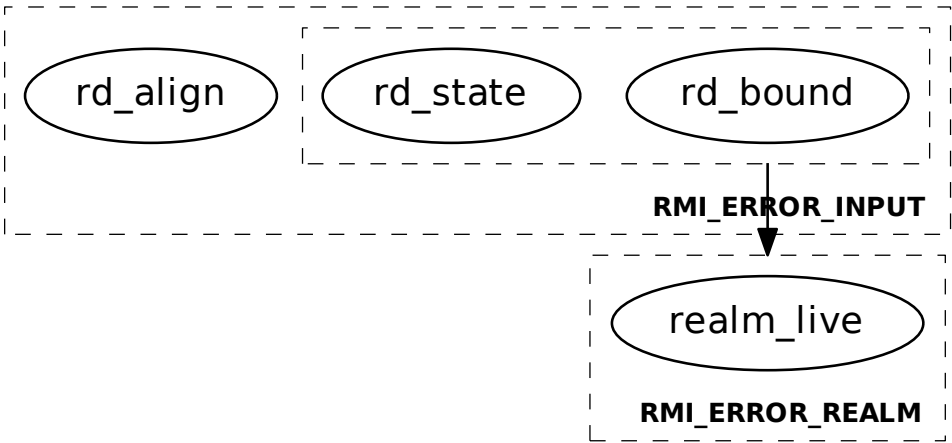
Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status

#### B3.3.10.2 Failure conditions

ID	Condition
rd_align	pre: <a href="#">!AddrIsGranuleAligned</a> (rd) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
rd_bound	pre: <a href="#">!PaIsDelegable</a> (rd) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
rd_state	pre: <a href="#">Granule</a> (rd).state != RD post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
realm_live	pre: <a href="#">RealmIsLive</a> (rd) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_REALM</a> )

**B3.3.10.2.1 Failure condition ordering**

[rd\_bound, rd\_state] < [realm\_live]



**B3.3.10.3 Success conditions**

ID	Condition
rtt_state	<code>RttsStateEqual( realm.rtt_base, realm.rtt_num_start, DELEGATED)</code>
rd_state	<code>Granule(rd).state == DELEGATED</code>
vmid	<code>VmidIsFree(realm.vmid)</code>

**B3.3.10.4 Footprint**

ID	Value
rd_state	<code>Granule(rd).state</code>
rtt_state	<code>RttsGranuleState( realm.rtt_base, realm.rtt_num_start)</code>

### B3.3.11 RMI\_REC\_AUX\_COUNT command

Get number of auxiliary Granules required for a REC.

See also:

- [A2.3 Realm Execution Context](#)
- [B3.3.12 RMI\\_REC\\_CREATE command](#)
- [B3.4.19 RmiRecParams type](#)
- [D1.2.4 REC creation flow](#)

#### B3.3.11.1 Interface

##### B3.3.11.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000167
rd	X1	63:0	<a href="#">Address</a>	PA of the RD for the target Realm

##### B3.3.11.1.2 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status
aux_count	X1	63:0	<a href="#">UInt64</a>	Number of auxiliary Granules required for a REC

#### B3.3.11.2 Failure conditions

ID	Condition
rd_align	pre: <a href="#">!AddrIsGranuleAligned</a> (rd) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
rd_bound	pre: <a href="#">!PaIsDelegable</a> (rd) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
rd_state	pre: <a href="#">Granule</a> (rd).state != <a href="#">RD</a> post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )

##### B3.3.11.2.1 Failure condition ordering

The RMI\_REC\_AUX\_COUNT command does not have any failure condition orderings.

#### B3.3.11.3 Success conditions

ID	Condition
aux_count	aux_count == <a href="#">RecAuxCount</a> (rd)

#### B3.3.11.4 Footprint

The RMI\_REC\_AUX\_COUNT command does not have any footprint.

### B3.3.12 RMI\_REC\_CREATE command

Creates a REC.

See also:

- [A2.3 Realm Execution Context](#)
- [A2.3.3 REC index and MPIDR value](#)
- [B3.3.11 RMI\\_REC\\_AUX\\_COUNT command](#)
- [B3.3.13 RMI\\_REC\\_DESTROY command](#)
- [D1.2.4 REC creation flow](#)

#### B3.3.12.1 Interface

##### B3.3.12.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC400015A
rd	X1	63:0	Address	PA of the RD for the target Realm
rec	X2	63:0	Address	PA of the target REC
params_ptr	X3	63:0	Address	PA of REC parameters

##### B3.3.12.1.2 Context

The RMI\_REC\_CREATE command operates on the following context.

Name	Type	Value	Before	Description
realm	RmmRealm	Realm(rd)	true	Realm
params	RmiRecParams	RecParams(params_ptr)	false	REC parameters
rec_index	UInt64	Realm(rd).rec_index	true	REC index

##### B3.3.12.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	RmiCommandReturnCode	Command return status

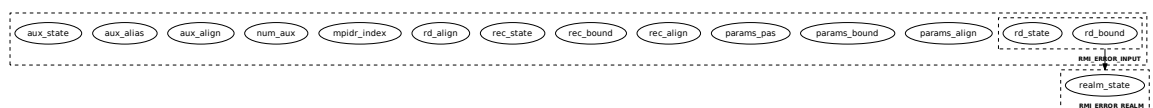
#### B3.3.12.2 Failure conditions

ID	Condition
params_align	pre: !AddrIsGranuleAligned(params_ptr) post: ResultEqual(result, RMI_ERROR_INPUT)

ID	Condition
params_bound	pre: !PaIsDelegable(params_ptr) post: ResultEqual(result, RMI_ERROR_INPUT)
params_pas	pre: Granule(params_ptr).pas != NS post: ResultEqual(result, RMI_ERROR_INPUT)
rec_align	pre: !AddrIsGranuleAligned(rec) post: ResultEqual(result, RMI_ERROR_INPUT)
rec_bound	pre: !PaIsDelegable(rec) post: ResultEqual(result, RMI_ERROR_INPUT)
rec_state	pre: Granule(rec).state != DELEGATED post: ResultEqual(result, RMI_ERROR_INPUT)
rd_align	pre: !AddrIsGranuleAligned(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_bound	pre: !PaIsDelegable(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_state	pre: Granule(rd).state != RD post: ResultEqual(result, RMI_ERROR_INPUT)
realm_state	pre: realm.state != NEW post: ResultEqual(result, RMI_ERROR_REALM)
mpidr_index	pre: RecIndex(params.mpidr) != realm.rec_index post: ResultEqual(result, RMI_ERROR_INPUT)
num_aux	pre: params.num_aux != RecAuxCount(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
aux_align	pre: !RecAuxAligned(params.aux, params.num_aux) post: ResultEqual(result, RMI_ERROR_INPUT)
aux_alias	pre: RecAuxAlias(rec, params.aux, params.num_aux) post: ResultEqual(result, RMI_ERROR_INPUT)
aux_state	pre: !RecAuxStateEqual( params.aux, params.num_aux, DELEGATED) post: ResultEqual(result, RMI_ERROR_INPUT)

#### B3.3.12.2.1 Failure condition ordering

[rd\_bound, rd\_state] < [realm\_state]



#### B3.3.12.3 Success conditions

ID	Condition
rec_index	<code>Realm(rd).rec_index == rec_index + 1</code>
rec_gran_state	<code>Granule(rec).state == REC</code>
rec_owner	<code>Rec(rec).owner == rd</code>
rec_attest	<code>Rec(rec).attest_state == NO_ATTEST_IN_PROGRESS</code>
rec_mpidr	<code>MpidrEqual(Rec(rec).mpidr, params.mpidr)</code>
rec_state	<code>Rec(rec).state == READY</code>
runnable	pre: <code>params.flags.runnable == RMI_RUNNABLE</code> post: <code>Rec(rec).flags.runnable == RUNNABLE</code>
not_runnable	pre: <code>params.flags.runnable == RMI_NOT_RUNNABLE</code> post: <code>Rec(rec).flags.runnable == NOT_RUNNABLE</code>
rec_gprs	<code>(Rec(rec).gprs[0] == params.gprs[0]</code> <code>&amp;&amp; Rec(rec).gprs[1] == params.gprs[1]</code> <code>&amp;&amp; Rec(rec).gprs[2] == params.gprs[2]</code> <code>&amp;&amp; Rec(rec).gprs[3] == params.gprs[3]</code> <code>&amp;&amp; Rec(rec).gprs[4] == params.gprs[4]</code> <code>&amp;&amp; Rec(rec).gprs[5] == params.gprs[5]</code> <code>&amp;&amp; Rec(rec).gprs[6] == params.gprs[6]</code> <code>&amp;&amp; Rec(rec).gprs[7] == params.gprs[7]</code> <code>&amp;&amp; Rec(rec).gprs[8] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[9] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[10] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[11] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[12] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[13] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[14] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[15] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[16] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[17] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[18] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[19] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[20] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[21] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[22] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[23] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[24] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[25] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[26] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[27] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[28] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[29] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[30] == Zeros()</code> <code>&amp;&amp; Rec(rec).gprs[31] == Zeros())</code>
rec_pc	<code>Rec(rec).pc == params.pc</code>
rim	pre: <code>params.flags.runnable == RMI_RUNNABLE</code> post: <code>Realm(rd).measurements[0] == RimExtendRec(</code> <code>realm, params)</code>



ID	Condition
rec_aux	<code>RecAuxEqual (</code> <code>Rec(rec).aux, params.aux,</code> <code>RecAuxCount (rd) )</code>
rec_aux_state	<code>RecAuxStateEqual (</code> <code>Rec(rec).aux, RecAuxCount (rd), REC_AUX)</code>
ripas_addr	<code>Rec(rec).ripas_addr == Zeros()</code>
ripas_top	<code>Rec(rec).ripas_top == Zeros()</code>
host_call	<code>Rec(rec).host_call_pending == NO_HOST_CALL_PENDING</code>

#### B3.3.12.4 RMI\_REC\_CREATE extension of RIM

On successful execution of RMI\_REC\_CREATE, if the new REC is runnable then the new RIM value of the target Realm is calculated by the RMM as follows:

1. Allocate a zero-filled [RmiRecParams](#) data structure to hold the measured REC parameters.
2. Copy the following attributes from the Host-provided [RmiRecParams](#) data structure into the measured REC parameters data structure:
  - gprs
  - pc
  - flags
3. Using the RHA of the target Realm, compute the hash of the measured REC parameters data structure.
4. Allocate an [RmmMeasurementDescriptorRec](#) data structure.
5. Populate the measurement descriptor:
  - Set the desc\_type field to the descriptor type.
  - Set the len field to the descriptor length.
  - Set the rim field to the current RIM value of the target Realm.
  - Set the content field to the hash of the measured REC parameters.
6. Using the RHA of the target Realm, compute the hash of the measurement descriptor. Set the RIM of the target Realm to this value, zero filling upper bytes if the RHA output is smaller than the size of the RIM.

See also:

- [A7.1.1 Realm Initial Measurement](#)
- [B2.43 RimExtendRec function](#)
- [B3.4.19 RmiRecParams type](#)
- [C1.6 RmmMeasurementDescriptorRec type](#)

#### B3.3.12.5 Footprint

ID	Value
rec_index	<code>Realm(rd).rec_index</code>
rec_state	<code>Granule(rec).state</code>

ID	Value
rec_aux_state	<code>RecAuxStates (Rec (rec) .aux, RecAuxCount (rd) )</code>
rim	<code>Realm (rd) .measurements [0]</code>

### B3.3.13 RMI\_REC\_DESTROY command

Destroys a REC.

See also:

- [A2.3 Realm Execution Context](#)
- [B3.3.12 RMI\\_REC\\_CREATE command](#)
- [D1.2.5 Realm destruction flow](#)

#### B3.3.13.1 Interface

##### B3.3.13.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC400015B
rec	X1	63:0	<a href="#">Address</a>	PA of the target REC

##### B3.3.13.1.2 Context

The RMI\_REC\_DESTROY command operates on the following context.

Name	Type	Value	Before	Description
rd	<a href="#">Address</a>	<code>Rec(rec).owner</code>	true	RD address
rec_obj	<a href="#">RmmRec</a>	<code>Rec(rec)</code>	true	REC

##### B3.3.13.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status

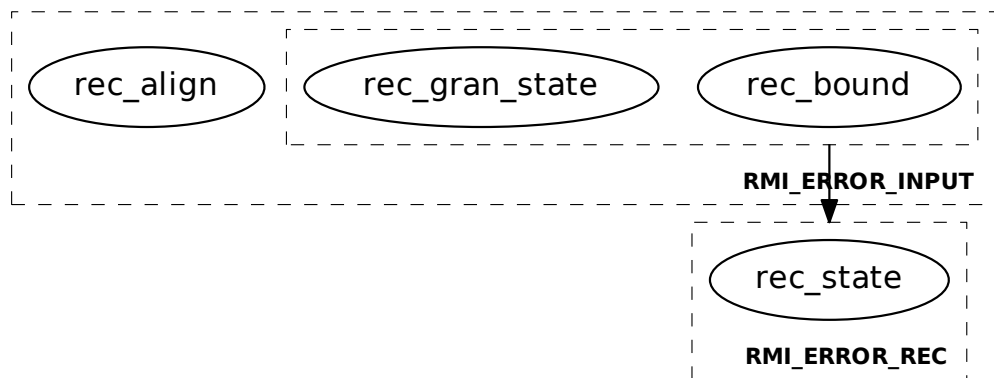
#### B3.3.13.2 Failure conditions

ID	Condition
rec_align	pre: <code>!AddrIsGranuleAligned(rec)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rec_bound	pre: <code>!PaIsDelegable(rec)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rec_gran_state	pre: <code>Granule(rec).state != REC</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>

ID	Condition
rec_state	pre: <code>Rec(rec).state == RUNNING</code> post: <code>ResultEqual(result, RMI_ERROR_REC)</code>

#### B3.3.13.2.1 Failure condition ordering

`[rec_bound, rec_gran_state] < [rec_state]`



#### B3.3.13.3 Success conditions

ID	Condition
rec_gran_state	<code>Granule(rec).state == DELEGATED</code>
rec_aux_state	<code>RecAuxStateEqual(</code> <code>rec_obj.aux, RecAuxCount(rd), DELEGATED)</code>

#### B3.3.13.4 Footprint

ID	Value
rec_state	<code>Granule(rec).state</code>
rec_aux_state	<code>RecAuxStates(rec_obj.aux, RecAuxCount(rd))</code>

### B3.3.14 RMI\_REC\_ENTER command

Enter a REC.

See also:

- [A2.3 Realm Execution Context](#)
- [Chapter A4 Realm exception model](#)
- [D1.3.1 Realm entry and exit flow](#)

#### B3.3.14.1 Interface

##### B3.3.14.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC400015C
rec	X1	63:0	<a href="#">Address</a>	PA of the target REC
run_ptr	X2	63:0	<a href="#">Address</a>	PA of RecRun object

##### B3.3.14.1.2 Context

The RMI\_REC\_ENTER command operates on the following context.

Name	Type	Value	Before	Description
run	<a href="#">RmiRecRun</a>	<a href="#">RecRun</a> (run_ptr)	false	RecRun object

##### B3.3.14.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status

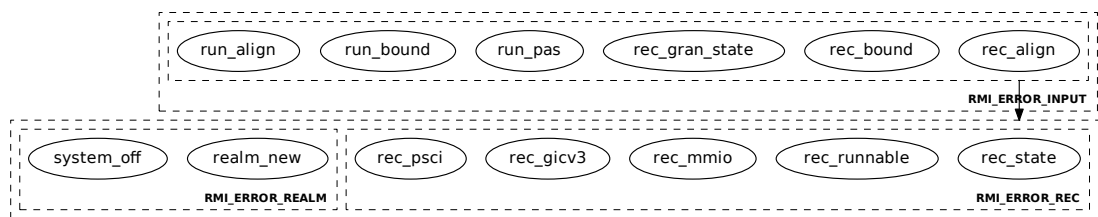
#### B3.3.14.2 Failure conditions

ID	Condition
run_align	pre: <a href="#">!AddrIsGranuleAligned</a> (run_ptr) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
run_bound	pre: <a href="#">!PaIsDelegable</a> (run_ptr) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
run_pas	pre: <a href="#">Granule</a> (run_ptr).pas != NS post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )
rec_align	pre: <a href="#">!AddrIsGranuleAligned</a> (rec) post: <a href="#">ResultEqual</a> (result, <a href="#">RMI_ERROR_INPUT</a> )

ID	Condition
rec_bound	pre: <code>!PaIsDelegable(rec)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
rec_gran_state	pre: <code>Granule(rec).state != REC</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
realm_new	pre: <code>Realm(Rec(rec).owner).state == NEW</code> post: <code>ResultEqual(result, RMI_ERROR_REALM, 0)</code>
system_off	pre: <code>Realm(Rec(rec).owner).state == SYSTEM_OFF</code> post: <code>ResultEqual(result, RMI_ERROR_REALM, 1)</code>
rec_state	pre: <code>Rec(rec).state == RUNNING</code> post: <code>ResultEqual(result, RMI_ERROR_REC)</code>
rec_runnable	pre: <code>Rec(rec).flags.runnable == NOT_RUNNABLE</code> post: <code>ResultEqual(result, RMI_ERROR_REC)</code>
rec_mmio	pre: <code>(run.enter.flags.emul_mmio == RMI_EMULATED_MMIO &amp;&amp; Rec(rec).emulatable_abort != EMULATABLE_ABORT)</code> post: <code>ResultEqual(result, RMI_ERROR_REC)</code>
rec_gicv3	pre: <code>!Gicv3ConfigIsValid( run.enter.gicv3_hcr, run.enter.gicv3_lrs)</code> post: <code>ResultEqual(result, RMI_ERROR_REC)</code>
rec_psci	pre: <code>Rec(rec).psci_pending == PSCI_REQUEST_PENDING</code> post: <code>ResultEqual(result, RMI_ERROR_REC)</code>

#### B3.3.14.2.1 Failure condition ordering

```
[rec_align, rec_bound, rec_gran_state, run_pas, run_bound, run_align] < [rec_state,
↪ rec_runnable, rec_mmio, realm_new, system_off, rec_gicv3, rec_psci]
```



#### B3.3.14.3 Success conditions

ID	Condition
rec_exit	<code>run.exit</code> contains Realm exit syndrome information.
rec_emul_abt	<code>rec.emulatable_abort</code> is updated.

#### B3.3.14.4 Footprint

ID	Value
emul_abt	<a href="#">Rec</a> (rd).emulatable_abort

### B3.3.15 RMI\_RTT\_CREATE command

Creates an RTT.

See also:

- [A5.5 Realm Translation Table](#)
- [A5.5.7 RTT unfolding](#)
- [B3.3.16 RMI\\_RTT\\_DESTROY command](#)
- [B3.3.17 RMI\\_RTT\\_FOLD command](#)

#### B3.3.15.1 Interface

##### B3.3.15.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC400015D
rd	X1	63:0	Address	PA of the RD for the target Realm
rtt	X2	63:0	Address	PA of the target RTT
ipa	X3	63:0	Address	Base of the IPA range described by the RTT
level	X4	63:0	Int64	RTT level

##### B3.3.15.1.2 Context

The RMI\_RTT\_CREATE command operates on the following context.

Name	Type	Value	Before	Description
realm	<a href="#">RmmRealm</a>	<a href="#">Realm</a> (rd)	true	Realm
walk	<a href="#">RmmRttWalkResult</a>	<a href="#">RttWalk</a> ( rd, ipa, level - 1)	false	RTT walk result
entry_idx	UInt64	<a href="#">RttEntryIndex</a> ( ipa, walk.level)	false	RTTE index
unfold	<a href="#">RmmRttEntry</a>	<a href="#">RttWalk</a> ( rd, ipa, level - 1).rtte	true	RTTE before command execution

##### B3.3.15.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status

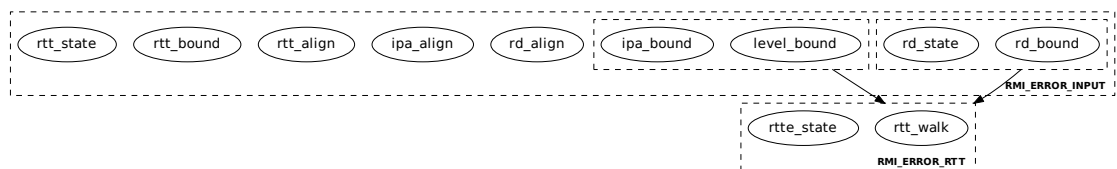


### B3.3.15.2 Failure conditions

ID	Condition
rd_align	pre: !AddrIsGranuleAligned(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_bound	pre: !PaIsDelegable(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_state	pre: Granule(rd).state != RD post: ResultEqual(result, RMI_ERROR_INPUT)
level_bound	pre: (!RttLevelIsValid(rd, level)    RttLevelIsStarting(rd, level)) post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_align	pre: !AddrIsRttLevelAligned(ipa, level - 1) post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_bound	pre: UInt(ipa) >= (2 ^ Realm(rd).ipa_width) post: ResultEqual(result, RMI_ERROR_INPUT)
rtt_align	pre: !AddrIsGranuleAligned(rtt) post: ResultEqual(result, RMI_ERROR_INPUT)
rtt_bound	pre: !PaIsDelegable(rtt) post: ResultEqual(result, RMI_ERROR_INPUT)
rtt_state	pre: Granule(rtt).state != DELEGATED post: ResultEqual(result, RMI_ERROR_INPUT)
rtt_walk	pre: walk.level < level - 1 post: ResultEqual(result, RMI_ERROR_RTT, walk.level)
rtte_state	pre: walk.rtte.state == TABLE post: ResultEqual(result, RMI_ERROR_RTT, walk.level)

#### B3.3.15.2.1 Failure condition ordering

[rd\_bound, rd\_state] < [rtt\_walk, rtte\_state]  
[level\_bound, ipa\_bound] < [rtt\_walk, rtte\_state]



### B3.3.15.3 Success conditions

ID	Condition
rtt_state	<code>Granule(rtt).state == RTT</code>
rtte_state	<code>walk.rtte.state == TABLE</code>
rtte_addr	<code>walk.rtte.addr == rtt</code>
rtte_c_ripas	pre: <code>AddrIsProtected(ipa, realm)</code> post: <code>RttAllEntriesRipas(Rtt(rtt), unfold.ripas)</code>
rtte_c_state	<code>RttAllEntriesState(Rtt(rtt), unfold.state)</code>
rtte_c_addr	pre: <code>(unfold.state != UNASSIGNED</code> <code>&amp;&amp; unfold.state != UNASSIGNED_NS)</code> post: <code>RttAllEntriesContiguous(Rtt(rtt), unfold.addr, level)</code>

#### B3.3.15.4 Footprint

ID	Value
rtt_state	<code>Granule(rtt).state</code>
rtte	<code>RttEntry(walk.rtt_addr, entry_idx)</code>

### B3.3.16 RMI\_RTT\_DESTROY command

Destroys an RTT.

See also:

- [A5.5 Realm Translation Table](#)
- [A5.5.9 RTT destruction](#)
- [B3.3.15 RMI\\_RTT\\_CREATE command](#)
- [B3.3.17 RMI\\_RTT\\_FOLD command](#)

#### B3.3.16.1 Interface

##### B3.3.16.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC400015E
rd	X1	63:0	Address	PA of the RD for the target Realm
ipa	X2	63:0	Address	Base of the IPA range described by the RTT
level	X3	63:0	Int64	RTT level

##### B3.3.16.1.2 Context

The RMI\_RTT\_DESTROY command operates on the following context.

Name	Type	Value	Before	Description
walk	RmmRttWalkResult	RttWalk( rd, ipa, level - 1)	false	RTT walk result
entry_idx	UInt64	RttEntryIndex( ipa, walk.level)	false	RTTE index
walk_top	Address	RttSkipNonLiveEntries( Rtt(walk.rtt_addr), walk.level, ipa)	false	Top IPA of non-live RTT entries, from entry at which the RTT walk terminated

##### B3.3.16.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	RmiCommandReturnCode	Command return status
rtt	X1	63:0	Address	PA of the RTT which was destroyed

Name	Register	Bits	Type	Description
top	X2	63:0	<a href="#">Address</a>	Top IPA of non-live RTT entries, from entry at which the RTT walk terminated

The `rtt` output value is valid only when the command result is `RMI_SUCCESS`.

The values of the `result` and `top` output values for different command outcomes are summarized in the following table.

Scenario	result	top	walk.rtte.state
Target RTT exists and is not live	<code>RMI_SUCCESS</code>	<code>&gt; ipa</code>	Before execution: <code>TABLE</code> After execution: <code>UNASSIGNED</code> and <code>RIPAS</code> is <code>DESTROYED</code>
Missing RTT	<code>(RMI_ERROR_RTT, &lt; level)</code>	<code>&gt; ipa</code>	<code>UNASSIGNED</code> or <code>UNASSIGNED_NS</code>
Block mapping at lower level	<code>(RMI_ERROR_RTT, &lt; level)</code>	<code>== ipa</code>	<code>ASSIGNED</code> or <code>ASSIGNED_NS</code>
Live RTT at target level	<code>(RMI_ERROR_RTT, level)</code>	<code>== ipa</code>	<code>TABLE</code>
RTT walk was not performed, due to any other command failure	Another error code	<code>0</code>	Unknown

See also:

- [A5.5.8 RTTE liveness and RTT liveness](#)

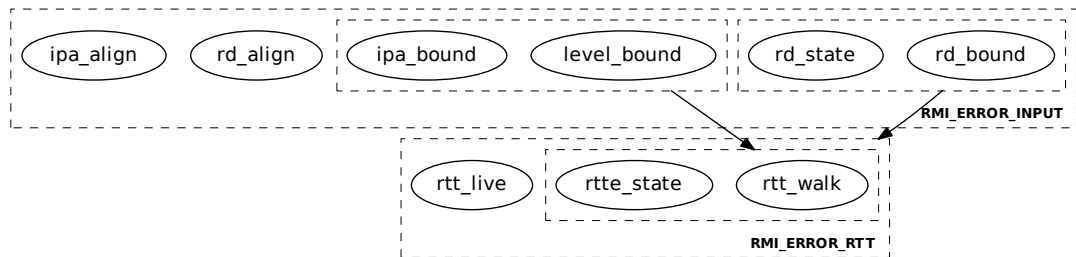
### B3.3.16.2 Failure conditions

ID	Condition
<code>rd_align</code>	pre: <code>!AddrIsGranuleAligned(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>rd_bound</code>	pre: <code>!PaIsDelegable(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>rd_state</code>	pre: <code>Granule(rd).state != RD</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>level_bound</code>	pre: <code>(!RttLevelIsValid(rd, level)    RttLevelIsStarting(rd, level))</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>ipa_align</code>	pre: <code>!AddrIsRttLevelAligned(ipa, level - 1)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>ipa_bound</code>	pre: <code>UInt(ipa) &gt;= (2 ^ Realm(rd).ipa_width)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>

ID	Condition
rtt_walk	pre: walk.level < level - 1 post: (ResultEqual(result, RMI_ERROR_RTT, walk.level) && (top == walk_top))
rtte_state	pre: walk.rtte.state != TABLE post: (ResultEqual(result, RMI_ERROR_RTT, walk.level) && (top == walk_top))
rtt_live	pre: RttIsLive(Rtt(walk.rtte.addr)) post: (ResultEqual(result, RMI_ERROR_RTT, level) && (top == ipa))

#### B3.3.16.2.1 Failure condition ordering

```
[rd_bound, rd_state] < [rtt_walk, rtte_state, rtt_live]
[level_bound, ipa_bound] < [rtt_walk, rtte_state]
```



#### B3.3.16.3 Success conditions

ID	Condition
rtte_state	walk.rtte.state == UNASSIGNED
ripas	walk.rtte.ripas == DESTROYED
rtt_state	Granule(walk.rtte.addr).state == DELEGATED
rtt	rtt == walk.rtte.addr
top	top == walk_top

#### B3.3.16.4 Footprint

ID	Value
rtt_state	Granule(walk.rtte.addr).state

ID	Value
rtte	<code>RttEntry(walk.rtt_addr, entry_idx)</code>

### B3.3.17 RMI\_RTT\_FOLD command

Destroys a homogeneous RTT.

See also:

- [A5.5 Realm Translation Table](#)
- [A5.5.6 RTT folding](#)
- [B3.3.15 RMI\\_RTT\\_CREATE command](#)
- [B3.3.16 RMI\\_RTT\\_DESTROY command](#)

#### B3.3.17.1 Interface

##### B3.3.17.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000166
rd	X1	63:0	Address	PA of the RD for the target Realm
ipa	X2	63:0	Address	Base of the IPA range described by the RTT
level	X3	63:0	Int64	RTT level

##### B3.3.17.1.2 Context

The RMI\_RTT\_FOLD command operates on the following context.

Name	Type	Value	Before	Description
walk	RmmRttWalkResult	RttWalk( rd, ipa, level - 1)	false	RTT walk result
entry_idx	UInt64	RttEntryIndex( ipa, walk.level)	false	RTTE index
fold	RmmRttEntry	RttFold( Rtt(walk.rtte.addr))	true	Result of folding RTT

##### B3.3.17.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	RmiCommandReturnCode	Command return status
rtt	X1	63:0	Address	PA of the RTT which was destroyed

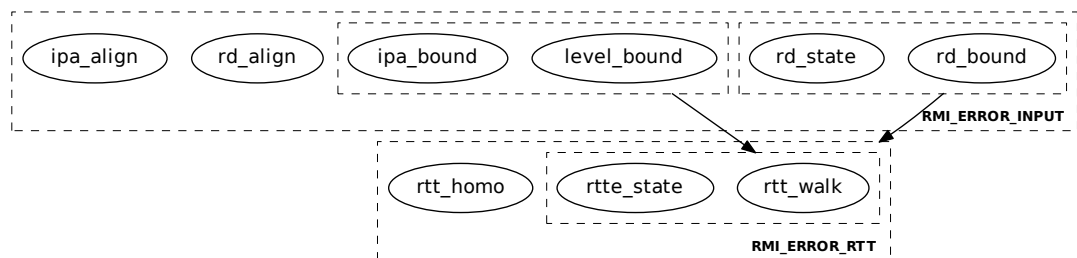
The `rtt` output value is valid only when the command result is RMI\_SUCCESS.

### B3.3.17.2 Failure conditions

ID	Condition
rd_align	pre: !AddrIsGranuleAligned(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_bound	pre: !PaIsDelegable(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_state	pre: Granule(rd).state != RD post: ResultEqual(result, RMI_ERROR_INPUT)
level_bound	pre: (!RttLevelIsValid(rd, level)    RttLevelIsStarting(rd, level)) post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_align	pre: !AddrIsRttLevelAligned(ipa, level - 1) post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_bound	pre: UInt(ipa) >= (2 ^ Realm(rd).ipa_width) post: ResultEqual(result, RMI_ERROR_INPUT)
rtt_walk	pre: walk.level < level - 1 post: ResultEqual(result, RMI_ERROR_RTT, walk.level)
rtte_state	pre: walk.rtte.state != TABLE post: ResultEqual(result, RMI_ERROR_RTT, walk.level)
rtt_homo	pre: !RttIsHomogeneous(Rtt(walk.rtte.addr)) post: ResultEqual(result, RMI_ERROR_RTT, level)

#### B3.3.17.2.1 Failure condition ordering

```
[rd_bound, rd_state] < [rtt_walk, rtte_state, rtt_homo]
[level_bound, ipa_bound] < [rtt_walk, rtte_state]
```



### B3.3.17.3 Success conditions

ID	Condition
rtte_state	walk.rtte.state == fold.state



ID	Condition
rtte_addr	pre: (fold.state != UNASSIGNED && fold.state != UNASSIGNED_NS) post: walk.rtte.addr == fold.addr
rtte_attr	pre: (fold.state == ASSIGNED    fold.state == ASSIGNED_NS) post: (walk.rtte.MemAttr == fold.MemAttr && walk.rtte.S2AP == fold.S2AP && walk.rtte.SH == fold.SH)
rtte_ripas	pre: AddrIsProtected(ipa, Realm(rd)) post: walk.rtte.ripas == fold.ripas
rtt_state	Granule(walk.rtte.addr).state == DELEGATED
rtt	rtt == walk.rtte.addr

#### B3.3.17.4 Footprint

ID	Value
rtt_state	Granule(walk.rtte.addr).state
rtte	RttEntry(walk.rtt_addr, entry_idx)

### B3.3.18 RMI\_RTT\_INIT\_RIPAS command

Set the RIPAS of a target IPA range to RAM, for a Realm in the NEW state.

See also:

- [A5.2.2 Realm IPA state](#)
- [D1.2.3 Initialize memory of New Realm flow](#)

#### B3.3.18.1 Interface

##### B3.3.18.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000168
rd	X1	63:0	<a href="#">Address</a>	PA of the RD for the target Realm
base	X2	63:0	<a href="#">Address</a>	Base of target IPA region
top	X3	63:0	<a href="#">Address</a>	Top of target IPA region

##### B3.3.18.1.2 Context

The RMI\_RTT\_INIT\_RIPAS command operates on the following context.

Name	Type	Value	Before	Description
realm	<a href="#">RmmRealm</a>	<a href="#">Realm</a> (rd)	true	Realm
walk	<a href="#">RmmRttWalkResult</a>	<a href="#">RttWalk</a> (rd, base, RMM_RTT_PAGE_LEVEL)	false	RTT walk result
walk_top	<a href="#">Address</a>	<a href="#">RttSkipEntriesWithRipas</a> ( <a href="#">Rtt</a> (walk.rtt_addr), walk.level, base, top, FALSE)	false	Top IPA of entries which have associated RIPAS values, starting from entry at which the RTT walk terminated

##### B3.3.18.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status
out_top	X1	63:0	<a href="#">Address</a>	Top IPA of range whose RIPAS was modified

The out\_top output value is valid only when the command result is RMI\_SUCCESS.

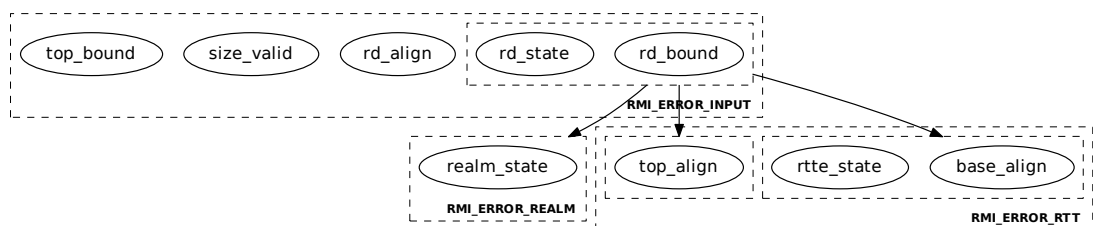
When the `out_top` output value is valid, it is aligned to the size of the address range described by the RTT entry at the level where the RTT walk terminated.

### B3.3.18.2 Failure conditions

ID	Condition
<code>rd_align</code>	pre: <code>!AddrIsGranuleAligned(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>rd_bound</code>	pre: <code>!PaIsDelegable(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>rd_state</code>	pre: <code>Granule(rd).state != RD</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>size_valid</code>	pre: <code>UInt(top) &lt;= UInt(base)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>top_bound</code>	pre: <code>!AddrIsProtected(ToAddress(UInt(top) - RMM_Granule_Size), realm)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>realm_state</code>	pre: <code>realm.state != NEW</code> post: <code>ResultEqual(result, RMI_ERROR_REALM)</code>
<code>base_align</code>	pre: <code>!AddrIsRttLevelAligned(base, walk.level)</code> post: <code>ResultEqual(result, RMI_ERROR_RTT, walk.level)</code>
<code>rtte_state</code>	pre: <code>walk.rtte.state != UNASSIGNED</code> post: <code>ResultEqual(result, RMI_ERROR_RTT, walk.level)</code>
<code>top_align</code>	pre: <code>UInt(top) &lt; UInt(AlignUpToRttLevel(ToAddress(UInt(base) + 1), walk.level))</code> post: <code>ResultEqual(result, RMI_ERROR_RTT, walk.level)</code>

#### B3.3.18.2.1 Failure condition ordering

```
[rd_bound, rd_state] < [realm_state]
[rd_bound, rd_state] < [base_align, rtte_state]
[rd_bound, rd_state] < [top_align]
```



### B3.3.18.3 Success conditions

ID	Condition
rtte_ripas	<code>RttEntriesInRangeRipas (</code> <code>    Rtt (walk.rtt_addr),</code> <code>    walk.level,</code> <code>    base, walk_top,</code> <code>    RAM)</code>
rim	<code>Realm (rd).measurements[0] == RimExtendRipas (</code> <code>    realm, base, walk_top, walk.level)</code>
out_top	<code>out_top == walk_top</code>

### B3.3.18.4 RMI\_RTT\_INIT\_RIPAS extension of RIM

On successful execution of RMI\_RTT\_INIT\_RIPAS, the new RIM value of the target Realm is calculated by the RMM as follows:

1. Allocate an [RmmMeasurementDescriptorRipas](#) data structure.
2. For each RTT entry in the range [base, top) described by the RMI\_RTT\_INIT\_RIPAS input values:
  - a. Populate the measurement descriptor:
    - Set the desc\_type field to the descriptor type.
    - Set the len field to the descriptor length.
    - Set the base field to the IPA of the RTT entry.
    - Set the top field to `Min(ipa + size, top)`, where
      - ipa is the IPA of the RTT entry
      - size is the size in bytes of the IPA region described by the RTT entry
      - top is the input value provided to the command
  - b. Using the RHA of the target Realm, compute the hash of the measurement descriptor. Set the RIM of the target Realm to this value, zero filling upper bytes if the RHA output is smaller than the size of the RIM.

See also:

- [A7.1.1 Realm Initial Measurement](#)
- [B2.44 RimExtendRipas function](#)
- [C1.7 RmmMeasurementDescriptorRipas type](#)

### B3.3.18.5 Footprint

ID	Value
rtte	<code>Rtt (walk.rtt_addr)</code>
rim	<code>Realm (rd).measurements[0]</code>

### B3.3.19 RMI\_RTT\_MAP\_UNPROTECTED command

Creates a mapping from an Unprotected IPA to a Non-secure PA.

See also:

- [A5.5 Realm Translation Table](#)
- [B3.3.22 RMI\\_RTT\\_UNMAP\\_UNPROTECTED command](#)

#### B3.3.19.1 Interface

##### B3.3.19.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC400015F
rd	X1	63:0	Address	PA of the RD for the target Realm
ipa	X2	63:0	Address	IPA at which the Granule will be mapped in the target Realm
level	X3	63:0	Int64	RTT level
desc	X4	63:0	Bits64	RTTE descriptor

The layout and encoding of fields in the `desc` input value match “Attribute fields in stage 2 VMSAv8-64 Block and Page descriptors” in *Arm Architecture Reference Manual for A-Profile architecture* [3].

See also:

- *Arm Architecture Reference Manual for A-Profile architecture* [3]
- [A5.5.11 RTT entry attributes](#)
- [B2.53 RttDescriptorIsValidForUnprotected function](#)

##### B3.3.19.1.2 Context

The RMI\_RTT\_MAP\_UNPROTECTED command operates on the following context.

Name	Type	Value	Before	Description
walk	<a href="#">RmmRttWalkResult</a>	<code>RttWalk(     rd, ipa, level)</code>	false	RTT walk result
entry_idx	UInt64	<code>RttEntryIndex(     ipa, walk.level)</code>	false	RTTE index
rtte	<a href="#">RmmRttEntry</a>	<code>RttEntryFromDescriptor(     ↔desc)</code>	false	RTT entry

##### B3.3.19.1.3 Output values

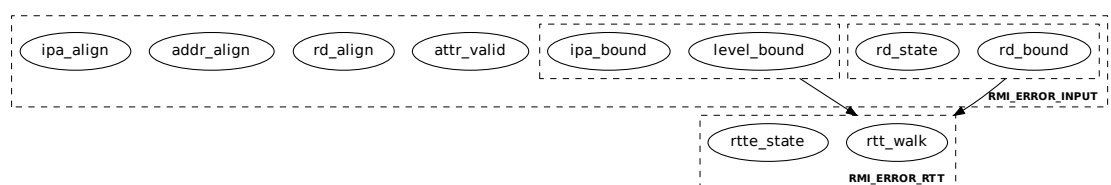
Name	Register	Bits	Type	Description
result	X0	63:0	RmiCommandReturnCode	Command return status

### B3.3.19.2 Failure conditions

ID	Condition
attr_valid	pre: !RttDescriptorIsValidForUnprotected(desc) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_align	pre: !AddrIsGranuleAligned(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_bound	pre: !PaIsDelegable(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_state	pre: Granule(rd).state != RD post: ResultEqual(result, RMI_ERROR_INPUT)
level_bound	pre: !RttLevelIsBlockOrPage(rd, level) post: ResultEqual(result, RMI_ERROR_INPUT)
addr_align	pre: !AddrIsRttLevelAligned(rtte.addr, level) post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_align	pre: !AddrIsRttLevelAligned(ipa, level) post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_bound	pre: (UInt(ipa) >= (2 ^ Realm(rd).ipa_width)    AddrIsProtected(ipa, Realm(rd))) post: ResultEqual(result, RMI_ERROR_INPUT)
rtt_walk	pre: walk.level < level post: ResultEqual(result, RMI_ERROR_RTT, walk.level)
rtte_state	pre: walk.rtte.state != UNASSIGNED_NS post: ResultEqual(result, RMI_ERROR_RTT, walk.level)

#### B3.3.19.2.1 Failure condition ordering

```
[rd_bound, rd_state] < [rtt_walk, rtte_state]
[level_bound, ipa_bound] < [rtt_walk, rtte_state]
```



### B3.3.19.3 Success conditions

ID	Condition
rtte_state	<code>walk.rtte.state == ASSIGNED_NS</code>
rtte_contents	<code>(walk.rtte.MemAttr == rtte.MemAttr &amp;&amp; walk.rtte.S2AP == rtte.S2AP &amp;&amp; walk.rtte.SH == rtte.SH &amp;&amp; walk.rtte.addr == rtte.addr)</code>

### B3.3.19.4 Footprint

ID	Value
rtte	<code>RttEntry(walk.rtt_addr, entry_idx)</code>

### B3.3.20 RMI\_RTT\_READ\_ENTRY command

Reads an RTTE.

See also:

- [A5.5 Realm Translation Table](#)

#### B3.3.20.1 Interface

##### B3.3.20.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000161
rd	X1	63:0	Address	PA of the RD for the target Realm
ipa	X2	63:0	Address	Realm Address for which to read the RTTE
level	X3	63:0	Int64	RTT level at which to read the RTTE

##### B3.3.20.1.2 Context

The RMI\_RTT\_READ\_ENTRY command operates on the following context.

Name	Type	Value	Before	Description
walk	<a href="#">RmmRttWalkResult</a>	<a href="#">RttWalk</a> ( rd, ipa, level)	false	RTT walk result
rtte	<a href="#">RmmRttEntry</a>	<a href="#">RttEntryFromDescriptor</a> ( ↔desc)	false	RTT entry

##### B3.3.20.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiCommandReturnCode</a>	Command return status
walk_level	X1	63:0	UInt64	RTT level reached by the RTT walk
state	X2	7:0	<a href="#">RmiRttEntryState</a>	State of RTTE reached by the walk
desc	X3	63:0	Bits64	RTTE descriptor
ripas	X4	7:0	<a href="#">RmiRipas</a>	RIPAS of RTTE reached by the walk

The following unused bits of RMI\_RTT\_READ\_ENTRY output values must be zero: X2[63:8], X4[63:8].

The layout and encoding of fields in the `rtte` output value match “Attribute fields in stage 2 VMSAv8-64 Block and Page descriptors” in *Arm Architecture Reference Manual for A-Profile architecture* [3].

See also:



- *Arm Architecture Reference Manual for A-Profile architecture* [3]
- [A5.5.11 RTT entry attributes](#)

### B3.3.20.2 Failure conditions

ID	Condition
rd_align	pre: !AddrIsGranuleAligned(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_bound	pre: !PaIsDelegable(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_state	pre: Granule(rd).state != RD post: ResultEqual(result, RMI_ERROR_INPUT)
level_bound	pre: !RttLevelIsValid(rd, level) post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_align	pre: !AddrIsRttLevelAligned(ipa, level) post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_bound	pre: UInt(ipa) >= (2 ^ Realm(rd).ipa_width) post: ResultEqual(result, RMI_ERROR_INPUT)

#### B3.3.20.2.1 Failure condition ordering

The RMI\_RTT\_READ\_ENTRY command does not have any failure condition orderings.

### B3.3.20.3 Success conditions

ID	Condition
state	state == RttEntryState(walk.rtte.state)
state_invalid	pre: (walk.rtte.state == UNASSIGNED    walk.rtte.state == UNASSIGNED_NS) post: (rtte.MemAttr == Zeros() && rtte.S2AP == Zeros() && rtte.SH == Zeros() && rtte.addr == Zeros())
state_prot	pre: (walk.rtte.state == ASSIGNED    walk.rtte.state == TABLE) post: (rtte.MemAttr == Zeros() && rtte.S2AP == Zeros() && rtte.SH == Zeros() && rtte.addr == walk.rtte.addr)
state_unprot	pre: walk.rtte.state == ASSIGNED_NS post: (rtte.MemAttr == walk.rtte.MemAttr && rtte.S2AP == walk.rtte.S2AP && rtte.SH == walk.rtte.SH && rtte.addr == walk.rtte.addr)

ID	Condition
ripas_unprot	<pre>pre: (walk.rtte.state != UNASSIGNED       &amp;&amp; walk.rtte.state != ASSIGNED) post: ripas == RMI_EMPTY</pre>

#### B3.3.20.4 Footprint

The RMI\_RTT\_READ\_ENTRY command does not have any footprint.

### B3.3.21 RMI\_RTT\_SET\_RIPAS command

Completes a request made by the Realm to change the RIPAS of a target IPA range.

See also:

- [A5.4 RIPAS change](#)

#### B3.3.21.1 Interface

##### B3.3.21.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000169
rd	X1	63:0	Address	PA of the RD for the target Realm
rec	X2	63:0	Address	PA of the target REC
base	X3	63:0	Address	Base of target IPA region
top	X4	63:0	Address	Top of target IPA region

##### B3.3.21.1.2 Context

The RMI\_RTT\_SET\_RIPAS command operates on the following context.

Name	Type	Value	Before	Description
walk	RmmRttWalkResult	<code>RttWalk( rd, base, RMM_RTT_PAGE_LEVEL)</code>	false	RTT walk result
walk_top	Address	<code>RttSkipEntriesWithRipas( Rtt(walk.rtt_addr), walk.level, base, top, Rec(rec). ripas_destroyed != CHANGE_DESTROYED)</code>	true	Top IPA of entries which have associated RIPAS values, starting from entry at which the RTT walk terminated

##### B3.3.21.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	RmiCommandReturnCode	Command return status
out_top	X1	63:0	Address	Top IPA of range whose RIPAS was modified

The `out_top` output value is valid only when the command result is RMI\_SUCCESS.

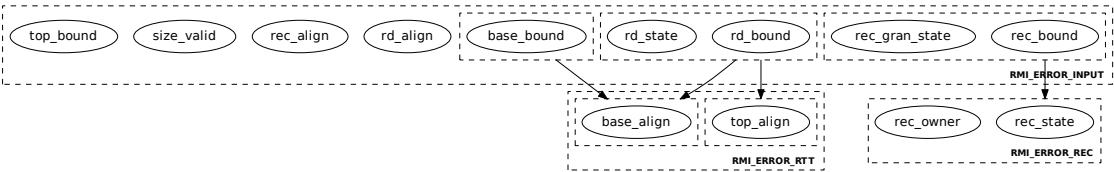
When the `out_top` output value is valid, it is aligned to the size of the address range described by the RTT entry at the level where the RTT walk terminated.

### B3.3.21.2 Failure conditions

ID	Condition
<code>rd_align</code>	pre: <code>!AddrIsGranuleAligned(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>rd_bound</code>	pre: <code>!PaIsDelegable(rd)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>rd_state</code>	pre: <code>Granule(rd).state != RD</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>rec_align</code>	pre: <code>!AddrIsGranuleAligned(rec)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>rec_bound</code>	pre: <code>!PaIsDelegable(rec)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>rec_gran_state</code>	pre: <code>Granule(rec).state != REC</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>rec_state</code>	pre: <code>Rec(rec).state == RUNNING</code> post: <code>ResultEqual(result, RMI_ERROR_REC)</code>
<code>rec_owner</code>	pre: <code>Rec(rec).owner != rd</code> post: <code>ResultEqual(result, RMI_ERROR_REC)</code>
<code>size_valid</code>	pre: <code>UInt(top) &lt;= UInt(base)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>base_bound</code>	pre: <code>base != Rec(rec).ripas_addr</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>top_bound</code>	pre: <code>UInt(top) &gt; UInt(Rec(rec).ripas_top)</code> post: <code>ResultEqual(result, RMI_ERROR_INPUT)</code>
<code>base_align</code>	pre: <code>!AddrIsRttLevelAligned(base, walk.level)</code> post: <code>ResultEqual(result, RMI_ERROR_RTT, walk.level)</code>
<code>top_align</code>	pre: <code>UInt(top) &lt; UInt(AlignUpToRttLevel(ToAddress(UInt(base) + 1), walk.level))</code> post: <code>ResultEqual(result, RMI_ERROR_RTT, walk.level)</code>

#### B3.3.21.2.1 Failure condition ordering

```
[rd_bound, rd_state] < [base_align]
[rd_bound, rd_state] < [top_align]
[rec_bound, rec_gran_state] < [rec_state, rec_owner]
[base_bound] < [base_align]
```



**B3.3.21.3 Success conditions**

ID	Condition
rtte_ripas	<code>RttEntriesInRangeRipas (</code> <code>Rtt (walk.rtt_addr),</code> <code>walk.level,</code> <code>base, walk_top,</code> <code>Rec (rec).ripas_value)</code>
ripas_addr	<code>Rec (rec).ripas_addr == walk_top</code>
out_top	<code>out_top == walk_top</code>

**B3.3.21.4 Footprint**

ID	Value
rtte	<code>Rtt (walk.rtt_addr)</code>
ripas_addr	<code>Rec (rec).ripas_addr</code>

### B3.3.22 RMI\_RTT\_UNMAP\_UNPROTECTED command

Removes a mapping at an Unprotected IPA.

See also:

- [A5.5 Realm Translation Table](#)
- [B3.3.19 RMI\\_RTT\\_MAP\\_UNPROTECTED command](#)

#### B3.3.22.1 Interface

##### B3.3.22.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000162
rd	X1	63:0	Address	PA of the RD for the target Realm
ipa	X2	63:0	Address	IPA at which the Granule is mapped in the target Realm
level	X3	63:0	Int64	RTT level

##### B3.3.22.1.2 Context

The RMI\_RTT\_UNMAP\_UNPROTECTED command operates on the following context.

Name	Type	Value	Before	Description
walk	RmmRttWalkResult	<code>RttWalk( rd, ipa, level)</code>	false	RTT walk result
entry_idx	UInt64	<code>RttEntryIndex( ipa, walk.level)</code>	false	RTTE index
walk_top	Address	<code>RttSkipNonLiveEntries( Rtt(walk.rtt_addr), walk.level, ipa)</code>	false	Top IPA of non-live RTT entries, from entry at which the RTT walk terminated

##### B3.3.22.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	RmiCommandReturnCode	Command return status
top	X1	63:0	Address	Top IPA of non-live RTT entries, from entry at which the RTT walk terminated

The `n1` output value is valid both when the command result is RMI\_SUCCESS and when it is RMI\_ERROR\_RTT.

The values of the `result` and `top` output values for different command outcomes are summarized in the following table.

Scenario	result	top	walk.rtte.state
ipa is mapped at the target level	RMI_SUCCESS	> ipa	Before execution: ASSIGNED_NS After execution: UNASSIGNED_NS
ipa is not mapped	(RMI_ERROR_RTT, <= level)	> ipa	UNASSIGNED_NS
ipa is mapped at a lower level	(RMI_ERROR_RTT, < level)	== ipa	ASSIGNED_NS
RTT walk was not performed, due to any other command failure	Another error code	0	Unknown

See also:

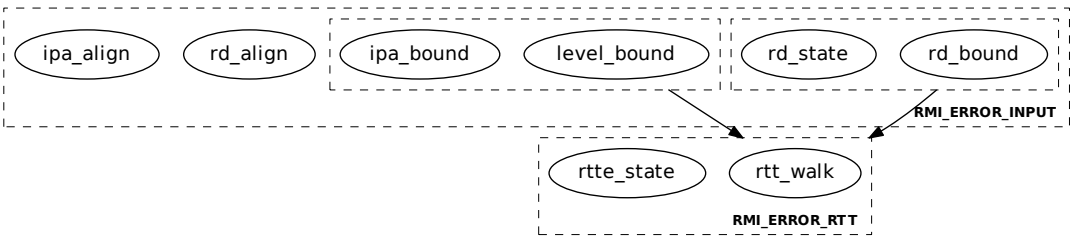
- [A5.5.8 RTTE liveness and RTT liveness](#)

### B3.3.22.2 Failure conditions

ID	Condition
rd_align	pre: !AddrIsGranuleAligned(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_bound	pre: !PaIsDelegable(rd) post: ResultEqual(result, RMI_ERROR_INPUT)
rd_state	pre: Granule(rd).state != RD post: ResultEqual(result, RMI_ERROR_INPUT)
level_bound	pre: !RttLevelIsBlockOrPage(rd, level) post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_align	pre: !AddrIsRttLevelAligned(ipa, level) post: ResultEqual(result, RMI_ERROR_INPUT)
ipa_bound	pre: (UInt(ipa) >= (2 ^ Realm(rd).ipa_width)    AddrIsProtected(ipa, Realm(rd))) post: ResultEqual(result, RMI_ERROR_INPUT)
rtt_walk	pre: walk.level < level post: (ResultEqual(result, RMI_ERROR_RTT, walk.level) && (top == walk_top))
rtte_state	pre: walk.rtte.state != ASSIGNED_NS post: (ResultEqual(result, RMI_ERROR_RTT, walk.level) && (top == walk_top))

#### B3.3.22.2.1 Failure condition ordering

```
[rd_bound, rd_state] < [rtt_walk, rtte_state]
[level_bound, ipa_bound] < [rtt_walk, rtte_state]
```



B3.3.22.3 Success conditions

ID	Condition
rtte_state	walk.rtte.state == UNASSIGNED_NS
top	top == walk_top

B3.3.22.4 Footprint

ID	Value
rtte	RttEntry(walk.rtt_addr, entry_idx)



### B3.3.23 RMI\_VERSION command

Returns RMI version.

#### B3.3.23.1 Interface

##### B3.3.23.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000150

##### B3.3.23.1.2 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RmiInterfaceVersion</a>	Interface version

See also:

- [B3.1 RMI version](#)

#### B3.3.23.2 Failure conditions

The RMI\_VERSION command does not have any failure conditions.

#### B3.3.23.3 Success conditions

The RMI\_VERSION command does not have any success conditions.

#### B3.3.23.4 Footprint

The RMI\_VERSION command does not have any footprint.

## B3.4 RMI types

This section defines types which are used in the RMI interface.

### B3.4.1 RmiCommandReturnCode type

The RmiCommandReturnCode fieldset contains a return code from an RMI command.

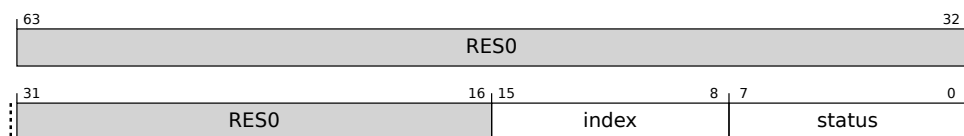
The RmiCommandReturnCode fieldset is a [concrete type](#).

The width of the RmiCommandReturnCode fieldset is 64 bits.

See also:

- [Chapter B1 Commands](#)

The fields of the RmiCommandReturnCode fieldset are shown in the following diagram.



The fields of the RmiCommandReturnCode fieldset are shown in the following table.

Name	Bits	Description	Value
status	7:0	Status of the command	<a href="#">RmiStatusCode</a>
index	15:8	Index which identifies the reason for a command failure	<a href="#">UInt8</a>
	63:16	Reserved	Must be zero

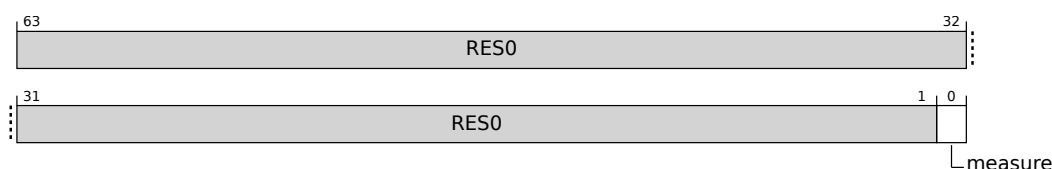
### B3.4.2 RmiDataFlags type

The RmiDataFlags fieldset contains flags provided by the Host during DATA Granule creation.

The RmiDataFlags fieldset is a [concrete type](#).

The width of the RmiDataFlags fieldset is 64 bits.

The fields of the RmiDataFlags fieldset are shown in the following diagram.



The fields of the RmiDataFlags fieldset are shown in the following table.

Name	Bits	Description	Value
measure	0:0	Whether to measure DATA Granule contents	<a href="#">RmiDataMeasureContent</a>

Name	Bits	Description	Value
	63:1	Reserved	Should be zero

### B3.4.3 RmiDataMeasureContent type

The RmiDataMeasureContent enumeration represents whether to measure DATA Granule contents.

The RmiDataMeasureContent enumeration is a [concrete type](#).

The width of the RmiDataMeasureContent enumeration is 1 bits.

The values of the RmiDataMeasureContent enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_NO_MEASURE_CONTENT	Do not measure DATA Granule contents.
1	RMI_MEASURE_CONTENT	Measure DATA Granule contents.

### B3.4.4 RmiEmulatedMmio type

The RmiEmulatedMmio enumeration represents whether the host has completed emulation for an Emulatable Abort.

The RmiEmulatedMmio enumeration is a [concrete type](#).

The width of the RmiEmulatedMmio enumeration is 1 bits.

The values of the RmiEmulatedMmio enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_NOT_EMULATED_MMIO	Host has not completed emulation for an Emulatable Abort.
1	RMI_EMULATED_MMIO	Host has completed emulation for an Emulatable Abort.

### B3.4.5 RmiFeature type

The RmiFeature enumeration represents whether a feature is supported or enabled.

The RmiFeature enumeration is a [concrete type](#).

The width of the RmiFeature enumeration is 1 bits.

The values of the RmiFeature enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_FEATURE_FALSE	<ul style="list-style-type: none"><li>During discovery: Feature is not supported.</li><li>During selection: Feature is not enabled.</li></ul>

Encoding	Name	Description
1	RMI_FEATURE_TRUE	<ul style="list-style-type: none"> <li>During discovery: Feature is supported.</li> <li>During selection: Feature is enabled.</li> </ul>

### B3.4.6 RmiFeatureRegister0 type

The RmiFeatureRegister0 fieldset contains feature register 0.

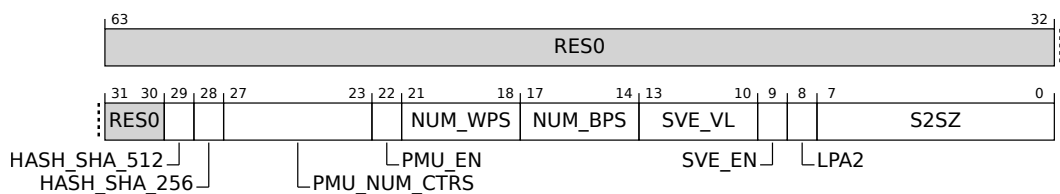
The RmiFeatureRegister0 fieldset is a [concrete type](#).

The width of the RmiFeatureRegister0 fieldset is 64 bits.

See also:

- [A3.1 Realm feature discovery and selection](#)
- [B3.3.4 RMI\\_FEATURES command](#)

The fields of the RmiFeatureRegister0 fieldset are shown in the following diagram.



The fields of the RmiFeatureRegister0 fieldset are shown in the following table.

Name	Bits	Description	Value
S2SZ	7:0	Maximum Realm IPA width supported by the RMM. Specifies the input address size for stage 2 translation to be $2^{\text{S2SZ}}$ . Note this format expresses the IPA width directly and is therefore different from the <code>VTCCR_EL2.T0SZ</code> encoding.	<a href="#">UInt8</a>
LPA2	8:8	Whether LPA2 is supported.	<a href="#">RmiFeature</a>
SVE_EN	9:9	Whether SVE is supported.	<a href="#">RmiFeature</a>
SVE_VL	13:10	Maximum SVE vector length supported by the RMM. The effective vector length supported by the RMM is $(\text{SVE\_VL} + 1) * 128$ , similar to the value of <code>ZCR_ELx.LEN</code> .	<a href="#">UInt4</a>
NUM_BPS	17:14	Number of breakpoints available	<a href="#">UInt4</a>
NUM_WPS	21:18	Number of watchpoints available	<a href="#">UInt4</a>
PMU_EN	22:22	Whether PMU is supported	<a href="#">RmiFeature</a>
PMU_NUM_CTRS	27:23	Number of PMU counters available	<a href="#">UInt5</a>
HASH_SHA_256	28:28	Whether SHA-256 is supported	<a href="#">RmiFeature</a>

Name	Bits	Description	Value
HASH_SHA_512	29:29	Whether SHA-512 is supported	<a href="#">RmiFeature</a>
	63:30	Reserved	Must be zero

### B3.4.7 RmiHashAlgorithm type

The RmiHashAlgorithm enumeration represents hash algorithm.

The RmiHashAlgorithm enumeration is a [concrete type](#).

The width of the RmiHashAlgorithm enumeration is 8 bits.

The values of the RmiHashAlgorithm enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_HASH_SHA_256	SHA-256 ( <i>Secure Hash Standard (SHS)</i> <a href="#">[15]</a> )
1	RMI_HASH_SHA_512	SHA-512 ( <i>Secure Hash Standard (SHS)</i> <a href="#">[15]</a> )

Unused encodings for the RmiHashAlgorithm enumeration are reserved for use by future versions of this specification.

### B3.4.8 RmiInjectSea type

The RmiInjectSea enumeration represents whether to inject a Synchronous External Abort into the Realm.

The RmiInjectSea enumeration is a [concrete type](#).

The width of the RmiInjectSea enumeration is 1 bits.

The values of the RmiInjectSea enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_NO_INJECT_SEA	Do not inject an SEA into the Realm.
1	RMI_INJECT_SEA	Inject an SEA into the Realm.

### B3.4.9 RmiInterfaceVersion type

The RmiInterfaceVersion fieldset contains an RMI interface version.

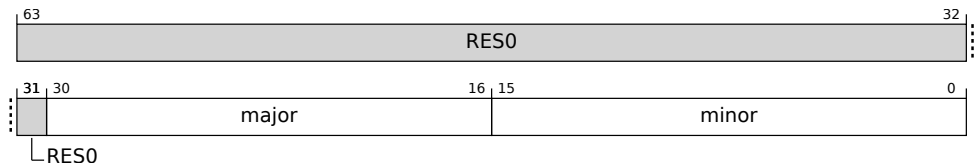
The RmiInterfaceVersion fieldset is a [concrete type](#).

The width of the RmiInterfaceVersion fieldset is 64 bits.

See also:

- [B3.1 RMI version](#)
- [B3.3.23 RMI\\_VERSION command](#)

The fields of the RmiInterfaceVersion fieldset are shown in the following diagram.



The fields of the RmiInterfaceVersion fieldset are shown in the following table.

Name	Bits	Description	Value
minor	15:0	Interface minor version number (the value $y$ in interface version $x.y$ )	UInt16
major	30:16	Interface major version number (the value $x$ in interface version $x.y$ )	UInt15
	63:31	Reserved	Must be zero

B3.4.10 RmiPmuOverflowStatus type

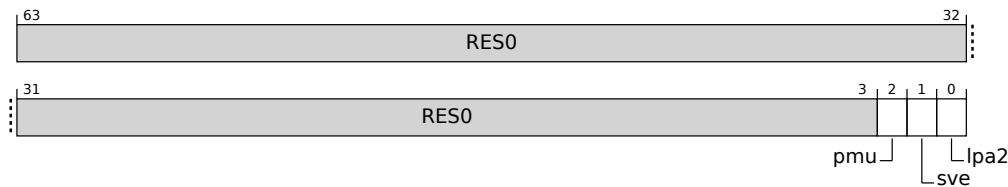
The RmiPmuOverflowStatus enumeration represents PMU overflow status.  
The RmiPmuOverflowStatus enumeration is a [concrete type](#).  
The width of the RmiPmuOverflowStatus enumeration is 8 bits.  
The values of the RmiPmuOverflowStatus enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_PMU_OVERFLOW_NOT_ACTIVE	PMU overflow is not active.
1	RMI_PMU_OVERFLOW_ACTIVE	PMU overflow is active.

Unused encodings for the RmiPmuOverflowStatus enumeration are reserved for use by future versions of this specification.

B3.4.11 RmiRealmFlags type

The RmiRealmFlags fieldset contains flags provided by the Host during Realm creation.  
The RmiRealmFlags fieldset is a [concrete type](#).  
The width of the RmiRealmFlags fieldset is 64 bits.  
The fields of the RmiRealmFlags fieldset are shown in the following diagram.



The fields of the RmiRealmFlags fieldset are shown in the following table.

Name	Bits	Description	Value
lpa2	0:0	Whether LPA2 is enabled	<a href="#">RmiFeature</a>
sve	1:1	Whether SVE is enabled	<a href="#">RmiFeature</a>
pmu	2:2	Whether PMU is enabled	<a href="#">RmiFeature</a>
	63:3	Reserved	Should be zero

### B3.4.12 RmiRealmParams type

The RmiRealmParams structure contains parameters provided by the Host during Realm creation.

The RmiRealmParams structure is a [concrete type](#).

The width of the RmiRealmParams structure is 4096 (0x1000) bytes.

See also:

- [A2.1.6 Realm parameters](#)
- [B3.3.9 RMI\\_REALM\\_CREATE command](#)

The members of the RmiRealmParams structure are shown in the following table.

Name	Byte offset	Type	Description
flags	0x0	<a href="#">RmiRealmFlags</a>	Flags
s2sz	0x8	<a href="#">UInt8</a>	Requested IPA width. Specifies the input address size for stage 2 translation to be $2^{\text{s2sz}}$ . Note this format expresses the IPA width directly and is therefore different from the <code>VTCCR_EL2.T0SZ</code> encoding.
sve_vl	0x10	<a href="#">UInt8</a>	Requested SVE vector length. The effective vector length requested is $(\text{sve\_vl} + 1) * 128$ , similar to the value of <code>ZCR_ELx.LEN</code> .
num_bps	0x18	<a href="#">UInt8</a>	Requested number of breakpoints
num_wps	0x20	<a href="#">UInt8</a>	Requested number of watchpoints
pmu_num_ctrs	0x28	<a href="#">UInt8</a>	Requested number of PMU counters
hash_algo	0x30	<a href="#">RmiHashAlgorithm</a>	Algorithm used to measure the initial state of the Realm
rpv	0x400	<a href="#">Bits512</a>	Realm Personalization Value
vmid	0x800	<a href="#">Bits16</a>	Virtual Machine Identifier
rtt_base	0x808	<a href="#">Address</a>	Realm Translation Table base
rtt_level_start	0x810	<a href="#">Int64</a>	RTT starting level
rtt_num_start	0x818	<a href="#">UInt32</a>	Number of starting level RTTs

Unused bits of the RmiRealmParams structure should be zero.

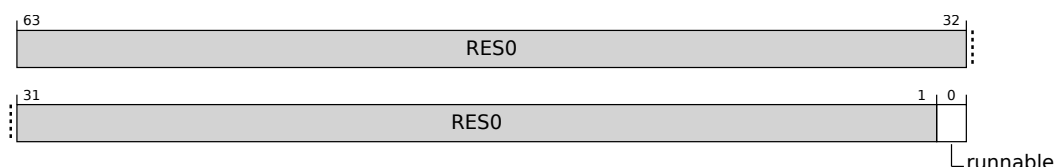
### B3.4.13 RmiRecCreateFlags type

The RmiRecCreateFlags fieldset contains flags provided by the Host during REC creation.

The RmiRecCreateFlags fieldset is a [concrete type](#).

The width of the RmiRecCreateFlags fieldset is 64 bits.

The fields of the RmiRecCreateFlags fieldset are shown in the following diagram.



The fields of the RmiRecCreateFlags fieldset are shown in the following table.

Name	Bits	Description	Value
runnable	0:0	Whether REC is eligible for execution	<a href="#">RmiRecRunnable</a>
	63:1	Reserved	Should be zero

### B3.4.14 RmiRecEnter type

The RmiRecEnter structure contains data passed from the Host to the RMM on REC entry.

The RmiRecEnter structure is a [concrete type](#).

The width of the RmiRecEnter structure is 2048 (0x800) bytes.

See also:

- [A4.2.1 RecEnter object](#)
- [B3.3.14 RMI\\_REC\\_ENTER command](#)
- [B3.4.16 RmiRecExit type](#)

The members of the RmiRecEnter structure are shown in the following table.

Name	Byte offset	Type	Description
flags	0x0	<a href="#">RmiRecEnterFlags</a>	Flags
gprs[0]	0x200	<a href="#">Bits64</a>	Registers
gprs[1]	0x208	<a href="#">Bits64</a>	Registers
gprs[2]	0x210	<a href="#">Bits64</a>	Registers
gprs[3]	0x218	<a href="#">Bits64</a>	Registers
gprs[4]	0x220	<a href="#">Bits64</a>	Registers
gprs[5]	0x228	<a href="#">Bits64</a>	Registers
gprs[6]	0x230	<a href="#">Bits64</a>	Registers
gprs[7]	0x238	<a href="#">Bits64</a>	Registers
gprs[8]	0x240	<a href="#">Bits64</a>	Registers



Name	Byte offset	Type	Description
gprs[9]	0x248	Bits64	Registers
gprs[10]	0x250	Bits64	Registers
gprs[11]	0x258	Bits64	Registers
gprs[12]	0x260	Bits64	Registers
gprs[13]	0x268	Bits64	Registers
gprs[14]	0x270	Bits64	Registers
gprs[15]	0x278	Bits64	Registers
gprs[16]	0x280	Bits64	Registers
gprs[17]	0x288	Bits64	Registers
gprs[18]	0x290	Bits64	Registers
gprs[19]	0x298	Bits64	Registers
gprs[20]	0x2a0	Bits64	Registers
gprs[21]	0x2a8	Bits64	Registers
gprs[22]	0x2b0	Bits64	Registers
gprs[23]	0x2b8	Bits64	Registers
gprs[24]	0x2c0	Bits64	Registers
gprs[25]	0x2c8	Bits64	Registers
gprs[26]	0x2d0	Bits64	Registers
gprs[27]	0x2d8	Bits64	Registers
gprs[28]	0x2e0	Bits64	Registers
gprs[29]	0x2e8	Bits64	Registers
gprs[30]	0x2f0	Bits64	Registers
gicv3_hcr	0x300	Bits64	GICv3 Hypervisor Control Register value
gicv3_lrs[0]	0x308	Bits64	GICv3 List Register values
gicv3_lrs[1]	0x310	Bits64	GICv3 List Register values
gicv3_lrs[2]	0x318	Bits64	GICv3 List Register values
gicv3_lrs[3]	0x320	Bits64	GICv3 List Register values
gicv3_lrs[4]	0x328	Bits64	GICv3 List Register values
gicv3_lrs[5]	0x330	Bits64	GICv3 List Register values
gicv3_lrs[6]	0x338	Bits64	GICv3 List Register values
gicv3_lrs[7]	0x340	Bits64	GICv3 List Register values
gicv3_lrs[8]	0x348	Bits64	GICv3 List Register values
gicv3_lrs[9]	0x350	Bits64	GICv3 List Register values
gicv3_lrs[10]	0x358	Bits64	GICv3 List Register values
gicv3_lrs[11]	0x360	Bits64	GICv3 List Register values

Name	Byte offset	Type	Description
<code>gicv3_lrs[12]</code>	<code>0x368</code>	<a href="#">Bits64</a>	GICv3 List Register values
<code>gicv3_lrs[13]</code>	<code>0x370</code>	<a href="#">Bits64</a>	GICv3 List Register values
<code>gicv3_lrs[14]</code>	<code>0x378</code>	<a href="#">Bits64</a>	GICv3 List Register values
<code>gicv3_lrs[15]</code>	<code>0x380</code>	<a href="#">Bits64</a>	GICv3 List Register values

Unused bits of the `RmiRecEnter` structure should be zero.

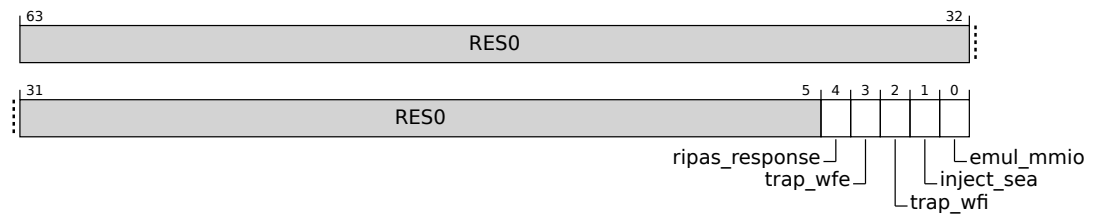
### B3.4.15 RmiRecEnterFlags type

The `RmiRecEnterFlags` fieldset contains flags provided by the Host during REC entry.

The `RmiRecEnterFlags` fieldset is a [concrete type](#).

The width of the `RmiRecEnterFlags` fieldset is 64 bits.

The fields of the `RmiRecEnterFlags` fieldset are shown in the following diagram.



The fields of the `RmiRecEnterFlags` fieldset are shown in the following table.

Name	Bits	Description	Value
<code>emul_mmio</code>	0:0	Whether the host has completed emulation for an Emulatable Data Abort	<a href="#">RmiEmulatedMmio</a>
<code>inject_sea</code>	1:1	Whether to inject a Synchronous External Abort into the Realm.	<a href="#">RmiInjectSea</a>
<code>trap_wfi</code>	2:2	Whether to trap WFI execution by the Realm.	<a href="#">RmiTrap</a>
<code>trap_wfe</code>	3:3	Whether to trap WFE execution by the Realm.	<a href="#">RmiTrap</a>
<code>ripas_response</code>	4:4	Host response to RIPAS change request.	<a href="#">RmiResponse</a>
	63:5	Reserved	Should be zero

### B3.4.16 RmiRecExit type

The `RmiRecExit` structure contains data passed from the RMM to the Host on REC exit.

The `RmiRecExit` structure is a [concrete type](#).

The width of the `RmiRecExit` structure is 2048 (`0x800`) bytes.

See also:

- [A4.3.1 RecExit object](#)

- [B3.3.14 RMI\\_REC\\_ENTER command](#)
- [B3.4.14 RmiRecEnter type](#)

The members of the RmiRecExit structure are shown in the following table.

Name	Byte offset	Type	Description
exit_reason	0x0	<a href="#">RmiRecExitReason</a>	Exit reason
esr	0x100	<a href="#">Bits64</a>	Exception Syndrome Register
far	0x108	<a href="#">Bits64</a>	Fault Address Register
hpfar	0x110	<a href="#">Bits64</a>	Hypervisor IPA Fault Address register
gprs[0]	0x200	<a href="#">Bits64</a>	Registers
gprs[1]	0x208	<a href="#">Bits64</a>	Registers
gprs[2]	0x210	<a href="#">Bits64</a>	Registers
gprs[3]	0x218	<a href="#">Bits64</a>	Registers
gprs[4]	0x220	<a href="#">Bits64</a>	Registers
gprs[5]	0x228	<a href="#">Bits64</a>	Registers
gprs[6]	0x230	<a href="#">Bits64</a>	Registers
gprs[7]	0x238	<a href="#">Bits64</a>	Registers
gprs[8]	0x240	<a href="#">Bits64</a>	Registers
gprs[9]	0x248	<a href="#">Bits64</a>	Registers
gprs[10]	0x250	<a href="#">Bits64</a>	Registers
gprs[11]	0x258	<a href="#">Bits64</a>	Registers
gprs[12]	0x260	<a href="#">Bits64</a>	Registers
gprs[13]	0x268	<a href="#">Bits64</a>	Registers
gprs[14]	0x270	<a href="#">Bits64</a>	Registers
gprs[15]	0x278	<a href="#">Bits64</a>	Registers
gprs[16]	0x280	<a href="#">Bits64</a>	Registers
gprs[17]	0x288	<a href="#">Bits64</a>	Registers
gprs[18]	0x290	<a href="#">Bits64</a>	Registers
gprs[19]	0x298	<a href="#">Bits64</a>	Registers
gprs[20]	0x2a0	<a href="#">Bits64</a>	Registers
gprs[21]	0x2a8	<a href="#">Bits64</a>	Registers
gprs[22]	0x2b0	<a href="#">Bits64</a>	Registers
gprs[23]	0x2b8	<a href="#">Bits64</a>	Registers
gprs[24]	0x2c0	<a href="#">Bits64</a>	Registers
gprs[25]	0x2c8	<a href="#">Bits64</a>	Registers
gprs[26]	0x2d0	<a href="#">Bits64</a>	Registers
gprs[27]	0x2d8	<a href="#">Bits64</a>	Registers

Name	Byte offset	Type	Description
gprs[28]	0x2e0	Bits64	Registers
gprs[29]	0x2e8	Bits64	Registers
gprs[30]	0x2f0	Bits64	Registers
gicv3_hcr	0x300	Bits64	GICv3 Hypervisor Control Register value
gicv3_lrs[0]	0x308	Bits64	GICv3 List Register values
gicv3_lrs[1]	0x310	Bits64	GICv3 List Register values
gicv3_lrs[2]	0x318	Bits64	GICv3 List Register values
gicv3_lrs[3]	0x320	Bits64	GICv3 List Register values
gicv3_lrs[4]	0x328	Bits64	GICv3 List Register values
gicv3_lrs[5]	0x330	Bits64	GICv3 List Register values
gicv3_lrs[6]	0x338	Bits64	GICv3 List Register values
gicv3_lrs[7]	0x340	Bits64	GICv3 List Register values
gicv3_lrs[8]	0x348	Bits64	GICv3 List Register values
gicv3_lrs[9]	0x350	Bits64	GICv3 List Register values
gicv3_lrs[10]	0x358	Bits64	GICv3 List Register values
gicv3_lrs[11]	0x360	Bits64	GICv3 List Register values
gicv3_lrs[12]	0x368	Bits64	GICv3 List Register values
gicv3_lrs[13]	0x370	Bits64	GICv3 List Register values
gicv3_lrs[14]	0x378	Bits64	GICv3 List Register values
gicv3_lrs[15]	0x380	Bits64	GICv3 List Register values
gicv3_misr	0x388	Bits64	GICv3 Maintenance Interrupt State Register value
gicv3_vmcr	0x390	Bits64	GICv3 Virtual Machine Control Register value
cntp_ctl	0x400	Bits64	Counter-timer Physical Timer Control Register value
cntp_cval	0x408	Bits64	Counter-timer Physical Timer CompareValue Register value
cntv_ctl	0x410	Bits64	Counter-timer Virtual Timer Control Register value
cntv_cval	0x418	Bits64	Counter-timer Virtual Timer CompareValue Register value
ripas_base	0x500	Bits64	Base address of target region for pending RIPAS change
ripas_top	0x508	Bits64	Top address of target region for pending RIPAS change
ripas_value	0x510	RmiRipas	RIPAS value of pending RIPAS change
imm	0x600	Bits16	Host call immediate value

Name	Byte offset	Type	Description
pmu_ovf_status	0x700	<a href="#">RmiPmuOverflowStatus</a>	PMU overflow status

Unused bits of the RmiRecExit structure must be zero.

### B3.4.17 RmiRecExitReason type

The RmiRecExitReason enumeration represents the reason for a REC exit.

The RmiRecExitReason enumeration is a [concrete type](#).

The width of the RmiRecExitReason enumeration is 8 bits.

The values of the RmiRecExitReason enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_EXIT_SYNC	REC exit due to synchronous exception
1	RMI_EXIT_IRQ	REC exit due to IRQ
2	RMI_EXIT_FIQ	REC exit due to FIQ
3	RMI_EXIT_PSCI	REC exit due to PSCI
4	RMI_EXIT_RIPAS_CHANGE	REC exit due to RIPAS change pending
5	RMI_EXIT_HOST_CALL	REC exit due to Host call
6	RMI_EXIT_SERROR	REC exit due to SError

Unused encodings for the RmiRecExitReason enumeration are reserved for use by future versions of this specification.

### B3.4.18 RmiRecMpidr type

The RmiRecMpidr fieldset contains MPIDR value which identifies a REC.

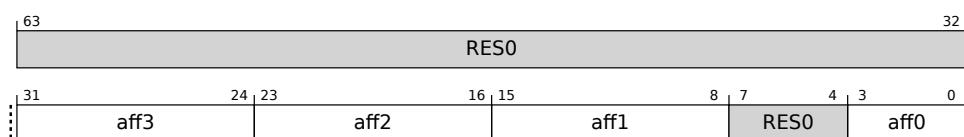
The RmiRecMpidr fieldset is a [concrete type](#).

The width of the RmiRecMpidr fieldset is 64 bits.

See also:

- [A2.3.3 REC index and MPIDR value](#)
- [B3.3.12 RMI\\_REC\\_CREATE command](#)

The fields of the RmiRecMpidr fieldset are shown in the following diagram.



The fields of the RmiRecMpidr fieldset are shown in the following table.

Name	Bits	Description	Value
aff0	3:0	Affinity level 0	<a href="#">Bits4</a>
	7:4	Reserved	Should be zero
aff1	15:8	Affinity level 1	<a href="#">Bits8</a>
aff2	23:16	Affinity level 2	<a href="#">Bits8</a>
aff3	31:24	Affinity level 3	<a href="#">Bits8</a>
	63:32	Reserved	Should be zero

### B3.4.19 RmiRecParams type

The RmiRecParams structure contains parameters provided by the Host during REC creation.

The RmiRecParams structure is a [concrete type](#).

The width of the RmiRecParams structure is 4096 (0x1000) bytes.

The number of valid entries in the `aux` array is determined by the return value from the `RMI_REC_AUX_COUNT` command.

See also:

- [B3.3.11 RMI\\_REC\\_AUX\\_COUNT command](#)

The members of the RmiRecParams structure are shown in the following table.

Name	Byte offset	Type	Description
flags	0x0	<a href="#">RmiRecCreateFlags</a>	Flags
mpidr	0x100	<a href="#">RmiRecMpidr</a>	MPIDR of the REC
pc	0x200	<a href="#">Bits64</a>	Program counter
gprs[0]	0x300	<a href="#">Bits64</a>	General-purpose registers
gprs[1]	0x308	<a href="#">Bits64</a>	General-purpose registers
gprs[2]	0x310	<a href="#">Bits64</a>	General-purpose registers
gprs[3]	0x318	<a href="#">Bits64</a>	General-purpose registers
gprs[4]	0x320	<a href="#">Bits64</a>	General-purpose registers
gprs[5]	0x328	<a href="#">Bits64</a>	General-purpose registers
gprs[6]	0x330	<a href="#">Bits64</a>	General-purpose registers
gprs[7]	0x338	<a href="#">Bits64</a>	General-purpose registers
num_aux	0x800	<a href="#">UInt64</a>	Number of auxiliary Granules
aux[0]	0x808	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[1]	0x810	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[2]	0x818	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[3]	0x820	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[4]	0x828	<a href="#">Address</a>	Addresses of auxiliary Granules

Name	Byte offset	Type	Description
aux[5]	0x830	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[6]	0x838	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[7]	0x840	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[8]	0x848	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[9]	0x850	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[10]	0x858	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[11]	0x860	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[12]	0x868	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[13]	0x870	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[14]	0x878	<a href="#">Address</a>	Addresses of auxiliary Granules
aux[15]	0x880	<a href="#">Address</a>	Addresses of auxiliary Granules

Unused bits of the RmiRecParams structure should be zero.

### B3.4.20 RmiRecRun type

The RmiRecRun structure contains fields used to share information between RMM and Host during REC entry and REC exit.

The RmiRecRun structure is a [concrete type](#).

The width of the RmiRecRun structure is 4096 (0x1000) bytes.

See also:

- [A4.2.1 RecEnter object](#)
- [A4.3.1 RecExit object](#)
- [B3.3.14 RMI\\_REC\\_ENTER command](#)

The members of the RmiRecRun structure are shown in the following table.

Name	Byte offset	Type	Description
enter	0x0	<a href="#">RmiRecEnter</a>	Entry information
exit	0x800	<a href="#">RmiRecExit</a>	Exit information

### B3.4.21 RmiRecRunnable type

The RmiRecRunnable enumeration represents whether a REC is eligible for execution.

The RmiRecRunnable enumeration is a [concrete type](#).

The width of the RmiRecRunnable enumeration is 1 bits.

The values of the RmiRecRunnable enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_NOT_RUNNABLE	Not eligible for execution.
1	RMI_RUNNABLE	Eligible for execution.

### B3.4.22 RmiResponse type

The RmiResponse enumeration represents whether the Host accepted or rejected a Realm request.

The RmiResponse enumeration is a [concrete type](#).

The width of the RmiResponse enumeration is 1 bits.

The values of the RmiResponse enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_ACCEPT	Host accepted the Realm request.
1	RMI_REJECT	Host rejected the Realm request.

### B3.4.23 RmiRipas type

The RmiRipas enumeration represents realm IPA state.

The RmiRipas enumeration is a [concrete type](#).

The width of the RmiRipas enumeration is 8 bits.

The values of the RmiRipas enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_EMPTY	Address where no Realm resources are mapped.
1	RMI_RAM	Address where private code or data owned by the Realm is mapped.
2	RMI_DESTROYED	Address which is inaccessible to the Realm due to an action taken by the Host.

Unused encodings for the RmiRipas enumeration are reserved for use by future versions of this specification.

### B3.4.24 RmiRttEntryState type

The RmiRttEntryState enumeration represents the state of an RTTE.

The RmiRttEntryState enumeration is a [concrete type](#).

The width of the RmiRttEntryState enumeration is 8 bits.

The values of the RmiRttEntryState enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_UNASSIGNED	This RTTE is not associated with any Granule.



Encoding	Name	Description
1	RMI_ASSIGNED	The output address of this RTTE points to: <ul style="list-style-type: none"><li>• a DATA Granule, if the input address is a Protected IPA, or</li><li>• an NS Granule, if the input address is an Unprotected IPA.</li></ul>
2	RMI_TABLE	The output address of this RTTE points to the next-level RTT.

Unused encodings for the RmiRttEntryState enumeration are reserved for use by future versions of this specification.

### B3.4.25 RmiStatusCode type

The RmiStatusCode enumeration represents the status of an RMI operation.

The RmiStatusCode enumeration is a [concrete type](#).

The width of the RmiStatusCode enumeration is 8 bits.

See also:

- [B1.3 Command registers](#)
- [B1.5 Command context values](#)

The values of the RmiStatusCode enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_SUCCESS	Command completed successfully
1	RMI_ERROR_INPUT	The value of a command input value caused the command to fail
2	RMI_ERROR_REALM	An attribute of a Realm does not match the expected value
3	RMI_ERROR_REC	An attribute of a REC does not match the expected value
4	RMI_ERROR_RTT	An RTT walk terminated before reaching the target RTT level, or reached an RTTE with an unexpected value

Unused encodings for the RmiStatusCode enumeration are reserved for use by future versions of this specification.

### B3.4.26 RmiTrap type

The RmiTrap enumeration represents whether a trap is enabled.

The RmiTrap enumeration is a [concrete type](#).

The width of the RmiTrap enumeration is 1 bits.

The values of the RmiTrap enumeration are shown in the following table.

Encoding	Name	Description
0	RMI_NO_TRAP	Trap is disabled.

Encoding	Name	Description
1	RMI_TRAP	Trap is enabled.

## Chapter B4

# Realm Services Interface

This chapter defines the interface used by Realm software to request services from the RMM.

## B4.1 RSI version

**R<sub>QKL</sub>GZ** This specification defines version 1.0 of the Realm Services Interface.

See also:

- [B4.3.9 RSI\\_VERSION command](#)

## B4.2 RSI command return codes

**I<sub>CYQD</sub>J** An RSI command return code indicates whether the command

- succeeded, or
- failed, and the reason for the failure.

**I<sub>DQJ</sub>SP** If an RSI command succeeds then it returns RSI\_SUCCESS.

**I<sub>YMH</sub>KC** Multiple failure conditions in an RSI command may return the same return code.

**R<sub>MLB</sub>DM** If an input to an RSI command uses an invalid encoding then the command fails and returns RSI\_ERROR\_INPUT.

Command inputs include registers and in-memory data structures.

Invalid encodings include:

- using a reserved encoding in an enumeration

See also:

- [B4.4.1 RsiCommandReturnCode type](#)

## B4.3 RSI commands

The following table summarizes the FIDs of commands in the RSI interface.

FID	Command
0xC4000195	<a href="#">RSI_ATTESTATION_TOKEN_CONTINUE</a>
0xC4000194	<a href="#">RSI_ATTESTATION_TOKEN_INIT</a>
0xC4000199	<a href="#">RSI_HOST_CALL</a>
0xC4000198	<a href="#">RSI_IPA_STATE_GET</a>
0xC4000197	<a href="#">RSI_IPA_STATE_SET</a>
0xC4000193	<a href="#">RSI_MEASUREMENT_EXTEND</a>
0xC4000192	<a href="#">RSI_MEASUREMENT_READ</a>
0xC4000196	<a href="#">RSI_REALM_CONFIG</a>
0xC4000190	<a href="#">RSI_VERSION</a>

### B4.3.1 RSI\_ATTESTATION\_TOKEN\_CONTINUE command

Continue the operation to retrieve an attestation token.

See also:

- [A7.2 Realm attestation](#)
- [B4.3.2 RSI\\_ATTESTATION\\_TOKEN\\_INIT command](#)

#### B4.3.1.1 Interface

##### B4.3.1.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000195
addr	X1	63:0	Address	IPA of the Granule to which the token will be written
offset	X2	63:0	UInt64	Offset within Granule to start of buffer in bytes
size	X3	63:0	UInt64	Size of buffer in bytes

##### B4.3.1.1.2 Context

The RSI\_ATTESTATION\_TOKEN\_CONTINUE command operates on the following context.

Name	Type	Value	Before	Description
realm	RmmRealm	CurrentRealm()	false	Current Realm
rec	RmmRec	CurrentRec()	false	Current REC

##### B4.3.1.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	RsiCommandReturnCode	Command return status
len	X1	63:0	UInt64	Number of bytes written to buffer

#### B4.3.1.2 Failure conditions

ID	Condition
addr_align	pre: !AddrIsGranuleAligned(addr) post: result == RSI_ERROR_INPUT
addr_bound	pre: !AddrIsProtected(addr, realm) post: result == RSI_ERROR_INPUT

ID	Condition
offset_bound	pre: offset >= RMM_GRANULE_SIZE post: result == RSI_ERROR_INPUT
size_bound	pre: offset + size > RMM_GRANULE_SIZE post: result == RSI_ERROR_INPUT
state	pre: rec.attest_state != ATTEST_IN_PROGRESS post: result == RSI_ERROR_STATE

#### B4.3.1.2.1 Failure condition ordering

The RSI\_ATTESTATION\_TOKEN\_CONTINUE command does not have any failure condition orderings.

#### B4.3.1.3 Success conditions

ID	Condition
incomplete	pre: Token generation is not complete. post: result == RSI_INCOMPLETE
complete	pre: Token generation is complete. post: rec.attest_state == NO_ATTEST_IN_PROGRESS

#### B4.3.1.4 Footprint

ID	Value
state	rec.attest_state

## B4.3.2 RSI\_ATTESTATION\_TOKEN\_INIT command

Initialize the operation to retrieve an attestation token.

See also:

- [A7.2 Realm attestation](#)
- [B4.3.1 RSI\\_ATTESTATION\\_TOKEN\\_CONTINUE command](#)

### B4.3.2.1 Interface

#### B4.3.2.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000194
challenge_0	X1	63:0	Bits64	Doubleword 0 of the challenge value
challenge_1	X2	63:0	Bits64	Doubleword 1 of the challenge value
challenge_2	X3	63:0	Bits64	Doubleword 2 of the challenge value
challenge_3	X4	63:0	Bits64	Doubleword 3 of the challenge value
challenge_4	X5	63:0	Bits64	Doubleword 4 of the challenge value
challenge_5	X6	63:0	Bits64	Doubleword 5 of the challenge value
challenge_6	X7	63:0	Bits64	Doubleword 6 of the challenge value
challenge_7	X8	63:0	Bits64	Doubleword 7 of the challenge value

#### B4.3.2.1.2 Context

The RSI\_ATTESTATION\_TOKEN\_INIT command operates on the following context.

Name	Type	Value	Before	Description
realm	<a href="#">RmmRealm</a>	<a href="#">CurrentRealm()</a>	false	Current Realm
rec	<a href="#">RmmRec</a>	<a href="#">CurrentRec()</a>	false	Current REC

#### B4.3.2.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RsiCommandReturnCode</a>	Command return status

### B4.3.2.2 Failure conditions

The RSI\_ATTESTATION\_TOKEN\_INIT command does not have any failure conditions.



### B4.3.2.3 Success conditions

ID	Condition
state	<code>rec.attest_state == ATTEST_IN_PROGRESS</code>
challenge	<code>rec.attest_challenge == [</code> <code>challenge_0,</code> <code>challenge_1,</code> <code>challenge_2,</code> <code>challenge_3,</code> <code>challenge_4,</code> <code>challenge_5,</code> <code>challenge_6,</code> <code>challenge_7</code> <code>]</code>

### B4.3.2.4 Footprint

ID	Value
state	<code>rec.attest_state</code>
challenge	<code>rec.attest_challenge</code>

### B4.3.3 RSI\_HOST\_CALL command

Make a Host call.

See also:

- [A4.5 Host call](#)

#### B4.3.3.1 Interface

##### B4.3.3.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000199
addr	X1	63:0	<a href="#">Address</a>	IPA of the Host call data structure

##### B4.3.3.1.2 Context

The RSI\_HOST\_CALL command operates on the following context.

Name	Type	Value	Before	Description
realm	<a href="#">RmmRealm</a>	<a href="#">CurrentRealm()</a>	false	Current Realm
rec	<a href="#">RmmRec</a>	<a href="#">CurrentRec()</a>	false	Current REC
data	<a href="#">RsiHostCall</a>	<a href="#">RealmHostCall(addr)</a>	false	Host call data structure

##### B4.3.3.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RsiCommandReturnCode</a>	Command return status

#### B4.3.3.2 Failure conditions

ID	Condition
addr_align	pre: <a href="#">!AddrIsAligned(addr, 256)</a> post: result == <a href="#">RSI_ERROR_INPUT</a>
addr_bound	pre: <a href="#">!AddrIsProtected(addr, realm)</a> post: result == <a href="#">RSI_ERROR_INPUT</a>

#### **B4.3.3.2.1 Failure condition ordering**

The RSI\_HOST\_CALL command does not have any failure condition orderings.

#### **B4.3.3.3 Success conditions**

The RSI\_HOST\_CALL command does not have any success conditions.

#### **B4.3.3.4 Footprint**

ID	Value
host_call	rec.host_call_pending

### B4.3.4 RSI\_IPA\_STATE\_GET command

Get RIPAS of a target page.

See also:

- [A5.2 Realm view of memory management](#)
- [B4.3.5 RSI\\_IPA\\_STATE\\_SET command](#)

#### B4.3.4.1 Interface

##### B4.3.4.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000198
addr	X1	63:0	<a href="#">Address</a>	IPA of target page

##### B4.3.4.1.2 Context

The RSI\_IPA\_STATE\_GET command operates on the following context.

Name	Type	Value	Before	Description
realm	<a href="#">RmmRealm</a>	<a href="#">CurrentRealm()</a>	false	Current Realm

##### B4.3.4.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RsiCommandReturnCode</a>	Command return status
ripas	X1	7:0	<a href="#">RsiRipas</a>	RIPAS value

The following unused bits of RSI\_IPA\_STATE\_GET output values must be zero: X1[63:8].

Note that the RIPAS of a Protected IPA can change at any time to DESTROYED without the Realm taking any action.

See also:

- [A5.2.5 Changes to RIPAS while Realm state is ACTIVE](#)

#### B4.3.4.2 Failure conditions

ID	Condition
addr_align	pre: <code>!AddrIsGranuleAligned(addr)</code> post: <code>result == RSI_ERROR_INPUT</code>

ID	Condition
addr_bound	pre: !AddrIsProtected(addr, realm) post: result == RSI_ERROR_INPUT

#### **B4.3.4.2.1 Failure condition ordering**

The RSI\_IPA\_STATE\_GET command does not have any failure condition orderings.

#### **B4.3.4.3 Success conditions**

The RSI\_IPA\_STATE\_GET command does not have any success conditions.

#### **B4.3.4.4 Footprint**

The RSI\_IPA\_STATE\_GET command does not have any footprint.

### B4.3.5 RSI\_IPA\_STATE\_SET command

Request RIPAS of a target IPA range to be changed to a specified value.

See also:

- [A5.2 Realm view of memory management](#)
- [A5.4 RIPAS change](#)
- [B4.3.4 RSI\\_IPA\\_STATE\\_GET command](#)

#### B4.3.5.1 Interface

##### B4.3.5.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000197
base	X1	63:0	Address	Base of target IPA region
top	X2	63:0	Address	Top of target IPA region
ripas	X3	7:0	RsiRipas	RIPAS value
flags	X4	63:0	RsiRipasChangeFlags	Flags

The following unused bits of RSI\_IPA\_STATE\_SET input values should be zero: X3[63:8].

##### B4.3.5.1.2 Context

The RSI\_IPA\_STATE\_SET command operates on the following context.

Name	Type	Value	Before	Description
realm	RmmRealm	CurrentRealm()	false	Current Realm
rec	RmmRec	CurrentRec()	false	Current REC

##### B4.3.5.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	RsiCommandReturnCode	Command return status
new_base	X1	63:0	Address	Base of IPA region which was not modified by the command
response	X2	0:0	RsiResponse	Whether the Host accepted or rejected the request

The following unused bits of RSI\_IPA\_STATE\_SET output values must be zero: X2[63:1].

### B4.3.5.2 Failure conditions

ID	Condition
base_align	pre: !AddrIsGranuleAligned(base) post: result == RSI_ERROR_INPUT
top_align	pre: !AddrIsGranuleAligned(top) post: result == RSI_ERROR_INPUT
size_valid	pre: UInt(top) <= UInt(base) post: result == RSI_ERROR_INPUT
rgn_bound	pre: !AddrRangeIsProtected(base, top, realm) post: result == RSI_ERROR_INPUT
ripas_valid	pre: (ripas != RSI_EMPTY) && (ripas != RSI_RAM) post: result == RSI_ERROR_INPUT

#### B4.3.5.2.1 Failure condition ordering

The RSI\_IPA\_STATE\_SET command does not have any failure condition orderings.

### B4.3.5.3 Success conditions

ID	Condition
new_base	new_base == rec.ripas_addr
response	response == RecRipasChangeResponse(rec)

### B4.3.5.4 Footprint

The RSI\_IPA\_STATE\_SET command does not have any footprint.

## B4.3.6 RSI\_MEASUREMENT\_EXTEND command

Extend Realm Extensible Measurement (REM) value.

### B4.3.6.1 Interface

#### B4.3.6.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000193
index	X1	63:0	UInt64	Measurement index
size	X2	63:0	UInt64	Measurement size in bytes
value_0	X3	63:0	Bits64	Doubleword 0 of the measurement value
value_1	X4	63:0	Bits64	Doubleword 1 of the measurement value
value_2	X5	63:0	Bits64	Doubleword 2 of the measurement value
value_3	X6	63:0	Bits64	Doubleword 3 of the measurement value
value_4	X7	63:0	Bits64	Doubleword 4 of the measurement value
value_5	X8	63:0	Bits64	Doubleword 5 of the measurement value
value_6	X9	63:0	Bits64	Doubleword 6 of the measurement value
value_7	X10	63:0	Bits64	Doubleword 7 of the measurement value

#### B4.3.6.1.2 Context

The RSI\_MEASUREMENT\_EXTEND command operates on the following context.

Name	Type	Value	Before	Description
realm	RmmRealm	CurrentRealm()	false	Current Realm
meas_old	RmmRealmMeasuremen	CurrentRealm(). ↪ measurements[index]	true	Previous measurement value

#### B4.3.6.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	RsiCommandReturnCode	Command return status



### B4.3.6.2 Failure conditions

ID	Condition
index_bound	pre: index < 1    index > 4 post: result == RSI_ERROR_INPUT
size_bound	pre: size > 64 post: result == RSI_ERROR_INPUT

#### B4.3.6.2.1 Failure condition ordering

The RSI\_MEASUREMENT\_EXTEND command does not have any failure condition orderings.

### B4.3.6.3 Success conditions

ID	Condition
realm_meas	realm.measurements[index] == RemExtend( realm.hash_algo, meas_old, [value_0, value_1, value_2, value_3, value_4, value_5, value_6, value_7][ (RMM_REALM_MEASUREMENT_WIDTH-1):0], size)

### B4.3.6.4 Footprint

ID	Value
realm_meas	realm.measurements[index]

### B4.3.7 RSI\_MEASUREMENT\_READ command

Read measurement for the current Realm.

See also:

- [A7.1 Realm measurements](#)
- [D1.2.1 Realm creation flow](#)

#### B4.3.7.1 Interface

##### B4.3.7.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000192
index	X1	63:0	<a href="#">UInt64</a>	Measurement index

`index` 0 selects the RIM. An `index` of 1 or greater selects the corresponding REM.

##### B4.3.7.1.2 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RsiCommandReturnCode</a>	Command return status
value_0	X1	63:0	<a href="#">Bits64</a>	Doubleword 0 of the Realm measurement identified by “index”
value_1	X2	63:0	<a href="#">Bits64</a>	Doubleword 1 of the Realm measurement identified by “index”
value_2	X3	63:0	<a href="#">Bits64</a>	Doubleword 2 of the Realm measurement identified by “index”
value_3	X4	63:0	<a href="#">Bits64</a>	Doubleword 3 of the Realm measurement identified by “index”
value_4	X5	63:0	<a href="#">Bits64</a>	Doubleword 4 of the Realm measurement identified by “index”
value_5	X6	63:0	<a href="#">Bits64</a>	Doubleword 5 of the Realm measurement identified by “index”
value_6	X7	63:0	<a href="#">Bits64</a>	Doubleword 6 of the Realm measurement identified by “index”
value_7	X8	63:0	<a href="#">Bits64</a>	Doubleword 7 of the Realm measurement identified by “index”

If the size of the measurement value is smaller than 512 bits, the output values are padded with zeroes.

#### B4.3.7.2 Failure conditions

ID	Condition
index_bound	pre: index > 4 post: result == <a href="#">RSI_ERROR_INPUT</a>

### B4.3.7.3 Success conditions

The RSI\_MEASUREMENT\_READ command does not have any success conditions.

### B4.3.7.4 Footprint

The RSI\_MEASUREMENT\_READ command does not have any footprint.

## B4.3.8 RSI\_REALM\_CONFIG command

Read configuration for the current Realm.

### B4.3.8.1 Interface

#### B4.3.8.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000196
addr	X1	63:0	Address	IPA of the Granule to which the configuration data will be written

#### B4.3.8.1.2 Context

The RSI\_REALM\_CONFIG command operates on the following context.

Name	Type	Value	Before	Description
realm	RmmRealm	CurrentRealm()	false	Current Realm
cfg	RsiRealmConfig	RealmConfig(addr)	false	Realm configuration

#### B4.3.8.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	RsiCommandReturnCode	Command return status

### B4.3.8.2 Failure conditions

ID	Condition
addr_align	pre: !AddrIsGranuleAligned(addr) post: result == RSI_ERROR_INPUT
addr_bound	pre: !AddrIsProtected(addr, realm) post: result == RSI_ERROR_INPUT

#### B4.3.8.2.1 Failure condition ordering

The RSI\_REALM\_CONFIG command does not have any failure condition orderings.

### B4.3.8.3 Success conditions

ID	Condition
ipa_width	<code>cfg.ipa_width == realm.ipa_width</code>
hash_algo	<code>Equal(cfg.hash_algo, realm.hash_algo)</code>

#### B4.3.8.4 Footprint

The RSI\_REALM\_CONFIG command does not have any footprint.

## B4.3.9 RSI\_VERSION command

Returns RSI version.

### B4.3.9.1 Interface

#### B4.3.9.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000190

#### B4.3.9.1.2 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">RsiInterfaceVersion</a>	Interface version

See also:

- [B4.1 RSI version](#)

### B4.3.9.2 Failure conditions

The RSI\_VERSION command does not have any failure conditions.

### B4.3.9.3 Success conditions

The RSI\_VERSION command does not have any success conditions.

### B4.3.9.4 Footprint

The RSI\_VERSION command does not have any footprint.

## B4.4 RSI types

This section defines types which are used in the RSI interface.

### B4.4.1 RsiCommandReturnCode type

The RsiCommandReturnCode enumeration represents a return code from an RSI command.

The RsiCommandReturnCode enumeration is a [concrete type](#).

The width of the RsiCommandReturnCode enumeration is 64 bits.

See also:

- [Chapter B1 Commands](#)

The values of the RsiCommandReturnCode enumeration are shown in the following table.

Encoding	Name	Description
0	RSI_SUCCESS	Command completed successfully
1	RSI_ERROR_INPUT	The value of a command input value caused the command to fail
2	RSI_ERROR_STATE	The state of the current Realm or current REC does not match the state expected by the command
3	RSI_INCOMPLETE	The operation requested by the command is not complete

Unused encodings for the RsiCommandReturnCode enumeration are reserved for use by future versions of this specification.

### B4.4.2 RsiHashAlgorithm type

The RsiHashAlgorithm enumeration represents hash algorithm.

The RsiHashAlgorithm enumeration is a [concrete type](#).

The width of the RsiHashAlgorithm enumeration is 8 bits.

See also:

- [B4.3.8 RSI\\_REALM\\_CONFIG command](#)

The values of the RsiHashAlgorithm enumeration are shown in the following table.

Encoding	Name	Description
0	RSI_HASH_SHA_256	SHA-256 ( <i>Secure Hash Standard (SHS)</i> <a href="#">[15]</a> )
1	RSI_HASH_SHA_512	SHA-512 ( <i>Secure Hash Standard (SHS)</i> <a href="#">[15]</a> )

Unused encodings for the RsiHashAlgorithm enumeration are reserved for use by future versions of this specification.

### B4.4.3 RsiHostCall type

The RsiHostCall structure contains data structure used to pass Host call arguments and return values.

The RsiHostCall structure is a [concrete type](#).

The width of the RsiHostCall structure is 256 (0x100) bytes.

See also:

- [A4.5 Host call](#)
- [B4.3.3 RSI\\_HOST\\_CALL command](#)

The members of the RsiHostCall structure are shown in the following table.

Name	Byte offset	Type	Description
imm	0x0	UInt16	Immediate value
gprs[0]	0x8	Bits64	Registers
gprs[1]	0x10	Bits64	Registers
gprs[2]	0x18	Bits64	Registers
gprs[3]	0x20	Bits64	Registers
gprs[4]	0x28	Bits64	Registers
gprs[5]	0x30	Bits64	Registers
gprs[6]	0x38	Bits64	Registers
gprs[7]	0x40	Bits64	Registers
gprs[8]	0x48	Bits64	Registers
gprs[9]	0x50	Bits64	Registers
gprs[10]	0x58	Bits64	Registers
gprs[11]	0x60	Bits64	Registers
gprs[12]	0x68	Bits64	Registers
gprs[13]	0x70	Bits64	Registers
gprs[14]	0x78	Bits64	Registers
gprs[15]	0x80	Bits64	Registers
gprs[16]	0x88	Bits64	Registers
gprs[17]	0x90	Bits64	Registers
gprs[18]	0x98	Bits64	Registers
gprs[19]	0xa0	Bits64	Registers
gprs[20]	0xa8	Bits64	Registers
gprs[21]	0xb0	Bits64	Registers
gprs[22]	0xb8	Bits64	Registers
gprs[23]	0xc0	Bits64	Registers
gprs[24]	0xc8	Bits64	Registers
gprs[25]	0xd0	Bits64	Registers



Name	Byte offset	Type	Description
gprs[26]	0xd8	Bits64	Registers
gprs[27]	0xe0	Bits64	Registers
gprs[28]	0xe8	Bits64	Registers
gprs[29]	0xf0	Bits64	Registers
gprs[30]	0xf8	Bits64	Registers

Unused bits of the RsiHostCall structure should be zero.

#### B4.4.4 RsilInterfaceVersion type

The `RsiInterfaceVersion` fieldset contains an RSI interface version.

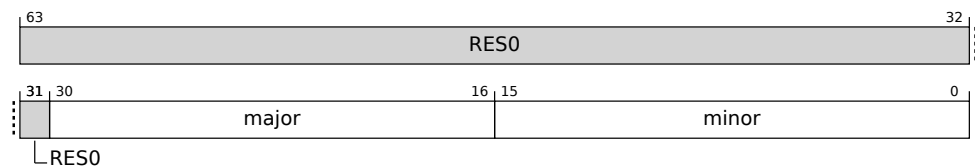
The RsiInterfaceVersion fieldset is a **concrete type**.

The width of the RsiInterfaceVersion fieldset is 64 bits.

See also:

- B4.1 *RSI version*
- B4.3.9 *RSI\_VERSION* *command*

The fields of the RsiInterfaceVersion fieldset are shown in the following diagram.



The fields of the RsiInterfaceVersion fieldset are shown in the following table.

Name	Bits	Description	Value
minor	15:0	Interface minor version number (the value $y$ in interface version $x.y$ )	UInt16
major	30:16	Interface major version number (the value $x$ in interface version $x.y$ )	UInt15
	63:31	Reserved	Should be zero

#### B4.4.5 RsiRealmConfig type

The `RsiRealmConfig` structure contains realm configuration.

The RsiRealmConfig structure is a **concrete type**.

The width of the RsiRealmConfig structure is 4096 (0x1000) bytes.

See also:

- B4.3.8 *RSI\_REALM\_CONFIG* command

The members of the RsiRealmConfig structure are shown in the following table.

Name	Byte offset	Type	Description
ipa_width	0x0	UInt64	IPA width in bits
hash_algo	0x8	RsiHashAlgorithm	Hash algorithm

Unused bits of the RsiRealmConfig structure must be zero.

#### B4.4.6 RsiResponse type

The RsiResponse enumeration represents whether the Host accepted or rejected a Realm request.

The RsiResponse enumeration is a [concrete type](#).

The width of the RsiResponse enumeration is 1 bits.

The values of the RsiResponse enumeration are shown in the following table.

Encoding	Name	Description
0	RSI_ACCEPT	Host accepted the Realm request.
1	RSI_REJECT	Host rejected the Realm request.

#### B4.4.7 RsiRipas type

The RsiRipas enumeration represents realm IPA state.

The RsiRipas enumeration is a [concrete type](#).

The width of the RsiRipas enumeration is 8 bits.

See also:

- [A5.4 RIPAS change](#)
- [B4.3.4 RSI\\_IPA\\_STATE\\_GET command](#)
- [B4.3.5 RSI\\_IPA\\_STATE\\_SET command](#)

The values of the RsiRipas enumeration are shown in the following table.

Encoding	Name	Description
0	RSI_EMPTY	Address where no Realm resources are mapped.
1	RSI_RAM	Address where private code or data owned by the Realm is mapped.
2	RSI_DESTROYED	Address which is inaccessible to the Realm due to an action taken by the Host.

Unused encodings for the RsiRipas enumeration are reserved for use by future versions of this specification.

### B4.4.8 RsiRipasChangeDestroyed type

The RsiRipasChangeDestroyed enumeration represents whether a RIPAS change from DESTROYED should be permitted.

The RsiRipasChangeDestroyed enumeration is a [concrete type](#).

The width of the RsiRipasChangeDestroyed enumeration is 1 bits.

The values of the RsiRipasChangeDestroyed enumeration are shown in the following table.

Encoding	Name	Description
0	RSI_NO_CHANGE_DESTROYED	A RIPAS change from DESTROYED should not be permitted.
1	RSI_CHANGE_DESTROYED	A RIPAS change from DESTROYED should be permitted.

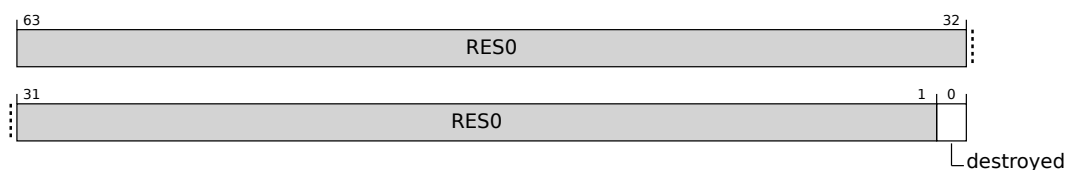
### B4.4.9 RsiRipasChangeFlags type

The RsiRipasChangeFlags fieldset contains flags provided by the Realm when requesting a RIPAS change.

The RsiRipasChangeFlags fieldset is a [concrete type](#).

The width of the RsiRipasChangeFlags fieldset is 64 bits.

The fields of the RsiRipasChangeFlags fieldset are shown in the following diagram.



The fields of the RsiRipasChangeFlags fieldset are shown in the following table.

Name	Bits	Description	Value
destroyed	0:0	Whether a RIPAS change from DESTROYED should be permitted	<a href="#">RsiRipasChangeDestroyed</a>
	63:1	Reserved	Should be zero

## Chapter B5

# Power State Control Interface

This section describes how Power State Control Interface (PSCI) function execution by a Realm execution of SMC instructions is handled.

## B5.1 PSCI overview

I<sub>GBVWX</sub>

In this section,

- `rec` refers to the currently executing REC
- `exit` refer to the RecExit object which was provided to the RMI\_REC\_ENTER command
- `target_rec` refers to the REC object identified by an MPIDR value passed to a PSCI function.

I<sub>GHKCJ</sub>

The RMM provides a trusted implementation of parts of the PSCI ABI. This section describes the checks performed by the RMM when a Realm executes a PSCI command, and the internal RMM state changes which result from a successful PSCI command execution. Successful execution by the RMM of some PSCI commands results in a *REC exit due to PSCI*, which allows the Host to perform further processing of the command.

I<sub>XHDQF</sub>

The HVC conduit for PSCI is not supported for Realms.

See also:

- *Arm Power State Coordination Interface (PSCI)* [16]
- [A2.3.2 REC attributes](#)
- [A4.3.7 REC exit due to PSCI](#)
- [A4.5 Host call](#)
- [D1.4 PSCI flows](#)

## B5.2 PSCI version

R<sub>TFCVF</sub>

The RMM must support version  $\geq$  1.1 of the Power State Control Interface.

See also:

- [B5.3.8 PSCI\\_VERSION command](#)

## B5.3 PSCI commands

The following table summarizes the FIDs of commands in the PSCI interface.

FID	Command
0xC4000004	PSCI_AFFINITY_INFO
0x84000002	PSCI_CPU_OFF
0xC4000003	PSCI_CPU_ON
0xC4000001	PSCI_CPU_SUSPEND
0x8400000A	PSCI_FEATURES
0x84000008	PSCI_SYSTEM_OFF
0x84000009	PSCI_SYSTEM_RESET
0x84000000	PSCI_VERSION

### B5.3.1 PSCI\_AFFINITY\_INFO command

Query status of a VPE.

This command causes a REC exit due to PSCI. In response, the Host should provide the target REC (identified by `target_affinity`) by calling `RMI_PSCI_COMPLETE`.

See also:

- [A2.3.2 REC attributes](#)
- [A4.3.7 REC exit due to PSCI](#)
- [B3.3.7 RMI\\_PSCI\\_COMPLETE command](#)
- [B5.3.2 PSCI\\_CPU\\_OFF command](#)
- [B5.3.3 PSCI\\_CPU\\_ON command](#)

#### B5.3.1.1 Interface

##### B5.3.1.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000004
target_affinity	X1	63:0	Bits64	This parameter contains a copy of the affinity fields of the MPIDR register
lowest_affinity_level	X2	31:0	UInt32	Denotes the lowest affinity level field that is valid in the <code>target_affinity</code> parameter

The following unused bits of `PSCI_AFFINITY_INFO` input values should be zero: X2[63:32].

##### B5.3.1.1.2 Context

The `PSCI_AFFINITY_INFO` command operates on the following context.

Name	Type	Value	Before	Description
target_rec	RmmRec	RecFromMpidr( target_affinity)	false	Target REC

##### B5.3.1.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	31:0	PsciReturnCode	Command return code

The following unused bits of `PSCI_AFFINITY_INFO` output values must be zero: X0[63:32].

#### B5.3.1.2 Failure conditions

ID	Condition
target_bound	pre: lowest_affinity_level != 0 post: result == PSCI_INVALID_PARAMETERS
target_match	pre: !MpidrIsUsed(target_affinity) post: result == PSCI_INVALID_PARAMETERS

#### B5.3.1.2.1 Failure condition ordering

The PSCI\_AFFINITY\_INFO command does not have any failure condition orderings.

#### B5.3.1.3 Success conditions

ID	Condition
runnable	pre: target_rec.flags.runnable == RUNNABLE post: result == PSCI_SUCCESS
not_runnable	pre: target_rec.flags.runnable == NOT_RUNNABLE post: result == PSCI_OFF

#### B5.3.1.4 Footprint

The PSCI\_AFFINITY\_INFO command does not have any footprint.



## B5.3.2 PSCI\_CPU\_OFF command

Power down the calling core.

This command causes a REC exit due to PSCI.

See also:

- [A2.3.2 REC attributes](#)
- [A4.3.7 REC exit due to PSCI](#)
- [B5.3.3 PSCI\\_CPU\\_ON command](#)
- [B5.3.4 PSCI\\_CPU\\_SUSPEND command](#)

### B5.3.2.1 Interface

#### B5.3.2.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0x84000002

#### B5.3.2.1.2 Context

The PSCI\_CPU\_OFF command operates on the following context.

Name	Type	Value	Before	Description
rec	RmmRec	CurrentRec()	false	Current REC

#### B5.3.2.1.3 Output values

The PSCI\_CPU\_OFF command does not have any output values.

Following execution of PSCI\_CPU\_OFF, control does not return to the caller.

### B5.3.2.2 Failure conditions

The PSCI\_CPU\_OFF command does not have any failure conditions.

### B5.3.2.3 Success conditions

The PSCI\_CPU\_OFF command does not have any success conditions.

Following execution of PSCI\_CPU\_OFF, control does not return to the caller.

### B5.3.2.4 Footprint

The PSCI\_CPU\_OFF command does not have any footprint.

### B5.3.3 PSCI\_CPU\_ON command

Power up a core.

This command causes a REC exit due to PSCI. In response, the Host should provide the target REC (identified by `target_cpu`) by calling `RMI_PSCI_COMPLETE`.

See also:

- [A2.3.2 REC attributes](#)
- [A4.3.7 REC exit due to PSCI](#)
- [B3.3.7 RMI\\_PSCI\\_COMPLETE command](#)
- [B5.3.2 PSCI\\_CPU\\_OFF command](#)
- [B5.3.4 PSCI\\_CPU\\_SUSPEND command](#)
- [D1.4.1 PSCI\\_CPU\\_ON flow](#)

#### B5.3.3.1 Interface

##### B5.3.3.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0xC4000003
target_cpu	X1	63:0	<a href="#">Bits64</a>	This parameter contains a copy of the affinity fields of the MPIDR register
entry_point_address	X2	63:0	<a href="#">Address</a>	Address at which the core must resume execution
context_id	X3	31:0	<a href="#">UInt32</a>	This parameter is only meaningful to the caller (must be present in X0 of the target PE upon first entry to Non-Secure exception level)

The following unused bits of PSCI\_CPU\_ON input values should be zero: X3[63:32].

##### B5.3.3.1.2 Context

The PSCI\_CPU\_ON command operates on the following context.

Name	Type	Value	Before	Description
realm	<a href="#">RmmRealm</a>	<a href="#">CurrentRealm()</a>	false	Current Realm
target_rec	<a href="#">RmmRec</a>	<a href="#">RecFromMpidr(target_cpu)</a>	false	Target REC

##### B5.3.3.1.3 Output values

Name	Register	Bits	Type	Description
result	X0	31:0	<a href="#">PsciReturnCode</a>	Command return code

The following unused bits of PSCI\_CPU\_ON output values must be zero: X0[63:32].

### B5.3.3.2 Failure conditions

ID	Condition
entry	pre: !AddrIsProtected(entry_point_address, realm) post: result == PSCI_INVALID_ADDRESS
mpidr	pre: !MpidrIsUsed(target_cpu) post: result == PSCI_INVALID_PARAMETERS
runnable	pre: target_rec.flags.runnable == RUNNABLE post: result == PSCI_ALREADY_ON

#### B5.3.3.2.1 Failure condition ordering

The PSCI\_CPU\_ON command does not have any failure condition orderings.

### B5.3.3.3 Success conditions

ID	Condition
entry	target_rec.pc == ToBits64(UInt(entry_point_address))
runnable	target_rec.flags.runnable == RUNNABLE

### B5.3.3.4 Footprint

ID	Value
runnable	target_rec.flags.runnable

### B5.3.4 PSCI\_CPU\_SUSPEND command

Suspend execution on the calling VPE.

This command causes a REC exit due to PSCI.

See also:

- [A4.3.7 REC exit due to PSCI](#)
- [B5.3.2 PSCI\\_CPU\\_OFF command](#)
- [B5.3.3 PSCI\\_CPU\\_ON command](#)

#### B5.3.4.1 Interface

##### B5.3.4.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0xC4000001
power_state	X1	31:0	UInt32	Identifier for a specific local state
entry_point_address	X2	63:0	Address	Address at which the core must resume execution
context_id	X3	63:0	UInt64	This parameter is only meaningful to the caller (must be present in X0 upon first entry to Non- Secure exception level)

The following unused bits of PSCI\_CPU\_SUSPEND input values should be zero: X1[63:32].

The RMM treats all target power states as suspend requests, and therefore the `entry_point_address` and `context_id` arguments are ignored.

##### B5.3.4.1.2 Output values

The PSCI\_CPU\_SUSPEND command does not have any output values.

Following execution of PSCI\_CPU\_SUSPEND, control does not return to the caller.

#### B5.3.4.2 Failure conditions

The PSCI\_CPU\_SUSPEND command does not have any failure conditions.

#### B5.3.4.3 Success conditions

The PSCI\_CPU\_SUSPEND command does not have any success conditions.

Following execution of PSCI\_CPU\_SUSPEND, control does not return to the caller.

#### B5.3.4.4 Footprint

The PSCI\_CPU\_SUSPEND command does not have any footprint.

### B5.3.5 PSCI\_FEATURES command

Query whether a specific PSCI feature is implemented.

See also:

- [B5.3.1 PSCI\\_AFFINITY\\_INFO command](#)
- [B5.3.2 PSCI\\_CPU\\_OFF command](#)
- [B5.3.3 PSCI\\_CPU\\_ON command](#)
- [B5.3.4 PSCI\\_CPU\\_SUSPEND command](#)
- [B5.3.6 PSCI\\_SYSTEM\\_OFF command](#)
- [B5.3.7 PSCI\\_SYSTEM\\_RESET command](#)

#### B5.3.5.1 Interface

##### B5.3.5.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0x8400000A
psci_func_id	X1	31:0	UInt32	Function ID for a PSCI Function

The following unused bits of PSCI\_FEATURES input values should be zero: X1[63:32].

##### B5.3.5.1.2 Output values

Name	Register	Bits	Type	Description
result	X0	31:0	PsciReturnCode	Command return code

The following unused bits of PSCI\_FEATURES output values must be zero: X0[63:32].

#### B5.3.5.2 Failure conditions

The PSCI\_FEATURES command does not have any failure conditions.

#### B5.3.5.3 Success conditions

ID	Condition
func_ok	pre: psci_func_id is a supported PSCI function. post: result == PSCI_SUCCESS
func_not_ok	pre: psci_func_id is not a supported PSCI function. post: result == PSCI_NOT_SUPPORTED

#### **B5.3.5.4 Footprint**

The PSCI\_FEATURES command does not have any footprint.

## B5.3.6 PSCI\_SYSTEM\_OFF command

Shut down the system.

This command causes a REC exit due to PSCI.

See also:

- [A2.3.2 REC attributes](#)
- [A4.3.7 REC exit due to PSCI](#)
- [B5.3.7 PSCI\\_SYSTEM\\_RESET command](#)

### B5.3.6.1 Interface

#### B5.3.6.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0x84000008

#### B5.3.6.1.2 Context

The PSCI\_SYSTEM\_OFF command operates on the following context.

Name	Type	Value	Before	Description
realm	RmmRealm	CurrentRealm()	false	Current Realm

#### B5.3.6.1.3 Output values

The PSCI\_SYSTEM\_OFF command does not have any output values.

Following execution of PSCI\_SYSTEM\_OFF, control does not return to the caller.

### B5.3.6.2 Failure conditions

The PSCI\_SYSTEM\_OFF command does not have any failure conditions.

### B5.3.6.3 Success conditions

ID	Condition
state	realm.state == SYSTEM_OFF

Following execution of PSCI\_SYSTEM\_OFF, control does not return to the caller.

### B5.3.6.4 Footprint

The PSCI\_SYSTEM\_OFF command does not have any footprint.

### B5.3.7 PSCI\_SYSTEM\_RESET command

Shut down the system.

This command causes a REC exit due to PSCI.

See also:

- [A2.3.2 REC attributes](#)
- [A4.3.7 REC exit due to PSCI](#)
- [B5.3.6 PSCI\\_SYSTEM\\_OFF command](#)

#### B5.3.7.1 Interface

##### B5.3.7.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	UInt64	FID, value 0x84000009

##### B5.3.7.1.2 Context

The PSCI\_SYSTEM\_RESET command operates on the following context.

Name	Type	Value	Before	Description
realm	RmmRealm	CurrentRealm()	false	Current Realm

##### B5.3.7.1.3 Output values

The PSCI\_SYSTEM\_RESET command does not have any output values.

Following execution of PSCI\_SYSTEM\_RESET, control does not return to the caller.

#### B5.3.7.2 Failure conditions

The PSCI\_SYSTEM\_RESET command does not have any failure conditions.

#### B5.3.7.3 Success conditions

ID	Condition
state	realm.state == SYSTEM_OFF

Following execution of PSCI\_SYSTEM\_RESET, control does not return to the caller.

#### B5.3.7.4 Footprint

The PSCI\_SYSTEM\_RESET command does not have any footprint.



## B5.3.8 PSCI\_VERSION command

Query the version of PSCI implemented.

### B5.3.8.1 Interface

#### B5.3.8.1.1 Input values

Name	Register	Bits	Type	Description
fid	X0	63:0	<a href="#">UInt64</a>	FID, value 0x84000000

#### B5.3.8.1.2 Output values

Name	Register	Bits	Type	Description
result	X0	63:0	<a href="#">PsciInterfaceVersion</a>	Interface version

See also:

- [B5.2 PSCI version](#)

### B5.3.8.2 Failure conditions

The PSCI\_VERSION command does not have any failure conditions.

### B5.3.8.3 Success conditions

The PSCI\_VERSION command does not have any success conditions.

### B5.3.8.4 Footprint

The PSCI\_VERSION command does not have any footprint.

## B5.4 PSCI types

This section defines types which are used in the PSCI interface.

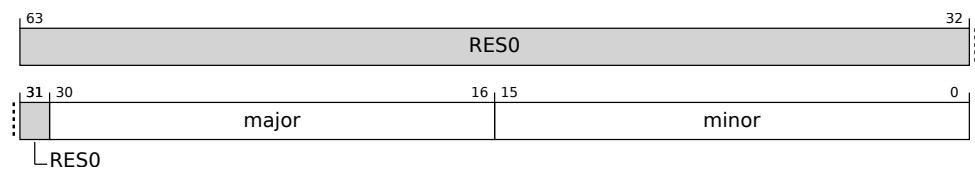
### B5.4.1 PscilInterfaceVersion type

The PsciInterfaceVersion fieldset contains an PSCI interface version.

The PsciInterfaceVersion fieldset is a **concrete type**.

The width of the PsciInterfaceVersion fieldset is 64 bits.

The fields of the PsciInterfaceVersion fieldset are shown in the following diagram.



The fields of the PsciInterfaceVersion fieldset are shown in the following table.

Name	Bits	Description	Value
minor	15:0	Interface minor version number (the value $y$ in interface version $x.y$ )	UInt16
major	30:16	Interface major version number (the value $x$ in interface version $x.y$ )	UInt15
	63:31	Reserved	Must be zero

### B5.4.2 PsciReturnCode type

The `PsciReturnCode` enumeration represents the return code of a PSCI command.

The PsciReturnCode enumeration is a **concrete type**.

The width of the PsciReturnCode enumeration is 32 bits.

The values of the PsciReturnCode enumeration are shown in the following table.

Encoding	Name	Description
-9	PSCI_INVALID_ADDRESS	Refer to PSCI specification
-8	PSCI_DISABLED	Refer to PSCI specification
-7	PSCI_NOT_PRESENT	Refer to PSCI specification
-6	PSCI_INTERNAL_FAILURE	Refer to PSCI specification
-5	PSCI_ON_PENDING	Refer to PSCI specification
-4	PSCI_ALREADY_ON	Refer to PSCI specification
-3	PSCI_DENIED	Refer to PSCI specification
-2	PSCI_INVALID_PARAMETERS	Refer to PSCI specification

Encoding	Name	Description
-1	PSCI_NOT_SUPPORTED	Refer to PSCI specification
0	PSCI_SUCCESS	Refer to PSCI specification
1	PSCI_OFF	Refer to PSCI specification

Unused encodings for the PsciReturnCode enumeration are reserved for use by future versions of this specification.

## **Part C**

### **Types**

## Chapter C1

### RMM types

This section describes types which are used to model the abstract state of the RMM.

#### C1.1 RmmGranule type

The RmmGranule structure contains attributes of a Granule.

The RmmGranule structure is an [abstract type](#).

The members of the RmmGranule structure are shown in the following table.

Name	Type	Description
pas	<a href="#">RmmPhysicalAddressSpace</a>	Physical Address Space
state	<a href="#">RmmGranuleState</a>	Lifecycle state

#### C1.2 RmmGranuleState type

The RmmGranuleState enumeration represents the state of a granule.

The RmmGranuleState enumeration is an [abstract type](#).

The values of the RmmGranuleState enumeration are shown in the following table.

Name	Description
DATA	Realm code or data.
DELEGATED	Delegated for use by the RMM.
RD	Realm Descriptor.
REC	Realm Execution Context.
REC_AUX	Realm Execution Context auxiliary Granule.
RTT	Realm Translation Table.
UNDELEGATED	Not delegated for use by the RMM.

### C1.3 RmmHashAlgorithm type

The RmmHashAlgorithm enumeration represents hash algorithm.

The RmmHashAlgorithm enumeration is an [abstract type](#).

The values of the RmmHashAlgorithm enumeration are shown in the following table.

Name	Description
HASH_SHA_256	SHA-256 ( <i>Secure Hash Standard (SHS)</i> <a href="#">[15]</a> )
HASH_SHA_512	SHA-512 ( <i>Secure Hash Standard (SHS)</i> <a href="#">[15]</a> )

### C1.4 RmmHostCallPending type

The RmmHostCallPending enumeration represents whether a Host call is pending.

The RmmHostCallPending enumeration is an [abstract type](#).

The values of the RmmHostCallPending enumeration are shown in the following table.

Name	Description
HOST_CALL_PENDING	No Host call is pending.
NO_HOST_CALL_PENDING	A Host call is pending.

### C1.5 RmmMeasurementDescriptorData type

The RmmMeasurementDescriptorData structure contains data structure used to calculate the contribution to the RIM of a DATA Granule.

The RmmMeasurementDescriptorData structure is a [concrete type](#).

The width of the RmmMeasurementDescriptorData structure is 256 (0x100) bytes.

See also:

- [B3.3.1.4 RMI\\_DATA\\_CREATE extension of RIM](#)

The members of the RmmMeasurementDescriptorData structure are shown in the following table.

Name	Byte offset	Type	Description
desc_type	0x0	<a href="#">Bits8</a>	Measurement descriptor type, value 0x0
len	0x8	<a href="#">UInt64</a>	Length of this data structure in bytes
rim	0x10	<a href="#">RmmRealmMeasurement</a>	Current RIM value
ipa	0x50	<a href="#">Address</a>	IPA at which the DATA Granule is mapped in the Realm
flags	0x58	<a href="#">RmiDataFlags</a>	Flags provided by Host
content	0x60	<a href="#">RmmRealmMeasurement</a>	Hash of contents of DATA Granule, or zero if flags indicate DATA Granule contents are unmeasured

Unused bits of the RmmMeasurementDescriptorData structure must be zero.

## C1.6 RmmMeasurementDescriptorRec type

The RmmMeasurementDescriptorRec structure contains data structure used to calculate the contribution to the RIM of a REC.

The RmmMeasurementDescriptorRec structure is a [concrete type](#).

The width of the RmmMeasurementDescriptorRec structure is 256 (0x100) bytes.

See also:

- [B3.3.12.4 RMI\\_REC\\_CREATE extension of RIM](#)

The members of the RmmMeasurementDescriptorRec structure are shown in the following table.

Name	Byte offset	Type	Description
desc_type	0x0	<a href="#">Bits8</a>	Measurement descriptor type, value 0x1
len	0x8	<a href="#">UInt64</a>	Length of this data structure in bytes
rim	0x10	<a href="#">RmmRealmMeasurement</a>	Current RIM value
content	0x50	<a href="#">RmmRealmMeasurement</a>	Hash of 4KB page which contains REC parameters data structure

Unused bits of the RmmMeasurementDescriptorRec structure must be zero.

## C1.7 RmmMeasurementDescriptorRipas type

The RmmMeasurementDescriptorRipas structure contains data structure used to calculate the contribution to the RIM of a RIPAS change.

The RmmMeasurementDescriptorRipas structure is a [concrete type](#).

The width of the RmmMeasurementDescriptorRipas structure is 256 (0x100) bytes.

See also:

- [B3.3.18.4 RMI\\_RTT\\_INIT\\_RIPAS extension of RIM](#)

The members of the RmmMeasurementDescriptorRipas structure are shown in the following table.

Name	Byte offset	Type	Description
desc_type	0x0	<a href="#">Bits8</a>	Measurement descriptor type, value 0x2
len	0x8	<a href="#">UInt64</a>	Length of this data structure in bytes
rim	0x10	<a href="#">RmmRealmMeasurement</a>	Current RIM value
base	0x50	<a href="#">Address</a>	Base IPA of the RIPAS change
top	0x58	<a href="#">Address</a>	Top IPA of the RIPAS change

Unused bits of the RmmMeasurementDescriptorRipas structure must be zero.

## C1.8 RmmPhysicalAddressSpace type

The RmmPhysicalAddressSpace enumeration represents the PAS of a Granule.

The RmmPhysicalAddressSpace enumeration is an [abstract type](#).

The values of the RmmPhysicalAddressSpace enumeration are shown in the following table.

Name	Description
NS	Non-secure PAS.
OTHER	PAS other than Non-secure or Realm.
REALM	Realm PAS.

## C1.9 RmmPsciPending type

The RmmPsciPending enumeration represents whether a PSCI request is pending.

The RmmPsciPending enumeration is an [abstract type](#).

The values of the RmmPsciPending enumeration are shown in the following table.

Name	Description
NO_PSCI_REQUEST_PENDING	A PSCI request is pending.
PSCI_REQUEST_PENDING	No PSCI request is pending.



## C1.10 RmmRealm type

The RmmRealm structure contains attributes of a Realm.

The RmmRealm structure is an [abstract type](#).

See also:

- [A2.1 Realm](#)

The members of the RmmRealm structure are shown in the following table.

Name	Type	Description
ipa_width	UInt8	IPA width in bits
measurements	RmmRealmMeasurement[5]	Realm measurements
hash_algo	RmmHashAlgorithm	Algorithm used to compute Realm measurements
rec_index	UInt64	Index of next REC to be created
rtt_base	Address	Realm Translation Table base address
rtt_level_start	Int64	RTT starting level
rtt_num_start	UInt64	Number of physically contiguous starting level RTTs
state	RmmRealmState	Lifecycle state
vmid	Bits16	Virtual Machine Identifier
rpv	Bits512	Realm Personalization Value

## C1.11 RmmRealmMeasurement type

The RmmRealmMeasurement type is realm measurement.

The RmmRealmMeasurement type is a [concrete type](#).

The width of the RmmRealmMeasurement type is 512 bits.

## C1.12 RmmRealmState type

The RmmRealmState enumeration represents the state of a Realm.

The RmmRealmState enumeration is an [abstract type](#).

The values of the RmmRealmState enumeration are shown in the following table.

Name	Description
ACTIVE	Eligible for execution.
NEW	Under construction. Not eligible for execution.
SYSTEM_OFF	System has been turned off. Not eligible for execution.

## C1.13 RmmRec type

The RmmRec structure contains attributes of a REC.

The RmmRec structure is an [abstract type](#).

See also:

- [A2.3 Realm Execution Context](#)

The members of the RmmRec structure are shown in the following table.

Name	Type	Description
attest_state	<a href="#">RmmRecAttestState</a>	Attestation token generation state
attest_challenge	<a href="#">Bits512</a>	Challenge for under-construction attestation token
aux	<a href="#">Address</a> [16]	Addresses of auxiliary Granules
emulatable_abort	<a href="#">RmmRecEmulatableAbort</a>	Whether the most recent exit from this REC was due to an Emulatable Data Abort
flags	<a href="#">RmmRecFlags</a>	Flags which control REC behavior
gprs	<a href="#">Bits64</a> [32]	General-purpose register values
mpidr	<a href="#">Bits64</a>	MPIDR value
owner	<a href="#">Address</a>	PA of RD of Realm which owns this REC
pc	<a href="#">Bits64</a>	Program counter value
psci_pending	<a href="#">RmmPsciPending</a>	Whether a PSCI request is pending
state	<a href="#">RmmRecState</a>	Lifecycle state
sysregs	<a href="#">RmmSystemRegisters</a>	EL1 and EL0 system register values
ripas_addr	<a href="#">Address</a>	Next address to be processed in RIPAS change
ripas_top	<a href="#">Address</a>	Top address of pending RIPAS change
ripas_value	<a href="#">RmmRipas</a>	RIPAS value of pending RIPAS change
ripas_destroyed	<a href="#">RmmRipasChangeDestroyed</a>	Whether a RIPAS change from DESTROYED should be permitted
ripas_response	<a href="#">RmmRecResponse</a>	Host response to RIPAS change request
host_call_pending	<a href="#">RmmHostCallPending</a>	Whether a Host call is pending

## C1.14 RmmRecAttestState type

The RmmRecAttestState enumeration represents whether an attestation token generation operation is ongoing on this REC.

The RmmRecAttestState enumeration is an [abstract type](#).

The values of the RmmRecAttestState enumeration are shown in the following table.

Name	Description
ATTEST_IN_PROGRESS	An attestation token generation operation is in progress.
NO_ATTEST_IN_PROGRESS	No attestation token generation operation is in progress.

## C1.15 RmmRecEmulatableAbort type

The RmmRecEmulatableAbort enumeration represents whether the most recent exit from a REC was due to an Emulatable Data Abort.

The RmmRecEmulatableAbort enumeration is an [abstract type](#).

The values of the RmmRecEmulatableAbort enumeration are shown in the following table.

Name	Description
EMULATABLE_ABORT	The most recent exit from a REC was due to an Emulatable Data Abort.
NOT_EMULATABLE_ABORT	The most recent exit from a REC was not due to an Emulatable Data Abort.

## C1.16 RmmRecFlags type

The RmmRecFlags structure contains REC flags.

The RmmRecFlags structure is an [abstract type](#).

The members of the RmmRecFlags structure are shown in the following table.

Name	Type	Description
runnable	<a href="#">RmmRecRunnable</a>	Whether the REC is eligible to run

## C1.17 RmmRecResponse type

The RmmRecResponse enumeration represents whether the Host accepted or rejected a Realm request.

The RmmRecResponse enumeration is an [abstract type](#).

The values of the RmmRecResponse enumeration are shown in the following table.

Name	Description
ACCEPT	Host accepted the Realm request.
REJECT	Host rejected the Realm request.

## C1.18 RmmRecRunnable type

The RmmRecRunnable enumeration represents whether a REC is eligible for execution.

The RmmRecRunnable enumeration is an [abstract type](#).

The values of the RmmRecRunnable enumeration are shown in the following table.

Name	Description
NOT_RUNNABLE	Not eligible for execution.
RUNNABLE	Eligible for execution.

## C1.19 RmmRecState type

The RmmRecState enumeration represents the state of a REC.

The RmmRecState enumeration is an [abstract type](#).

The values of the RmmRecState enumeration are shown in the following table.

Name	Description
READY	REC is not currently running.
RUNNING	REC is currently running.

## C1.20 RmmRipas type

The RmmRipas enumeration represents realm IPA state.

The RmmRipas enumeration is an [abstract type](#).

The values of the RmmRipas enumeration are shown in the following table.

Name	Description
DESTROYED	Address which is inaccessible to the Realm due to an action taken by the Host.
EMPTY	Address where no Realm resources are mapped.
RAM	Address where private code or data owned by the Realm is mapped.

## C1.21 RmmRipasChangeDestroyed type

The RmmRipasChangeDestroyed enumeration represents whether a RIPAS change from DESTROYED should be permitted.

The RmmRipasChangeDestroyed enumeration is an [abstract type](#).

The values of the RmmRipasChangeDestroyed enumeration are shown in the following table.

Name	Description
CHANGE_DESTROYED	A RIPAS change from DESTROYED should be permitted.
NO_CHANGE_DESTROYED	A RIPAS change from DESTROYED should not be permitted.

## C1.22 RmmRtt type

The RmmRtt structure contains an RTT.

The RmmRtt structure is an [abstract type](#).

The members of the RmmRtt structure are shown in the following table.

Name	Type	Description
entries	<a href="#">RmmRttEntry</a> [512]	Entries

## C1.23 RmmRttEntry type

The RmmRttEntry structure contains attributes of an RTT Entry.

The RmmRttEntry structure is an [abstract type](#).

See also:

- [A5.5 Realm Translation Table](#)

The members of the RmmRttEntry structure are shown in the following table.

Name	Type	Description
addr	<a href="#">Address</a>	Output address
ripas	<a href="#">RmmRipas</a>	RIPAS
state	<a href="#">RmmRttEntryState</a>	State
MemAttr	<a href="#">Bits3</a>	MemAttr
S2AP	<a href="#">Bits2</a>	S2AP
SH	<a href="#">Bits2</a>	SH

## C1.24 RmmRttEntryState type

The RmmRttEntryState enumeration represents the state of an RTTE.

The RmmRttEntryState enumeration is an [abstract type](#).

The values of the RmmRttEntryState enumeration are shown in the following table.

Name	Description
ASSIGNED	This RTTE is identified by a Protected IPA. The output address of this RTTE points to a DATA Granule.
ASSIGNED_NS	This RTTE is identified by an Unprotected IPA. The output address of this RTTE points to an NS Granule.
TABLE	The output address of this RTTE points to the next-level RTT.
UNASSIGNED	This RTTE is identified by a Protected IPA. This RTTE is not associated with any Granule.
UNASSIGNED_NS	This RTTE is identified by an Unprotected IPA. This RTTE is not associated with any Granule.

## C1.25 RmmRttWalkResult type

The RmmRttWalkResult structure contains result of an RTT walk.

The RmmRttWalkResult structure is an [abstract type](#).

See also:

- [A5.5.10 RTT walk](#)

The members of the RmmRttWalkResult structure are shown in the following table.

Name	Type	Description
level	<a href="#">Int8</a>	RTT level reached by the walk
rtt_addr	<a href="#">Address</a>	Address of RTT reached by the walk
rtte	<a href="#">RmmRttEntry</a>	RTTE reached by the walk

## C1.26 RmmSystemRegisters type

The RmmSystemRegisters structure contains EL0 and EL1 system registers.

The RmmSystemRegisters structure is an [abstract type](#).

## Chapter C2

### Generic types

This section defines types which are shared between RMM interfaces and descriptions of RMM abstract state.

See also:

- [B3.4 RMI types](#)
- [B4.4 RSI types](#)
- [B5.4 PSCI types](#)
- [Chapter C1 RMM types](#)

#### C2.1 Address type

The Address type is an address.

The Address type is a [concrete type](#).

The width of the Address type is 64 bits.

#### C2.2 BitsN type

The BitsN type is an N-bit field.

The BitsN type is a [concrete type](#).

The width of the BitsN type is N bits.

## C2.3 IntN type

The IntN type is an signed N-bit integer.

The IntN type is a [concrete type](#).

The width of the IntN type is N bits.

## C2.4 UIntN type

The UIntN type is an unsigned N-bit integer.

The UIntN type is a [concrete type](#).

The width of the UIntN type is N bits.



## **Part D**

### **Usage**

## Chapter D1

### Flows

This section presents flows which explain how the RMM architecture can be used by the Host, and by Realm software.

Note that parts of the sequences below are for illustration only. For example, in the Realm creation flows, the `RMI_GRANULE_DELEGATE` and `RMI_GRANULE_UNDELEGATE` commands are called immediately before or after the `RMI_X_CREATE` and `RMI_X_DESTROY` commands respectively. An alternative flow would be for the Host to maintain a pool of Granules in the `DELEGATED` state, from which RMM data structures and Realm data can be allocated on demand.

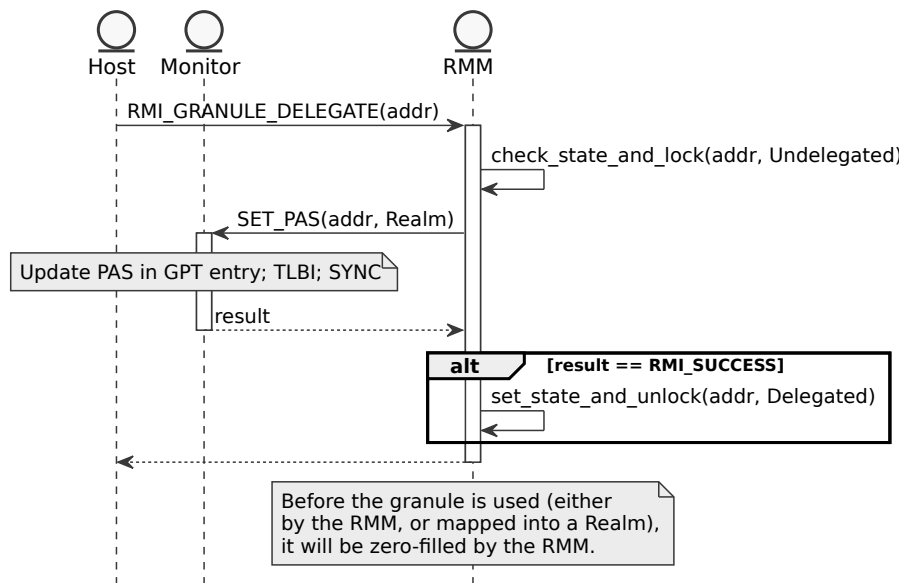
## D1.1 Granule delegation flows

### D1.1.1 Granule delegation flow

The following diagram shows how the PAS of a Granule is changed from NS to REALM.

See *Arm Architecture Reference Manual Supplement, The Realm Management Extension (RME), for Armv9-A* [2] for example software flows for the operations performed by the Monitor in this flow.

It is anticipated that the Monitor software will be required to use synchronization mechanisms to serialize access to the GPT.



See also:

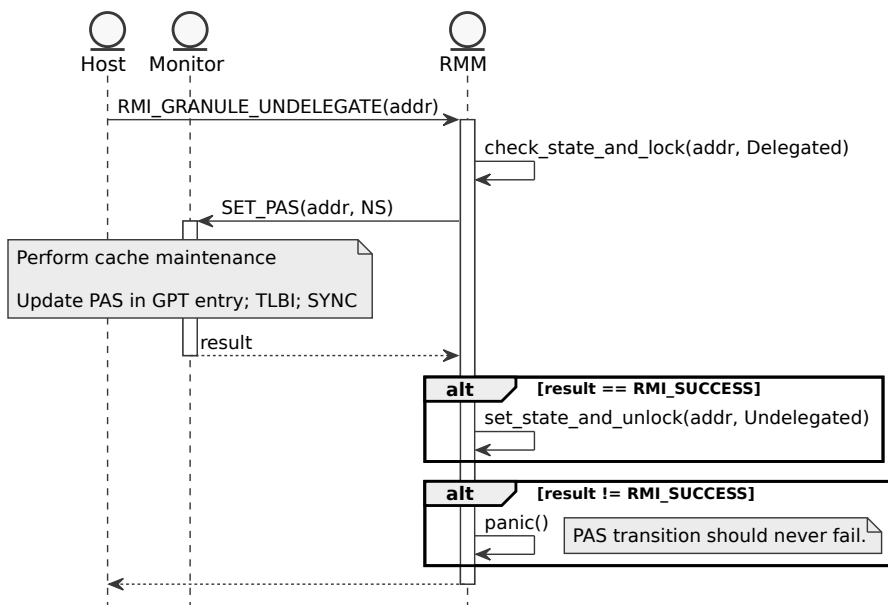
- [A2.2.1 Granule attributes](#)
- [B3.3.5 RMI\\_GRANULE\\_DELEGATE command](#)
- [D1.1.2 Granule undelegation flow](#)

### D1.1.2 Granule undelegation flow

The following diagram shows how the PAS of a Granule is changed from REALM to NS.

See *Arm Architecture Reference Manual Supplement, The Realm Management Extension (RME), for Armv9-A* [2] for example software flows for the operations performed by the Monitor in this flow.

It is anticipated that the Monitor software will be required to use synchronization mechanisms to serialize access to the GPT.



See also:

- [A2.2.1 Granule attributes](#)
- [B3.3.6 RMI\\_GRANULE\\_UNDELEGATE command](#)
- [D1.1.1 Granule delegation flow](#)

## D1.2 Realm lifecycle flows

This section contains flows which relate to the Realm lifecycle.

See also:

- [A2.1.5 Realm lifecycle](#)

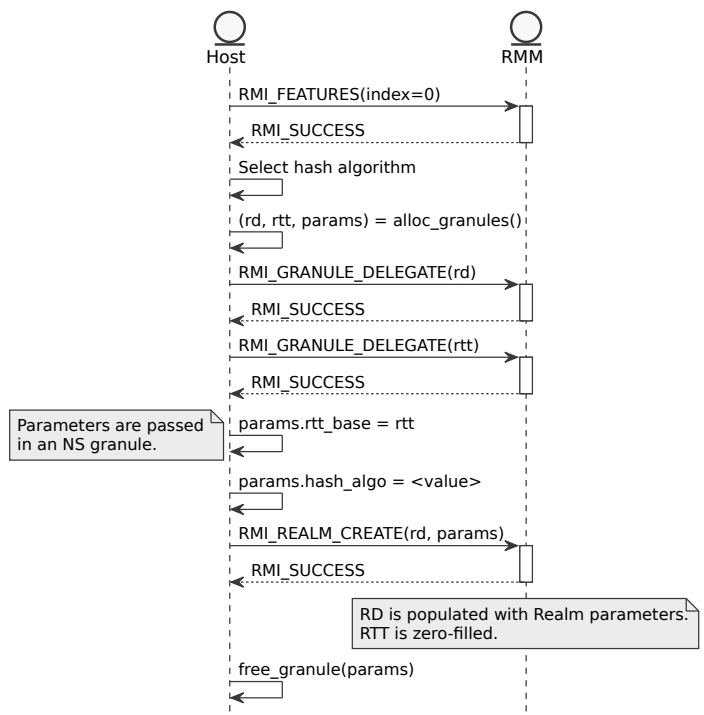
### D1.2.1 Realm creation flow

The following diagram shows the flow for creating a Realm.

To create a Realm, the Host must allocate and delegate two Granules:

- `rd` to store the Realm Descriptor
- `rtt` which will be the starting level Realm Translation Table (RTT)

The Host also provides an NS Granule (`params`) containing Realm creation parameters.



See also:

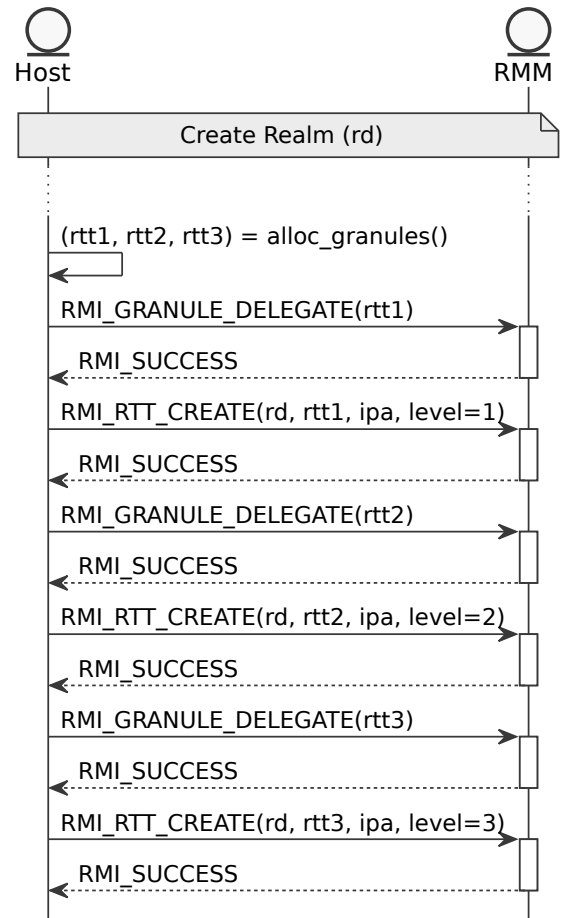
- [B3.3.5 RMI\\_GRANULE\\_DELEGATE command](#)
- [B3.3.9 RMI\\_REALM\\_CREATE command](#)
- [D1.2.5 Realm destruction flow](#)

### D1.2.2 Realm Translation Table creation flow

The following diagram shows the flow for populating the Realm Translation Tables (RTTs).

The starting level Realm Translation Tables (RTTs) are provided at Realm creation time.

Subsequent levels of RTT are added using the `RMI_RTT_CREATE` command. This can be performed when the state of the Realm is `NEW` or `ACTIVE`.



See also:

- [Chapter A5 Realm memory management](#)
- [B3.3.15 RMI\\_RTT\\_CREATE command](#)
- [D1.2.1 Realm creation flow](#)
- [D1.2.3 Initialize memory of New Realm flow](#)

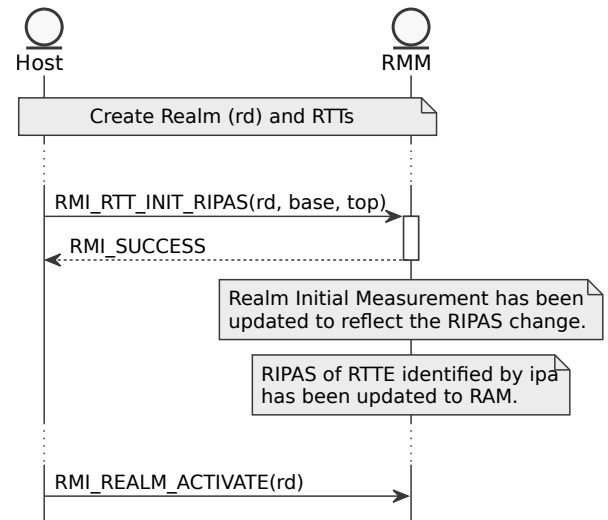
### D1.2.3 Initialize memory of New Realm flow

Immediately following Realm creation, every page in the Protected IPA space has its RIPAS set to EMPTY. There are two ways in which the Host can set the RIPAS of a given page of Protected IPA space to RAM:

1. Change the RIPAS by executing RMI\_RTT\_INIT\_RIPAS, but do not populate the contents of the page. The RIM is extended to reflect the RIPAS change.
2. Change the RIPAS by executing RMI\_RTT\_INIT\_RIPAS, and then populate the page with contents provided by the Host. The RIM is extended to reflect the contents added by the Host.

Once the Host has performed either of these actions for a given page of Protected IPA space, that page cannot be further modified prior to Realm activation.

The following diagram shows the flow for initializing the RIPAS without providing contents.

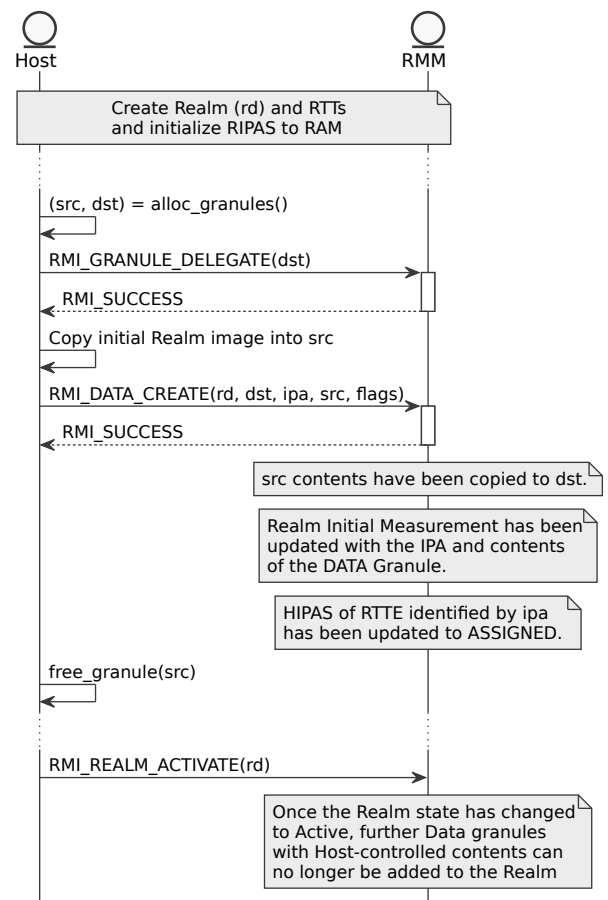


The following diagram shows the flow for populating the page with contents provided by the Host.

To do this, the Host must:

- Delegate a destination Granule (*dst*).
- Provide an NS Granule (*src*), whose contents will be copied into the destination Granule.
- Specify the Protected IPA *ipa* at which the *dst* Granule should be mapped in the Realm's IPA space.
- Ensure that the level 3 RTT which contains the RTTE identified by the Protected IPA has been created.

Once the Data Granule has been created, the *src* Granule can be reallocated by the Host.



See also:

- [A2.2.1 Granule attributes](#)
- [A5.2.2 Realm IPA state](#)
- [A7.1.1 Realm Initial Measurement](#)
- [B3.3.1 RMI\\_DATA\\_CREATE command](#)
- [B3.3.5 RMI\\_GRANULE\\_DELEGATE command](#)
- [B3.3.18 RMI\\_RTT\\_INIT\\_RIPAS command](#)
- [D1.2.1 Realm creation flow](#)
- [D1.2.2 Realm Translation Table creation flow](#)
- [D1.2.5 Realm destruction flow](#)

#### D1.2.4 REC creation flow

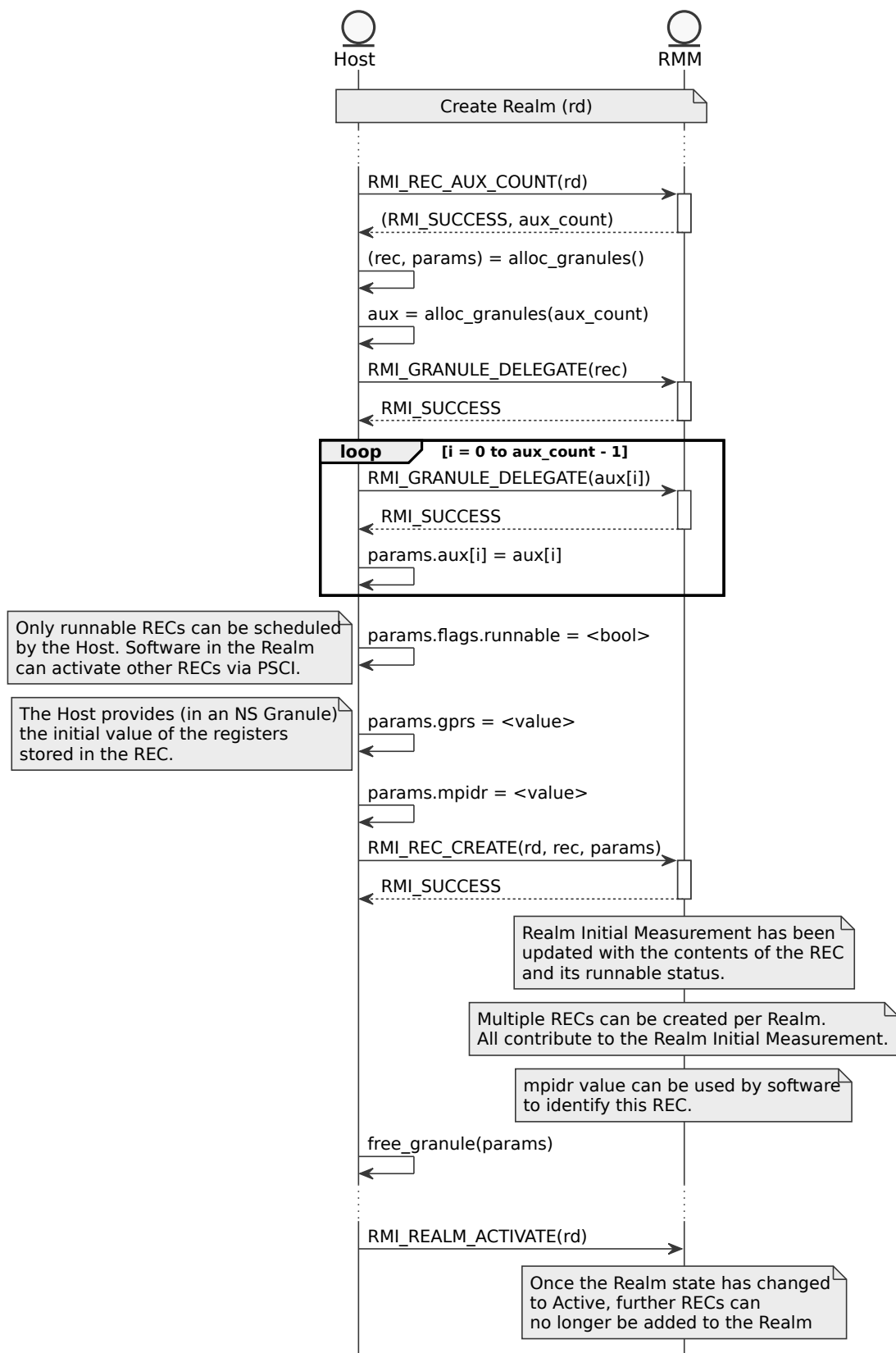
The following diagram shows the flow for creating a REC during Realm creation.

To create a REC, the Host must:

- Delegate a destination Granule (`rec`).
- Query the number of auxiliary Granules required, by calling `RMI_REC_AUX_COUNT`
- Delegate the required number of auxiliary Granules (`aux`)
- Provide auxiliary Granule addresses, register values and REC activation status in an NS Granule (`params`).

Once the REC has been created, the `params` Granule can be reallocated by the Host.





See also:

- [B3.3.5 RMI\\_GRANULE\\_DELEGATE command](#)

- [B3.3.11 RMI\\_REC\\_AUX\\_COUNT command](#)
- [B3.3.12 RMI\\_REC\\_CREATE command](#)
- [D1.2.1 Realm creation flow](#)
- [D1.2.5 Realm destruction flow](#)

## D1.2.5 Realm destruction flow

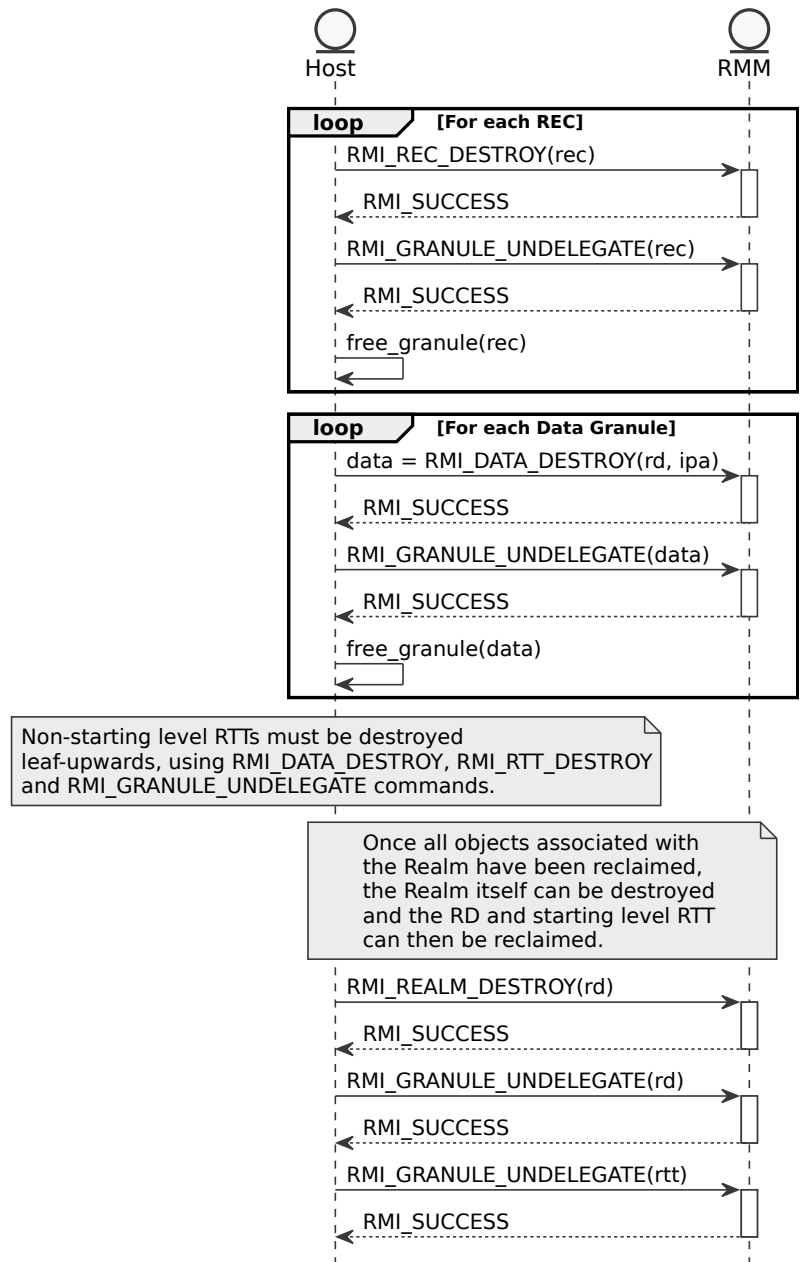
The following diagram shows the flow for destroying a Realm.

To destroy a Realm, the Host must first make the Realm non-live. This is done by destroying (in any order) the objects which are associated with the Realm:

- Data Granules
- RECs
- RTTs

Finally, the Realm itself can be destroyed.

Once each of these objects has been destroyed, the corresponding Granules can be undelegated and reallocated by the Host.



See also:

- [A2.1.4 Realm liveness](#)
- [B3.3.3 RMI\\_DATA\\_DESTROY command](#)
- [B3.3.6 RMI\\_GRANULE\\_UNDELEGATE command](#)
- [B3.3.10 RMI\\_REALM\\_DESTROY command](#)
- [B3.3.13 RMI\\_REC\\_DESTROY command](#)
- [D1.2.1 Realm creation flow](#)

## D1.3 Realm exception model flows

This section contains flows which relate to the Realm exception model.

See also:

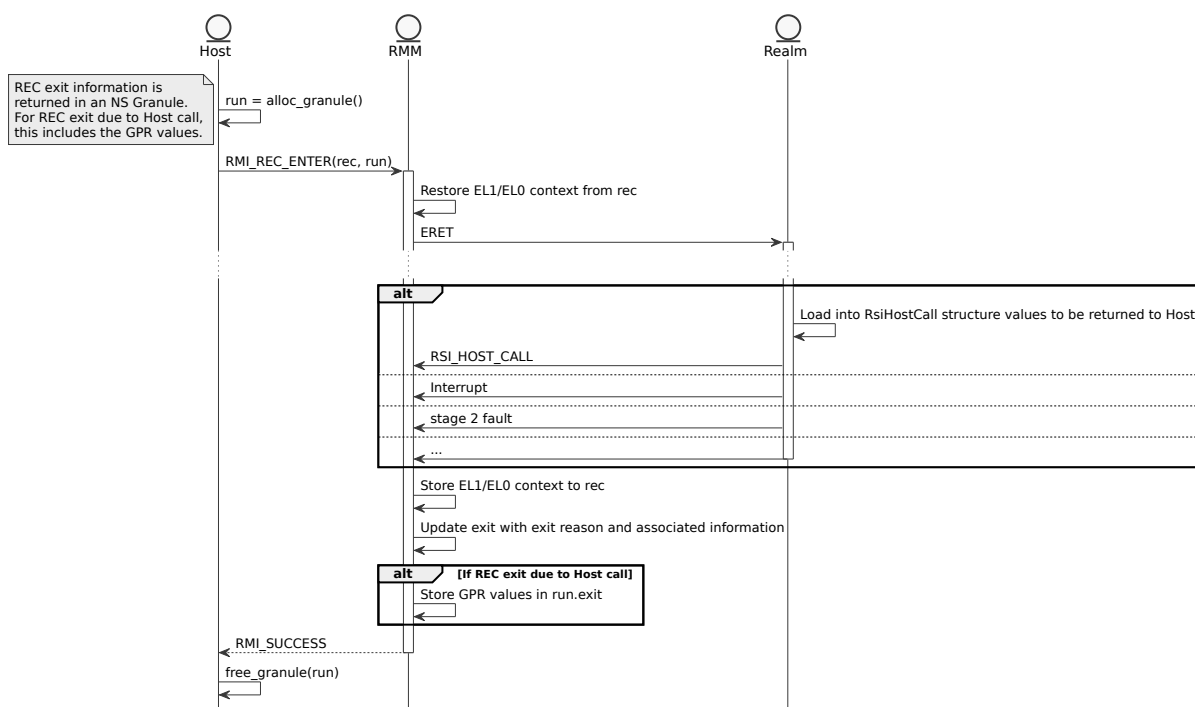
- [Chapter A4 Realm exception model](#)

### D1.3.1 Realm entry and exit flow

The following diagram shows how a Realm is executed, and illustrates the different reasons for exiting the Realm and returning control to the Host.

A REC is entered using the RMI\_REC\_ENTER command. The parameters to this command include:

- a *RecEnter* object, which is a data structure used to pass values from the Host to the RMM on REC entry
- a *RecExit* object, which is a data structure used to pass values from the RMM to the Host on REC exit



See also:

- [Chapter A4 Realm exception model](#)
- [D1.3.2 Host call flow](#)
- [D1.3.3 REC exit due to Data Abort fault flow](#)
- [D1.3.4 MMIO emulation flow](#)

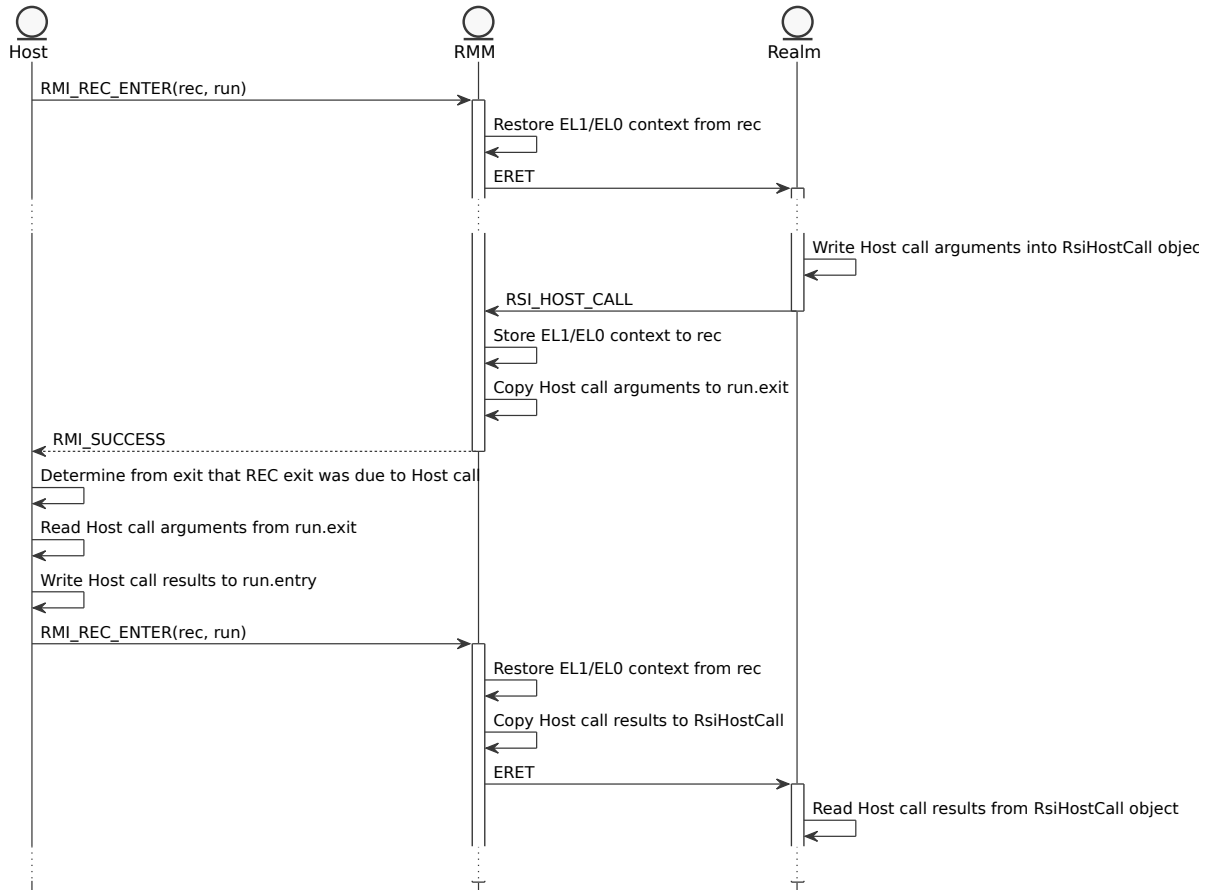
### D1.3.2 Host call flow

The following diagram shows how software executing inside the Realm can voluntarily yield control back to the Host by making a Host call.

A REC is entered using the RMI\_REC\_ENTER command. The parameters to this command include:

- a *RecEnter* object, which is a data structure used to pass values from the Host to the RMM on REC entry
- a *RecExit* object, which is a data structure used to pass values from the RMM to the Host on REC exit

On execution of RSI\_HOST\_CALL, arguments are copied from the RsiHostCall object in Realm memory into the RecExit object in NS memory. On the subsequent RMI\_REC\_ENTER, return values are copied from the RecEnter object in NS memory into the RsiHostCall object in Realm memory.



See also:

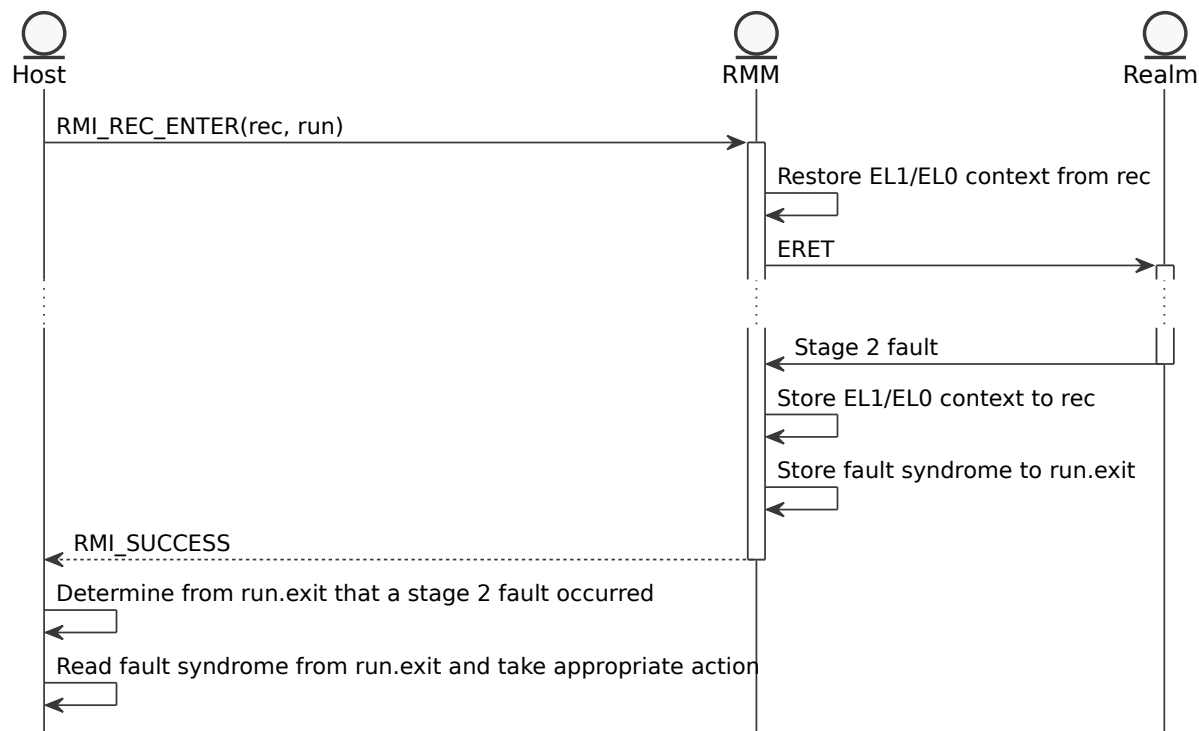
- [A4.5 Host call](#)

### D1.3.3 REC exit due to Data Abort fault flow

The following diagram shows how a Data Abort due to a Realm access is taken to the Host.

A REC is entered using the RMI\_REC\_ENTER command. The parameters to this command include:

- a *RecEnter* object, which is a data structure used to pass values from the Host to the RMM on REC entry
- a *RecExit* object, which is a data structure used to pass values from the RMM to the Host on REC exit

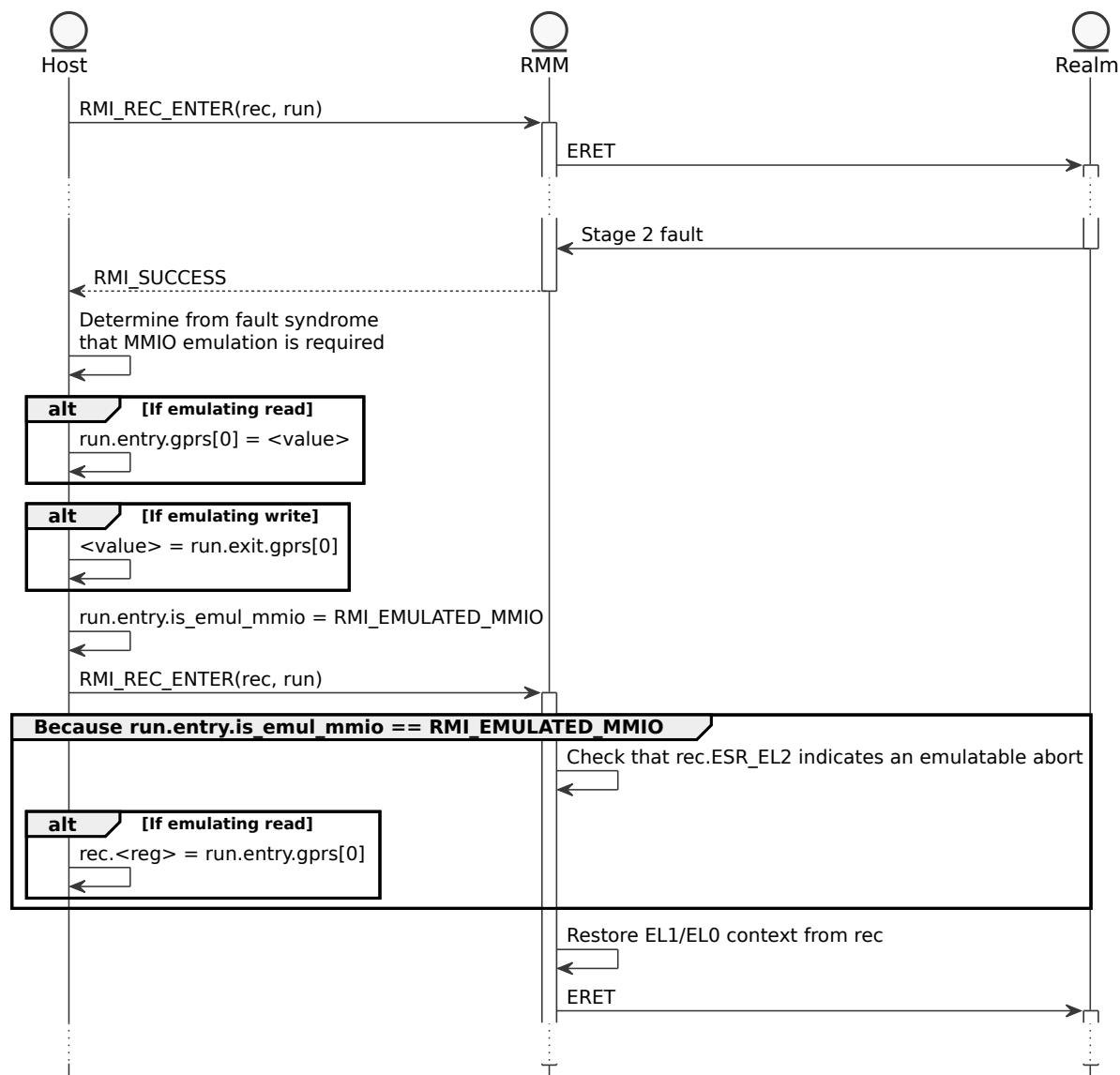


See also:

- [Chapter A4 Realm exception model](#)

### D1.3.4 MMIO emulation flow

The following diagram shows how an MMIO access by a Realm can be emulated by the Host.



See also:

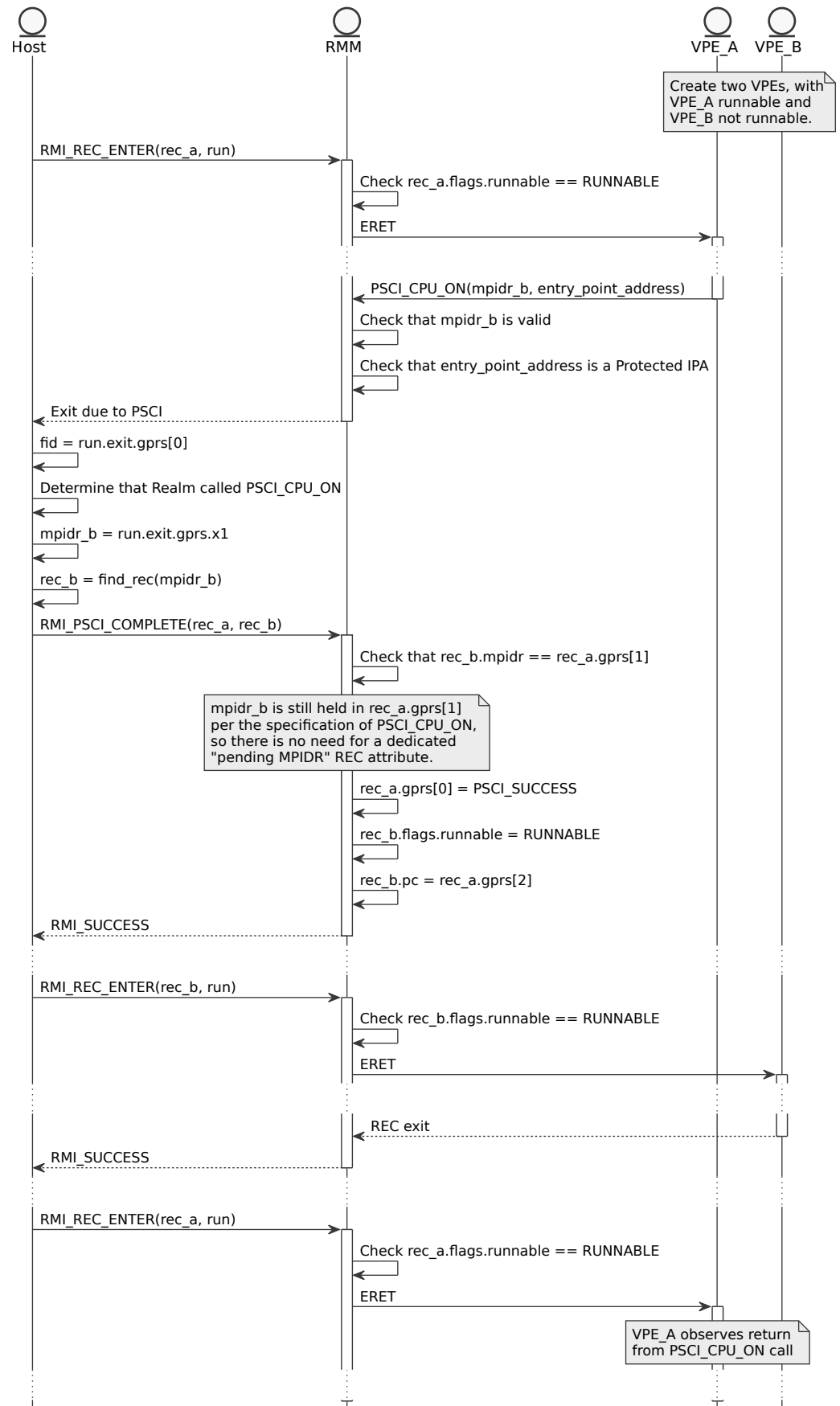
- [Chapter A4 Realm exception model](#)

## D1.4 PSCI flows

### D1.4.1 PSCI\_CPU\_ON flow

The following diagram shows how one Realm VPE can set the “runnable” flag in another Realm VPE by executing PSCI\_CPU\_ON.





See also:

- [B3.3.7 RMI\\_PSCI\\_COMPLETE command](#)
- [B5.3.3 PSCI\\_CPU\\_ON command](#)

## D1.5 Realm memory management flows

This section contains flows which relate to management of Realm memory.

See also:

- [Chapter A5 Realm memory management](#)

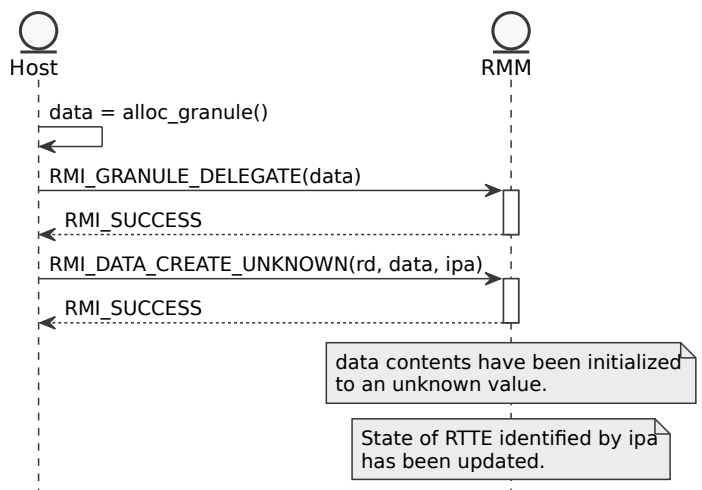
### D1.5.1 Add memory to Active Realm flow

The following diagram shows the flow for adding memory to a Realm whose state is ACTIVE.

To add memory to a Realm whose state is ACTIVE, the Host must:

- Delegate a destination Granule (*dst*).
- Specify the Protected IPA at which the *dst* Granule will be mapped in the Realm's IPA space.
- Ensure that the level 3 RTT which contains the RTTE identified by the Protected IPA has been created.
- Ensure that the RIPAS of the Protected IPA is RAM.

Once a given Protected IPA has been populated with unknown content, it cannot be repopulated.

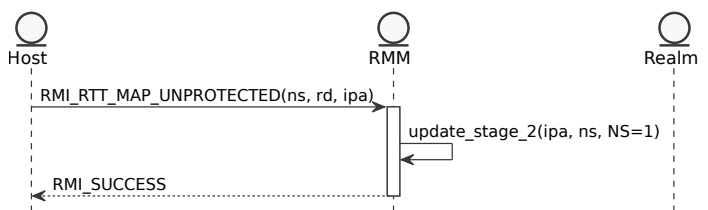


See also:

- [A2.1.5 Realm lifecycle](#)
- [Chapter A5 Realm memory management](#)
- [B3.3.2 RMI\\_DATA\\_CREATE\\_UNKNOWN command](#)
- [B3.3.5 RMI\\_GRANULE\\_DELEGATE command](#)

### D1.5.2 NS memory flow

The following diagram describes how NS memory can be mapped into a Realm.



See also:

- [Chapter A5 Realm memory management](#)
- [B3.3.19 RMI\\_RTT\\_MAP\\_UNPROTECTED command](#)
- [B3.3.22 RMI\\_RTT\\_UNMAP\\_UNPROTECTED command](#)

### D1.5.3 RIPAS change flow

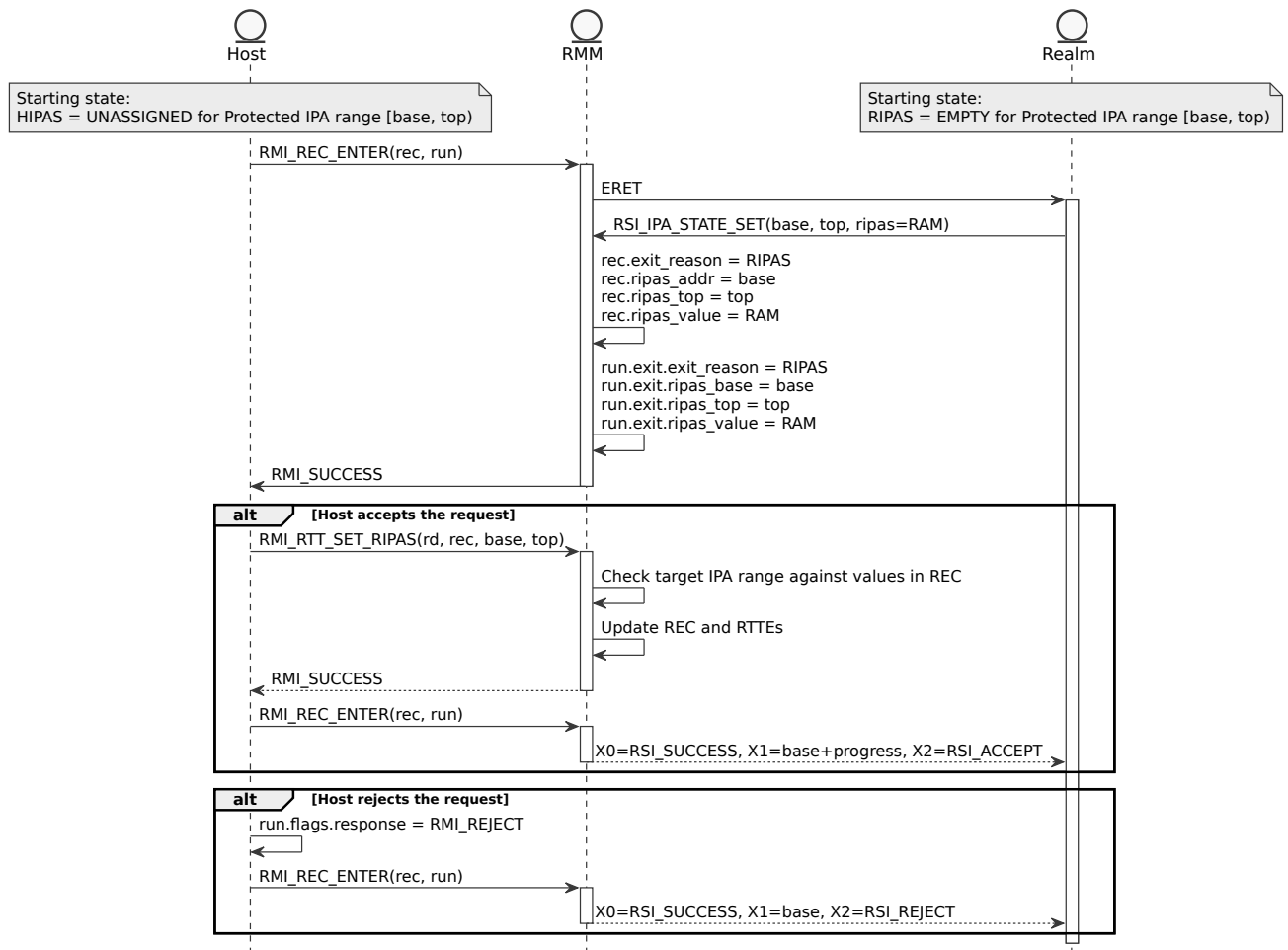
The following diagram describes how a Realm requests a RIPAS change, and how that request is handled by the Host.

- The Realm calls `RSI_IPA_STATE_SET` to request a RIPAS change for IPA range [base, top).
- This causes a REC exit due to RIPAS change pending.

On taking a REC exit due to RIPAS change pending, the Host does the following:

- Reads the region base and top addresses from the RecExit object.
- Applies the requested RIPAS change to an IPA range starting from the base of the target region, and extending no further than the top of the target region.
- Calls `RMI_REC_ENTER` to re-enter the REC.

The Realm observes in X1 the top of the region for which the RIPAS change was applied.



See also:

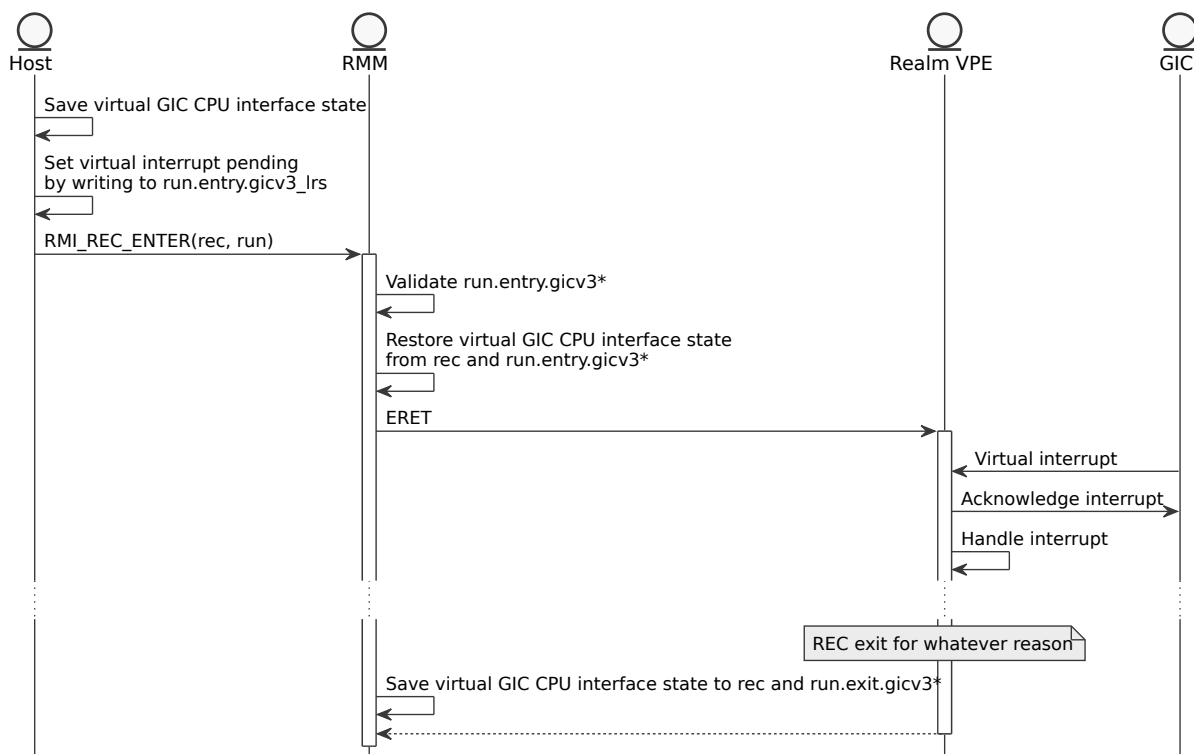
- [A5.4 RIPAS change](#)

- [B3.3.14 RMI\\_REC\\_ENTER command](#)
- [B3.3.21 RMI\\_RTT\\_SET\\_RIPAS command](#)
- [B4.3.5 RSI\\_IPA\\_STATE\\_SET command](#)
- [D2.2 Realm shared memory protocol flow](#)

## D1.6 Realm interrupts and timers flows

### D1.6.1 Interrupt flow

The following diagram shows how a virtual interrupt is injected into a Realm by the Host.

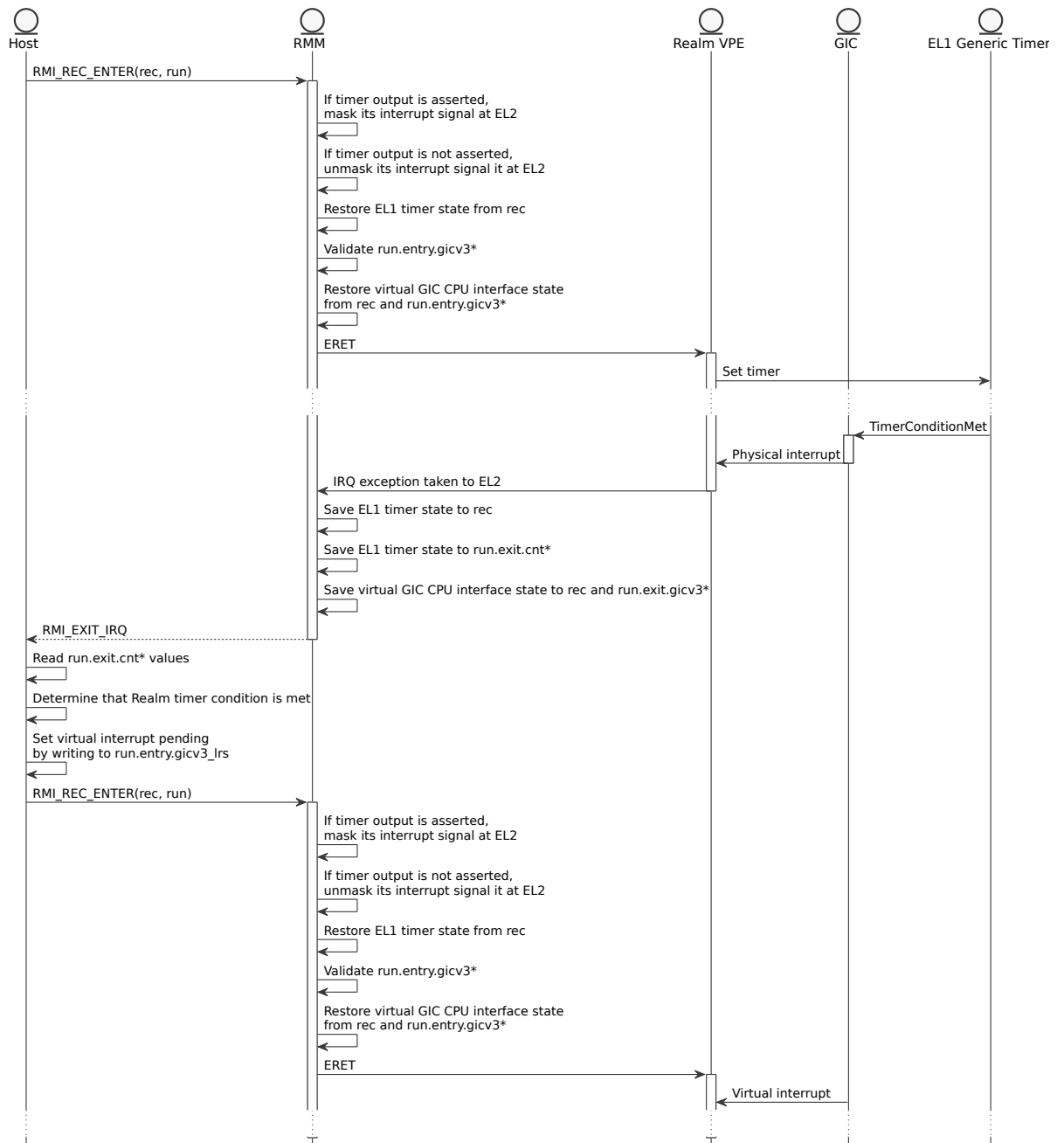


See also:

- [A6.1 Realm interrupts](#)

### D1.6.2 Timer interrupt delivery flow

The following diagram shows how a timer interrupt is delivered to and handled by a Realm.



See also:

- [A6.2 Realm timers](#)

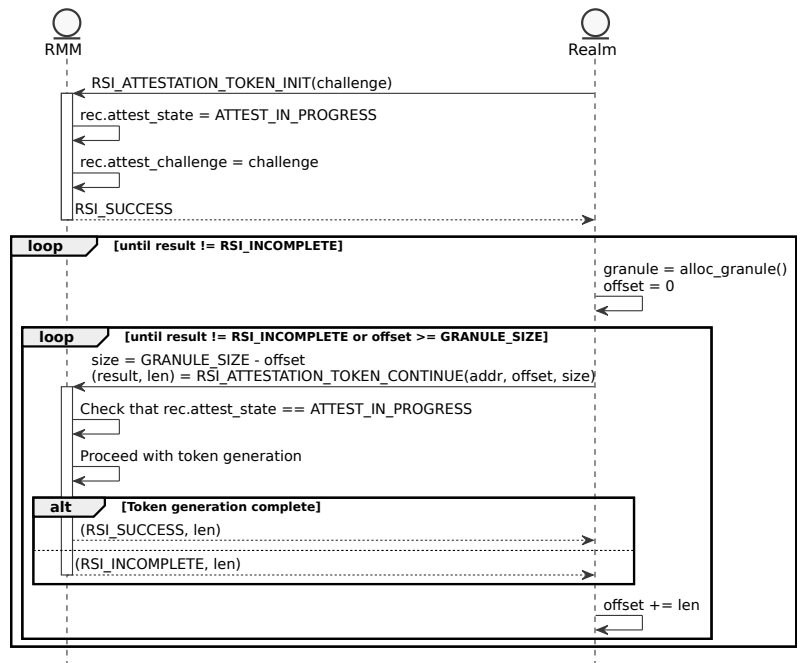
## D1.7 Realm attestation flows

### D1.7.1 Attestation token generation flow

The following diagram shows the flow for a Realm to obtain an attestation token.

The Realm first calls `RSI_ATTESTATION_TOKEN_INIT`, providing the address where the attestation token will be written, and a challenge value.

The Realm then calls `RSI_ATTESTATION_TOKEN_CONTINUE`, providing the same address. This command is called in a loop, until the result is not `RSI_INCOMPLETE`.



See also:

- [A7.2.2 Attestation token generation](#)
- [B4.3.1 RSI\\_ATTESTATION\\_TOKEN\\_CONTINUE command](#)
- [B4.3.2 RSI\\_ATTESTATION\\_TOKEN\\_INIT command](#)

### D1.7.2 Handling interrupts during attestation token generation flow

The following diagram shows how interrupts are handled during generation of an attestation token.

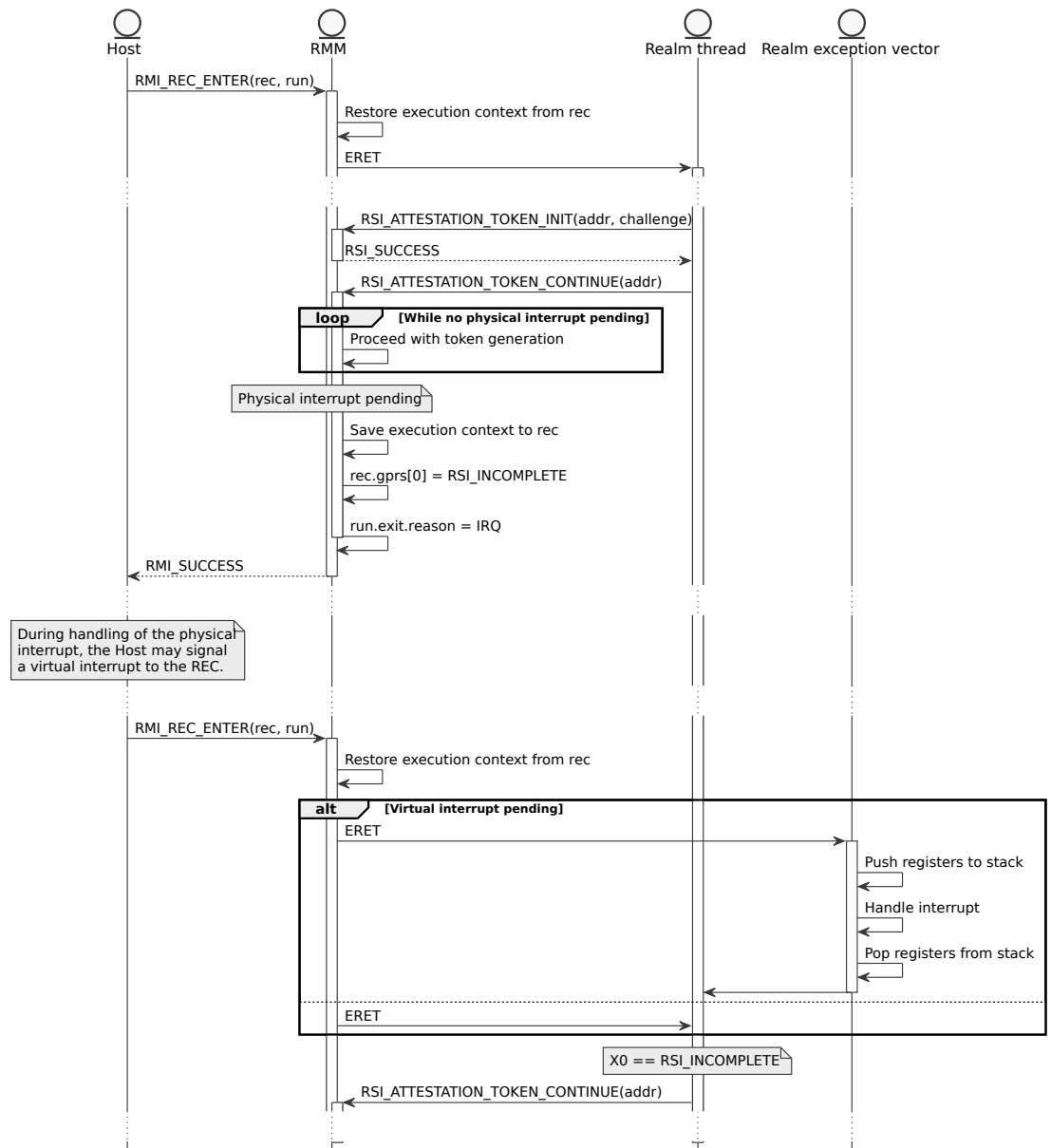
If the RMM detects that a physical interrupt is pending during execution of `RSI_ATTESTATION_TOKEN_CONTINUE`, it saves the execution context to the REC object, and performs a REC exit due to IRQ.

During handling of the IRQ, the Host may signal a virtual interrupt to the REC.

On the next entry to the REC, if a virtual interrupt is pending, it is taken to the REC's exception vector.

Whether or not a virtual interrupt was taken, on return to the original thread, the REC determines that `X0` is `RSI_INCOMPLETE`, and therefore calls `RSI_ATTESTATION_TOKEN_CONTINUE` again.





See also:

- [A4.3.5 REC exit due to IRQ](#)
- [A6.1 Realm interrupts](#)
- [A7.2.2 Attestation token generation](#)
- [B4.3.1 RSI\\_ATTESTATION\\_TOKEN\\_CONTINUE command](#)
- [B4.3.2 RSI\\_ATTESTATION\\_TOKEN\\_INIT command](#)
- [D1.3.1 Realm entry and exit flow](#)

## Chapter D2

# Realm shared memory protocol

This section describes a protocol for management of memory which is shared between a Realm and the Host. This protocol makes use of the primitives described in this specification. However, the protocol itself is not part of the RMM architecture. Use of this protocol is subject to a contract between the Realm and Host software agents.

See also:

- [Chapter A5 Realm memory management](#)

## D2.1 Realm shared memory protocol description

The Host agrees to provide the Realm with a certain amount of memory. This memory is referred to below as the Realm's "memory footprint".

The memory footprint is described to the Realm, for example via firmware tables. The Realm can choose, at any point during its execution, how much of its memory footprint is protected (accessible only to the Realm) and how much is shared with the Host.

Realm software treats the most significant IPA bit as a "protection attribute" bit. This means that for every Protected IPA (in which the most significant bit is '0'), there exists a corresponding Unprotected IPA alias, which is generated by setting the most significant bit to '1'.

The choice of whether a given page is protected or shared at a given time is expressed by setting the RIPAS of the Protected IPA:

- If the RIPAS of the Protected IPA is RAM, the page is protected and access to the Unprotected IPA alias causes a Synchronous External Abort taken to the Realm.
- If the RIPAS of the Protected IPA is EMPTY, the page is shared and access to the Unprotected IPA alias does not cause a Synchronous External Abort taken to the Realm.

The initial RIPAS for every page in the Realm's memory footprint is described to the Realm, for example via firmware tables. The Host agrees that during Realm execution, it will accept a RIPAS change request on any page within the Realm's memory footprint.

See also:

- [A5.2.1 Realm IPA space](#)
- [A5.2.2 Realm IPA state](#)
- [A5.4 RIPAS change](#)

## D2.2 Realm shared memory protocol flow

The following diagram illustrates how the protocol is used to set up and tear down a shared memory buffer.

Chapter D2. Realm shared memory protocol  
D2.2. Realm shared memory protocol flow

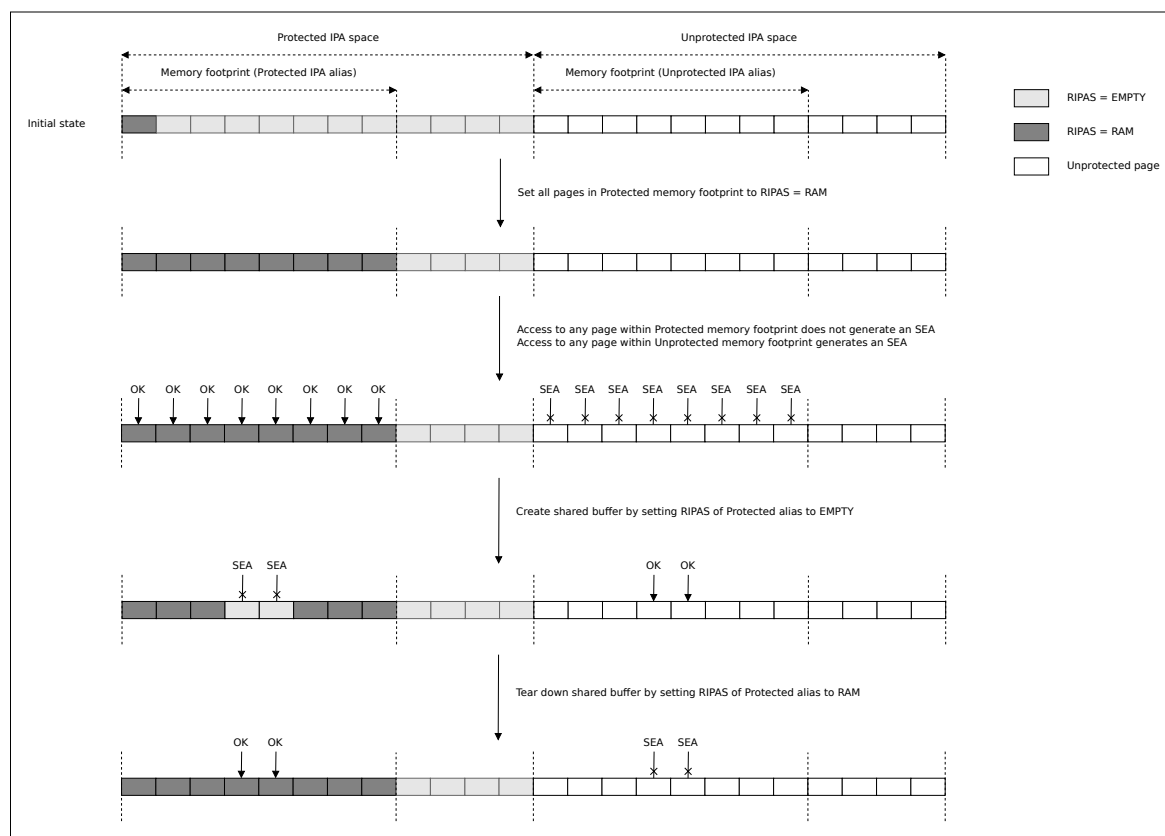


Figure D2.1: Realm shared memory protocol flow

See also:

- [D1.5.3 RIPAS change flow](#)

# Glossary

## ASL

Arm Specification Language  
Language used to express pseudocode implementations. Formal language definition can be found in *Arm Specification Language Reference Manual* [14].

## CBOR

Concise Binary Object Representation

## CCA

Confidential Compute Architecture

## CCA platform

All hardware and firmware components which are involved in delivering the CCA security guarantee. See *Arm CCA Security model* [4].

## CDDL

Concise Data Definition Language

## COSE

CBOR Object Signing and Encryption

## EAT

Entity Attestation Token

## FID

Function Identifier

## GIC

Generic Interrupt Controller  
See *Arm Generic Interrupt Controller (GIC) Architecture Specification version 3 and version 4* [5]

## GPF

Granule Protection Fault

## GPT

Granule Protection Table  
Table which determines the Physical Address Space of each Granule.

## HIPAS

Host IPA state

## Host

Software executing in Non-secure Security state which manages resources used by Realms

## IAK

Initial Attestation Key Key used to sign the CCA platform attestation token.

## IPA

	Intermediate Physical Address Address space visible to software executing at EL1 in the Realm.
<b>IPI</b>	
	Inter-processor interrupt
<b>IRI</b>	
	Interrupt Routing Infrastructure A subset of the components which make up the GIC.
<b>ITS</b>	
	Interrupt Translation Service A service provided by the GIC.
<b>MMIO</b>	
	Memory-mapped I/O
<b>MPIDR</b>	
	Multiprocessor Affinity Register
<b>NS</b>	
	Non-secure
<b>PAS</b>	
	Physical Address Space
<b>PE</b>	
	Processing Element
<b>PMU</b>	
	Performance Monitor Unit
<b>PSCI</b>	
	Power State Control Interface See <i>Arm Power State Coordination Interface (PSCI)</i> <a href="#">[16]</a>
<b>RAK</b>	
	Realm Attestation Key Key used to sign the Realm attestation token.
<b>RD</b>	
	Realm Descriptor Object which stores attributes of a Realm.
<b>Realm</b>	
	A protected execution environment
<b>REC</b>	
	Realm Execution Context Object which stores PE state associated with a thread of execution within a Realm.
<b>REM</b>	
	Realm Extensible Measurement Measurement value which can be extended during the lifetime of a Realm.
<b>RHA</b>	
	Realm Hash Algorithm

**RIM**

Realm Initial Measurement Measurement of the state of a Realm at the time of activation.

**RIPAS**

Realm IPA state

**RMI**

Realm Management Interface The ABI exposed by the RMM for use by the Host.

**RMM**

Realm Management Monitor

**RNVS**

Root Non-volatile Storage

**RPV**

Realm Personalization Value

**RSI**

Realm Services Interface The ABI exposed by the RMM for use by the Realm.

**RTT**

Realm Translation Table  
Object which describes the IPA space of a Realm.

**RTTE**

Realm Translation Table Entry

**SEA**

Synchronous External Abort

**SIG**

Software Generated Interrupt

**SMCCC**

SMC Calling Convention  
See *Arm SMC Calling Convention* [\[13\]](#)

**SPM**

Secure Partition Manager

**TA**

Trusted Application

**TOS**

Trusted OS

**VMM**

Virtual Machine Monitor

**VMSA**

Virtual Memory System Architecture

**VPE**

Virtual Processing Element

**Wiping**

An operation which changes the value of a memory location from  $X$  to  $Y$ , such that the value  $X$  cannot be determined from the value  $Y$