



Arm[®] Cortex[®]-A720AE Core Cryptographic Extension

Revision: r0p0

Technical Reference Manual

Non-Confidential

Issue 02

Copyright © 2023–2024 Arm Limited (or its affiliates). 102830_0000_02_en
All rights reserved.



Arm® Cortex®-A720AE Core Cryptographic Extension

Technical Reference Manual

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

Release Information

Document history

Issue	Date	Confidentiality	Change
0000-01	16 November 2023	Confidential	First early access release for rOp0
0000-02	13 March 2024	Non-Confidential	Second early access release for rOp0

Proprietary Notice

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

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

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

This document may include technical inaccuracies or typographical errors. THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES

OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, any patents, copyrights, trade secrets, trademarks, or other rights.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Reference by Arm to any third party's products or services within this document is not an express or implied approval or endorsement of the use thereof.

This document consists solely of commercial items. You shall be responsible for ensuring that any permitted use, duplication, or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of this document shall prevail.

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

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

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

PRE-1121-V1.0

Confidentiality Status

This document is Non-Confidential. The right to use, copy and disclose this document may be subject to license restrictions in accordance with the terms of the agreement entered into by Arm and the party that Arm delivered this document to.

Unrestricted Access is an Arm internal classification.

Product Status

The information in this document is Final, that is for a developed product.

Feedback

Arm welcomes feedback on this product and its documentation. To provide feedback on the product, create a ticket on <https://support.developer.arm.com>.

To provide feedback on the document, fill the following survey: <https://developer.arm.com/documentation-feedback-survey>.

Inclusive language commitment

Arm values inclusive communities. Arm recognizes that we and our industry have used language that can be offensive. Arm strives to lead the industry and create change.

We believe that this document contains no offensive language. To report offensive language in this document, email terms@arm.com.

Contents

- 1. Introduction..... 6**
 - 1.1 Product revision status..... 6
 - 1.2 Intended audience..... 6
 - 1.3 Conventions..... 6
 - 1.4 Useful resources..... 8
- 2. Cryptographic Extension support in the Cortex®-A720AE core..... 10**
 - 2.1 Disabling the Cryptographic Extension..... 10
 - 2.2 Product revisions..... 11
- 3. AArch64 instruction identification system registers..... 12**
 - 3.1 Cryptographic Extensions register summary..... 12
 - 3.2 ID_AA64ISAR0_EL1, AArch64 Instruction Set Attribute Register 0..... 12
 - 3.3 ID_AA64ZFR0_EL1, SVE Feature ID register 0..... 16
- A. Document revisions..... 19**
 - A.1 Revisions..... 19

1. Introduction

1.1 Product revision status

The r_xp_y identifier indicates the revision status of the product described in this manual, for example, $r1p2$, where:

r_x	Identifies the major revision of the product, for example, $r1$.
p_y	Identifies the minor revision or modification status of the product, for example, $p2$.

1.2 Intended audience

This manual is for system designers, system integrators, and programmers who are designing or programming a *System-on-Chip* (SoC) that uses the Cortex®-A720AE core with the optional Cryptographic Extension.

1.3 Conventions

The following subsections describe conventions used in Arm documents.

Glossary

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

See the Arm Glossary for more information: developer.arm.com/glossary.

Convention	Use
<i>italic</i>	Citations.
bold	Terms in descriptive lists, where appropriate.
monospace	Text that you can enter at the keyboard, such as commands, file and program names, and source code.
monospace <u>underline</u>	A permitted abbreviation for a command or option. You can enter the underlined text instead of the full command or option name.

Convention	Use
<and>	Encloses replaceable terms for assembler syntax where they appear in code or code fragments. For example: <div>MRC p15, 0, <Rd>, <CRn>, <CRm>, <Opcode_2></div>
SMALL CAPITALS	Terms that have specific technical meanings as defined in the Arm® Glossary. For example, IMPLEMENTATION DEFINED , IMPLEMENTATION SPECIFIC , UNKNOWN , and UNPREDICTABLE .



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



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



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



This information is important and needs your attention.



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



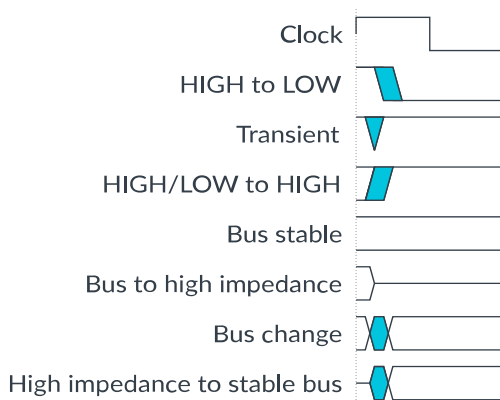
A reminder of something important that relates to the information you are reading.

Timing diagrams

The following figure explains the components used in timing diagrams. Variations, when they occur, have clear labels. You must not assume any timing information that is not explicit in the diagrams.

Shaded bus and signal areas are undefined, so the bus or signal can assume any value within the shaded area at that time. The actual level is unimportant and does not affect normal operation.

Figure 1-1: Key to timing diagram conventions



Signals

The signal conventions are:

Signal level

The level of an asserted signal depends on whether the signal is active-HIGH or active-LOW. Asserted means:

- HIGH for active-HIGH signals.
- LOW for active-LOW signals.

Lowercase n

At the start or end of a signal name, n denotes an active-LOW signal.

Register descriptions

Reset definitions

Replication Operator {}

Verilog replication operators are used for reset values over 8-bits.

For example, {16{1'b0}} indicates a binary value of 16 zeros.

x

Resets that are unknown are indicated with x.

1.4 Useful resources

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

Access to Arm documents depends on their confidentiality:

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

Arm product resources	Document ID	Confidentiality
Arm® Cortex®-A720AE Core Configuration and Integration Manual	102829	Confidential
Arm® Cortex®-A720AE Core Cryptographic Extension Release Note (MP171)	109556	Confidential
Arm® Cortex®-A720AE Core Technical Reference Manual	102828	Non-Confidential
Arm® DynamIQ™ Shared Unit-120AE Technical Reference Manual	107721	Non-Confidential
Arm® DynamIQ™ Shared Unit-120AE Configuration and Integration Manual	107720	Confidential

Arm architecture and specifications	Document ID	Confidentiality
Arm® Architecture Reference Manual for A-profile architecture	DDI 0487	Non-Confidential
Arm® Architecture Reference Manual Supplement, Memory System Resource Partitioning and Monitoring (MPAM), for A-profile architecture	DDI 0598	Non-Confidential
AMBA® 5 CHI Architecture Specification	IHI 0050	Non-Confidential
Arm® Generic Interrupt Controller Architecture Specification, GIC architecture version 3 and version 4	IHI 0069	Non-Confidential
Arm® CoreSight™ Architecture Specification v3.0	IHI 0029	Non-Confidential
Arm® CoreSight™ ELA-600 Embedded Logic Analyzer Technical Reference Manual	101088	Non-Confidential



Note

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

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

2. Cryptographic Extension support in the Cortex®-A720AE core

The Cortex®-A720AE core supports the optional Arm® Cryptographic Extension.

The Arm® Cryptographic Extension adds A64 instructions to Advanced SIMD to:

- Accelerate *Advanced Encryption Standard* (AES) encryption and decryption
- Implement the *Secure Hash Algorithm* (SHA) functions
- Perform *Polynomial Multiply Long* (PMULL) instructions

Supported features

The Arm® Cryptographic Extension supports the following features:

Table 2-1: Features supported by the Arm® Cryptographic Extension

Feature	Description	Architecture version
FEAT_AES	Advanced SIMD AES instructions	Arm®v8.0
FEAT_PMULL	Advanced SIMD PMULL instructions	
FEAT_SHA1	Advanced SIMD SHA1 instructions	
FEAT_SHA256	Advanced SIMD SHA256 instructions	
FEAT_SHA512	Advanced SIMD SHA512 instructions	Arm®v8.2
FEAT_SHA3	Advanced SIMD EOR3, RAX1, XAR, and BCAX instructions	
FEAT_SM3	Advanced SIMD SM3 instructions	
FEAT_SM4	Advanced SIMD SM4 instructions	
FEAT_SVE_AES	SVE AES instructions	Arm®v9.0
FEAT_SVE_PMULL128	SVE PMULL instructions	
FEAT_SVE_SHA3	SVE SHA3 instructions	
FEAT_SVE_SM4	SVE SM4 instructions	

2.1 Disabling the Cryptographic Extension

Disabling the Cryptographic Extension applies to all Cortex®-A720AE cores in a cluster.

To disable the Cryptographic Extension, assert the CRYPTODISABLE signal.

When the CRYPTODISABLE signal is asserted:

- Executing a cryptographic instruction results in an **UNDEFINED** exception.
- ID_AA64ISAR0_EL1 and ID_AA64ZFR0_EL1 indicate that the Cryptographic Extension is not implemented.

Related information

[3.2 ID_AA64ISAR0_EL1, AArch64 Instruction Set Attribute Register 0](#) on page 12

[3.3 ID_AA64ZFR0_EL1, SVE Feature ID register 0](#) on page 16

2.2 Product revisions

The product revision increments at each release.

The following table indicates the main differences in functionality between product revisions.

Table 2-2: Product revisions

Revision	Notes
r0p0	First release

Changes in functionality that have an impact on the documentation also appear in [A.1 Revisions](#) on page 19.

3. AArch64 instruction identification system registers

This chapter describes the ID_AA64ISAR0_EL1 and ID_AA64ZFR0_EL1 registers. These identification registers provide information about the instructions implemented in the Cortex®-A720AE core, including the instructions provided by the Cryptographic Extension.

3.1 Cryptographic Extensions register summary

Software can identify the cryptographic instructions that are implemented in the Cortex®-A720AE core by reading the identification registers.

The following table shows the identification registers for the Cortex®-A720AE core Cryptographic Extension.

Table 3-1: Cryptographic Extension register summary

Name	Description
ID_AA64ISAR0_EL1	See 3.2 ID_AA64ISAR0_EL1, AArch64 Instruction Set Attribute Register 0 on page 12
ID_AA64ZFR0_EL1	See 3.3 ID_AA64ZFR0_EL1, SVE Feature ID register 0 on page 16

3.2 ID_AA64ISAR0_EL1, AArch64 Instruction Set Attribute Register 0

Provides information about the instructions implemented in AArch64 state.

For general information about the interpretation of the ID registers, see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations

This register is available in all configurations.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

0000	0010	0010	0001	0001	xxxx	xxxx	xxxx	0001	0000	0010	0001	xxxx	xxxx	xxxx	xxxx
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure 3-1: AArch64_id_aa64isar0_el1 bit assignments

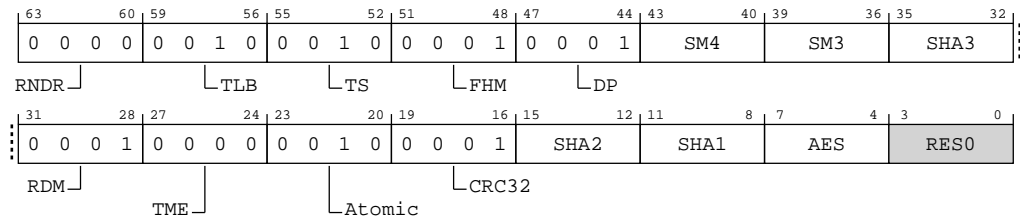


Table 3-2: ID_AA64ISAR0_EL1 bit descriptions

Bits	Name	Description	Reset
[63:60]	RNDR	Indicates support for Random Number instructions in AArch64 state. When FEAT_RNG_TRAP is implemented, the value returned by a direct read of ID_AA64ISAR0_EL1.RNDR is further controlled by the value of AArch64-SCR_EL3.TRNDR. Defined values are: 0b0000 No Random Number instructions are implemented.	0b0000
[59:56]	TLB	Indicates support for Outer Shareable and TLB range maintenance instructions. Defined values are: 0b0010 Outer Shareable and TLB range maintenance instructions are implemented.	0b0010
[55:52]	TS	Indicates support for flag manipulation instructions. Defined values are: 0b0010 CFINV, RMIF, SETF16, SETF8, AXFLAG, and XAFLAG instructions are implemented.	0b0010
[51:48]	FHM	Indicates support for FMLAL and FMLSL instructions. Defined values are: 0b0001 FMLAL and FMLSL instructions are implemented.	0b0001

Bits	Name	Description	Reset
[47:44]	DP	Indicates support for Dot Product instructions in AArch64 state. Defined values are: 0b0001 UDOT and SDOT instructions implemented.	0b0001
[43:40]	SM4	Indicates support for SM4 instructions in AArch64 state. Defined values are: 0b0000 No SM4 instructions implemented. This value is reported when the Cryptographic Extension is not implemented or is disabled. 0b0001 SM4E and SM4EKEY instructions implemented. This value is reported when the Cryptographic Extension is implemented and enabled. When the CRYPTO configuration parameter is true and the CRYPTODISABLE input is low at reset the Cryptographic Extension is implemented	The reset values can be the following: 0b0000, 0b0001, respective to the value.
[39:36]	SM3	Indicates support for SM3 instructions in AArch64 state. Defined values are: 0b0000 No SM3 instructions implemented. This value is reported when the Cryptographic Extension is not implemented or is disabled. 0b0001 SM3SS1, SM3TT1A, SM3TT1B, SM3TT2A, SM3TT2B, SM3PARTW1, and SM3PARTW2 instructions implemented. This value is reported when the Cryptographic Extension is implemented and enabled. When the CRYPTO configuration parameter is true and the CRYPTODISABLE input is low at reset the Cryptographic Extension is implemented	The reset values can be the following: 0b0000, 0b0001, respective to the value.
[35:32]	SHA3	Indicates support for SHA3 instructions in AArch64 state. Defined values are: 0b0000 No SHA3 instructions implemented. This value is reported when the Cryptographic Extension is not implemented or is disabled. 0b0001 EOR3, RAX1, XAR, and BCAX instructions implemented. This value is reported when the Cryptographic Extension is implemented and enabled. When the CRYPTO configuration parameter is true and the CRYPTODISABLE input is low at reset the Cryptographic Extension is implemented	The reset values can be the following: 0b0000, 0b0001, respective to the value.
[31:28]	RDM	Indicates support for SQRDMLAH and SQRDMLSH instructions in AArch64 state. Defined values are: 0b0001 SQRDMLAH and SQRDMLSH instructions implemented.	0b0001
[27:24]	TME	Indicates support for TME instructions. Defined values are: 0b0000 TME instructions are not implemented.	0b0000
[23:20]	Atomic	Indicates support for Atomic instructions in AArch64 state. Defined values are: 0b0010 LDADD, LDCLR, LDEOR, LDSET, LDSMAX, LDSMIN, LDUMAX, LDUMIN, CAS, CASP, and SWP instructions implemented.	0b0010

Bits	Name	Description	Reset
[19:16]	CRC32	Indicates support for CRC32 instructions in AArch64 state. Defined values are: 0b0001 CRC32B, CRC32H, CRC32W, CRC32X, CRC32CB, CRC32CH, CRC32CW, and CRC32CX instructions implemented.	0b0001
[15:12]	SHA2	Indicates support for SHA2 instructions in AArch64 state. Defined values are: 0b0000 No SHA2 instructions implemented. This value is reported when the Cryptographic Extension is not implemented or is disabled. 0b0010 SHA256H, SHA256H2, SHA256SU0, SHA256SU1, SHA512H, SHA512H2, SHA512SU0, and SHA512SU1 instructions implemented. This value is reported when the Cryptographic Extension is implemented and enabled. When the CRYPTO configuration parameter is true and the CRYPTODISABLE input is low at reset the Cryptographic Extension is implemented	The reset values can be the following: 0b0000, 0b0010, respective to the value.
[11:8]	SHA1	Indicates support for SHA1 instructions in AArch64 state. Defined values are: 0b0000 No SHA1 instructions implemented. This value is reported when the Cryptographic Extension is not implemented or is disabled. 0b0001 SHA1C, SHA1P, SHA1M, SHA1H, SHA1SU0, and SHA1SU1 instructions implemented. This value is reported when the Cryptographic Extension is implemented and enabled. When the CRYPTO configuration parameter is true and the CRYPTODISABLE input is low at reset the Cryptographic Extension is implemented	The reset values can be the following: 0b0000, 0b0001, respective to the value.
[7:4]	AES	Indicates support for AES instructions in AArch64 state. Defined values are: 0b0000 No AES instructions implemented. This value is reported when the Cryptographic Extension is not implemented or is disabled. 0b0010 AESE, AESD, AESMC, and AESIMC instructions are implemented plus PMULL/PMULL2 instructions operating on 64-bit data quantities. This value is reported when the Cryptographic Extension is implemented and enabled. When the CRYPTO configuration parameter is true and the CRYPTODISABLE input is low at reset the Cryptographic Extension is implemented	The reset values can be the following: 0b0000, 0b0010, respective to the value.
[3:0]	RES0	Reserved	RES0

Access

MRS <Xt>, ID_AA64ISAR0_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0110	0b000

Accessibility

MRS <Xt>, ID_AA64ISAR0_EL1

```
if PSTATE.EL == EL0 then
    if EL2Enabled() && HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        return ID_AA64ISAR0_EL1;
elseif PSTATE.EL == EL2 then
    return ID_AA64ISAR0_EL1;
elseif PSTATE.EL == EL3 then
    return ID_AA64ISAR0_EL1;
```

3.3 ID_AA64ZFR0_EL1, SVE Feature ID register 0

Provides additional information about the implemented features of the AArch64 Scalable Vector Extension, when the AArch64-ID_AA64PFR0_EL1.SVE field is not zero.

For general information about the interpretation of the ID registers see *Principles of the ID scheme for fields in ID registers* in the [Arm® Architecture Reference Manual for A-profile architecture](#).

Configurations



Prior to the introduction of the features described by this register, this register was unnamed and reserved, RES0 from EL1, EL2, and EL3.

Attributes

Width

64

Functional group

Identification registers

Access type

See bit descriptions

Reset value

xxxx	xxxx	xxxx	xxxx	0001	xxxx	xxxx	xxxx	xxxx	xxxx	0001	0001	xxxx	xxxx	xxxx	0001
63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3 0



Where the reset reads xxxx, see individual bits.

Bit descriptions

Figure 3-2: AArch64_id_aa64zfr0_el1 bit assignments

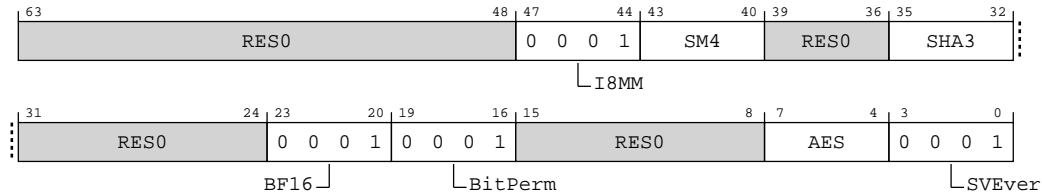


Table 3-4: ID_AA64ZFR0_EL1 bit descriptions

Bits	Name	Description	Reset
[63:48]	RES0	Reserved	RES0
[47:44]	I8MM	Indicates support for SVE Int8 matrix multiplication instructions. Defined values are: 0b0001 SMMLA, SUDOT, UMMLA, USMMLA, and USDOT instructions are implemented.	0b0001
[43:40]	SM4	Indicates support for SVE SM4 instructions. Defined values are: 0b0000 SVE2 SM4 instructions are not implemented. This value is reported when the Cryptographic Extension is not implemented or is disabled. 0b0001 SVE2 SM4E and SM4EKEY instructions are implemented. This value is reported when the Cryptographic Extension is implemented and enabled.	The reset values can be the following: 0b0000, 0b0001, respective to the value.
[39:36]	RES0	Reserved	RES0
[35:32]	SHA3	Indicates support for the SVE SHA3 instructions. Defined values are: 0b0000 SVE2 SHA3 instructions are not implemented. This value is reported when the Cryptographic Extension is not implemented or is disabled. 0b0001 SVE2 RAX1 instruction is implemented. This value is reported when the Cryptographic Extension is implemented and enabled.	The reset values can be the following: 0b0000, 0b0001, respective to the value.
[31:24]	RES0	Reserved	RES0
[23:20]	BF16	Indicates support for SVE BFloat16 instructions. Defined values are: 0b0001 BFCVT, BFCVTNT, BFDOT, BFMLALB, BFMLALT, and BFMMMLA instructions are implemented.	0b0001

Bits	Name	Description	Reset
[19:16]	BitPerm	Indicates support for SVE bit permute instructions. Defined values are: 0b0001 SVE BDEP, BEXT, and BGRP instructions are implemented.	0b0001
[15:8]	RES0	Reserved	RES0
[7:4]	AES	Indicates support for SVE AES instructions. Defined values are: 0b0000 SVE2-AES instructions are not implemented. This value is reported when the Cryptographic Extension is not implemented or is disabled. 0b0010 SVE2 AESE, AESD, AESMC, and AESIMC instructions are implemented plus SVE2 PMULLB and PMULLT instructions with 64-bit source. This value is reported when the Cryptographic Extension is implemented and enabled.	The reset values can be the following: 0b0000, 0b0010, respective to the value.
[3:0]	SVEver	Indicates support for SVE. Defined values are: 0b0001 The SVE and non-optional SVE2 instructions are implemented.	0b0001

Access

MRS <Xt>, ID_AA64ZFR0_EL1

op0	op1	CRn	CRm	op2
0b11	0b000	0b0000	0b0100	0b100

Accessibility

MRS <Xt>, ID_AA64ZFR0_EL1

```

if PSTATE.EL == EL0 then
    if EL2Enabled() && HCR_EL2.TGE == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        AArch64.SystemAccessTrap(EL1, 0x18);
elseif PSTATE.EL == EL1 then
    if EL2Enabled() && HCR_EL2.TID3 == '1' then
        AArch64.SystemAccessTrap(EL2, 0x18);
    else
        return ID_AA64ZFR0_EL1;
elseif PSTATE.EL == EL2 then
    return ID_AA64ZFR0_EL1;
elseif PSTATE.EL == EL3 then
    return ID_AA64ZFR0_EL1;

```

Appendix A Document revisions

This appendix records the changes between released issues of this document.

A.1 Revisions

Changes between released issues of this book are summarized in tables.

Table A-1: Issue 0000-01

Change	Location
First Confidential early access release for r0p0	-

Table A-2: Differences between issue 0000-01 and issue 0000-02

Change	Location
Second Non-Confidential early access release for r0p0	-
Editorial changes	Throughout document
Updated product name	Throughout document