

AS ISO/IEC 14443.4:2022
ISO/IEC 14443-4:2018
ISO/IEC 14443-4:2018/Amd 1:2021
ISO/IEC 14443-4:2018/Amd 2:2020



STANDARDS
Australia



Cards and security devices for personal identification — Contactless proximity objects

Part 4: Transmission protocol



currently in review, click buy full version

AS ISO/IEC 14443.4:2022

This Australian Standard ® was prepared by IT-017, Cards and security devices for personal identification. It was approved on behalf of the Council of Standards Australia on 7 June 2022.

This Standard was published on 24 June 2022.

The following are represented on Committee IT-017:

- Australia Post
- Australian Hotels Association
- Australian Industry Group
- Australian Passport Office
- Australian Security Industry Association
- Department of Home Affairs — Identity and Biometrics Division
- Department of Transport and Main Roads, QLD

This Standard was issued in draft form for comment as DR AS ISO/IEC 14443.4:2022.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

ISBN 978 1 76113 857 7

AS ISO/IEC 14443.4:2022
ISO/IEC 14443-4:2018
ISO/IEC 14443-4:2018/Amd 1:2021
ISO/IEC 14443-4:2018/Amd 2:2020

Cards and security devices for personal identification — Contactless proximity objects

Part 4: Transmission protocol

Originated as AS 14443.4—2003.
Second edition 2022.

COPYRIGHT

© ISO/IEC 2022 — All rights reserved
© Standards Australia Limited 2022

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

Preface

This Standard was prepared by the Standards Australia Committee IT-017, Cards and security devices for personal identification, to supersede AS 14443.4:2003, *Identification cards — Contactless integrated circuit(s) cards — Proximity cards, Part 4: Transmission protocol*.

The objective of this document is to specify a half-duplex block transmission protocol featuring the special needs of a contactless environment and defines the activation and deactivation sequence of the protocol.

This document is intended to be used in conjunction with other parts of the AS ISO/IEC 14443 series and is applicable to proximity cards or objects of Type A and Type B.

This document is identical with, and has been reproduced from, ISO/IEC 14443-4:2018, *Cards and security devices for personal identification — Contactless proximity objects — Part 4: Transmission protocol* and its Amendment No. 1 (2021) and Amendment No. 2 (2020) which have been added at the end of the source text.

As this document has been reproduced from an International document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical or options of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface	ii
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols, abbreviated terms and notation	2
4.1 Symbols and abbreviated terms	2
4.2 Notations	4
5 Protocol activation of PICC Type A	4
5.1 Activation sequences	4
5.2 Request for answer to select	6
5.3 Answer to select	7
5.3.1 Structure of the bytes	8
5.3.2 Length byte	8
5.3.3 Format byte	8
5.3.4 Interface byte TA(1)	9
5.3.5 Interface byte TB(1)	9
5.3.6 Interface byte TC(1)	10
5.3.7 Historical bytes	11
5.4 Protocol and parameter selection request	11
5.4.1 Start byte	11
5.4.2 Parameter 0	11
5.4.3 Parameter 1	12
5.5 Protocol and parameter selection response	12
5.6 Activation frame waiting time	13
5.7 Error detection and recovery	13
5.7.1 Handling of RATs and ATS	13
5.7.2 Handling of P.S. request and PPS response	13
5.7.3 Handling of the CID during activation	14
6 Protocol activation of PICC Type B	14
7 Half-duplex block transmission protocol	15
7.1 Elements and mechanisms	15
7.2 Block format	15
7.2.1 Length field	16
7.2.2 Prologue field	16
7.2.3 Information field	19
7.2.4 Epilogue field	19
7.3 Frame waiting time	19
7.4 Frame waiting time extension	20
7.5 Power level indication	21
7.6 Protocol operation	21
7.6.1 S(PARAMETERS) blocks	21
7.6.2 Multi-Activation	23
7.6.3 Chaining	23
7.6.4 Block numbering rules	24
7.6.5 Block handling rules	25
7.6.6 PICC presence check	26
7.6.7 Error detection and recovery	26
8 Protocol deactivation of PICC Type A and Type B	27
8.1 Deactivation frame waiting time	27

8.2	Error detection and recovery.....	27
9	Activation of bit rates and framing options in PROTOCOL state	27
10	Frame with error correction	30
10.1	General.....	30
10.2	Type A PCD frame format for bit rates up to $fc/16$ and higher than $fc/2$ and Type A PICC frame format for all bit rates.....	30
10.3	Type A PCD frame format for bit rates of $fc/8$, $fc/4$ and $fc/2$ and Type B PCD and PICC frame format for all bit rates.....	31
10.4	Enhanced block with error correction.....	31
10.4.1	General.....	31
10.4.2	Modified Hamming sub-block format.....	31
10.4.3	Hamming control byte.....	31
10.4.4	Hamming control generation matrix A	32
10.4.5	Hamming control bits calculation.....	32
10.4.6	Hamming control check matrix H	32
10.4.7	Error correction.....	33
10.5	Activation of frame with error correction in PROTOCOL state.....	33
Annex A	(informative) Multi-Activation example	37
Annex B	(informative) Protocol scenarios	38
Annex C	(informative) Block and frame coding overview	47
Annex D (deliberately left blank).....	49
Annex E	(informative) CRC_32 encoding	50
Annex F	(informative) Frame with error correction	52
Annex G	(informative) Framing options	54
Bibliography	55
Amendment 1	56
Annex H	(informative) Examples of PCD usage	59
Amendment 2	61

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology, SC 17, Cards and security devices for personal identification*.

This fourth edition cancels and replaces the third edition (ISO/IEC 14443-4:2016), which has been technically revised.

A list of all the parts in the ISO/IEC 14443 series can be found on the ISO website.

Introduction

The ISO/IEC 14443 series of standards describes the parameters for identification cards or objects for international interchange.

The protocol, as defined in this document, is capable of transferring the application protocol data units as defined in ISO/IEC 7816-4. Thus, application protocol data units and application selection may be used as defined in ISO/IEC 7816-4.

The ISO/IEC 14443 series of standards is intended to allow operation of proximity cards in the presence of other contactless cards or objects conforming to the ISO/IEC 10536 series of standards and the ISO/IEC 15693 series of standards and near field communication (NFC) devices conforming to ISO/IEC 18092 and ISO/IEC 21481.

Australian Standard®

Cards and security devices for personal identification — Contactless proximity objects

Part 4: Transmission protocol

1 Scope

This document specifies a half-duplex block transmission protocol featuring the special needs of a contactless environment and defines the activation and deactivation sequence of the protocol.

This document is intended to be used in conjunction with other parts of ISO/IEC 14443 and is applicable to proximity cards or objects of Type A and Type B.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7816-3, *Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols*

ISO/IEC 7816-4:2013, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 14443-2¹⁾, *Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface*

ISO/IEC 14443-3, *Cards and security devices for personal identification — Contactless proximity objects — Part 3: Initialization and anticollision*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia, available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

3.1

bit duration

one elementary time unit (etu), calculated by the following formula:

$$1 \text{ etu} = 128 / (D \times fc)$$

Note 1 to entry: The initial value of the divisor D is 1, giving the initial etu as follows:

$$1 \text{ etu} = 128 / fc$$

where fc is the carrier frequency as defined in ISO/IEC 14443-2.

1) Fourth edition to be published. Current stage: 40.60.