

Australian Standard™

**Identification cards—Contactless
integrated circuit(s) cards—
Proximity cards**

Part 4: Transmission protocol



Standards Australia



Documents

Document Sharing Hub

This Australian Standard was prepared by Committee IT-012, Information Systems, Security and Information Technology. It was approved on behalf of the Council of Standards Australia on 4 March 2003 and published on 31 March 2003.

The following are represented on Committee IT-012:

Attorney General's Department
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber of Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Australian Information Industry Association
Certification Forum of Australia
Department of Defence (Australia)
Department of Social Welfare New Zealand
Government Communications Security Bureau, New Zealand
Internet Industry Association
NSW Police Service
New Zealand Defence Force
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Australia web site at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Australian Standard*, has a full listing of revisions and amendments published each month.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.com.au, or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

This Standard was issued in draft form for comment as DR 02529.

Australian Standard™

**Identification cards—Contactless
integrated circuit(s) cards—
Proximity cards**

Part 4: Transmission protocol

First published as AS 14443.4—2003.

COPYRIGHT

© Standards Australia International

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.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 5117 2

 **Documents**
Document Sharing Hub

PREFACE

This Standard was prepared by the Australian members of the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Information Technology. After consultation with stakeholders in both countries, Standards Australia and Standards New Zealand decided to develop this Standard as an Australian, rather than an Australian/New Zealand Standard.

It is identical with, and has been reproduced from ISO/IEC 14443-4:2001, *Identification cards—Contactless integrated circuit(s) cards—Proximity cards*, Part 4: *Transmission protocol*.

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

This Standard is Part 4 of AS/NZS 14443, *Identification cards—Contactless integrated circuit(s) cards—Proximity cards*, which is published in parts as follows:

Part 1: Physical characteristics

Part 2: Radio frequency power and signal interface

Part 3: Initialization and anticollision

Part 4: Transmission protocol (this Standard)

The terms ‘normative’ and ‘informative’ are used to define the application of the annex to which they apply. A normative annex is an integral part of a Standard, whereas an informative annex is only for information and guidance.

As this Standard is reproduced from an International Standard, the following applies:

- (a) Its number appears on the cover and title page while the International Standard number appears only on the cover.
- (b) In the source text ‘this part of ISO/IEC 14443’ should read ‘this Australian Standard’.
- (c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

<i>Reference to International Standard</i>		<i>Australian Standard</i>	
ISO/IEC		AS	
14443	Identification cards—Contactless integrated circuit(s) cards—Proximity cards	14443	Identification cards—Contactless integrated circuit(s) cards—Proximity cards
14443-2	Part 2: Radio frequency power and signal interface	14443.2	Part 2: Radio frequency power and signal interface
14443-3	Part 3: Initialization and anticollision	14443.3	Part 3: Initialization and anticollision

CONTENTS

Page

1	Scope.....	1
2	Normative references	1
3	Terms and definitions.....	1
4	Symbols and abbreviated terms.....	2
5	Protocol activation of PICC Type A.....	4
5.1	Request for answer to select	6
5.2	Answer to select.....	6
5.2.1	Structure of the bytes	7
5.2.2	Length byte.....	7
5.2.3	Format byte.....	7
5.2.4	Interface byte TA(1).....	8
5.2.5	Interface byte TB(1).....	8
5.2.6	Interface byte TC(1).....	9
5.2.7	Historical bytes	9
5.3	Protocol and parameter selection request	10
5.3.1	Start byte.....	10
5.3.2	Parameter 0.....	11
5.3.3	Parameter 1.....	11
5.4	Protocol and parameter selection response.....	12
5.5	Activation frame waiting time	12
5.6	Error detection and recovery	12
5.6.1	Handling of RATS and ATS.....	12
5.6.2	Handling of PPS request and PPS response	13
5.6.3	Handling of the CID during activation.....	13
6	Protocol activation of PICC Type B.....	14
7	Half-duplex block transmission protocol	14
7.1	Block format	15
7.1.1	Prologue field	15
7.1.2	Information field	17
7.1.3	Epilogue field.....	18
7.2	Frame waiting time.....	18
7.3	Frame waiting time extension.....	18
7.4	Power level indication	19
7.5	Protocol operation	20
7.5.1	Multi-Activation	20
7.5.2	Chaining	20
7.5.3	Block numbering rules	21
7.5.4	Block handling rules.....	21
7.5.5	Error detection and recovery	22
8	Protocol deactivation of PICC Type A and Type B.....	23
8.1	Deactivation frame waiting time	23
8.2	Error detection and recovery	23
	Annex A (informative) Multi-Activation example	24
	Annex B (informative) Protocol scenarios.....	25
B.1	Notation.....	25
B.2	Error-free operation	25
B.2.1	Exchange of I-blocks	25
B.2.2	Request for waiting time extension	26

B.2.3	DESELECT	26
B.2.4	Chaining.....	26
B.3	Error handling.....	27
B.3.1	Exchange of I-blocks	27
B.3.2	Request for waiting time extension.....	28
B.3.3	DESELECT	30
B.3.4	Chaining.....	30
Annex C (informative)	Block and frame coding overview	33

AUSTRALIAN STANDARD

Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol

1 Scope

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

2 Normative references

The following normative documents contain provisions, which, through reference in this text, constitute provisions of this part of ISO/IEC 14443. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 14443 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 7816-3, *Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols.*

ISO/IEC 7816-4, *Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange.*

ISO/IEC 7816-5, *Identification cards – Integrated circuit(s) cards with contacts – Part 5: Numbering system and registration procedure for application identifiers.*

ISO/IEC 14443-2, *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface.*

ISO/IEC 14443-3, *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision.*

3 Terms and definitions

For the purposes of this part of ISO/IEC 14443, the following terms and definitions apply.

3.1

bit duration

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

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

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

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

Where f_c is the carrier frequency as defined in ISO/IEC 14443-2.

3.2 block

special type of frame, which contains a valid protocol data format

NOTE A valid protocol data format includes I-blocks, R-blocks or S-blocks.

3.3 invalid block

type of frame, which contains an invalid protocol format

NOTE A time-out, when no frame has been received, is not interpreted as an invalid block.

3.4 frame

sequence of bits as defined in ISO/IEC 14443-3

NOTE The PICC Type A uses the standard frame defined for Type A and the PICC Type B uses the frame defined for Type B.

4 Symbols and abbreviated terms

ACK	positive ACKnowledgement
ATS	Answer To Select
ATQA	Answer To reQuest, Type A
ATQB	Answer To reQuest, Type B
CID	Card IDentifier
CRC	Cyclic Redundancy Check, as defined for each PICC Type in ISO/IEC 14443-3
D	Divisor
DR	Divisor Receive (PCD to PICC)
DRI	Divisor Receive Integer (PCD to PICC)
DS	Divisor Send (PICC to PCD)
DSI	Divisor Send Integer (PICC to PCD)
EDC	Error Detection Code
etu	elementary time unit
f_c	carrier frequency
FSC	Frame Size for proximity Card
FSCI	Frame Size for proximity Card Integer
FSD	Frame Size for proximity coupling Device
FSDI	Frame Size for proximity coupling Device Integer
FWI	Frame Waiting time Integer

FWT	Frame Waiting Time
FWT _{TEMP}	temporary Frame Waiting Time
HLTA	HALT Command, Type A
I-block	Information block
INF	INformation Field
MAX	Index to define a maximum value
MIN	Index to define a minimum value
NAD	Node ADdress
NAK	Negative AcKnowledge
OSI	Open Systems Interconnection
PCB	Protocol Control Byte
PCD	Proximity Coupling Device
PICC	Proximity Card
PPS	Protocol and Parameter Selection
PPSS	Protocol and Parameter Selection Start
PPS0	Protocol and Parameter Selection parameter 0
PPS1	Protocol and Parameter Selection parameter 1
R-block	Receive ready block
R(ACK)	R-block containing a positive acknowledge
R(NAK)	R-block containing a negative acknowledge
RATS	Request for Answer To Select
REQA	REQuest Command, Type A
RFU	Reserved for Future Use
S-block	Supervisory block
SAK	Select AcKnowledge
SFGI	Start-up Frame Guard time Integer
SFGT	Start-up Frame Guard Time
WUPA	Wake-Up Command, Type A
WTX	Waiting Time eXtension
WTXM	Waiting Time eXtension Multiplier

5 Protocol activation of PICC Type A

The following activation sequence shall be applied:

- PICC activation sequence as defined in ISO/IEC 14443-3 (request, anticollision loop and select).
- At the beginning the SAK byte shall be checked for availability of an ATS. The SAK is defined in ISO/IEC 14443-3.
- The PICC may be set to HALT state, using the HLTA Command as defined in ISO/IEC 14443-3, if no ATS is available.
- The RATS may be sent by the PCD as next command after receiving the SAK if an ATS is available.
- The PICC shall send its ATS as answer to the RATS. The PICC shall only answer to the RATS if the RATS is received directly after the selection.
- If the PICC supports any changeable parameters in the ATS, a PPS request may be used by the PCD as the next command after receiving the ATS to change parameters.
- The PICC shall send a PPS Response as answer to the PPS request.

A PICC does not need to implement the PPS, if it does not support any changeable parameters in the ATS.

The PCD activation sequence for a PICC Type A is shown in Figure 1.

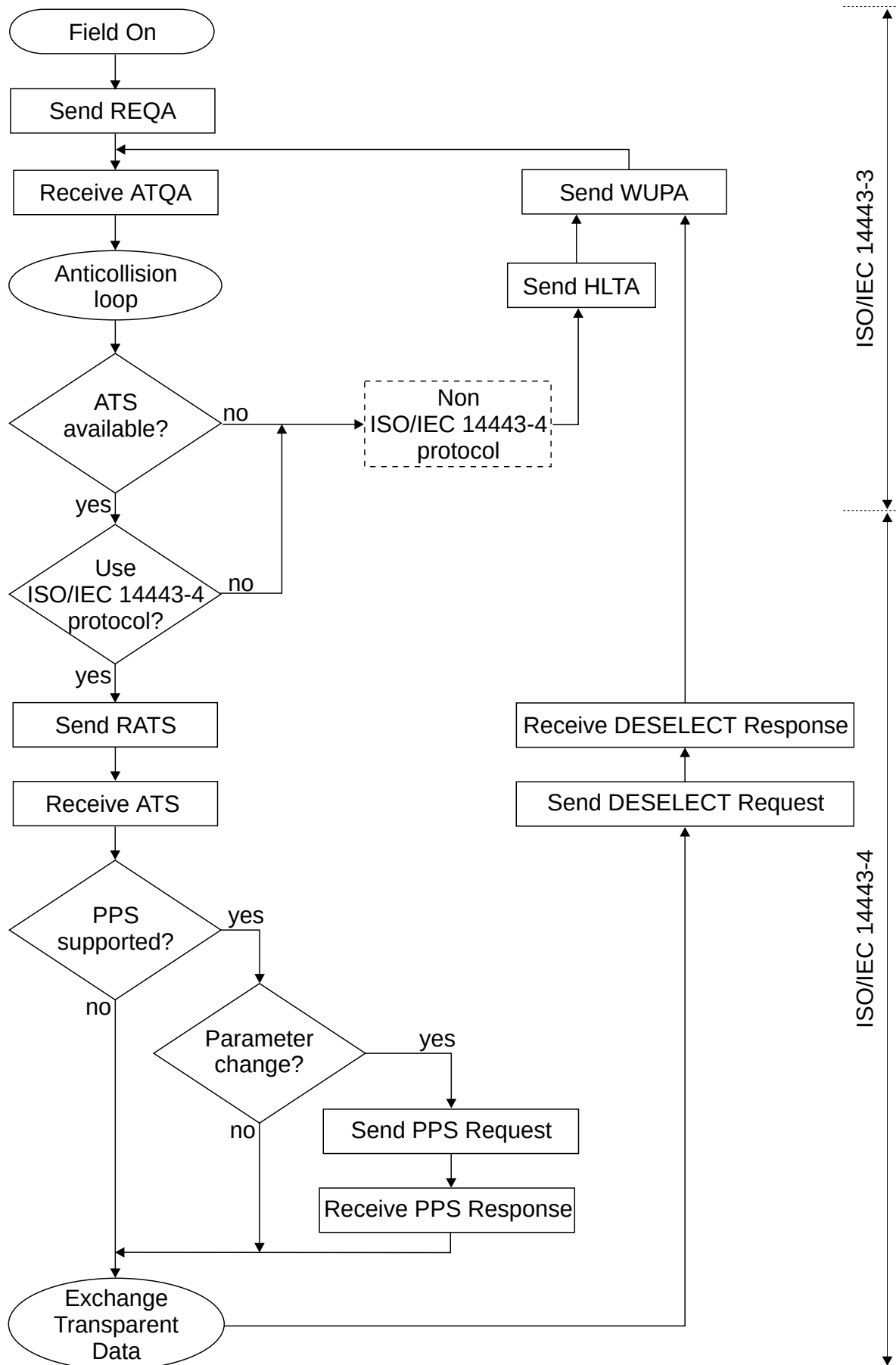


Figure 1 — Activation of a PICC Type A by a PCD

5.1 Request for answer to select

This clause defines the RATS with all its fields (see Figure 2).

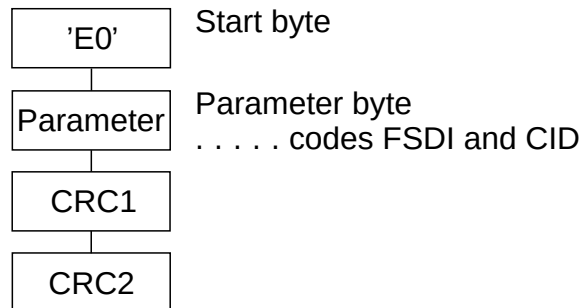


Figure 2 — Request for answer to select

The parameter byte consists of two parts (see Figure 3):

- The most significant half-byte b8 to b5 is called FSDI and codes FSD. The FSD defines the maximum size of a frame the PCD is able to receive. The coding of FSD is given in Table 1.
- The least significant half byte b4 to b1 is named CID and it defines the logical number of the addressed PICC in the range from 0 to 14. The value 15 is RFU. The CID is specified by the PCD and shall be unique for all PICCs, which are in the ACTIVE state at the same time. The CID is fixed for the time the PICC is active and the PICC shall use the CID as its logical identifier, which is contained in the first error-free RATS received.

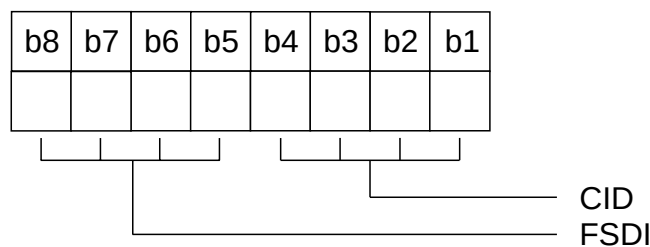


Figure 3 — Coding of RATS parameter byte

Table 1 — FSDI to FSD conversion

FSDI	'0'	'1'	'2'	'3'	'4'	'5'	'6'	'7'	'8'	'9'-'F'
FSD (bytes)	16	24	32	40	48	64	96	128	256	RFU >256

5.2 Answer to select

This clause defines the ATS with all its available fields (see Figure 4).

In the case that one of the defined fields is not present in an ATS sent by a PICC the default values for that field shall apply.

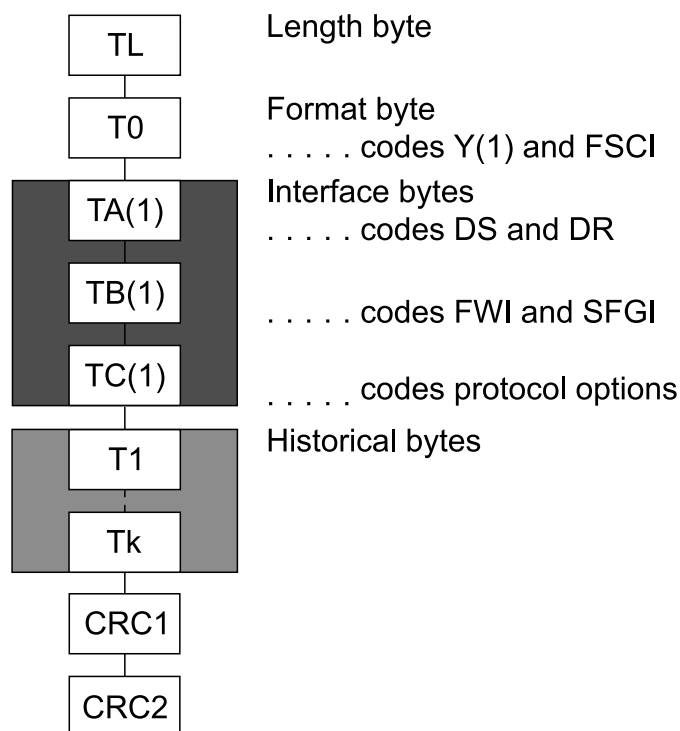


Figure 4 — Structure of the ATS

5.2.1 Structure of the bytes

The length byte TL is followed by a variable number of optional subsequent bytes in the following order:

- format byte T0,
- interface bytes TA(1), TB(1), TC(1) and
- historical bytes T1 to Tk.

5.2.2 Length byte

The length byte TL is mandatory and specifies the length of the transmitted ATS including itself. The two CRC bytes are not included in TL. The maximum size of the ATS shall not exceed the indicated FSD. Therefore the maximum value of TL shall not exceed FSD-2.

5.2.3 Format byte

The format byte T0 is optional and is present as soon as the length is greater than 1. The ATS can only contain the following optional bytes when this format byte is present.

T0 consists of three parts (see Figure 5):

- The most significant bit b8 shall be set to 0. The value 1 is RFU.
- The bits b7 to b5 contain Y(1) indicating the presence of subsequent interface bytes TC(1), TB(1) and TA(1).
- The least significant half byte b4 to b1 is called FSCI and codes FSC. The FSC defines the maximum size of a frame accepted by the PICC. The default value of FSCI is 2 and leads to a FSC of 32 bytes. The coding of FSC is equal to the coding of FSD (see Table 1).

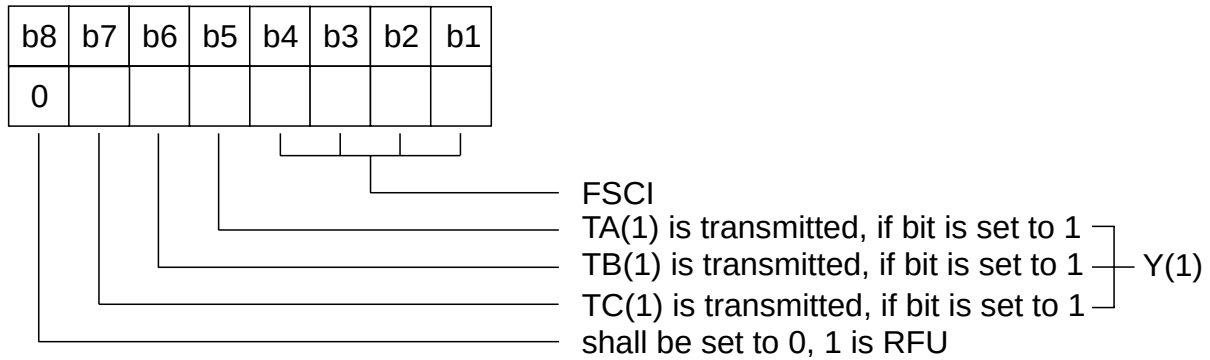


Figure 5 — Coding of format byte

5.2.4 Interface byte TA(1)

The interface byte TA(1) consists of four parts (see Figure 6):

- The most significant bit b8 codes the possibility to handle different divisors for each direction. When this bit is set to 1 the PICC is unable to handle different divisors for each direction.
- The bits b7 to b5 code the bit rate capability of the PICC for the direction from PICC to PCD, called DS. The default value shall be (000)b.
- The bit b4 shall be set to (0)b and the other value is RFU.
- The bits b3 to b1 code the bit rate capability of the PICC for the direction from PCD to PICC, called DR. The default value shall be (000)b.

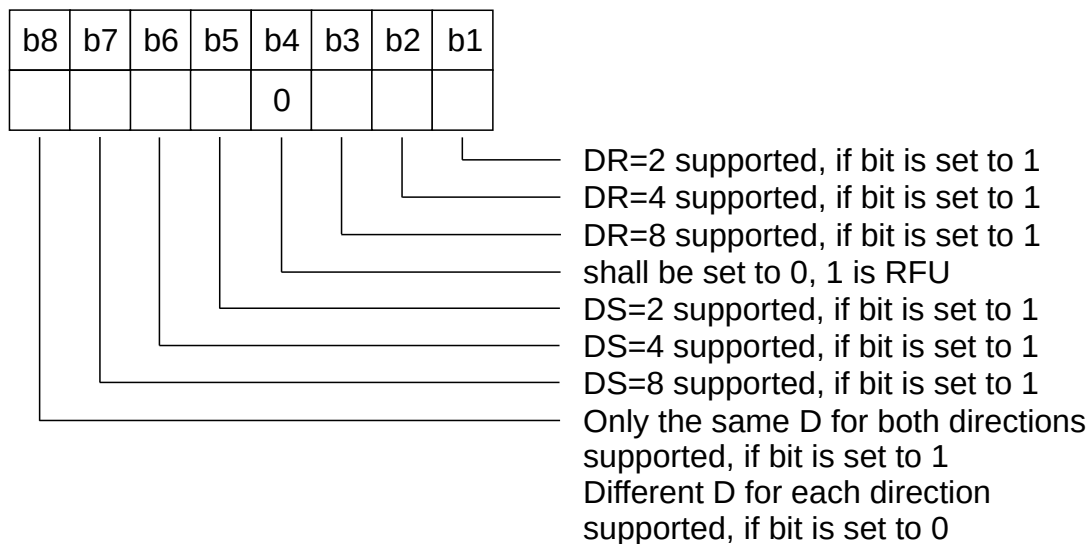


Figure 6 — Coding of interface byte TA(1)

The selection of a specific divisor D for each direction may be done by the PCD using a PPS.

5.2.5 Interface byte TB(1)

The interface byte TB(1) conveys information to define the frame waiting time and the start-up frame guard time.

The interface byte TB(1) consists of two parts (see Figure 7):

- The most significant half-byte b8 to b5 is called FWI and codes FWT (see 7.2).