



BSI Standards Publication

Cards and security devices for personal identification — Contactless proximity objects

Part 4: Transmission protocol

National foreword

This British Standard is the UK implementation of ISO/IEC 14443-4:2018+A2:2020. It supersedes BS ISO/IEC 14443-4:2018, which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to ISO/IEC text carry the number of the ISO/IEC amendment. For example, text altered by ISO/IEC amendment 1 is indicated by A1 A1.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and security devices for personal identification.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 03309 0

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2018.

Amendments/corrigenda issued since publication

Date	Text affected
30 June 2021	Implementation of ISO/IEC amendment 1:2021 and ISO/IEC amendment 2:2020

INTERNATIONAL
STANDARD

ISO/IEC
14443-4

Fourth edition
2018-07-01

**Cards and security devices for
personal identification — Contactless
proximity objects —**

**Part 4:
Transmission protocol**

*Cartes et dispositifs de sécurité pour l'identification personnelle —
Objets sans contact de proximité —*

Partie 4: Protocole de transmission



Reference number
ISO/IEC 14443-4:2018(E)

AVA Documents
Document Sharing Hub
© ISO 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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	5
5.1 Activation sequences	5
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 PPS 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 (optional) 	21
7.6 Protocol operation	22
7.6.1 S(PARAMETERS) blocks	22
7.6.2 Multi-Activation	24
7.6.3 Chaining	24
7.6.4 Block numbering rules	25
7.6.5 Block handling rules	26
7.6.6 PICC presence check	27
7.6.7 Error detection and recovery	27
8 Protocol deactivation of PICC Type A and Type B	28
8.1 Deactivation frame waiting time	28
8.2 Error detection and recovery	28

9	Activation of bit rates and framing options in PROTOCOL state	28
10	Frame with error correction	31
10.1	General	31
10.2	Type A PCD frame format for bit rates up to $f_c/16$ and higher than $f_c/2$ and Type A PICC frame format for all bit rates	31
10.3	Type A PCD frame format for bit rates of $f_c/8$, $f_c/4$ and $f_c/2$ and Type B PCD and PICC frame format for all bit rates	32
10.4	Enhanced block with error correction	32
10.4.1	General	32
10.4.2	Modified Hamming sub-block format	32
10.4.3	Hamming control byte	32
10.4.4	Hamming control generation matrix A	33
10.4.5	Hamming control bits calculation	33
10.4.6	Hamming control check matrix H	33
10.4.7	Error correction	34
10.5	Activation of frame with error correction in PROTOCOL state	34
	Annex A (informative) Multi-Activation example	38
	Annex B (informative) Protocol scenarios	39
	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
	Annex H (informative) Examples of PLI_{CID} usage	55
	Bibliography	57

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) ^[A2] or the IEC list of patent declarations received (see <http://patents.iec.ch>) ^[A2].

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.

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 A_2 deactivation A_2 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 14443-2^{1\)}](#), *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:

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

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

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 1 to entry: 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 1 to entry: 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 1 to entry: The PICC independent from its type may use the frame with error correction defined in [Clause 10](#). Alternatively, the PICC Type A can use one of the standard frames defined for Type A and the PICC Type B can use the frame defined for Type B. This Type B frame is called standard frame, too, within this document.

4 Symbols, abbreviated terms and notation

4.1 Symbols and abbreviated terms

A	Hamming control bits generation matrix (6 rows, 56 columns)
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
CRC1	most significant byte of CRC (b16 to b9)
CRC2	least significant byte of CRC (b8 to b1)
CRC_32	Cyclic Redundancy Check error detection code used within enhanced block
c_n	Hamming control bit n
$\underline{d}$	vector containing 56 data bits
d_n	data bit n
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
H	matrix needed to calculate Hamming syndrome $\underline{s}$ (6 rows, 62 columns)
$h'_{m,n}$	element in row m and column n of matrix H'
H'	matrix needed to get matrix A (6 rows, 62 columns)
$\underline{h}'_n$	column vector of matrix H'
$\langle A_1 \rangle H_{LP}$	minimum requested field strength $\langle A_1 \rangle$
HLTA	HALT command, Type A
$\langle A_1 \rangle H_{step, max}$	PCD maximum field strength step increase or step decrease $\langle A_1 \rangle$
$I_{6 \times 6}$	6 by 6 Identity matrix
I-block	Information block
INF	INformation field
LEN	two bytes LENgth field used within enhanced block
m	row index
MAX	index to define a MAXimum value
MIN	index to define a MINimum value
n	column index
NAD	Node ADdress
NAK	Negative AcKnowledgegement
OSI	Open Systems Interconnection
PCB	Protocol Control Byte
PCD	Proximity Coupling Device

PICC	Proximity card or object
$\langle A_1 \rangle$ PLI _{CID}	Power Level Indication in CID field $\langle A_1 \rangle$
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 acknowledgement
R(NAK)	R-block containing a negative acknowledgement
RATS	Request for Answer To Select
REQA	REQuest command, Type A
RFU	Reserved for Future Use
$\underline{s}$	6-bit vector containing Hamming syndrome
s'	error position code
s	error position
S-block	Supervisory block
SAK	Select AcKnowledge
SFGI	Start-up Frame Guard time Integer
SFGT	Start-up Frame Guard Time
SYNC	SYNChronization sequence
$\langle A_1 \rangle t_{PL}$	guard time for PCD power level change $\langle A_1 \rangle$
WUPA	Wake-UP command, Type A
WTX	Waiting Time eXtension
WTXM	Waiting Time eXtension Multiplier
$\underline{y}$	64-bit vector ($\underline{y}'$ with no padding bits)
$\underline{y}'$	64-bit vector containing received modified Hamming sub-block
y'_n	received bit n in each modified Hamming sub-block

4.2 Notations

For the purposes of this document, the following notations apply:

- (xxxxx)b data bit representation;
- 'XY' hexadecimal notation, equal to XY to the base 16.

5 Protocol activation of PICC Type A

5.1 Activation sequences

The following activation sequence shall be applied.

- PICC activation sequence as defined in [ISO/IEC 14443-3](#) (request, anticollision loop and select).
- The SAK byte shall be checked to get information if the PICC is compliant with ISO/IEC 14443-4. The SAK byte 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 e.g. no ISO/IEC 14443-4 protocol is used at the PCD (the PCD cannot continue the activation sequence in that case).
- If the PICC is compliant to ISO/IEC 14443-4, the RATS may be sent by the PCD as next command after receiving the SAK.
- 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.

The 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](#).

The RFU handling specified in ISO/IEC 14443-3:2018, 5.3 applies for [Clause 5](#).

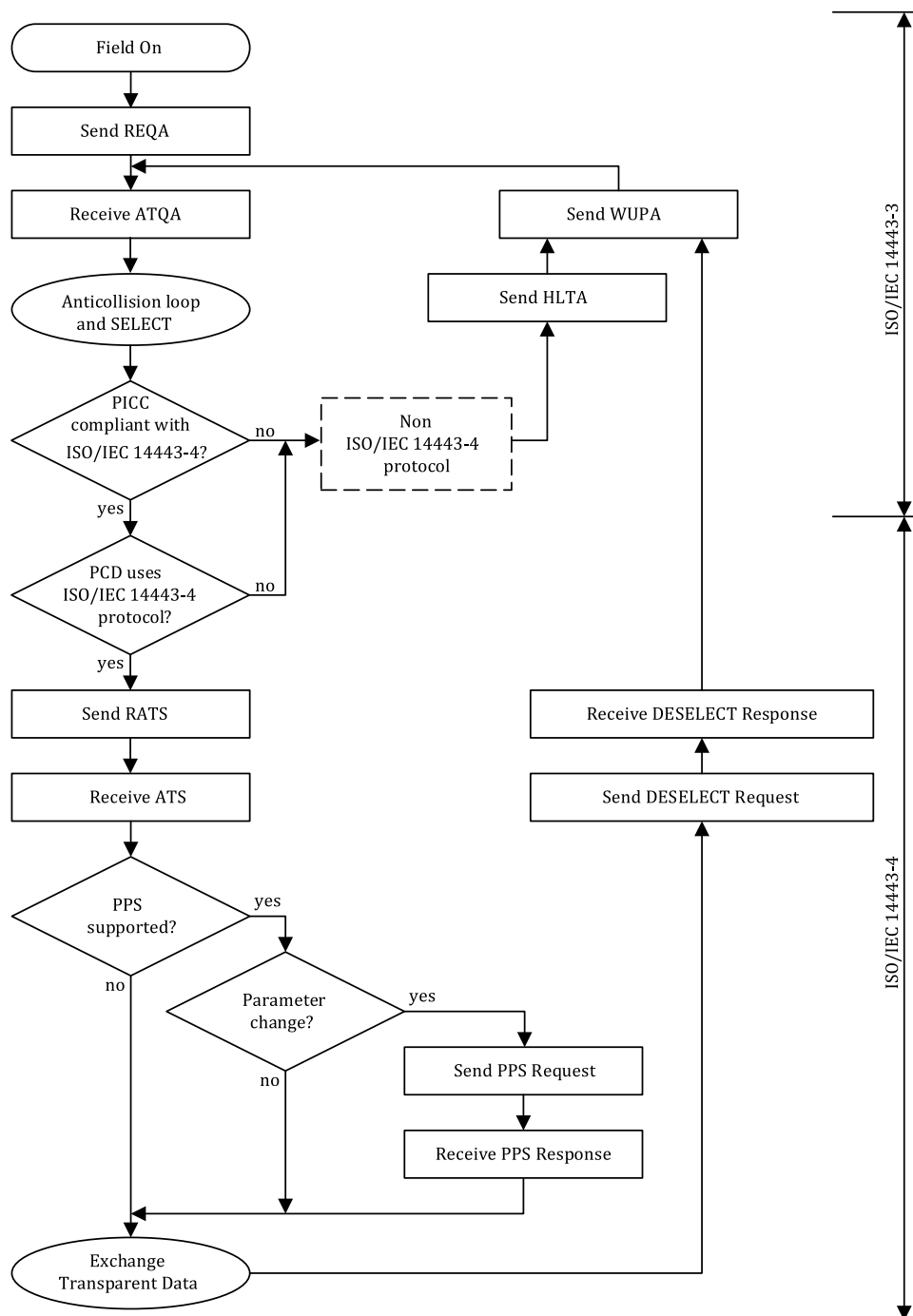
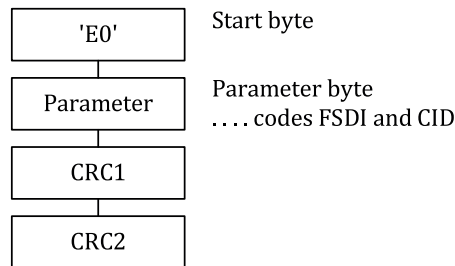


Figure 1 — Activation of a PICC Type A by a PCD

5.2 Request for answer to select

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

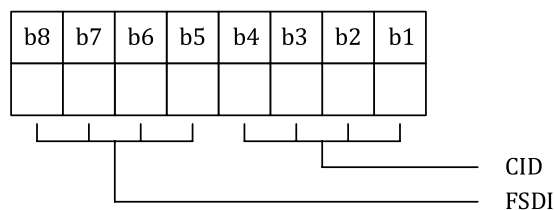
**Figure 2 — Request for answer to select**

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](#).
- Until the RFU values 'D'-'F' are assigned, a PICC receiving an FSDI with a value = 'D'-'F' shall interpret it as FSDI = 'C' (FSD = 4 096 bytes).

NOTE This PCD requirement is added for PCD's compatibility with future PICCs when a revision to this document further defines the behaviour for the RFU values of 'D'-'F'.

- 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 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'	'A'	'B'	'C'	'D' - 'F'
FSD (bytes)	16	24	32	40	48	64	96	128	256	512	1 024	2 048	4 096	RFU

5.3 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 the PICC, the default values for that field shall apply.

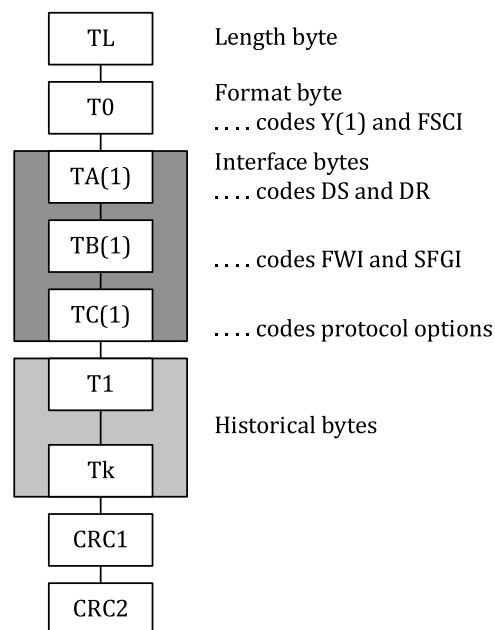


Figure 4 — Structure of the ATS

5.3.1 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);
- historical bytes T1 to Tk.

5.3.2 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.

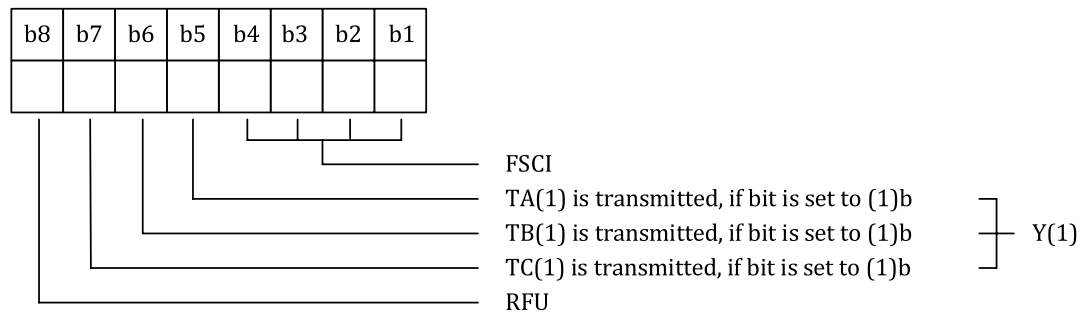
5.3.3 Format byte

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](#)).

- b8 is RFU.
- 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](#)).
- Until the RFU values 'D'-'F' are assigned, a PCD receiving an FSCI with a value = 'D'-'F' shall interpret it as FSCI = 'C' (FSC = 4 096 bytes).

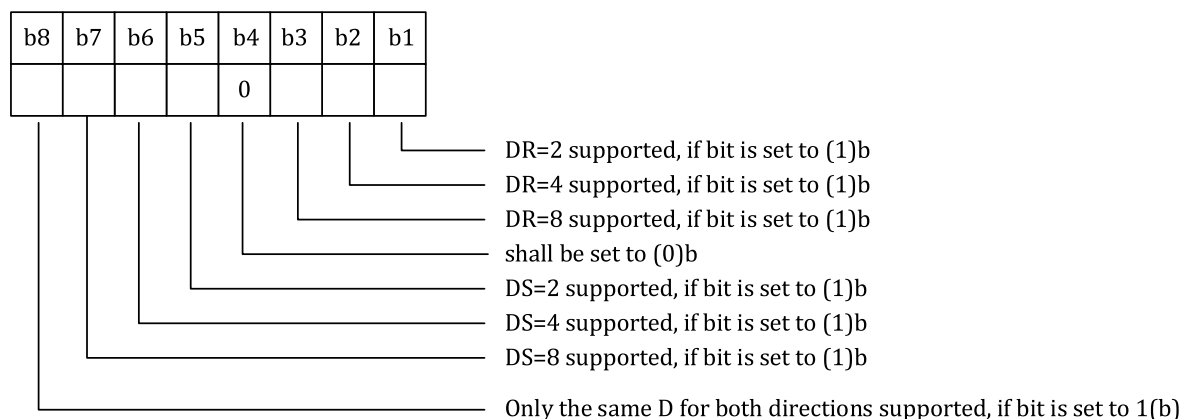
NOTE This PICC requirement is added for PICC's compatibility with future PCDs when a revision to this document further defines the behaviour for the RFU values 'D' – 'F'.

**Figure 5 — Coding of format byte**

5.3.4 Interface byte TA(1)

The interface byte TA(1) consists of four parts (see [Figure 6](#)).

- 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.
- 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.
- b4 shall be set to (0)b.
- 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 PPS.

A PCD receiving TA(1) with b4 = (1)b shall interpret it as (b8 to b1) = (00000000)b, implying only ~106 kbit/s supported in both directions. The definition of TA(1) with b4 = (1)b is otherwise undefined.

5.3.5 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 [7.3](#)).

- The least significant half byte b4 to b1 is called SFGI and codes a multiplier value used to define the SFGT. The SFGT defines a specific guard time needed by the PICC before it is ready to receive the next frame after it has sent the ATS. SFGI is coded in the range from 0 to 14. The value of 15 is RFU. The value of 0 indicates no SFGT needed and the values in the range from 1 to 14 are used to calculate the SFGT with the formula given below. The default value of SFGI is 0.

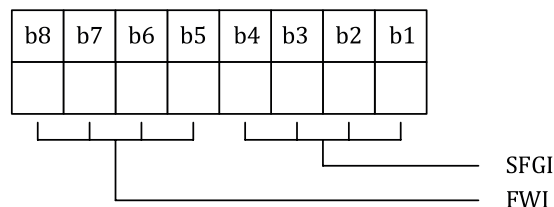


Figure 7 — Coding of interface byte TB(1)

SFGT is calculated by the following formulae:

$$\text{SFGT} = (256 \times 16/fc) \times 2^{\text{SFGI}}$$

SFGT_{MIN} = minimum value of the frame delay time as defined in ISO/IEC 14443-3

$\text{SFGT}_{\text{DEFAULT}}$ = minimum value of the frame delay time as defined in ISO/IEC 14443-3

$$\text{SFGT}_{\text{MAX}} = (256 \times 16/fc) \times 2^{14} (\sim 4\,949 \text{ ms})$$

Until the RFU value 15 is assigned, a PCD receiving SFGI = 15 shall interpret it as SFGI = 0.

Until the RFU value 15 is assigned, a PCD receiving FWI = 15 shall interpret it as FWI = 4.

5.3.6 Interface byte TC(1)

The interface byte TC(1) specifies a parameter of the protocol.

The specific interface byte TC(1) consists of two parts (see [Figure 8](#)).

- b8 to b3 are each RFU.
- b2 and b1 define which optional fields in the prologue field a PICC does support. The PCD is allowed to skip fields, which are supported by the PICC, but a field not supported by the PICC shall never be transmitted by the PCD. The default value shall be (10)b indicating CID supported and NAD not supported.

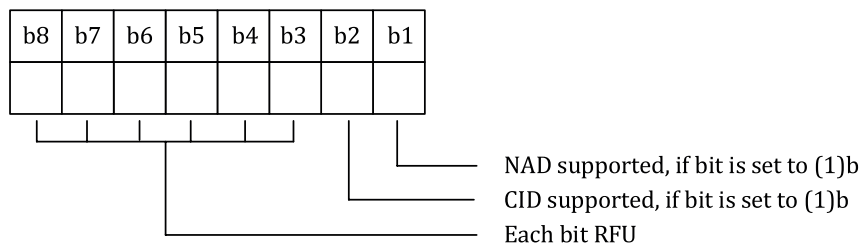


Figure 8 — Coding of interface byte TC(1)

5.3.7 Historical bytes

The historical bytes T1 to Tk are optional and designate general information. The maximum length of the ATS gives the maximum possible number of historical bytes. [ISO/IEC 7816-4](#) specifies the content of the historical bytes.

5.4 Protocol and parameter selection request

PPS request contains the start byte that is followed by two parameter bytes (see [Figure 9](#)).

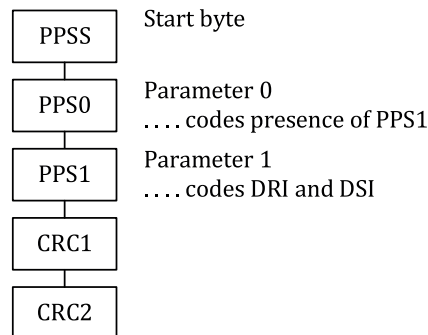


Figure 9 — Protocol and parameter selection request

5.4.1 Start byte

PPSS consists of two parts (see [Figure 10](#)).

- The most significant half byte b8 to b5 shall be set to (1101)b and identifies the PPS.
- The least significant half byte b4 to b1 is named CID and it defines the logical number of the addressed PICC.

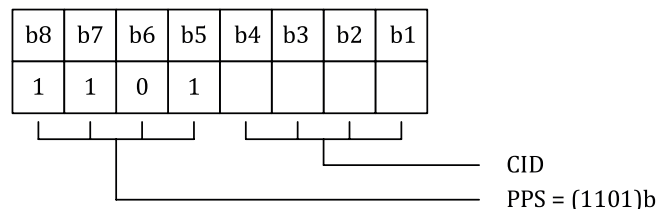


Figure 10 — Coding of PPSS

5.4.2 Parameter 0

PPS0 indicates the presence of the optional byte PPS1 (see [Figure 11](#)).

The PCD shall set (b4 to b1) = (0001)b and (b8 to b6) = (000)b.

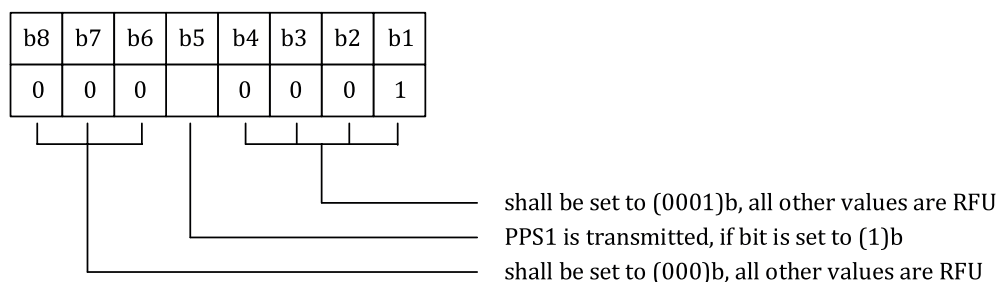


Figure 11 — Coding of PPS0

5.4.3 Parameter 1

PPS1 consists of three parts (see [Figure 12](#)).

- b8 to b5 shall each be (0)b; a PICC receiving any bit b8 to b5 set to (1)b shall apply [5.7.2.2 b](#)).
- The two-bit value field (b4, b3) is called DSI and codes the selected divisor integer from PICC to PCD.
- The two-bit value field (b2, b1) is called DRI and codes the selected divisor integer from PCD to PICC.

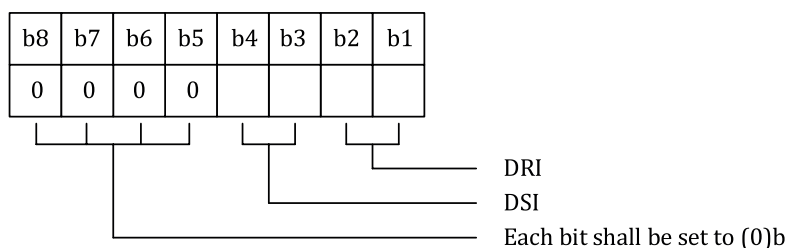


Figure 12 — Coding of PPS1

DS and DR are specified in [5.3.4](#).

The coding of D is given in [Table 2](#).

Table 2 — DRI, DSI to D conversion

DRI, DSI	(00)b	(01)b	(10)b	(11)b
D	1	2	4	8

5.5 Protocol and parameter selection response

The PPS response acknowledges the received PPS request (see [Figure 13](#)) and it contains only the start byte (see [5.4.1](#)).

The new bit rates shall become effective in the PICC immediately after it has sent the PPS response. The PCD shall not change the bit rate when the PPS response is missing or invalid or when the PPSS returned by the PICC is not identical with the PPSS sent by the PCD.