FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
14443-4**

ISO/IEC JTC **1**/SC **17**

Secretariat: BSI

Voting begins on:
2016-01-14

Voting terminates on:
2016-03-14

Identification cards — Contactless integrated circuit cards — Proximity cards —

Part 4: Transmission protocol

Cartes d'identification — Cartes à circuit intégré sans contact — Cartes de proximité —

Partie 4: Protocole de transmission

Reference number
ISO/IEC FDIS 14443-4:2016(E)

COPYRIGHT PROTECTED DOCUMENT

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

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 17, *Cards and personal identification*.

This third edition cancels and replaces the second edition (ISO/IEC 14443-4:2008), which has been technically revised. It also incorporates the Amendments ISO/IEC 14443-4:2008/Amd 1:2012, ISO/IEC 14443-4:2008/Amd 2:2012, ISO/IEC 14443-4:2008/Amd 3:2013 and ISO/IEC 14443-4:2008/Amd 4:2014.

ISO/IEC 14443 consists of the following parts, under the general title *Identification cards — Contactless integrated circuit cards — Proximity cards*:

— *Part 1: Physical characteristics*

— *Part 2: Radio frequency power and signal interface*

— *Part 3: Initialization and anticollision*

— *Part 4: Transmission protocol*

Introduction

ISO/IEC 14443 is one of a series of International Standards describing the parameters for identification cards as defined in ISO/IEC 7810, and the use of such cards for international interchange.

The protocol, as defined in this part of ISO/IEC 14443, is capable of transferring the application protocol data units as defined in ISO/IEC 7816-4. Thus, application protocol data units may be mapped as defined in ISO/IEC 7816-4 and application selection may be used as defined ISO/IEC 7816-5.

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

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this International Standards may involve the use of patents.

Identification cards — Contactless integrated circuit 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 or objects of Type A and Type B.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

ISO/IEC 14443-2, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 2: Radio frequency power and signal interface*

ISO/IEC 14443-3, *Identification cards — Contactless integrated circuit cards — Proximity cards — Part 3: Initialization and anticollision*

3 Terms and definitions

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

3.1
bit duration
one elementary time unit (etu), calculated by the following formula:

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

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

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 part of ISO/IEC 14443.

4 Symbols and abbreviated terms

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

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
$\underline{\boldsymbol{d}}$	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
fc	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
$\boldsymbol{H}$	matrix needed to calculate Hamming syndrome $\underline{s}$ (6 rows, 62 columns)
$h'_{m,n}$	element in row m and column n of matrix $\boldsymbol{H}'$
$\boldsymbol{H}'$	matrix needed to get matrix A (6 rows, 62 columns)
$\underline{\boldsymbol{h}}'_n$	column vector of matrix $\boldsymbol{H}'$
HLTA	HALT Command, Type A
$\boldsymbol{I}_{6 \times 6}$	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 AcKnowledgement
OSI	Open Systems Interconnection
PCB	Protocol Control Byte
PCD	Proximity Coupling Device
PICC	Proximity Card or Object
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 by ISO/IEC
$\underline{\boldsymbol{s}}$	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
WUPA	Wake-Up Command, Type A
WTX	Waiting Time eXtension
WTXM	Waiting Time eXtension Multiplier
$\underline{\boldsymbol{y}}$	64-bit vector ($\underline{\boldsymbol{y}}'$ with no padding bits)
$\underline{\boldsymbol{y}}'$	64-bit vector containing received modified Hamming sub-block
y'_n	received bit n in each modified Hamming sub-block

For the purposes of this part of ISO/IEC 14443, 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

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.

NOTE 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.

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.

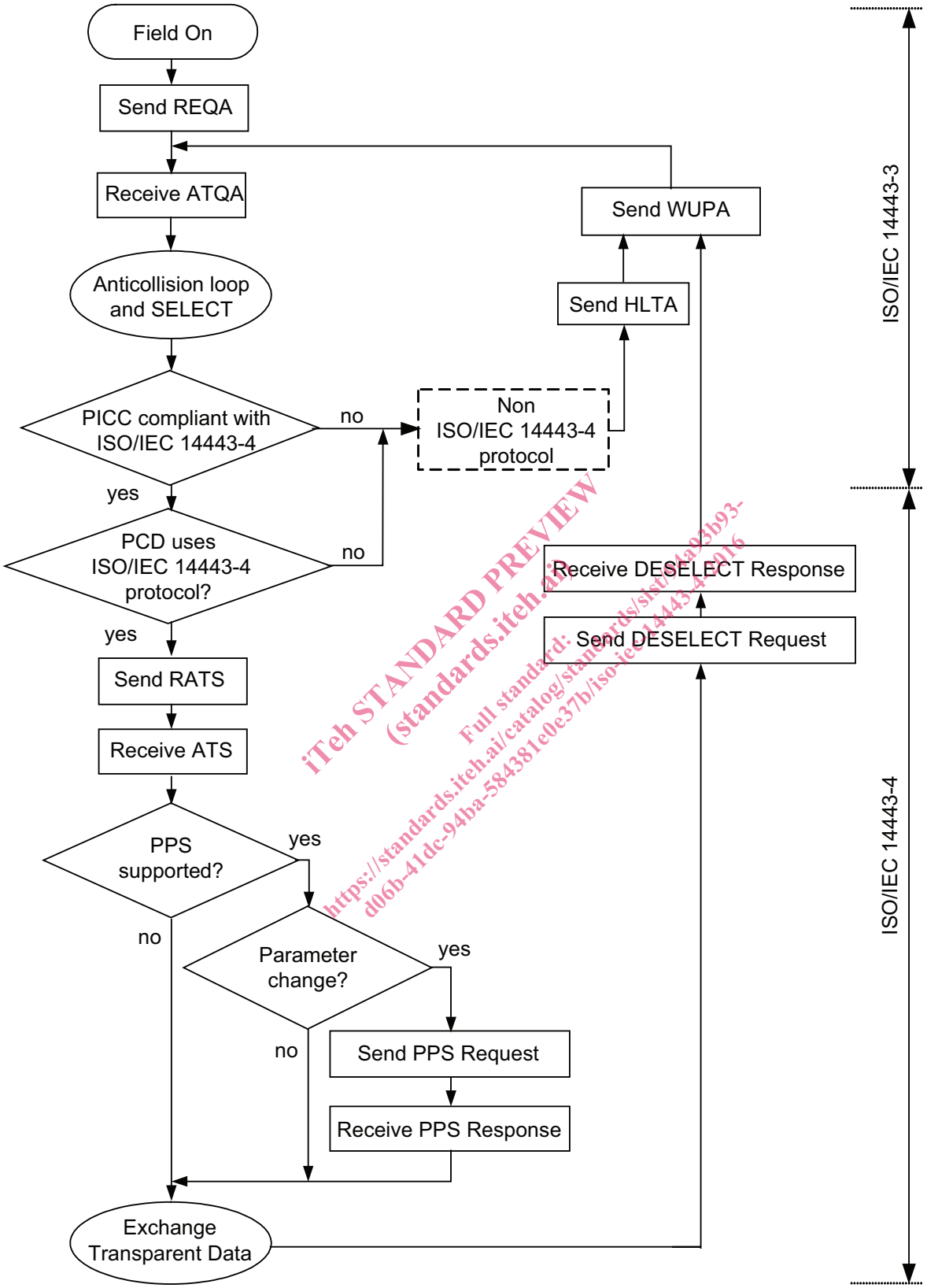

Figure 1 — Activation of a PICC Type A by a PCD

5.1 Request for answer to select

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

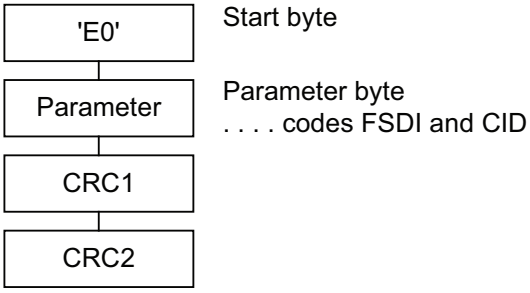

Figure 2 — Request for answer to select

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.

— A PCD setting FSDI = 'D'–'F' is not compliant with this part of ISO/IEC 14443. Until the RFU values 'D'–'F' are assigned by ISO/IEC, a PICC receiving value of FSDI = 'D'–'F' should interpret it as FSDI = 'C' (FSD = 4096 bytes).

NOTE This PCD recommendation is added for PCD's compatibility with future PICC's when ISO/IEC 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 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.

— A PCD setting CID = 15 is not compliant with this part of ISO/IEC 14443. For PICC behaviour see 5.6.1.2 c).

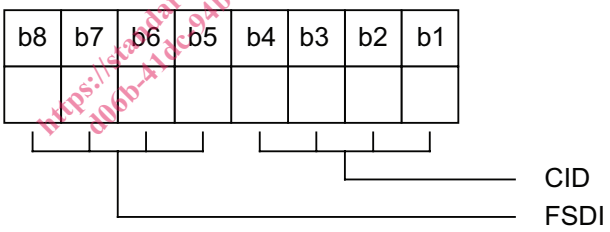

Figure 3 — Coding of RATS parameter byte