INTERNATIONAL STANDARD

ISO/IEC 14443-4

Fourth edition
2018-07

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)

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

Published in Switzerland

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 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 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 14443-2[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 *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 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
$\underline{\boldsymbol{d}}$	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)
$\boldsymbol{h'}_{m,n}$	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 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
$\underline{\boldsymbol{s}}$	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

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.

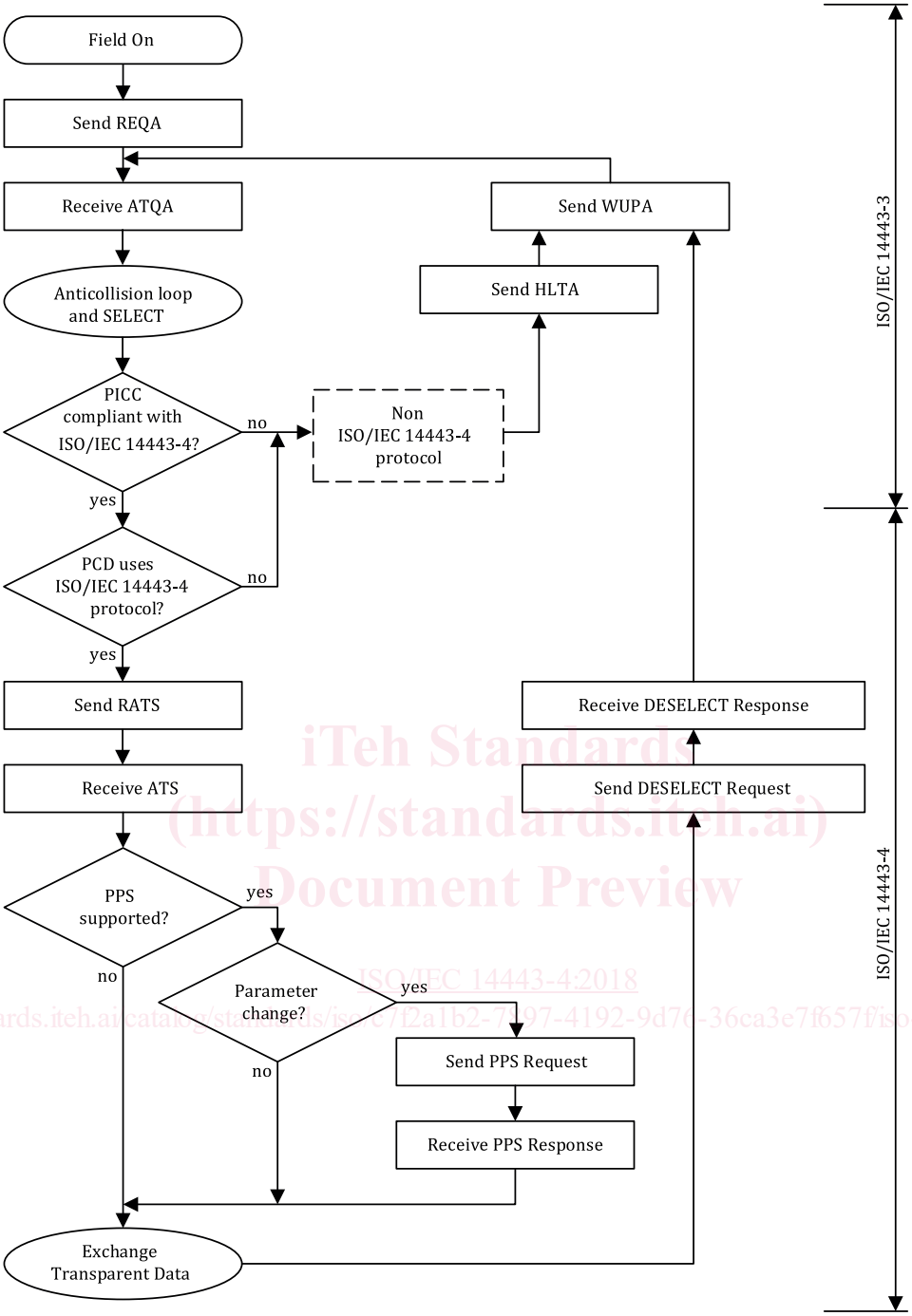

Figure 1 — Activation of a PICC Type A by a PCD

5.2 Request for answer to select

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

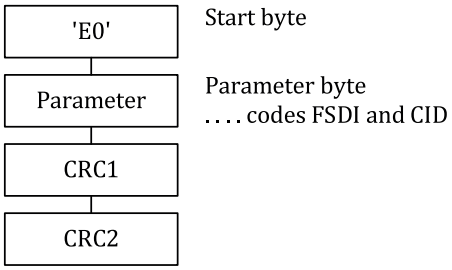

Figure 2 — Request for answer to select

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.

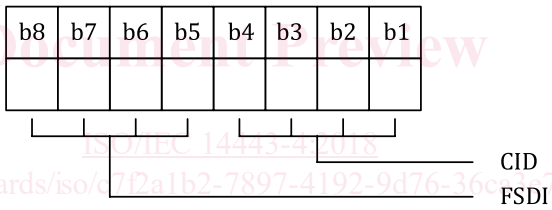

Figure 3 — Coding of RATS parameter byte

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.

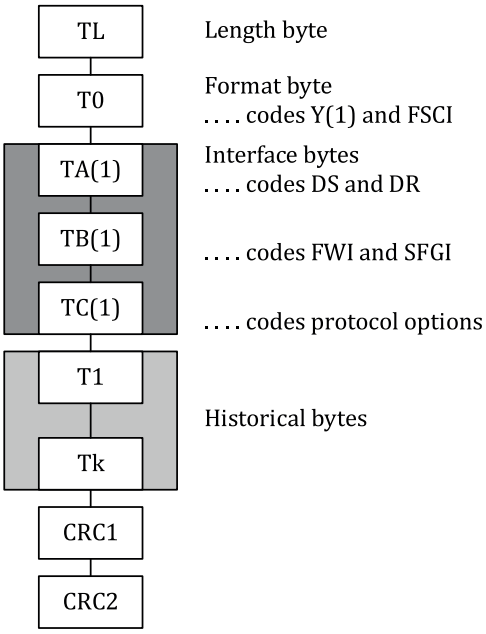

Figure 4 — Structure of the ATS

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'.