JIS

JAPANESE
INDUSTRIAL
STANDARD

Translated and Published by
Japanese Standards Association

JIS X 6319-4 : 2005

(JICSAP/JSA)

Specification of implementation for integrated circuit(s) cards— Part 4 : High Speed proximity cards

ICS 35.240.15

Reference number : JIS X 6319-4 : 2005 (E)

Date of Establishment: 2005-07-20
Date of Public Notice in Official Gazette: 2005-07-20
Investigated by: Japanese Industrial Standards Committee
Standards Board
Technical Committee on Information Technology

JIS X 6319-4 : 2005, First English edition published in 2007-02

Translated and published by: Japanese Standards Association
4-1-24, Akasaka, Minato-ku, Tokyo, 107-8440 JAPAN

In the event of any doubts arising as to the contents,
the original JIS is to be the final authority.

Printed in Japan

AT

Foreword

This translation has been made based on the original Japanese Industrial Standard established by the Minister of Economy, Trade and Industry through deliberations at the Japanese Industrial Standards Committee according to the proposal of establishing a Japanese Industrial Standard from Japan IC Card System Application Council (JICSAP)/ Japanese Standards Association (JSA) with a draft of Industrial Standard prepared from association standard (JICSAP IC card specification V2.1 : 2004) based on the provision of Article 12 Clause 1 of the Industrial Standardization Law.

Being in conformance with this Standard may come under the use of the patent rights held by the following:

Title of invention: Information card (Patent number: 2550931)
Registration date of establishment of patent right: August 22nd, 1996
Sony Corporation

Title of invention: Reflection type transmitter (Patent number: 2705076)
Registration date of establishment of patent right: October 9th, 1997
Sony Corporation

Title of invention: Reflection transmitter (Patent number: 2840832)
Registration date of establishment of patent right: October 23rd, 1998
Sony Corporation

Title of invention: Data processor and its method, transmitting/receiving device and its method (Unexamined publication number: H10-13312)
Sony Corporation

Title of utility model: Information card apparatus (Utility model number: 2137036)
Publication date of establishment of utility model: January 16th, 1998
Sony Corporation

Besides, this description does not affect to any extent the validity, the scope and the like of the above patent rights.

The relevant holders of the above-mentioned industrial property rights have indicated to the Japanese Industrial Standards Committee an intention of granting license to anyone under the nondiscriminatory and reasonable conditions.

Attention is drawn to the possibility that some parts of this Standard may conflict with a patent right, application for a patent after opening to the public, utility model right or application for registration of utility model after opening to the public which have technical properties other than mentioned above. The Minister of Economy, Trade and Industry and the Japanese Industrial Standards Committee are not responsible for identifying the patent right, application for a patent after opening to the public, utility model right or application for registration of utility model after opening to the public which have the said technical properties.

JIS X 6319 series consists of the following parts under the general title "*Specification of implementation for integrated circuit(s) cards*":

Part 1: Integrated circuit(s) cards with contacts

Part 2: Proximity cards

Part 3: Common commands for interchange

Part 4: High speed proximity cards

Contents

Specification of implementation for integrated circuit(s) cards— Part 4 : High speed proximity cards

Introduction This Japanese Industrial Standard specifies the characteristics of the high speed contactless proximity integrated circuit(s) cards and the proximity coupling devices.

In order to ensure the interoperability of contactless interfaces, this part of **JIS X 6319** extends to more concrete implementation specifications than International Standards. Use of new standards in building and operating integrated circuit(s) card systems is in no way constricted because contactless proximity integrated circuit(s) cards have the potential to be used for a variety of applications and operations, while the performance of IC chips, such as power consumption, is constantly being improved by technological advances. Consideration is also given to the possibility that integrated circuit(s) cards with or without contacts may be integrated into the same system.

1 Scope This part of **JIS X 6319** specifies the physical characteristics, the air interface, the transmission protocols, the file structure and the commands of high-speed contactless proximity integrated circuit(s) cards (hereafter referred to as "cards").

The cards can process multiple files at one time with smaller transactions while maintaining the security of individual files, and also offer a function for handling power interruption during processing.

With these features, the cards are ideally suited for use in applications such as electronic ticketing at railway stations and event sites, where high-speed confirmation and processing of accesses with quickly moving users are essential.

2 Normative references The following standards contain provisions which, through reference in this text, constitute provisions of this part of **JIS X 6319**. The most recent editions of the standards (including amendments) indicated below shall be applied.

JIS X 6301 *Identification cards—Physical characteristics*

JIS X 6303 *Integrated circuit(s) cards with contacts—Physical characteristics and location of contacts*

JIS X 6304 *Identification cards—Integrated circuit(s) cards with contacts—Part 3 : Electronic signals and transmission protocols*

JIS X 6305-1 *Identification cards—Test methods—Part 1 : General characteristics tests*

JIS X 6305-6 *Identification cards—Test methods—Part 6 : Proximity cards*

JIS X 6306 *Identification cards—Integrated circuit(s) cards with contacts—Part 4 : Interindustry commands for interchange*

JIS X 6322-1 *Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 1 : Physical characteristics*

JIS X 6322-2 *Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 2 : Radio frequency power and signal interface*

JIS X 6322-3 *Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 3 : Initialization and anticollision*

JIS X 6322-4 *Identification cards—Contactless integrated circuit(s) cards—Proximity cards—Part 4 : Transmission protocol*

ISO/IEC 18092 *Information technology—Telecommunications and information exchange between systems—Near Field Communication—Interface and Protocol-1 (NFCIP-1)*

3 Terms and definitions

3.1 Terms For the purposes of this Standard, the definitions given in **JIS X 6322-1** to **JIS X 6322-4**, **JIS X 6304** and **JIS X 6305-6**, and the following definitions apply.

3.1.1 access key key used in authentication

3.1.2 area key key used to authenticate the right for use of an area

3.1.3 area definition block block defining the range of the service IDs and the number of user blocks available for the card system administrator, and the authority and so on granted to that card system administrator

3.1.4 cash back access the access that makes possible to add a value which is within the value subtracted immediately before from the add-subtract calculation block

3.1.5 service unit of the access from the external device to the card, and the area defined to have the same access attributes in the memory area of the card

3.1.6 service code list list which declares the use of service(s)

3.1.7 area code list list which declares the use of area(s)

3.1.8 service key key used to authenticate the right for use of a service

3.1.9 service definition block block defining the corresponding service's access attributes, and the position and range of the accessible user blocks

3.1.10 system block block mainly records information necessary for the internal control of the card

This is the general term of the manufacture ID block, issue ID block, system definition block area definition block, and service definition block.

3.1.11 status flag flag indicating the result of processing

The status flag 1 shows the result of processing, and the status flag 2 shows the detail of the information.

3.1.12 manufacture ID, IDm information to identify the card uniquely and be written at the time of the card production

3.1.13 manufacture ID block block recorded at the time of the card production

The block is composed of the manufacture ID (*IDm*) and the manufacture parameter (*PMm*).

3.1.14 manufacture parameter, PMm information that shows the card's functions and transmitting control characteristics, which is written at the time of the card production

3.1.15 authentication to authenticate if PCD and PICC have the same access key

3.1.16 direct access overwriting access of 16-bit data in the add-subtract calculation block

3.1.17 decrement access subtracting access in the add-subtract calculation block

3.1.18 power load load for consuming the energy of operating magnetic field in reference PICC or test target PICC

3.1.19 issuer ID, IDi information written at the time of the card issuance

3.1.20 issue ID block block recorded at the card issuance

The block is composed of the issuer ID (*IDi*) and issue parameter (*PMi*).

3.1.21 issue parameter, PMi supplementary information written at the time of the issuance

3.1.22 block minimum unit in writing to and deleting the memory

3.1.23 block number number for managing the logical position of the user block in the specific service

This number is used when the external device accesses the memory in the card.

3.1.24 block list list that shows the relation among the block access attribute, block number, and key used in authentication

3.1.25 contactless interface interface method for signal sending/receiving and power supplying to the card without using conduction contact points (i.e. without direct touch of the external device and the IC built in the card)

3.1.26 user block block allocated to the memory for a specific service

3.1.27 access attribute information that shows the necessity of prior authentication on accessing

3.2 Abbreviations and symbols

ASK	amplitude shift keying
Fc	frequency of operating field (carrier frequency)
Hmax	maximum fieldstrength of the PCD antenna field
Hmin	minimum fieldstrength of the PCD antenna field

IDi	issuer ID
IDm	manufacture ID
LSB	least significant bit
MSB	most significant bit
N	number of anticollision slots or PICC response probability in each slot
PCD	proximity coupling device
PICC	proximity card
PMi	issue parameter
PMm	manufacture parameter
R	slot number chosen by PICC during the anticollision sequence
REQC	request command, type C
RF	radio frequency

For the purpose of this Standard, data values are expressed as follows.

b'xxxx xxxx'	bit of binary numbers
'XX'	hexadecimal numbers

4 Physical characteristics

4.1 General physical characteristics The card shall have physical characteristics of the card type ID-1 specified in **JIS X 6301**.

4.2 Dimensions The nominal dimensions of the card shall satisfy the specification in **JIS X 6301** as the card type ID-1.

4.3 Surface condition The card surface shall be flat and smooth to allow the card to be carried, etc.

4.4 Substrate material The substrate of the card shall be made of PET (polyethylene terephthalate) or materials having equal or better performance.

4.5 Additional physical characteristics

4.5.1 Static electricity The card shall continue to operate after testing in accordance with the test methods specified in **JIS X 6305-6**, where the test voltage is 6 kV. Any information recorded in the card shall not be altered; besides, data shall be able to be re-written.

4.5.2 Static magnetic field The card shall continue to operate after having been exposed to a static 640 kA/m magnetic field.

NOTE : The data on a magnetic stripe in such field might be erased.

4.5.3 Operating temperature The card shall continue to operate under the environmental temperature of −5 °C to 50 °C.

4.5.4 Cold-and heat-proof properties After having been subjected to the temperature conditions specified in **JIS X 6305-1**, the card shall continue to operate and satisfy the warpage specification.

4.5.5 Moisture proof After having been left for 48 h in an environment of 40 °C temperature and 90 % relative humidity, the card shall continue to operate and satisfy the warpage specification.

4.5.6 Cyclic thermal proof The card shall continue to operate after having been applied of ten thermal test cycles, each consisting of 30 min at −25 °C, 5 min at room temperature and humidity (23 °C ± 3 °C, relative humidity: 40 % to 60 %), 30 min at +85 °C and 5 min at room temperature and humidity.

4.5.7 Drop impact proof The card shall continue to operate after having been dropped twice in three directions (longitudinal, lateral and surface directions) from the height of 1.5 m onto a concrete surface.

4.5.8 Bending stiffness The card shall continue to operate after having been applied a load of 0.7 N for 1 min in accordance with the method specified in **JIS X 6305-1**.

4.5.9 Point pressure stiffness The card shall continue to operate after a pressure, generated by applying a force of 1.5 N to a ø1 mm steel ball, is applied to the position of the IC chip (see **JIS X 6303**).

4.5.10 Delamination The card shall possess the minimum peel strength of at least 6 N/cm when tested by the method specified in **JIS X 6305-1**.

4.5.11 Adhesion or coking The card shall show no adverse effects and be easily separated after having been subjected to the 2.5 kPa pressure test described in **JIS X 6305-1**.

4.5.12 Chemical proof The card shall show no adverse effects and continue to operate after having been immersed for 1 min in each chemical solution specified in **JIS X 6305-1**.

4.5.13 Optical transparency The optical transparency density of the card shall be at least 1.5 when tested using the method specified in **JIS X 6305-1**.

4.5.14 Storage temperature The card shall continue to operate after having been stored in −35 °C and +85 °C temperatures for 60 min each.

4.5.15 Environment protection The card shall not cause toxic hazard in the normal use. The card shall not cause toxic gas when it is disposed or incinerated.

4.5.16 Curl, burr and chipped particles The card shall not cause any malfunction of the issuing or processing machine by curl, burr or chipped particles.

5 Air interface

5.1 Power transmission PCD shall transfer power to PICC by producing RF operating magnetic field and make communications by magnetic field modulation.

5.1.1 Frequency The frequency *fc* of the RF operating magnetic field shall be 13.56 MHz.

5.1.2 Tolerance deviation of frequency The tolerance deviation of frequency shall be ± 50 ppm or under.

5.1.3 Leakage electric field strength The leakage electric field strength shall conform to the regulations of the Radio Law.

5.1.4 Operating magnetic field See **JIS X 6322-2**.

5.2 Signal transmission from PCD to PICC

5.2.1 Bit rate The bit rate shall be *fc*/64 (approximately 212 kbit/s).

5.2.2 Occupied frequency bandwidth The occupied frequency bandwidth shall be not more than 7R (R: the number of bits/s of the modulated signal composed of pulse streams).

5.2.3 Modulation Transmission from PCD to PICC shall use the modulation principle of ASK 10 % of the RF operating magnetic field.

The modulation index shall be between 8 % and 14 %.

The modulated waveform shall satisfy values shown in figure 1. The rising and falling edges of the waveform shall be monotonic.

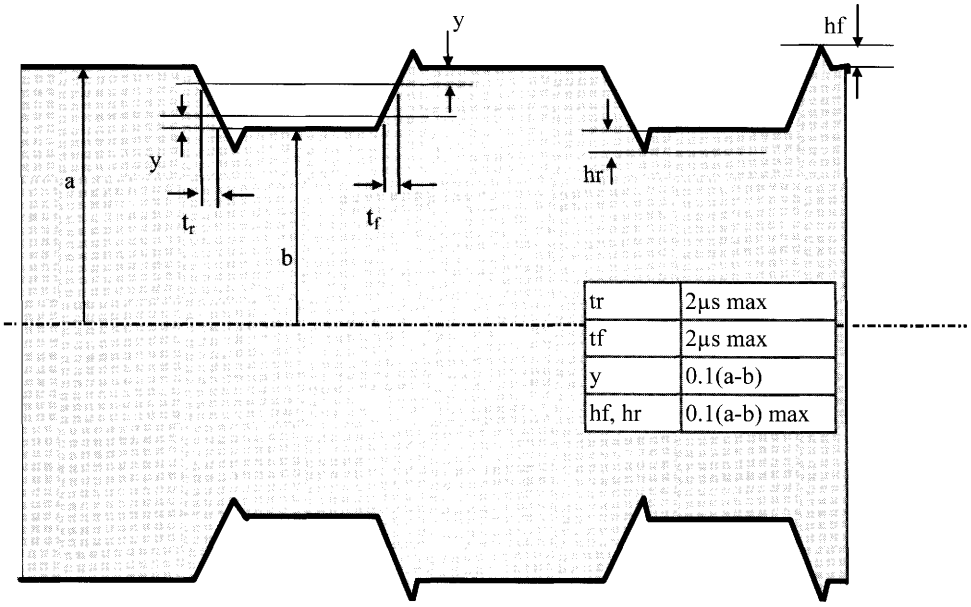


Figure 1 Modulated waveform

5.2.4 Bit coding method Manchester coding method shall be used for bit coding.

Logic 1: The first half (50 %) of the bit duration shall correspond to the high field amplitude (non-modulated state) of the carrier, and the second half (50 %) shall correspond to the low field amplitude.

Logic 0: The first half (50 %) of the bit duration shall correspond to the low field amplitude of the carrier, and the second half (50 %) shall correspond to the high field amplitude (non-modulated state).

No signal state: The amplitude of the carrier wave shall be high (non-modulated) throughout the entire bit duration.

Figure 2 shows the example of bit coding method.

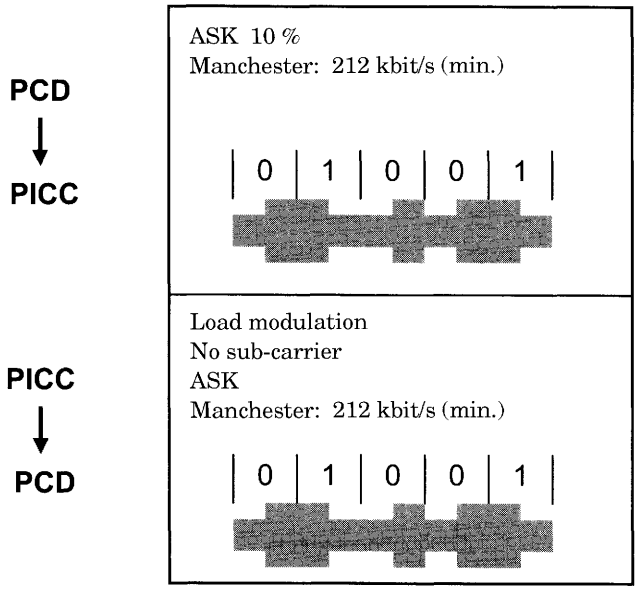


Figure 2 Example of bit coding

5.3 Signal transmission from PICC to PCD

5.3.1 Bit transmission rate The bit transmission rate shall be $fc/64$ (approximately 212 kbit/s).

5.3.2 Modulation method PICC shall be capable of making communications to PCD by load modulation (load is switched to ON or OFF in PICC) of carrier wave via an inductive coupling.

The load modulation amplitude shall be at least $30/H^{1.2}$ (mVpeak) when measured by the test method specified in **JIS X 6305-6**.

H is the magnetic field strength in A/m (rms).

5.3.3 Bit coding method Manchester coding method shall be used for bit coding.

Logic 1: The first half (50 %) of the bit duration shall correspond to the high field amplitude (non-modulated state) of the carrier wave, while the second half (50 %) shall correspond to the low field amplitude.

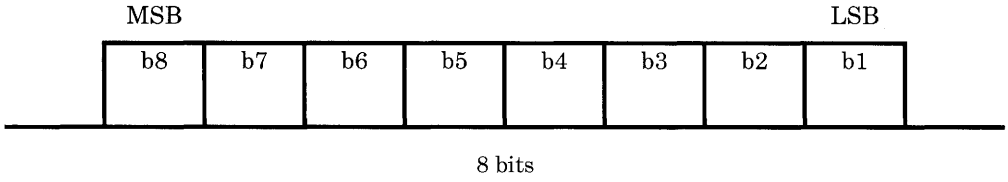
Logic 0: The first half (50 %) of the bit duration shall correspond to the low field amplitude of the carrier wave, while the second half (50 %) shall correspond to the amplitude (non-modulated state).

No signal state: The amplitude of the carrier wave shall be high (non-modulated) throughout the entire bit duration.

6 Character, frame format and timing The character, frame format and timing shall be specified as follows. The bit coding method shall be specified in **5.2.4** and **5.3.3**.

6.1 Character transmission

6.1.1 Character transmission format A character is transmitted from MSB by 1 byte composed of 8 bits as shown in figure 3.



NOTE : The start bit and the stop bit of Type B PICC specified in **JIS X 6322-3** shall no exist. The parity bit shall not exist.

Figure 3 Character format

6.1.2 Character interval No interval shall exist between any consecutive characters.

The data stream shall be sent out from the MSB of each byte and after sending out the LSB, the consecutive character shall be sent out without interval as shown in figure 4.

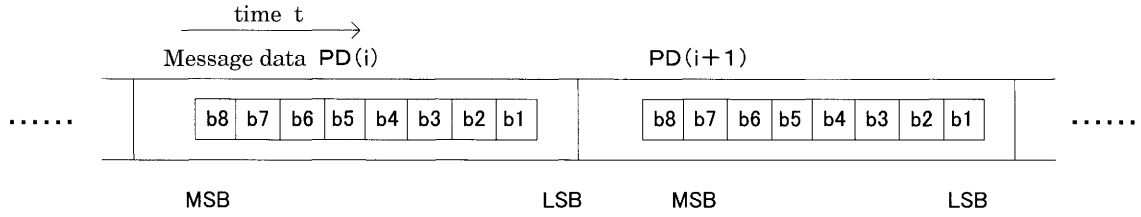
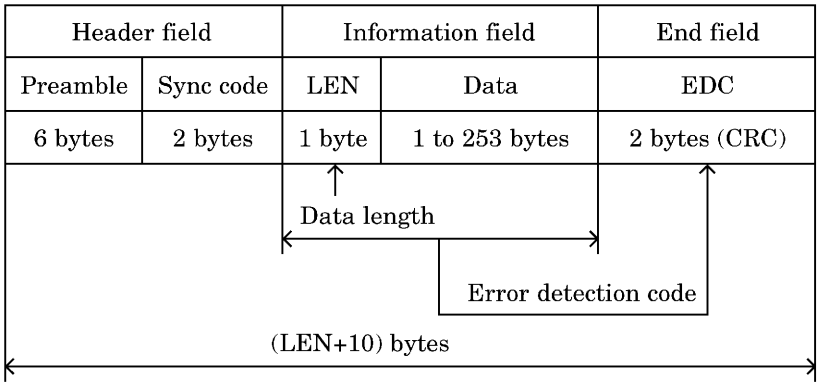


Figure 4 Data stream

6.2 Frame format Characters shall be transmitted between PCD and PICC by frames.

The frame is composed of the header field, the information field and the end field (see figure 5).



Data length (LEN): 1 byte

Data: (LEN-1) bytes

Figure 5 Frame structure

6.2.1 Header field The header field is composed of the preamble (6 bytes) and the sync code (2 bytes). The values shall conform to **ISO/IEC 18092** (see figure 5).

Preamble (6 bytes): '000000000000'

Sync code (2 bytes): 'B24D'

6.2.2 Information field The information field is composed of the length byte (LEN) and the data field (see figure 6).

LEN is located in the first byte of the information field. The value of LEN indicates the number of bytes in the information field including LEN.

LEN codes shall be '01' to 'FE' (the number of bytes in the information field).

The data field shall be composed of the command message or the response message.

Information field	
LEN	Data field
1 byte	(LEN-1) bytes

Figure 6 Information field structure

6.2.3 End field The end field (EDC) shall transmit the error detection code [the Cyclic Redundancy Check (CRC) code] of the transmission block (see figure 5).

The frame becomes effective only when EDC is correct.

The CRC is a function of data bits, which is composed of all the data bits in the information field.

Calculation formula is as follows.

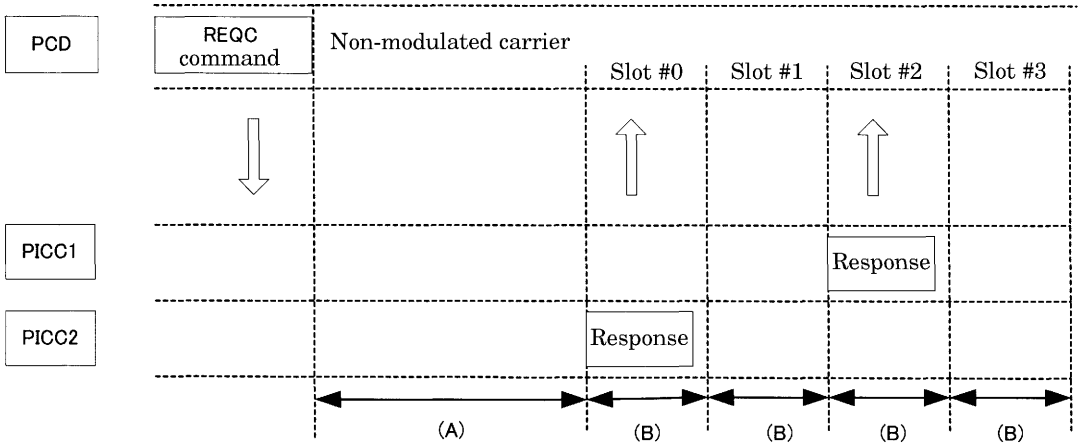
CRC: 2 bytes ($X^{16} + X^{12} + X^5 + 1$)

The initial value shall be set to '0000'.

6.3 Byte order All binary data which is composed of 2 to 4 bytes shall use the little endian format for sending and receiving [see **JIS X 9205** : 1999 *Graphic technology—Prepress digital data exchange—Tag image file format for image technology (TIFF/IT)*].

6.4 PICC response timing PICC shall respond as specified in **6.4.1** and **6.4.2** after the reception of the command frame from PCD. The response timing in the anticollision sequence and that for the normal command is different.

6.4.1 Response timing in anticollision sequence PICC shall respond by sending ATQC (see **7.6**) at the start timing of one of the time slots. The first time slot shall start after 512 × 64/fc (approximately 2.417 ms) from the completion of REQC command frame (see **7.5**). The time slot duration is 256 × 64/fc (approximately 1.208 ms). The example of response timing is shown in figure 7 where two PICCs answer ATQCs to the 1st and 3rd slots.



PICC processing time (A): 512 × 64/fc (approximately 2.417 ms)

Time slot duration (B): 256 × 64/fc (approximately 1.208 ms)

Figure 7 Example of response timing for REQC command

6.4.2 Response timing for normal command PICC shall inform PCD of the response time calculation parameter for the command as the response of anticollision sequence. For the calculation method of the response time, refer to the request response (ATQC) (see **7.6.3**).

NOTE : This is designed to optimize the sending/receiving of each card by considering performance dispersion. Moreover, this time is regarded as maximum waiting time for response from PICC, when seeing from PCD.

After the completion of the received command frame, PICC shall start the response for the command and complete within the waiting time calculated from the calculation parameters described above (see figure 8).

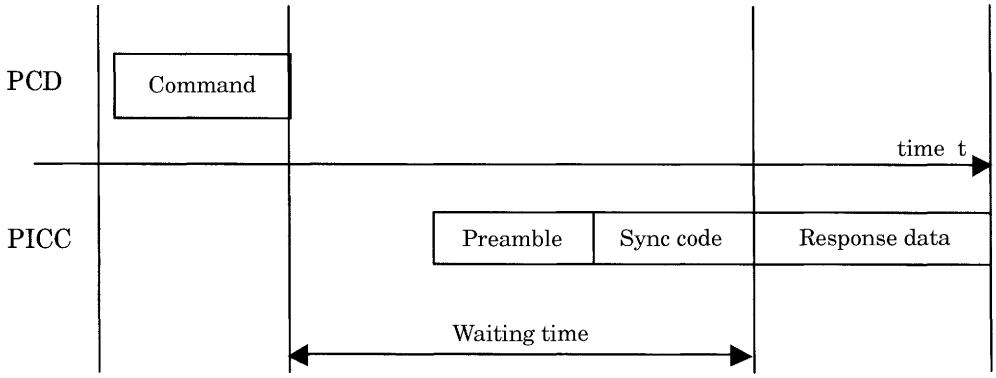


Figure 8 Waiting time

7 PICC initialization and anticollision The PICC initialization and collision detection protocol shall be specified as follows.

7.1 Initialization communication Initialization communication between PCD and PICC shall be as follows.

— PICC shall be powered up when it enters the RF operating magnetic field generated by PCD.

— PICC shall wait for REQC command or the command of which NFCID2 is matched (see **7.6.2**).

— If the parameter of the system code in REQC command matches, PICC shall respond its ID data (NFCID2 and Pad) (see **ISO/IEC 18092**). If two or more PICCs respond at the same time, PCD shall select one PICC to be allowed to communicate in accordance with the anticollision sequence specified in **7.2**.

— PICC shall respond the received the command of which NFCID2 is matched.

— After receiving REQC command of which the system code is matched, PICC shall generate a random number R, wait until the time slot number becomes R, then respond.

— PCD may repeat to send REQC command until detecting PICCs in the RF operating magnetic field.

7.2 Anticollision sequence The anticollision sequence shall be controlled by PCD using REQC command.

PCD shall act to make communications with one or more PICCs. PCD shall issue REQC command to make PICC respond and enable to communicate.

It is regarded as the collision of PICCs in the case where two or more PICCs respond simultaneously during the anticollision sequence.

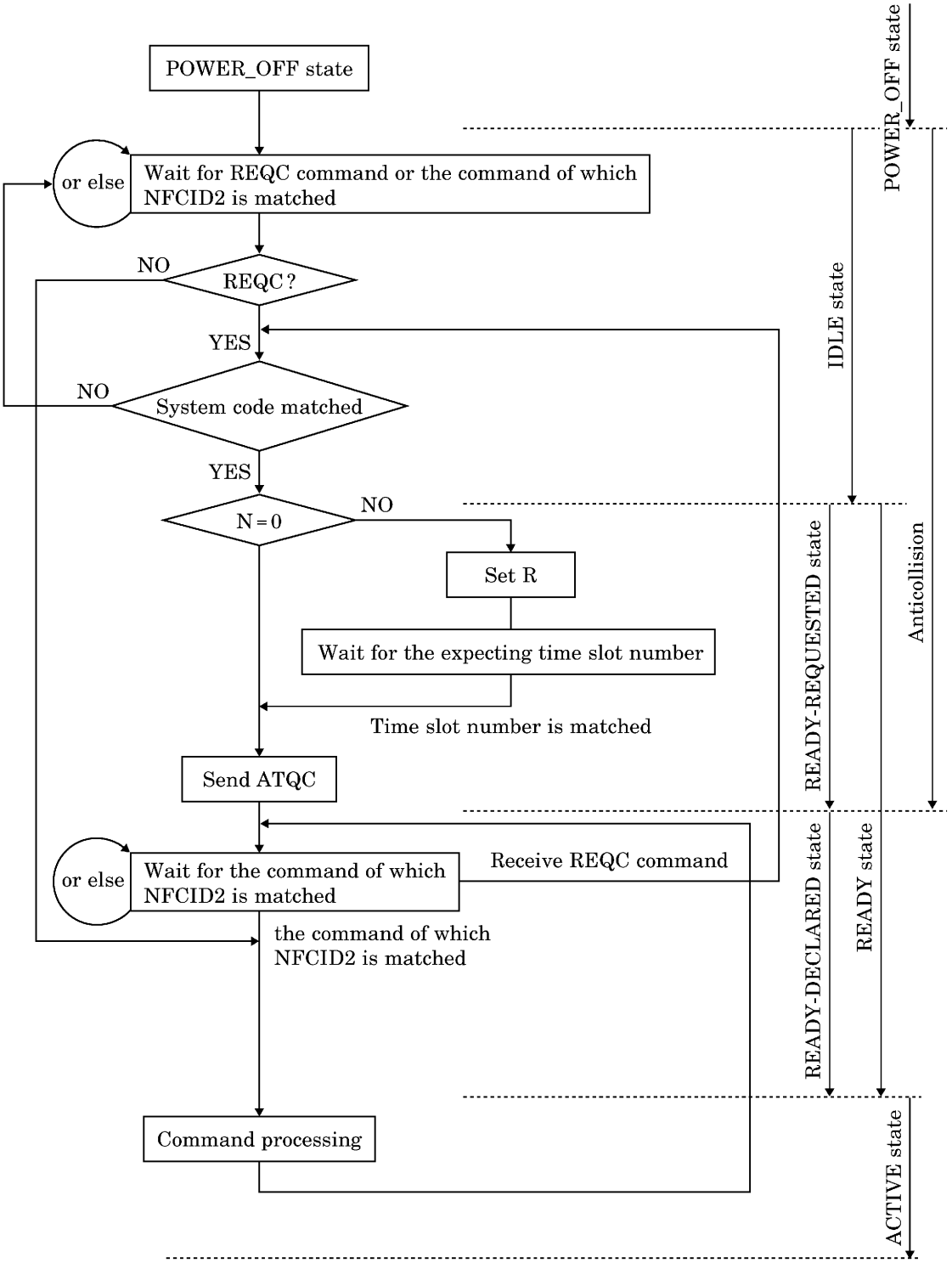
As the result of the anticollision process, the communication from PICC shall be controlled by PCD, and at the same time, only one PICC shall be allowed to communicate.

The anticollision mechanism is based on a time slot principle. PCD shall set the REQC parameter with the time slot number of integer zero or more. PICCs shall respond randomly to one of the controllable time slots. PCD shall detect PICC's ID data at any of the time slots. If multiple PICCs exist in the RF operating magnetic field generated by PCD and if only one of PICCs responded, PCD shall detect the ID data. PCD shall identify PICC with the acquired ID data. After this, one or more PICCs may be selected by confirming one by one in the anticollision sequence to make communication of application data.

PCD can make the specified PICC no longer accept REQC command by executing Authentication1 command (see **9.6.5**). PCD may reduce the collision load of the responses to REQC command through this authentication.

7.3 States of PICC During the anticollision sequence, PICC detail operation shall be shown by several states or by state transitions among them.

7.3.1 State transition There are POWER_OFF state (see **7.3.3**), IDLE state (see **7.3.4**), READY-REQUESTED (see **7.3.5**), READY-DECLARED (see **7.3.6**) and ACTIVE (see **7.3.7**) in PICC states. PICC shall transit among these states. The example of PICC state transition is shown in figure 9.



NOTES 1 N = Number in time slot

2 R = Random number selected by PICC from 0 to N

3 NFCID2 is described as IDm after **7.6.2**.

Figure 9 Example of state transition of PICC

7.3.2 General requirement for state transition The conditions below shall be required for any state transition.

— PICC shall transit to the POWER_OFF state when the carrier wave power lacks.

Conditions for anticollision state except for the ACTIVE state shall be as follows.

— PICC shall adopt the communication parameters specified in **7.2**.

— If PICC detects a frame (with valid CRC), PICC shall operate or respond in accordance with the situation.

— If PICC recognizes the frame correctly, PICC shall respond (if error is detected, PICC shall not respond).

7.3.3 POWER_OFF state

Definition: In the POWER_OFF state, PICC is not powered due to lack of carrier power.

State transition condition: If PICC is placed in an operating magnetic field greater than *H*min (see **JIS X 6322-2**), it shall enter the IDLE state.

7.3.4 IDLE state

Definition: In the IDLE state, PICC is powered. PICC shall recognize REQC command or the command of which NFCID2 is matched by monitoring the command frame signal.

State transition condition: If REQC command is correctly recognized, PICC shall enter the READY-REQUESTED state. (The correct REQC recognition means to recognize correctly REQC command and the frame with the matched system code. See REQC command specifications.)

PICC shall enter ACTIVE state when it detects that NFCID2 in a command other than REQC matches that of PICC.

7.3.5 READY-REQUESTED state (sub-state)

Definition: In the READY-REQUESTED state, PICC is powered and confirms REQC command with control parameter N. PICC also generates a random number R which is used to control its subsequent operation specified in **7.4**.

State transition condition: After sending ATQC response at the timing in accordance with **7.4**, PICC shall enter the READY-DECLARED state.

7.3.6 READY-DECLARED state (sub-state)

Definition: In the READY-DECLARED state, PICC is powered and has sent its ATQC response corresponding to the last confirmed REQC command.

PICC shall then recognize the next REQC command or other commands.

State transition condition: If NFCID2 in a command other than REQC does not match that of PICC, PICC shall maintain the READY-DECLARED state. If NFCID2 in a command matches that of PICC, PICC shall enter the ACTIVE state.

On reception of REQC command, the same conditions and transitions apply as those on reception of REQC command in the IDLE state.

7.3.7 ACTIVE state

Definition: In the ACTIVE state, PICC is powered and receives a command message of a proper format (with proper NFCID2 and valid CRC).

PICC shall not respond when the CRC is invalid or when NFCID2 differs from the value in PICC.

State transition condition: PICC shall return to the POWER_OFF state when the power goes off.

7.4 Anticollision response rules Upon reception of valid REQC command with which the system code is set to 'FFFF' or an internally set value representing application, PICC in the READY-REQUESTED state shall return a response in accordance with the following rules. The parameter N is a value given by REQC command.

N = 0: PICC shall send a response message and wait for the next command.

N > 0: PICC shall internally generate a random number R, which is uniformly dispersed value between 0 and N.

R = 0: PICC shall send a response message and wait for the next command.

R > 0: PICC shall wait for the concurrence of the selected time slot time and send a response message, and wait for the next command.

7.5 REQC command REQC command is used by PCD to detect whether PICC of type C exist in the RF operating magnetic field or not.

In the anticollision algorithm, the number of time slot (N + 1) is optimized for applications and set in the command. Figure 9 shows PICC operation in detail when receiving REQC command.

7.5.1 REQC command format The format of REQC command sent out from PCD is shown in figure 10.

Command code	System code	Reserved	Time slot number
1 byte ('00')	2 bytes	1 byte '00'	1 byte

Command code encoding: The command code shall be set to "00".

Figure 10 REQC format

7.5.2 System code encoding The system code is used to specify the application by PCD and is used to select PICC before sending ATQC.

All PICCs shall respond when the system code is 'FFFF'. When other than 'FFFF', PICC in the application distinguished by the system code shall respond, and those in other application shall not respond.

'0000' is reserved for future use.

Correspondence between the system code and application is not specified in this Standard.

7.5.3 Time slot coding The maximum time slot number for PICC to avoid collision shall be encoded. Assignable values shall be '00', '01', '03', '07' and '0F' and each time slot number N shall be encoded as shown in table 1. Other values are reserved for future use.

Table 1 Time slot number encoding

b8 ····· b1	Time slot number
00000000	1
00000001	2
00000011	4
00000111	8
00001111	16

7.6 ATQC The response to REQC command is called ATQC.

7.6.1 ATQC format ATQC (response message) format sent from PICC is shown in figure 11.

Command code	NFCID2	PAD
1 byte ('00')	8 bytes	8 bytes

Command code encoding: The command code shall be set to '01'.

Figure 11 ATQC format

7.6.2 NFCID2 (Near Field Communication Interface Protocol-2) NFCID2 shall be 8 bytes which is unique among all PICCs, and is used in the anticollision sequence to identify PICC.

Information: NFCID2 may be composed of manufacture ID (IDm) which is 2-byte unique IC manufacturer code and 6-byte unique manufacturer code (see figure 12.)

Hereafter, NFCID2 is referred to as the manufacture ID (IDm) in this Standard.

IC manufacturer code is not specified in this Standard.

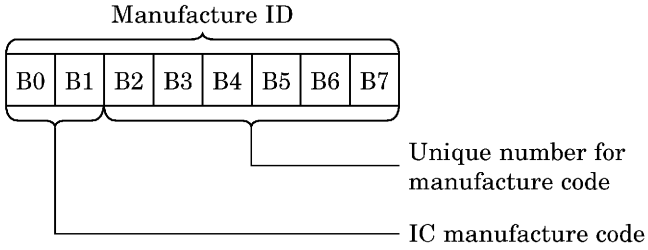


Figure 12 Structure of manufacture ID

7.6.3 Pad Pad is specified as undefined field in **ISO/IEC 18092**, however, it is defined as manufacture parameter (PMm) in this Standard. The manufacture parameter (PMm) is composed of IC code (2 bytes) and PICC response time calculation parameter which corresponds to each command sent from PCD to PICC (see figure 13).

The IC code is not specified in this Standard. Manufacturers may use the IC code to distinguish the functions of IC chips.

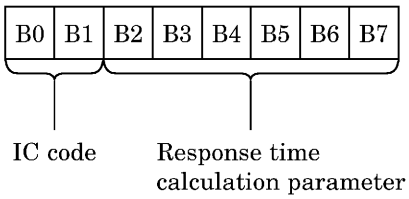


Figure 13 Structure of manufacture parameter

Each byte of the response time calculation parameter shall determine the corresponding command's timeout. The correspondence between B2 to B7 of manufacture parameter (PMm) and commands shall be shown in table 2.

Table 2 B2 to B7 of manufacture parameter (PMm) and commands

Manufacture parameter	Command
B2	Request Service command (see **9.6.2**)
B3	Request Response command (see **9.6.1**)
B4	Authentication commands (see **9.6.5**, **9.6.6**)
B5	Read commands (see **9.6.3**)
B6	Write commands (see **9.6.4**)
B7	(Reserved)

The response time calculation parameter shall be composed of an index part (E) and two real number parts (A and B). Figure 14 shows the structure of response time calculation parameter.

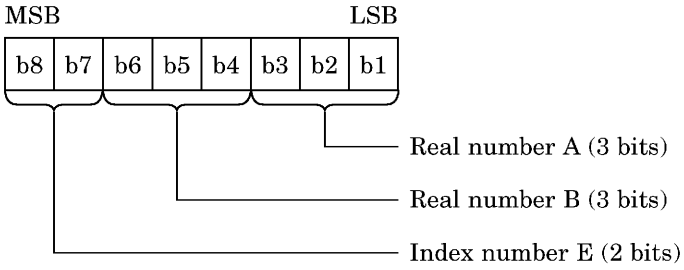


Figure 14 Structure of response time calculation parameter

The formula to calculate response time using the response time calculation parameter shall be as follows.

$$\text{Response time} = T \times [(B + 1) \times n + (A + 1)] \times 4^{E}$$

$$T = 256 \times 16/fc \text{ (approximately 0.302 0 ms)}$$

where,

n: Number of blocks or services of the command parameter (see table 4 of **9.1**).

8 Basic configuration File structures and access methods to files and records shall be specified as follows.

The data area shall be composed of 16-byte fixed length logical blocks. The logical block is managed by 2-byte management information.

Commands specified in this Standard are limited to those accessed (read and write) by blocks. Other access methods, for example, byte-unit access or logical-object-unit access by future regulation amendment or commands configured by manufacturers, shall never be limited.

Logical blocks may be handled as logical records in files.

8.1 File structure Three types of files shall be specified as follows.

Area file: The area file corresponds to DF which is defined in **JIS X 6306**.

The area file with the file ID "0000" corresponds to MF.

Other area files may exist under the area file. Any area file shall contain one or more service files. The area file hierarchy can be up to 8 layers.

Service file: The service file corresponds to EF which is defined in **JIS X 6306**.

No other file shall exist under the service file. Any service file shall contain one or more records.

Overlapped service file: The service file is a file where the value of the lower 6 bits of the file ID is modified. The record of the overlapped service file shall be allocated to the same block of the record of the service file.

All files shall be composed of 16-byte fixed length records.

Files shall be managed by a 2-byte file ID, which is unique in PICC.

An example of the logical file structure in PICC shall be shown in figure 15.

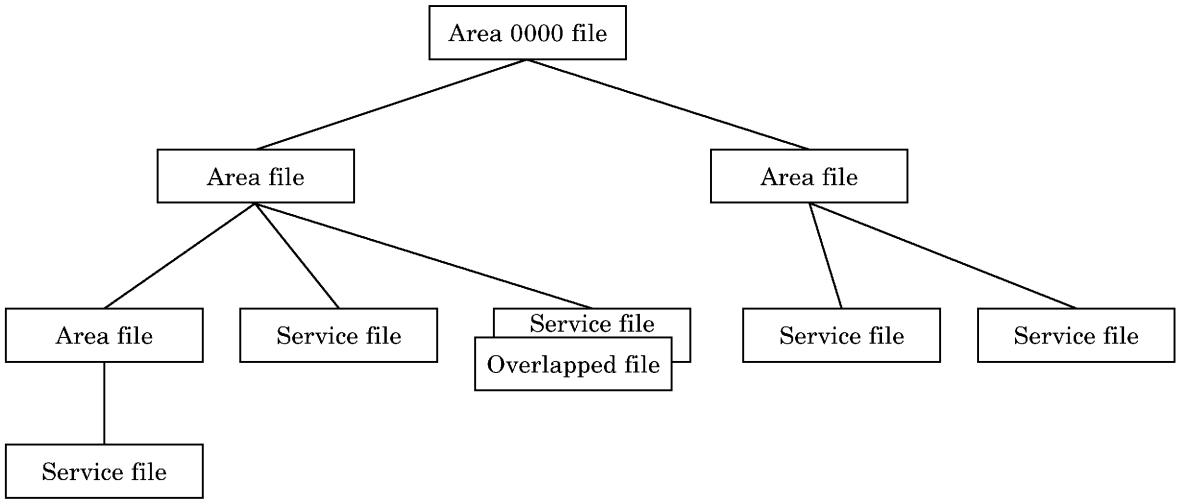


Figure 15 Example of the logical file structure in PICC

8.2 File reference method Files shall be referred to by file IDs.

Referencing by path, short ID and AID shall not be supported.

In the file ID, the upper 10 bits and lower 6 bits of 2 bytes (16 bits) shall be encoded separately.

8.2.1 Encoding method of file ID of area file The file ID of the area file shall be encoded as follows (see figure 16).

The upper 10 bits shall be set to the upper 10 bits of the smallest service file ID under the area file.

The lower 6 bits shall be set to b“000000” or b“000001”. Other values are reserved for future use.

In the case of b“000000”, the lower-level area files under this area file shall be allowed.

In the case of b“000001”, the lower-level area files under this area file shall not be allowed.

Hereafter, the file ID of the area file shall be referred to as “area code” in this Standard.

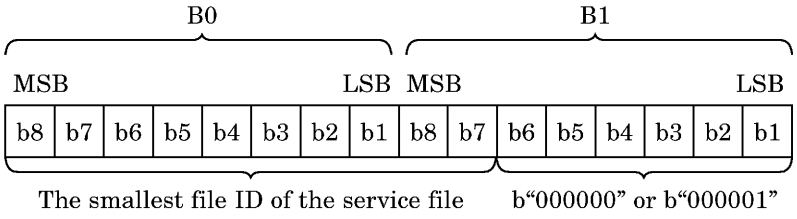


Figure 16 Structure of file ID of area file

8.2.2 Encoding method of file ID of service file The file ID of the service file shall be encoded as follows (see figure 17).

In upper 10 bits, the value of the service number used for service file identification shall be stored.

In lower 6 bits, the value of the access control process category code used to control access shall be stored.

Hereafter, the file ID of the service file shall be referred to as “service code” in this Standard.

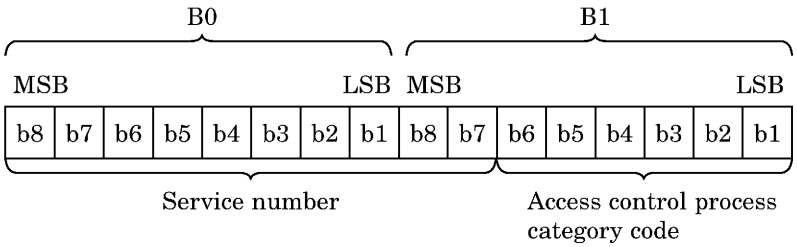


Figure 17 Structure of file ID of service file

8.2.3 Encoding method of overlapped service code It shall be same as the encoding of service code.

8.3 File definition

8.3.1 Definition of area file In the area file, the information to manage the area file [the range of service IDs (service numbers) of 2 bytes (the smallest service code and the last service code), the number of usable blocks of 2 bytes, the area key version and the area key] shall be defined.

The area key is used for authentication and the area key version is used for managing the area key.

There shall be an area file whose area code is '0000' and their usable service codes shall be '0000' to 'FFFE'.

8.3.2 Definition of service file In the service file, the information to manage the service file (the service code of 2 bytes, the number of allocated records of 2 bytes, the service key version of 2 bytes and the service key of 8 bytes) shall be defined. The information of the service key version and the service key shall be defined when the authentication is necessary for the access control process category code.

The service code shall be composed the service number of upper 10 bits and access control process category of lower 6 bits. No two service codes shall be the same within an area file.

The number of allocated records shall be the number of user records allocated to the service.

The service key is used for authentication and the service key version is used for managing the service key.

Multiple access control shall be defined using the overlapped service file.

8.3.3 Definition of overlapped service file In the overlapped service, the information to manage the service file shall be defined.

In the information to manage the service file, the service codes that have the same service number and use the same access method (linear with fixed length, cyclic or add-subtract) although with different access control process category codes shall be defined.

8.4 Service file structure and file data reference All service files shall be linear with fixed length structure or cyclic structure.

Service files may have add-subtract calculation function.

Service files with add-subtract calculation function shall be linear with fixed length structure.

8.4.1 Service file structure

8.4.1.1 Linear with fixed length structure file Access to the service file shall be performed by specifying the record number at the beginning of the file. Record number shall start from "0".

8.4.1.2 Cyclic structure file Logical positions of records shall be allocated in reverse order of the created order.

When reading, the most recent record shall be specified as record number "0" and the subsequent shall be in ascending order.

When writing, the record number shall be always specified as "0".

The write command shall not be executed when the content of the record is exactly the same as the last record. The normal completion response, however, shall be returned as the result of process.

8.4.2 File data reference When accessing to the data, service file shall be controlled by the lower 6 digits of the service code. The list is shown in table 3. The processing method in accordance with the combination with each file structure shall be specified in **8.4.2.1** and **8.4.2.2**.

Table 3 Relation between access control process category code and access without authentication

Access control process category code	Function
001001	Fixed length structure access (read or write)
001011	Fixed length structure access (read only)
001101	Cyclic structure access (read or write)
001111	Cyclic structure access (read only)
010001	Add-subtract calculation access (direct)
010011	Add-subtract calculation access (cash back)
010101	Add-subtract calculation access (decrement)
010111	Add-subtract calculation access (read only)

NOTE : '001000', '001010', '001100', '001110', '010000', '010010', '010100' and '010110' shall not be used in this Standard.

Access control process may require prior mutual authentication and if mutual authentication is performed, subsequent communications shall be encrypted. Also, for access control process without mutual authentication, mutual authentication can be processed.

The access control process category code shall be composed of the access type data and the access attributes. Available access types shall be fixed length access, cyclic access and add-subtract access.

Relation between access control process category code and access without authentication shall be shown in table 3.

8.4.2.1 Fixed length structure file without add-subtract calculation function File access shall be performed by specifying the record number.

— Read access or write access: with/without authentication

Read and write enabled

— Read only access: with/without authentication

Read enabled and write disabled

8.4.2.2 Cyclic structure file without add-subtract calculation function When reading, the record number shall be “0” for the latest record and specified in ascending order for the subsequent.

When writing, all record numbers shall be specified to “0”.

— Read access or write access: with/without authentication

Read and write enabled

— Read only access: with/without authentication

Read enabled and write disabled

8.4.3 Fixed length structure file with add-subtract calculation function Three access types are provided for the add-subtract calculation function in this Standard: direct access, decrement access, and cash back access. The record for add-subtract access shall include balance data (4 bytes); cash back data (4 bytes), user data (6 bytes), and execution ID (2 bytes). The balance data and cash back data shall be positive integers only.

Direct access shall directly read from the specified record or write to the specified record.

Decrement access shall subtract the specified value from the balance data, and overwrite the subtracted value as the cash back data.

Cash back access shall confirm the specified data in the cash back data and add the specified value which is within the cash back data to the balance.

— Direct access: with/without authentication

Read and write enabled

The structure of the record used for direct access is shown in figure 18.

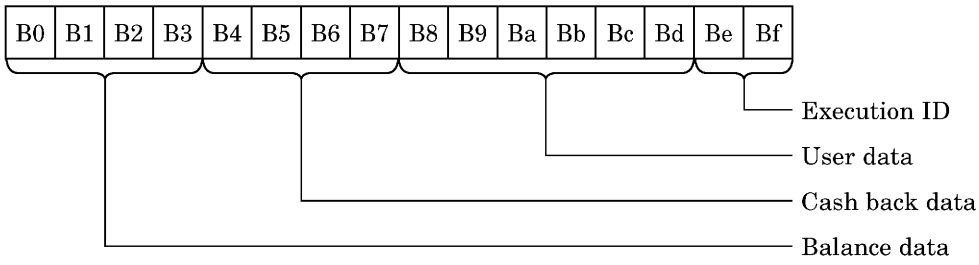


Figure 18 Record data structure for direct access

— Cash back access and decrement access: with/without authentication

Read and write enabled. In writing, cash back access and decrement access are available.

In cash back access, the add data shown in figure 20 shall be added to the balance data in PICC as the value in the cash back data in PICC is the upper limit. After completing the add process, the cash back data in PICC shall become ‘0’.

In decrement access, the subtract data shown in figure 19 shall be subtracted from the balance data in PICC as the value in the balance data in PICC is the

upper limit. After completing the subtract process, the result shall be written to cash back data in PICC.

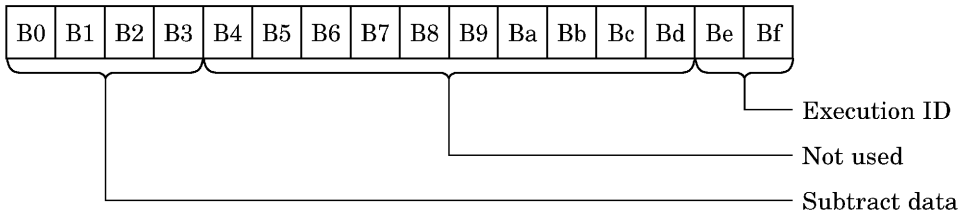


Figure 19 Record data structure for decrement access

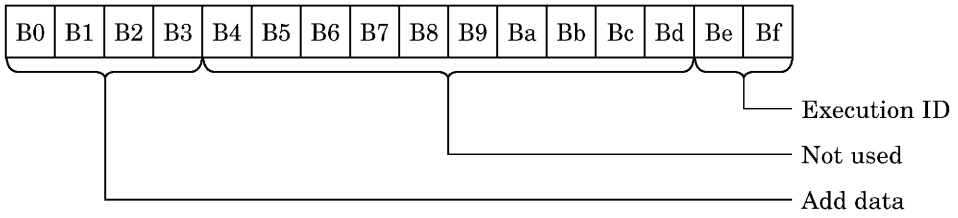


Figure 20 Record data structure for cash back access

— Read only access: with/without authentication

Only read enabled

Cash back access and decrement access do not process commands with the same execution ID written in the records, however, the successful completion response of the process shall be returned. The definition of execution ID is optional.

Each service shall be identified with 2-byte service code. The service code shall define each user record's ID, and the access method for the record.

9 PICC command

9.1 PICC command list The list of PICC commands shall be shown in table 4.

Table 4 Commands list

Command	Command code	Response code	"n" in calculation formula of response time
REQC	'00'	'01'	0
Request Response	'04'	'05'	0
Request Service	'02'	'03'	Number of services
Read	'06'	'07'	Number of blocks
Write	'08'	'09'	Number of blocks
Authentication1	'10'	'11'	Total number of areas and services
Authentication2	'12'	'13'	0
Read from Secure File	'14'	'15'	Number of blocks
Write to Secure File	'16'	'17'	Number of blocks

NOTE : Command code "80" to "85", "8E" to "8F" and "90" to "93" shall not be used in this Standard.

9.2 PICC mode transition and command PICC shall operate in three modes: mode 0, mode 1 and mode 2, and executable commands depend on the modes. PICC shall perform the mode transition to the predetermined mode upon the successful completion of the command. In the initial state in which the power is supplied, PICC shall be in mode 0.

Figure 21 shows the mode transition of PICC by command execution. The mode transition shall be performed only when the command is correctly executed.

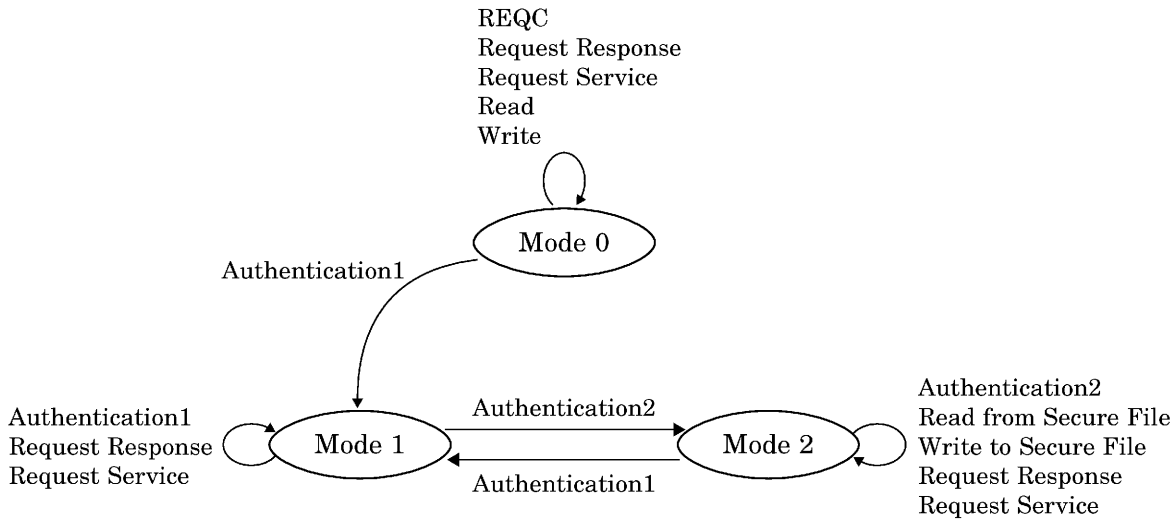


Figure 21 Commands and mode transition in each PICC mode

9.3 Data protection upon transaction error and incomplete processing Simultaneity of writing shall be ensured when multiple blocks are specified with a single write command. When failed in writing a part of blocks, all data blocks specified by the command shall be restored. When power is turned off in the middle of writing, either all blocks or no block shall be updated.

9.4 File and record specification in command On each command, PICC shall be able to process (or open) simultaneously at least 16 services.

9.4.1 File specification in command The file to be processed shall be specified by the service code list and the area code list as the command's file list parameter.

The file list parameter shall be composed of one or more block list elements. The block list element shall be 2 bytes. The file list parameter shall be composed of the number of files of 1-byte and the non-breaking successive block list element corresponding to the number.

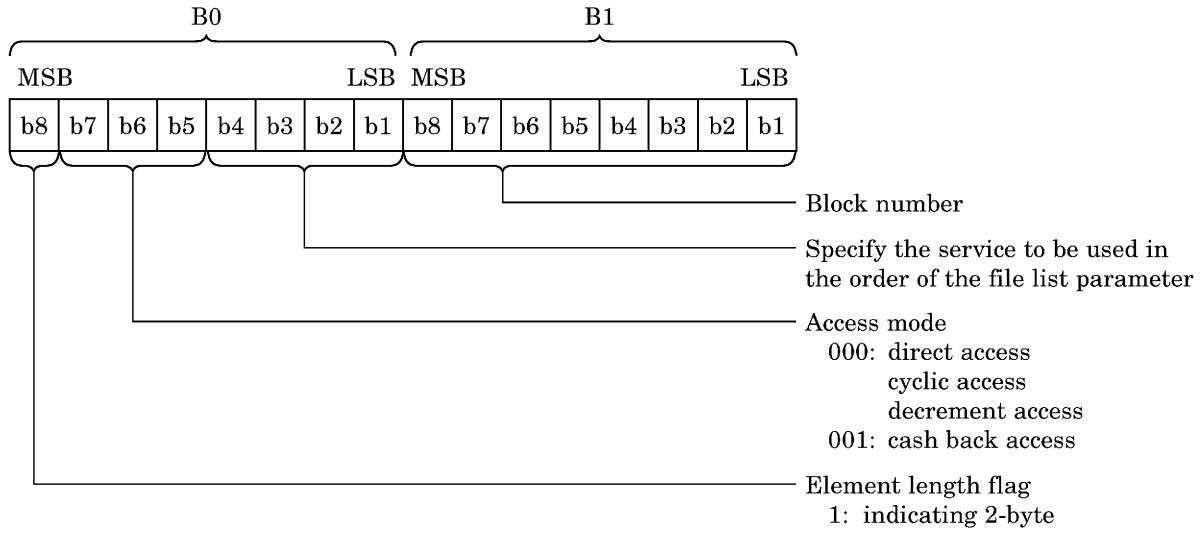
Some commands may omit the file list parameter and refer to the file list of the command executed immediately before.

9.4.2 Record specification method in command The record to be processed shall be specified by the block list parameter as the record list parameter.

The record list parameter shall be composed of one or more block list elements. The block list element shall be either 2 bytes or 3 bytes and the length shall be distinguished

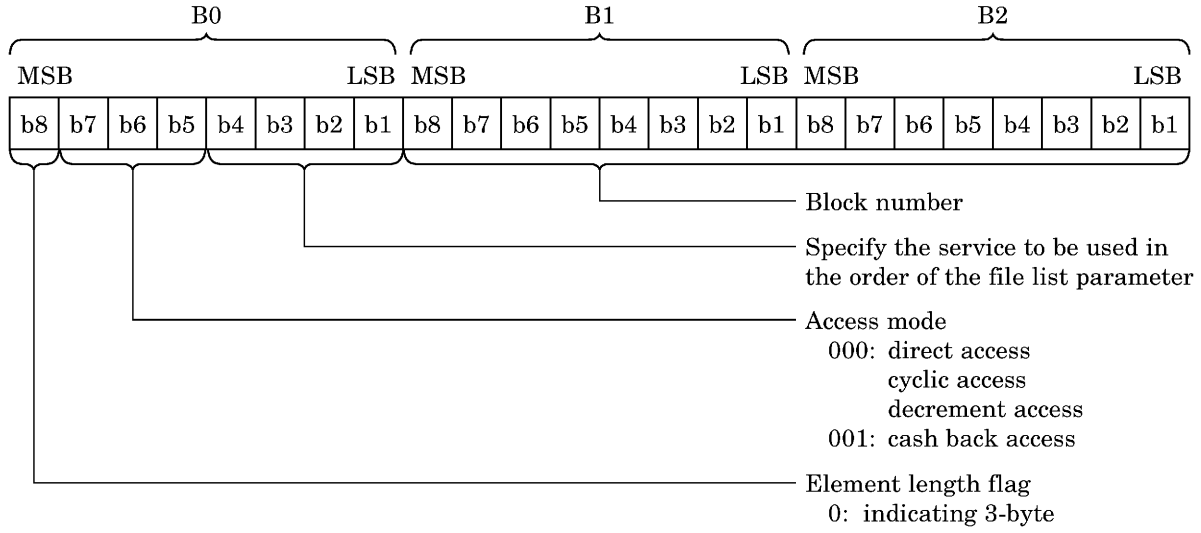
by the MSB of the first byte of each block list element. The structure of 2-byte block list element is shown in figure 22 and the structure of 3-byte block list element is shown in figure 23.

The block list element shall be composed of the element length flag, the access mode, the order of services specified in the file list parameter, and the record number.



NOTE : Access mode of '100' to '111' shall not be used in this Standard.

Figure 22 2-byte block list element



NOTE : Access mode of '100' to '111' shall not be used in this Standard.

Figure 23 3-byte block list element

9.5 Command execution status flag The status flag shall be 2 bytes and composed of the status flag 1 and the status flag 2.

The status flag 1 shall indicate the status code after command execution. Each status code shall be as shown in table 5.

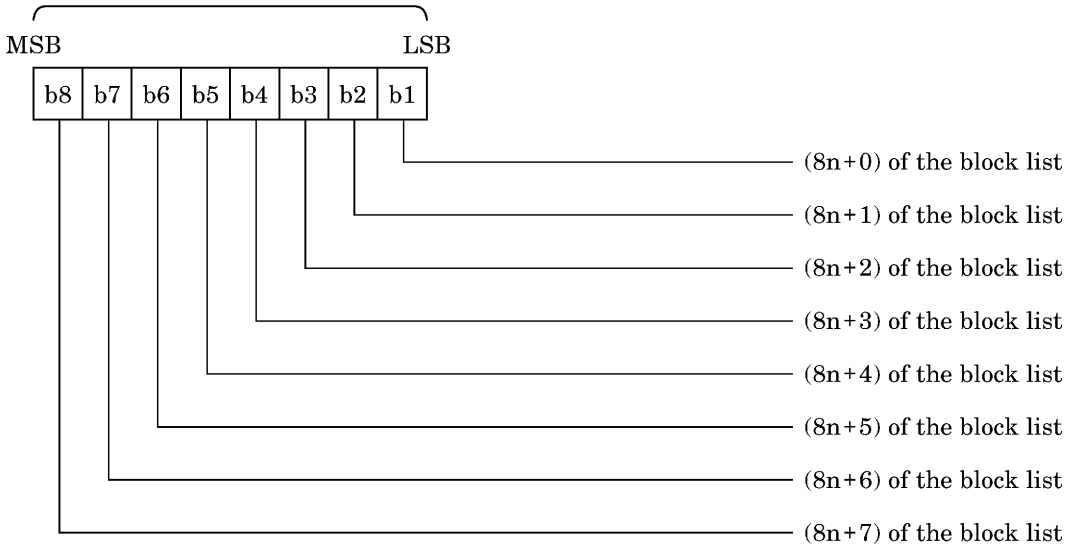
Table 5 Status code list

Code	Meaning	Function
'00'	Successful	Processing successfully terminated.
'01'	Add-Subtract error	In decrement access, balance lack has occurred. In cash back access, balance overflow has occurred.
'02'	Cash back error	In cash back access, the last decrement value is smaller than the cash back data.
'70'	Memory error	Impossible to write to memory or bit error occurred in memory.
'71'	Write error	Excessive write access to memory has occurred.

NOTE : Other codes shall not be used this Standard.

The status flag 2 indicates the location where the error has occurred. Details of the status flag 2 shall be shown in figure 24.

The number of the element of the block list shall start from zero. When designating 8 elements or more, cyclic access shall be used.



Bit representation
0: No error
1: Error

NOTES 1 Error detection is performed in sequence from the top of the list, and the error detected position shall be shown in the status flag 2.

2 In the case where an error is independent of the block list, the status flag 1 becomes 'FF'.

Figure 24 Error position indication

9.6 Command

9.6.1 Request Response command

< Definitions and scope >

PICC shall return the current mode. When normally terminated, PICC shall maintain the mode of that before the command reception.

< Execution condition >

This command shall be executed when its manufacture ID (IDm) is equal to PICC's IDm.

< Command message > Request Response command message format

Command code	IDm
1 byte ('04')	8 bytes

< Response message > Request Response response message format

Response code	IDm	Mode
1 byte ('05')	8 bytes	1 byte
		'00': Mode 0 '01': Mode 1 '02': Mode 2

< Status > The status information does not exist. PICC shall not respond when IDm is different.

9.6.2 Request Service command

< Definitions and scope >

PICC shall return the area key version of the specified area and service key version of the specified service.

PICC shall process up to 16 services even when they are specified at the same time.

When normally terminated, PICC shall maintain the mode of that before the command reception.

< Execution condition >

This command shall be executed when its manufacture ID (IDm) is equal to PICC's IDm.

The number of services or areas (n) specified in the command message shall be $1 \leqq n \leqq N$ ($N \geqq 16$), where, "N" is the maximum number of requested services.

The format of service list or area code list shall be described in **9.4**.

< Command message > Request Service command message format

Command code	IDm	Number of service or areas (n)	Service code list or area code list
1 byte ('02')	8 bytes	1 byte ($1 \leqq n \leqq N \leqq 121$)	$2 \times n$ bytes

<Response message> Request Service response message format

PICC shall respond the area key version of the specified area or service key version of the specified service. ("FFFF" shall be returned when the specified area or service does not exist.)

Response code	IDm	Number of service or areas (n)	Service version or area version list
1 byte ('03')	8 bytes	1 byte ($1 \leqq n \leqq N \leqq 121$)	$2 \times n$ bytes
			'FFFF': No service or no area Other than 'FFFF': Key version

<Status> The status information does not exist. PICC shall not respond when IDm is different.

9.6.3 Read command

<Definitions and scope>

PICC shall respond the record value of the specified service. When normally terminated, PICC shall maintain the mode of that before the command reception. PICC shall process up to 8 services even when they are specified at the same time.

<Execution condition>

This command shall be executed when its manufacture ID (IDm) is equal to PICC's IDm.

The number of services (n) and the number of blocks (m) specified in the command message shall be $1 \leqq n \leqq N$ ($N \geqq 8$) and $1 \leqq m \leqq M$ ($M \geqq 8$).

The format of service code list 1 and block list shall be described in **9.4**.

All service codes specified in the service code list 1 shall be registered in PICC.

Access control process category code of all service files specified in the service code list 1 shall be without authentication.

All record numbers specified in the block list parameter shall be within the number of allocated records of the specified service file.

<Command message> Read command message format

Command code	IDm	Number of services (n)	Service code list 1	Number of blocks (m)	Block list
1 byte ('06')	8 bytes	1 byte [$1 \leqq n \leqq N$ ($N \geqq 8$)]	$2 \times n$ bytes	1 byte [$1 \leqq m \leqq M$ ($M \geqq 8$)]	$2 \times m$ to $3 \times m$ bytes

<Response message> Read response message format

Response code	IDm	Status flag 1	Status flag 2	Number of blocks (m)	Block data
1 byte ('07')	8 bytes	1 byte	1 byte	1 byte	$16 \times m$ bytes
		'00': Normally terminated Others: Failed			

Block data shall be composed of blocks aligned in the sequence specified in the command's block list.

< Status > PICC shall not respond when IDm is different.

When the status flag 1 is set to "00", all blocks have been read with no error. Other codes indicate failure of reading, and PICC does not return the number of blocks and block data.

9.6.4 Write command

< Definitions and scope >

PICC shall write the records of the specified service. When normally terminated, PICC shall maintain the mode of that before the command reception. PICC shall process up to 8 services even when they are specified at the same time.

Simultaneity of writing shall be ensured when multiple blocks are specified by the command.

< Execution condition >

This command shall be executed when its manufacture ID (IDm) is equal to PICC's IDm.

The number of services (n) and the number of blocks (m) specified in the command message shall be $1 \leqq n \leqq N$ ($N \geqq 8$) and $1 \leqq m \leqq M$ ($M \geqq 8$).

The format of service code list 1 and block list shall be described in **9.4**.

All service codes specified in the service code list 1 shall be registered in PICC.

Access control process category code of all service files specified in the service code list 1 shall be without authentication.

All record numbers specified in the block list parameter shall be within the number of allocated records of the specified service file.

< Command message > Write command message format

Command code	IDm	Number of services (n)	Service code list 1	Number of blocks (m)	Block list	Block data
1 byte ('08')	8 bytes	1 byte [$1 \leqq n \leqq N$ ($N \geqq 8$)]	$2 \times n$ bytes	1 byte [$1 \leqq m \leqq M$ ($M \geqq 8$)]	$2 \times m$ to $3 \times m$ bytes	$16 \times m$ bytes

Block data shall be composed of write data aligned in the sequence specified in the command's block list.

< Response message > Write response message format

Response code	IDm	Status flag 1	Status flag 2
1 byte ('09')	8 bytes	1 byte	1 byte
		'00': Normally terminated Others: Failed	

<Status> PICC shall not respond when IDm is different.

When the status flag 1 is set to "00", all blocks have been written with no error. Other codes indicate failure of writing.

9.6.5 Authentication1 command

<Definitions and scope>

PCD authenticates PICC in mutual authentication between PCD and PICC. PICC shall transit to mode 1 when normally terminated.

<Execution condition>

IDm of the command shall be equal to the IDm of PICC.

The command message parameter shall contain the number of areas to be accessed (n), area code list, number of services (m), service code list and challenge data 1.

The response message parameter shall contain challenge data 1' and challenge data 2 (see Annex 1).

<Command message> Authentication1 command message format

Command code	IDm	Parameter
1 byte ('10')	8 bytes	Variable length not more than 246 bytes [Number of areas (n), area code list, number of service (m), service code list and challenge data 1]

NOTE : The parameter format is not specified in this Standard.

<Response message> Authentication1 response message format

Response code	IDm	Parameter
1 byte ('11')	8 bytes	(challenge data 1' and challenge data 2)

NOTE : The parameter format is not specified in this Standard.

<Status> The status information does not exist. PICC shall not respond when IDm is different.

9.6.6 Authentication2 command

<Definitions and scope>

PICC authenticates PCD in mutual authentication between PCD and PICC. PICC shall transit to mode 2 when normally terminated.

After mutual authentication, PICC shall respond the encrypted issuer ID.

<Execution condition>

This command shall be executed after Authentication1 command.

PICC shall be in mode 1 or mode 2.

IDm of the command shall be equal to IDm of PICC.

The command message parameter shall contain challenge data 2'.

The response message parameter shall contain the issuer ID (see Annex 1).

< Command message > Authentication2 command message format

Command code	IDm	Parameter
1 byte ('12')	8 bytes	(challenge data 2')

NOTE : The parameter format is not specified in this Standard.

< Response message > Authentication2 response message format

Response code	Parameter
1 byte ('13')	(communication ID, issuer ID and issue parameter)

NOTE : The parameter format is not specified in this Standard.

< Status > The status information does not exist. PICC shall not respond when IDm is different.

9.6.7 Read from Secure File command

< Definitions and scope >

PICC shall respond the record value of the specified service. When normally terminated, PICC shall maintain the mode of that before the command reception.

Sending/receiving data shall be encrypted.

< Execution condition >

NOTE : Execution condition is not specified in this Standard.

< Command message > Read (encrypted) command message format

Command code	Parameter
1 byte ('14')	Variable length not more than 254 bytes [communication ID, number of blocks (n) and block list]

NOTE : The parameter format is not specified in this Standard.

< Response message > Read (encrypted) response message format

Response code	Parameter
1 byte ('15')	Variable length not more than 254 bytes [communication ID, status flag 1, status flag 2, number of blocks (n) and block data]

NOTE : The parameter format is not specified in this Standard.

< Status >

NOTE : Status is not specified in this Standard.

9.6.8 Write to Secure File command

< Definitions and scope >

PICC shall write the record value of the specified service. When normally terminated, PICC shall maintain the mode of that before the command reception.

Sending/receiving data shall be encrypted.

＜Execution condition＞

NOTE : Execution condition is not specified in this Standard.

＜Command message＞ Write (encrypted) command message format

Command code	Parameter
1 byte ('16')	Variable length not more than 254 bytes [communication ID, number of blocks (n), block list, and block data]

NOTE : The parameter format is not specified in this Standard.

＜Response message＞ Write (encrypted) response message format

Response code	Parameter
1 byte ('17')	(communication ID, status flag 1 and status flag 2)

NOTE : The parameter format is not specified in this Standard.

＜Status＞

NOTE : Status is not specified in this Standard.

Annex 1 (informative)
Security

This Annex is to supplement the matters related to the text and not to constitute the provisions of this Standard.

This Annex describes the access method to authenticated area and service.

For the security, only the architecture is specified, and the implementation method to the commands depends on implementation.

The security covers the following.

— The access key generating

— Mutual authentication between PCD and PICC

— Encryption of the communication path between PCD and PICC

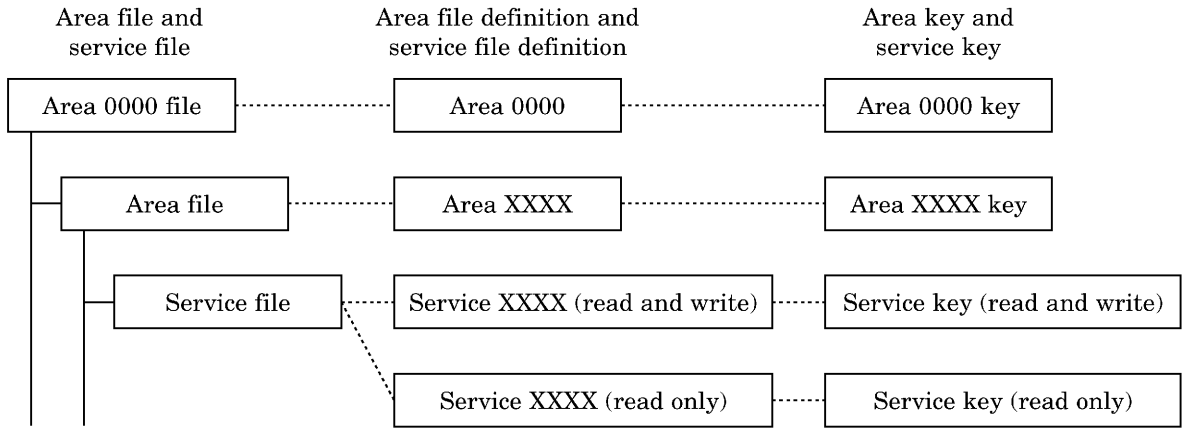
The access key is generated from the area key and service key of the area and service to be accessed.

Mutual authentication is a process of cross-checking confirmation between PCD and PICC, using the access key mentioned above.

By using information as the key, which is generated in the mutual authentication process, the subsequent data on the communication path is encrypted.

Each operation shall be as follows.

1 Access key As shown in Annex 1 figure 1, the area and service with mutual authentication have one area key or service key(s) for each area file and service file.

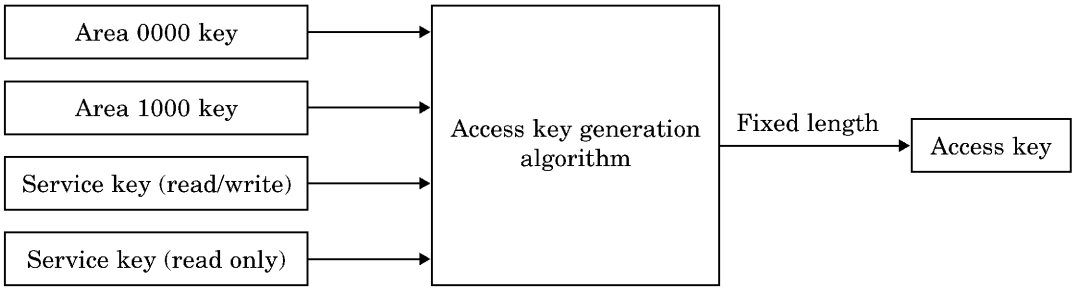


NOTE : Area files are illustrated for descriptive purposes only. No entity of files exist.

Annex 1 Figure 1 Block diagram of area key and service key

The access key is a fixed length key obtained by the calculation using a specific algorithm (hereafter referred to as “access key generation algorithm”) and the area key and service key corresponding to area and service to be simultaneously accessed (or opened).

When accessing all areas and services shown in Annex 1 figure 1, it is necessary to input all keys in the access key generation algorithm. Then an access key of fixed length is generated. Annex 1 figure 2 shows the block diagram of access key generation. Although this example shows the case of two areas and two services, the access key generation algorithm shall be able to handle at least 8 areas and 8 services simultaneously.



Annex 1 Figure 2 Block diagram of access key generation

2 Mutual authentication The purpose of the mutual authentication is to authenticate the validity of PCD and PICC each other.

The mutual authentication procedure shall be shown in Annex 1 figure 3.

a) PCD shall have the access key by means whatever. PCD generates challenge data 1 from the access key by using mutual authentication algorithm A. Then PCD shall transmit the following information to PICC as the parameter of Authentication1 command.

   i) area file ID and service file ID of the area and service to be simultaneously accessed

   ii) challenge data 1

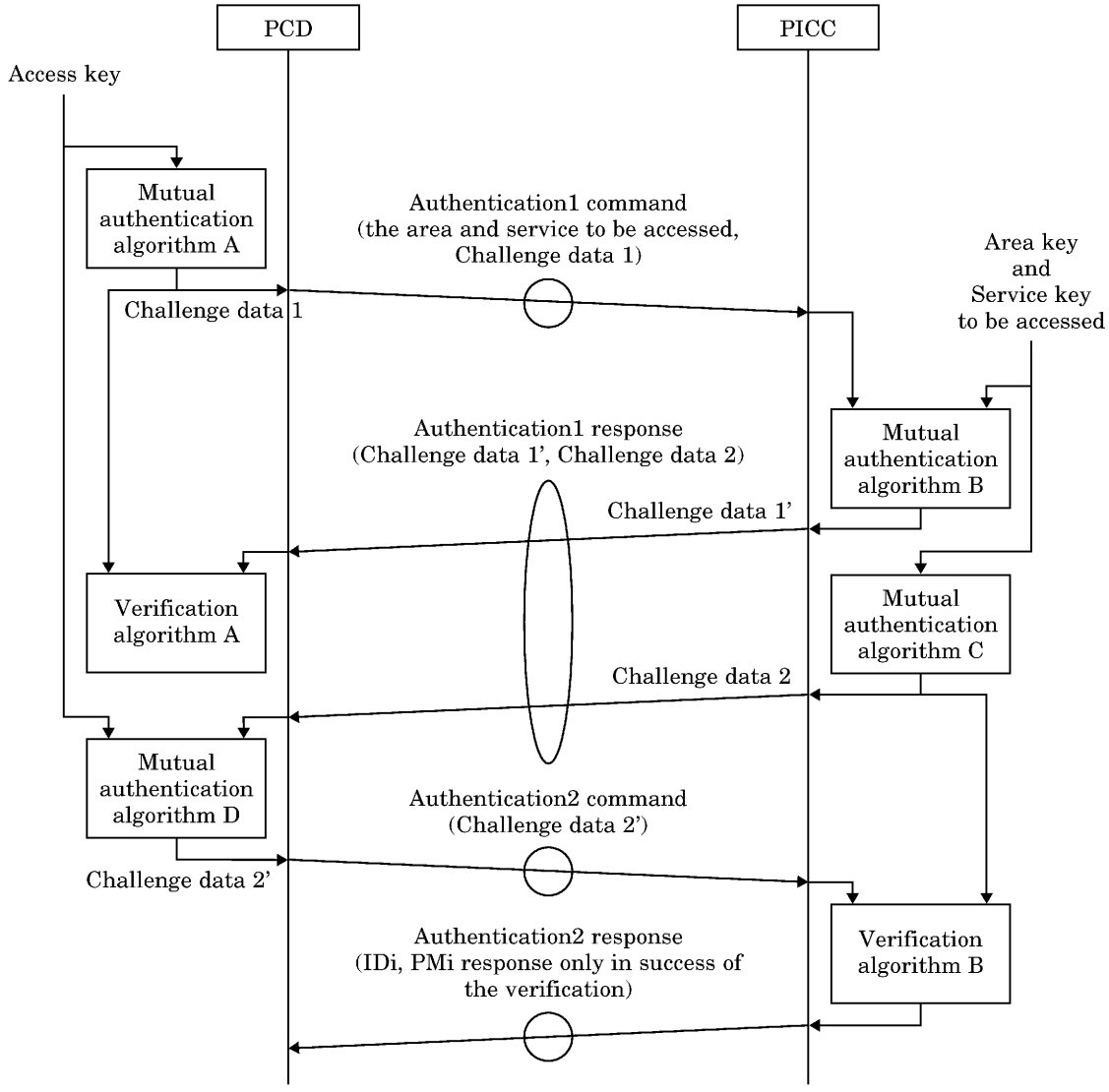
b) Upon the reception of Authentication1 command, PICC generates challenge data 1' from challenge data 1 and the area key and service key for the area and service to be accessed, using mutual authentication algorithm B. Similarly, PICC generates challenge data 2 from the area key and service key, using mutual authentication algorithm C. Then PICC transmits challenge data 1' and challenge data 2 to PCD as the response to the Authentication1 command.

c) Upon the reception of Authentication1 response, PCD performs predetermined calculation with challenge data 1' and challenge data 1 generated in the above step **a**) by using verification algorithm A. This calculation employs the algorithm that reflects the calculation characteristics of mutual authentication algorithm B, so that the validity of challenge data 1' can be confirmed. When verification is completed successfully, PCD interprets that the same access key is shared between PCD and PICC. Authentication process is discontinued immediately if verification completes in failure.

d) PCD generates challenge data 2' from the access key and the challenge data 2 using mutual authentication algorithm D. This data is sent to PICC as the parameter of Authentication2 command.

e) Upon the reception of Authentication2 command, PICC performs predetermined calculation with challenge data 2' and challenge data 2 generated in the above step **b**) by using verification algorithm B. This calculation employs the algorithm that reflects the calculation characteristics of mutual authentication algorithm D, so that the validity of challenge data 2' can be confirmed. When verification is completed successfully, PICC interprets that the same access key is shared between PCD and PICC and returns a success message, including the encrypted 8-byte issue ID (IDi) and 8-byte issue parameter (PMi), as the response to the Authentication2 command. The method of encryption is explained later.

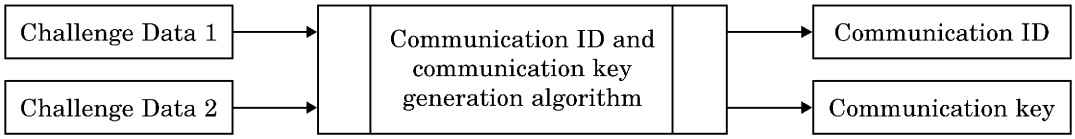
f) Mutual authentication is completed when the Authentication2 response is received by PCD.



Annex 1 Figure 3 Mutual authentication procedure

3 Encryption of communication path Encryption of the communication path uses the communication key generated from challenge data 1 and challenge data 2 using the communication key generation algorithm.

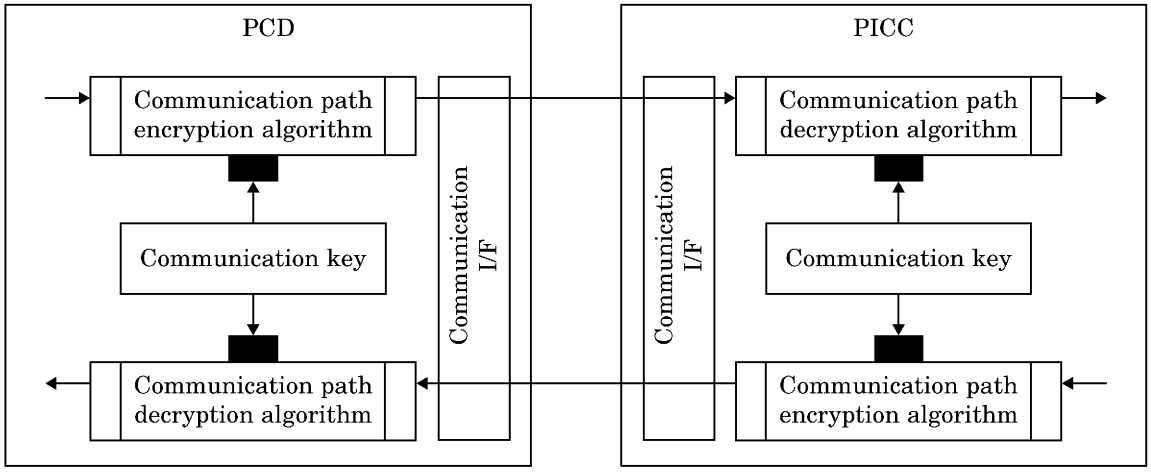
The block diagram of communication key generation is shown in Annex 1 figure 4.



Annex 1 Figure 4 Block diagram of communication key generation

The block diagram of communication path encryption is shown in Annex 1 figure 5. PCD and PICC have not only encryption and decryption algorithms but also share the same communication key and perform encryption and decryption.

All data other than the command code shall be encrypted.



NOTE : (■) indicates key inputs for encryption and decryption process.

Annex 1 Figure 5 Block diagram of communication path encryption

Errata for JIS (English edition) are printed in *Standardization Journal*, published monthly by the Japanese Standards Association, and also provided to subscribers of JIS (English edition) in *Monthly Information*.

Errata will be provided upon request, please contact:

Standards Promotion Department, Japanese Standards Association
4-1-24, Akasaka, Minato-ku, Tokyo, 107-8440 JAPAN
TEL. 03-3583-8002 FAX. 03-3583-0462