RFID Function Instruction

Version: V 1.0.28

Definitions and Declarations

A. The numbers in this paper are represented by hexadecimal except that they are represented by adding (DEC) after hexadecimal numbers
B. An integer is represented by a high-order byte before the low-order byte
C. None in the body of the following agreement means empty, and this field needs to be skipped
D. XX in the following documents represents an unfixed dynamic value

Instruction description

CMD_REQUEST_TYPEA

Describe

Search the IC card of ISO14443 TypeA protocol in the sensing area

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 05	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 00	
DATA	FindMode	1 byte
CHK	XX	

Data domain

FindMode: Card search mode，values and meanings are as follows：
26: find non dormant card
52:find all cards (whether dormant or not)

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Card type(atqa)	2
Card response(sak)	1
Card number	4 or 7

Example

→ AA BB 00 05 00 00 10 00 52 FC
← AA BB 00 0C 00 00 10 00 00 04 00 20 A1 B2 C3 D4 87

CMD_AUTHEN_CLASS

Describe

Verify the sector password of ISO14443 TypeA protocol classic card

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 06	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 01	
DATA	AuthenMode	1 byte
	Sector	1 byte
	Key	6 byte
CHK	XX	

Data domain

AuthenMode: Verification mode, values and meanings shown in the appendix
Sector:Sector code, value range: 00 ~ 28
Key: Sector password

Response data domain

Nothing

Example

→ AA BB 00 0C 00 00 10 01 60 00 FF FF FF FF FF FF C6
← AA BB 00 05 00 00 10 01 00 AF

CMD_READ_CLASS

Describe

Read the data block of ISO14443 TypeA protocol classic (class) IC card

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 05	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 02	
DATA	Block	1 byte
CHK	XX	

Data domain

Block: The block number of the data block to be read

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Data of a block	16(dec)

Example

→ AA BB 00 05 00 00 10 02 01 AD
← AA BB 00 15 00 00 10 02 00 B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 BA BB BC BD BE BF BC

CMD_WRITE_CLASS

Describe

Write the data block of ISO14443 TypeA protocol classic card

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 15	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 03	
DATA	Block	1 byte
	BlockData	16 byte
CHK	XX	

Data domain

Block: The block number of the data block to be write
BlockData: Block data to write

Response data domain

Nothing

Example

→ AA BB 00 15 00 00 10 03 01 B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 BA BB BC BD BE BF BC
← AA BB 00 05 00 00 10 03 00 AD

CMD_HALT

Describe

The block data to be written puts the found ISO14443 TypeA protocol card into sleep state

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 04
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: 04
DATA	none
CHK	XX

Data domain

Nothing

Response data domain

Nothing

Example

→ AA BB 00 04 00 00 10 04 AB
← AA BB 00 05 00 00 10 04 00 AA

CMD_QREAD_CLASS

Describe

The classic card of fast reading ISO14443 TypeA protocol can directly call this instruction to realize fast card reading after connecting to the communication port.

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 0C	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 05	
DATA	AuthenMode	1 byte
	Block	1 byte
	fNeedSearchCard	1 byte
	Key	6 byte
CHK	XX	

Data domain

AuthenMode: Verification mode, values and meanings shown in the appendix
Block: Block data to read
fNeedSearchCard: Specify card search operation, 1 - required, 0 - not required
Key: The password of the sector where the block to be read is located

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Data of card block	16(dec)

Example

→ AA BB 00 0D 00 00 10 05 60 01 01 FF FF FF FF FF FF C3
← AA BB 00 15 00 00 10 05 00 B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 BA BB BC BD BE BF BB

CMD_QWRITE_CLASS

Describe

The classic card of fast writing ISO14443 TypeA protocol can directly call this instruction to realize fast card writing after connecting to the communication port

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 1C	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 06	
DATA	AuthenMode	1 byte
	Block	1 byte
	Key	6 byte
	BlockData	16 byte
	fNeedSearchCard	1 byte
CHK	XX	

Data domain

AuthenMode: Verification mode, values and meanings shown in the appendix
Block: Block data to read
Key: The password of the sector where the block to be read is located
BlockData: Data of the block to be written
fNeedSearchCard: Specify card search operation, 1 - required, 0 - not required

Response data domain

Nothing

Example

Write block1
→ AA BB 00 1D 00 00 10 06 60 01 FF FF FF FF FF FF B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 BA BB BC BD BE BF 01 D0
← AA BB 00 05 00 00 10 06 00 A8

CMD_INITVAL_CLASS

Describe

Format a block into a value block (wallet) and set the initial value

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 09	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 07	
DATA	Block	1 byte
	Value	4 byte
CHK	XX	

Data domain

Block: Block number to format
Value: Initial value to set

Response data domain

Nothing

Example

Format block 4 into a wallet block with an initial value of 0
→ AA BB 00 09 0 00 10 07 04 00 00 00 00 83
← AA BB 00 05 0 00 10 07 00 CF

CMD_INC_CLASS

Describe

Increment the value block by one value

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00

	LL: 09	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 08	
DATA	Block	1 byte
	Value	4 byte
CHK	XX	

Data domain

Block: Value block number
Value: Value to increase

Response data domain

Nothing

Example

Increase value block 4 by 100
→ AA BB 00 09 00 00 10 08 04 00 00 00 64 CA
← AA BB 00 05 00 00 10 08 00 A6

CMD_DEC_CLASS

Describe

Reduce the value block by one value

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 09	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 09	
DATA	Block	1 byte

	Value	4 byte
CHK	XX	

Data domain

Block: Value block number
Value: Value to subtract

Response data domain

Nothing

Example

Reduce value block 4 by 100
→ AA BB 00 09 00 00 10 09 04 00 00 00 64 CB
← AA BB 00 05 00 00 10 09 00 A7

CMD_READVAL_CLASS

Describe

Read value block

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 09	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 0A	
DATA	Block	1 byte
CHK	XX	

Data domain

Block: Value block number to read

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Value	4

Example

Read value block 4
→ AA BB 00 05 00 00 10 0A 04 A0
← AA BB 00 09 00 00 10 0A 00 00 00 00 64 CC

CMD_RESTORE_CLASS

Describe

Back up the value of a value block to another block

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 06	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 0B	
DATA	Block_To	1 byte
	Block_From	1 byte
CHK	XX	

Data domain

Block_To: Block number backed up to
Block_From : Value block backed up

Response data domain

Nothing

Example

Back up value block 4 to block 5
→ AA BB 00 06 00 00 10 0B 05 04 A7
← AA BB 00 05 00 00 10 0B 00 A5
Note: if the two blocks related to backup are not in the same sector, both sectors need to be verified before backup

CMD_READ_TAG

Describe

Read the data block of the ntag tag of ISO14443 TypeA protocol (including Ultralight card)

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 05	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 10	
DATA	Page	1 byte
CHK	XX	

Data domain

Page: The page number of the data page to be read

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Data of one page	4(dec)

Example

→ AA BB 00 05 00 00 10 10 06 B8

← AA BB 00 09 00 00 10 10 00 B0 B1 B2 B3 B2

CMD_WRITE_TAG

Describe

Write the data block of the ntag tag of ISO14443 TypeA protocol (including Ultralight card)

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 15	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 11	
DATA	Page	1 byte
	PageData	4 byte
CHK	XX	

Data domain

Page: The page number of the data page to write
PageData: Page data to write

Response data domain

Nothing

Example

→ AA BB 00 09 00 00 10 11 08 B0 B1 B2 B3 BB
← AA BB 00 05 00 00 10 11 00 BF

CMD_AUTHEN_TAG

Describe

Verify the password of TAG of ISO14443 TypeA protocol

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 08	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 12	
DATA	Key	4 byte
CHK	XX	

Data domain

Key: NTAG password

Response data domain

Nothing

Example

→ AA BB 00 08 00 00 10 12 FF FF FF FF B1
← AA BB 00 05 00 00 10 12 00 BC

CMD_TYPEA_CPU_ATR

Describe

Reset the CPU card of ISO14443 TypeA protocol to obtain ATR information

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 04
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: 1E
DATA	none
CHK	1A

Data domain

Nothing

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
ATR	XX

Example

→ AA BB 00 04 00 00 10 1E B1
← AA BB 00 0B 00 00 10 1E 00 A0 A1 A2 A3 A4 A5 BF

CMD_TYPEA_CPU_APDU

Describe

The reader / writer exchanges instructions with the ISO14443 TypeA protocol CPU card

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: XX

	LL: XX	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 1F	
DATA	TimeDelay	1 byte
	SecLen	1 byte
	APDU_CMD	XX byte
CHK	XX	

Data domain

TimeDelay: Command acquisition response waiting time, unit: 10ms, recommended value: 7
SecLen: Instruction transmission unit length, which cannot exceed 63 (DEC)
APDU_CMD: Need to sent to instruction package of card

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Card response packet APDU_REP	XX

Example

→ AA BB 00 0B 00 00 10 1F 07 3C 00 84 00 00 08 08
← AA BB 00 0C 00 00 10 1F 00 C0 C1 C2 C3 C4 C5 C6 C7 B8

CMD_TYPEA_RAW_EXC

Describe

The reader / writer exchanges protocol commands with ISO14443 TypeA protocol card. Many specific functions can be completed with this instruction

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: XX

	LL: XX	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 20	
DATA	EXC_IN	XX byte
CHK	XX	

Data domain

EXC_IN: Need to sent to card exchange instruction

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Card response packet REP	XX

Example

Send command 60
→ AA BB 00 05 00 00 10 20 60 EE
← AA BB 00 0C 00 00 10 20 00 C0 C1 C2 C3 C4 C5 C6 C7 B8

CMD_GET_PBOC_PAN

Describe

The reader / writer obtains the main account number (string code printed on the card surface) of the UnionPay identification card. There is no need to execute other instructions before this instruction

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 06
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: 26

DATA	Get_Mode
	SLOT (1 byte)
CHK	XX

Data domain

Get_Mode: 0 - each card can only be read once, 1 - each card can be read multiple times
SLOT: Which slot the card locate, 0-Normal Contact Slot, 100-RFID area

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Account string code (string)	XX

Example

→ AA 00 00 06 00 00 10 26 01 64 55
← AA 00 00 15 00 00 10 26 00 36 32 32 32 35 33 31 33 31 34 31 33 37 38 2D // Return to Account:" 6222531314137178"

CMD_GET_SSC

Describe

The reader / writer get the information of Social Security Card (CN). There is no need to execute other instructions before this instruction

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 05
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: 27
DATA	SLOT (1 byte)
CHK	XX

Data domain

SLOT: Which slot the card locate, 0-Normal Contact Slot, 100-RFID area

Response data domain

All the information is string format. Each item split by String "\r\n"
Items defined as follow:

Flag	Definition
'1'	Specification Version
'2'	Card UID
'3'	Issue Date
'4'	Expiration Date
'5'	Issue Area Code
'8'	Certification Of Citizenship
'9'	Owner's Name
'A'	Owner's Gender
'B'	Owner's Nation
'C'	Birth Date

Example

→ AA 00 00 05 00 00 10 27 64 56
← AA 00 00 69 00 00 10 27 00 31 32 2E 30 30 0D 0A 32 42 35 55 34 37 32 37 35 36 0D 0A 33 32 30 31 34 31 32 33 31 0D 0A 34 32 30 32 34 31 32 33 31 0D 0A 35 34 34 30 33 30 30 0D 0A 38 34 34 31 34 32 31 31 39 38 34 31 31 32 34 34 30 31 31 0D 0A 39 C1 CE D4 A3 C1 BC 0D 0A 41 31 0D 0A 42 30 31 0D 0A 43 31 39 38 34 31 31 32 34 0D 0A 22

CMD_GET_PBOC

Describe

The reader / writer get the information of UnionPay Card. There is no need to execute other instructions before this instruction

Command message

Domain	Value
STX	AA
INX	XX

LEN	LH: 00 LL: 05
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: 28
DATA	SLOT (1 byte)
CHK	XX

Data domain

SLOT: Which slot the card locate, 0-Normal Contact Slot, 100-RFID area

Response data domain

All the information is string format. Each item split by String "\r\n"
Items defined as follow:

Flag	Definition
'1'	Primary Account Number (PAN)
'2'	Valid Date
'3'	Cardholder's Name (Maybe missing)
'4'	ID Number (Maybe missing)

Example

→ AA 02 00 05 00 00 10 28 64 5b
← AA 02 00 24 00 00 10 28 00 31 36 32 33 30 37 31 30 31 30 39 30 31 34 34 36 35 30 38 39 0D 0A 32 32 33 31 32 33 31 0D 0A 27

CMD_RF_SET_TXCW

Describe

Set the conductance of TX antenna driver

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00

	LL: 06	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 2C	
DATA	PT	1 byte
	REG	1 byte
CHK	XX	

Data domain

PT: The protocol type of the card for operating. Set to 41 if ISO14443A, 42 if ISO14443B, 31 if ISO15693
REG: The value for setting. The maximum value maybe different depend to devices.

Response data domain

Nothing

Example

→ AA BB 00 06 00 00 10 2C 41 3F FF
← AA BB 00 05 00 00 10 2C 00 82

CMD_RF_GET_TXCW

Describe

Get the conductance value of TX antenna driver

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 05	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 2D	
DATA	PT	1 byte
CHK	XX	

Data domain

PT: The protocol type of the card for operating. Set to 41 if ISO14443A, 42 if ISO14443B, 31 if ISO15693

Response data domain

REG: The value saved.

Example

→ AA BB 00 05 00 00 10 2D 41 C2
← AA BB 00 06 00 00 10 2D 00 3F BF

CMD_RF_RST

Describe

Radio Frequency Reset on Device

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 05	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 2E	
DATA	Time	2 byte
CHK	XX	

Data domain

Time: Reset time in MS

Response data domain

Nothing

Example

Radio Frequency Reset 10ms
→ AA BB 00 06 00 00 10 2E 00 0A 89
← AA BB 00 05 00 00 10 2E 00 15 95

CMD_RF_ANT

Describe

Control antenna on or off

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 05	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 2F	
DATA	Action	1 byte
CHK	XX	

Data domain

Action: Antenna is on, set to 01; Antenna is off, set to 00

Response data domain

Nothing

Example

Turn off antenna
→ AA BB 00 05 00 00 10 2F 00 81
← AA BB 00 05 00 00 10 2F 00 81

CMD_RF_SET_RODATA_PARA

Describe

When setting read-only mode, the data format of the original data to be returned

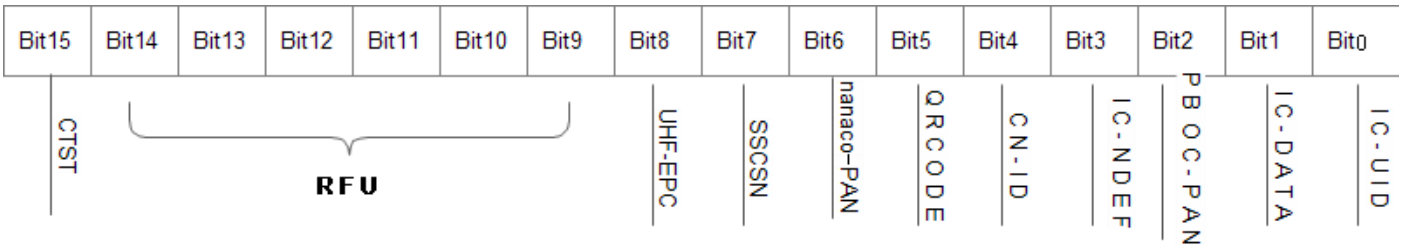
Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 0F	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 30	
DATA	DATA_SIZE	1 byte
	DIR	1 byte
	DATA_SYS	1 byte
	LEN_SHOW	1 byte
	BLK_RO	1 byte
	KEY_RO	6 byte
	AUTH_MODE	1 byte
	OBJ_TYPE	2 byte
	OBJ_PROTOCOL	1 byte
CHK	XX	

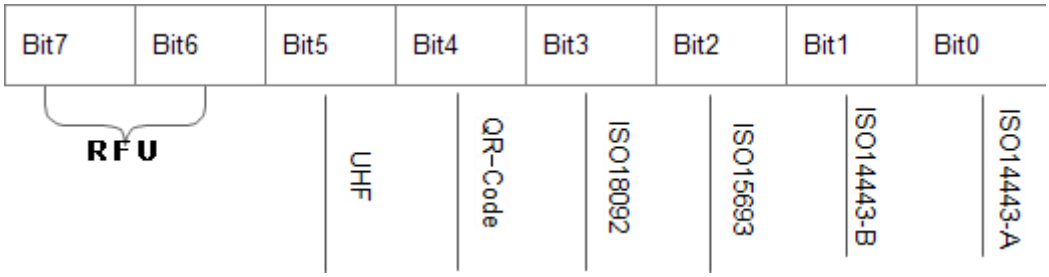
Data domain

DATA_SIZE: Number of bytes read, 0-output per unit of data by object, X-output X bytes
DIR: Show data direction, 01-forward, 00-reverse
DATA_SYS: Binary, 00-decimal, 01-hexadecimal, 02-16 string, 03-Wiegand
LEN_SHOW: Alignment digits, excluding the front and back codes, before''0'if insufficient. When 0, the output will be in actual length
BLK_RO: Read-only start block number or page number address output
KEY_RO: Password used for read-only blocks or pages, MF classic card password 6 bytes, NTAG card first 4 bytes
AUTH_MODE: Validation card mode (see appendix), for NTAG cards, KeyA uses KEY_RO password validation, KeyB uses one-card-one-secret scheme, and needs to set device key
OBJ_TYPE: Read-only (identify) target types, supported types include IC card number UID (IC-UID), IC-DATA user data, UnionPay account (PBOC-PAN), IC card NDEF standard data (IC-NDEF), Chinese identity card internal code (CN-ID), two-dimensional code (QRCODE), Nanaco card account,Social-security-card-number(SSCSN),State Of Contact Card Inser/Out (CTST), each type

corresponds to a Bit, if the function is turned on in state 1, the failed state is 0; UHF-EPC



OBJ_PROTOCOL: Read-only targets conform to standard protocols, and the corresponding Bit bit locations for each protocol are defined as follows:



Response data domain

Nothing

Example

→ AA BB 00 13 00 00 10 30 00 00 01 00 00 FF FF FF FF FF FF FF 60 00 01 01 16
← AA BB 00 05 00 00 10 30 00 9E

CMD_RF_GET_RODATA_PARA

Describe

Gets the data format of the original data in the device's current read-only mode

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 05
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: 31

DATA	none
CHK	XX

Data domain

Nothing

Response data domain

See to the DATA field of CMD_RF_SET_RODATA_PARA

Example

→ AA BB 00 04 00 00 10 31 9E
← AA BB 00 14 00 00 10 31 00 00 00 01 00 00 FF FF FF FF FF FF 60 00 01 01 EF

CMD_RF_SET_APPENDDATA

Describe

When setting read-only mode, the data to be returned, the output data appended to the original data

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: XX LL: XX	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 32	
DATA	FADDR	1 byte
	FTIME	1 byte
	SIZE_FORWORD	1 byte
	DATA_FORWORD	4 byte
	SIZE_BEHIND	1 byte
	DATA_BEHIND	4 byte
	FADD_DATA_LEN	1 byte
	FADD_DATA_CRC	1 byte
	FADD_OBJ_TYPE	1 byte

	FADD_PACK_TYPE	1 byte
	FADD_FRAME_WRAP	1 byte
	FADD_DEVSN	1 byte
CHK	XX	

Data domain

FADDR: Does the device address code come with it? 00-Not included, 01-Included
FTIME: Whether time information is included (6 bytes, years, months, days, minutes, seconds). 00-Not included, 01-Included
SIZE_FORWORD: Length before attachment, range: 0~4
DATA_FORWORD: Pre-attached data
SIZE_BEHIND: After additional length, range: 0~4
DATA_BEHIND: Post-attached data
FADD_DATA_LEN: A flag indicate whether to append data length before data, 00-no, 01-append
FADD_DATA_CRC: Verification of data, 00-No, 01-XOR, 02-Checksum
FADD_OBJ_TYPE: A flag indicate whether to append object's type, 00-no, 01-append
FADD_PACK_TYPE: A flag indicate whether to append package's type, 00-no, 01-yes
FADD_FRAME_WRAP: A flag indicate whether to wrap with frame format, 00-no, 01-yes
FADD_DEVSN: A flag indicate whether to append device's SN, 00-no, 01-yes

Response data domain

Nothing

Example

Append 1 byte 31 before, without address code, without time, not append data-length, not append verify byte, append object type, not append package type, not wrap, not append devices'sn
→ AA BB 00 16 00 00 10 32 00 00 01 31 00 00 00 00 00 00 00 00 00 00 01 00 00 00 BD
← AA BB 00 05 00 00 10 32 00 9C

Append 2 bytes 0D 0A after, without address code and time, no append data-length, no append verify byte, no append object type, not append package type, not wrap
→ AA BB 00 16 00 00 10 32 00 00 00 00 00 00 00 00 02 0D 0A 00 00 00 00 00 00 00 00 89
← AA BB 00 05 00 00 10 32 00 9C

CMD_RF_GET_APPENDDATA

Describe

Gets the additional data format before auto output in the device's current read-only mode

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 04
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: 33
DATA	none
CHK	XX

Data domain

Nothing

Response data domain

See the Data domain of instruction CMD_RF_SET_APPENDDATA

Example

→ AA BB 00 04 00 00 10 33 9C
← AA BB 00 14 00 00 10 33 00 00 00 00 00 00 00 00 02 00 00 0D 0A 00 00 00 89

CMD_RF_SET_REP_RODATA_SEQ

Describe

Set the order of each data (byte) before the original data is returned in the read-only mode

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: XX LL: XX
DEVICE	DH:XX DL: XX

CMD	CH: 10 CL: 34	
DATA	SEQ	X byte
CHK	XX	

Data domain

SEQ: The return order of each data. The first half byte is the original order and the second half byte is the adjusted byte. The maximum length is 16 bytes

Response data domain

Nothing

Example

Change the original data order of 8 bytes to:
04->00,05->01,06->02,07->03,00->04,01->05,02->06,03->07
→ AA BB 00 0C 00 00 10 34 40 51 62 73 04 15 26 37 93
← AA BB 00 05 00 00 10 34 00 9A

CMD_RF_GET_REP_RODATA_SEQ

Describe

Gets the order of each data (byte) before the original data is returned in read-only mode

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 04
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: 35
DATA	none
CHK	XX

Data domain

Nothing

Response data domain

SEQ: The return order of each data. The first half byte is the original order and the second half byte is the adjusted byte. The maximum length is 16 bytes

Example

→ AA BB 00 04 00 00 10 35 9A
← AA BB 00 05 00 00 10 35 00 40 51 62 73 04 15 26 37 9B

CMD_RF_SET_RWMODE

Describe

Gets the order of each data (byte) before the original data is returned in read-only mode

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 06	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 36	
DATA	MODE	1 byte
	fWMem	1 byte
CHK	XX	

Data domain

MODE:RFID operation mode. 00 read-write mode, 01 read-only mode
fWMem: The parameter to indicate whether save this setting. 00 don’t save, 01 save.

Response data domain

Nothing

Example

Set enable read only RFID mode
→ AA BB 00 06 00 00 10 36 01 01 9B
← AA BB 00 05 00 00 10 36 00 98

CMD_RF_GET_RWMODE

Describe

Get the behavior mode of the device in RFID operation, read-only or read-write

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 04
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: 37
DATA	none
CHK	XX

Data domain

Nothing

Response data domain

MODE: RFID operation mode. 00 read-write mode, 01 read-only mode

Example

→ AA BB 00 04 00 00 10 37 98
← AA BB 00 05 00 00 10 37 01 98

CMD_REQUEST_TYPEB

Describe

Search the IC card of ISO14443 TypeB protocol in the sensing area

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 04
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: 50
DATA	fSel: 1Byte
CHK	XX

Data domain

sSel: The flag to set whether select card or not. 0- No select, 1- Select.

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
start(50)	1
PUPI	4
Application Data	4
Protocol Info	3

Example

→ AA 00 00 04 00 00 10 50 44
← AA 00 00 11 00 00 10 50 00 50 00 00 00 00 D1 03 86 05 00 80 80 50

CMD_TYPEB_APDU

Describe

The reader / writer exchanges instructions with the ISO14443 TypeB protocol IC card

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: XX LL: XX	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 52	
DATA	APDU_CMD	XX byte
CHK	XX	

Data domain

APDU_CMD: Instruction package to send to card

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Card response packet APDU_REP	XX

Example

→ AA 00 00 09 00 00 10 52 00 36 00 00 08 75
← AA 00 00 0F 00 00 10 52 00 20 C9 24 32 20 36 81 7F 90 00 CA

CMD_REQUEST_15693

Describe

Search the IC card of ISO15693 protocol in the sensing area, such as ICode

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 05
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: 60
DATA	Request Mode
CHK	XX

Data domain

Request Mode: Request card search mode, the value 36 is to find a single card each time, and the value 16 is to find multiple cards each time

Response data domain

Successfully return the card UID. If multiple cards are returned, list each UID in turn

Example

Find a card
→ AA 00 00 05 00 00 10 60 36 43
← AA 00 00 0D 00 00 10 60 00 E0 04 01 50 82 26 A9 D4 11

Find multi card
→ AA 00 00 05 00 00 10 60 16 63
← AA 00 00 15 00 00 10 60 00 E0 04 01 50 82 26 A9 D4 E0 04 01 50 65 70 F7 E9 B7

CMD_15693_EXC_COM

Describe

The reader / writer and the ISO15693 protocol IC card execute the general instruction exchange in accordance with the 15693-3 rules

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: XX LL: XX	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 61	
DATA	Command Code	1
	UID	8
	User Parameter	XX
CHK	XX	

Data domain

Command Code : General instruction code to be sent to the card (see rule 15693-3)
UD: Card UID returned from card search
User Parameter: In 15693-3, the parameter before CRC16 after UID in each instruction package. If there are no parameters, ignore this item.

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Card response packet APDU_REP	XX

Example

Read the data on page 8
→ AA 00 00 0E 00 00 10 61 20 E0 04 01 50 82 26 A9 D4 08 3B
← AA 00 00 09 00 00 10 61 00 88 88 88 88 78

CMD_15693_EXC_CUST

Describe

The reader / writer and ISO15693 protocol IC card execute the exchange of card user instructions

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: XX LL: XX	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 62	
DATA	Custom Code	1 byte
	Mfg Code	1 byte
	UID	8 byte
	User Parameter	XX byte
CHK	XX	

Data domain

Custom Code: User instruction code to send to card
Mfg Code: Card manufacturer code, which takes the byte immediately after E0 in the UID
UID: Card UID returned from card search
User Parameter: The card corresponds to the document. After the UID in each instruction package, the parameter before CRC16. If there are no parameters, ignore this item.

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Card response packet APDU_REP	XX

Example

Take random number
→ AA 00 00 0E 00 00 10 62 B2 04 E0 04 01 50 82 26 A9 D4 A6
← AA 00 00 07 00 00 10 62 00 8D 73 8B

CMD_15693_EXC_EX

Describe

The reader / writer deal with ISO15693 protocol IC card, execute the exchange of card instructions, which can user-defined mostly.

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: XX LL: XX	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 63	
DATA	Request Frame	XX
CHK	XX	

Data domain

Request Frame: The card corresponds to the document. Begin with flags in each request frame, and the parameter before CRC. Notice that the UID should be reverse by the sequence got by CMD_REQUEST_15693.

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Card response packet APDU_REP	XX

Example

Take random number
→ AA 00 00 0F 00 00 10 63 22 B2 04 E0 04 01 50 82 26 A9 D4 84
← AA 00 00 07 00 00 10 63 00 8D 73 8A

CMD_REQUEST_TYPEF

Describe

Search the IC card of ISO14443 typef protocol in the sensing area (Felica)

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 04	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 70	
DATA	System Code	2
CHK	XX	

Data domain

System Code: Card system code,FFFF is filled in by default

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
IDm(Vendor ID)	8
PMm (Vendor parameters)	8

Example

→ AA 00 00 06 00 00 10 70 FF FF 66

← AA 00 00 15 00 00 10 70 00 D0 D1 D2 D3 D4 D5 D6 D7 D8 D9 DA DB DC DD DE DF 75

CMD_TYPEF_APDU

Describe

The reader / writer exchanges instructions with the ISO14443 typef protocol IC card

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: XX LL: XX	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 72	
DATA	APDU_CMD	XXbyte
CHK	XX	

Data domain

APDU_CMD: Need to sent to instruction package of card

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Card response packet APDU_REP	XX

Example

//Request System Code, assuming ID D0 ~ D7
→ AA 00 00 0D 00 00 10 72 0C D0 D1 D2 D3 D4 D5 D6 D7 63
← AA 00 00 0F 00 00 10 72 00 0D D0 D1 D2 D3 D4 D5 D6 D7 02 04 C7 FE 00

CMD_QWRITE_FM12XX

Describe

A instructions to write data easily to FM12XX serial card (Product of Fudan Microelectronics), this is a dedicated command.

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: XX LL: XX	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 81	
DATA	Offset	2 byte
	Length	2 byte
	Data	XX byte
CHK	XX	

Data domain

Offset: The start address the data for writing, 2 bytes
Length: Data length of the data, 2 bytes
Data: Data for writing to card

Response data domain

None

Example

→ AA 00 00 0C 00 00 10 81 00 00 00 04 01 02 03 04 9D
← AA 00 00 05 00 00 10 81 00 94

CMD_QREAD_FM12XX

Describe

A instructions to read data easily from FM12XX serial card (Product of Fudan Microelectronics), this is a dedicated command.

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 08	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 82	
DATA	Offset	2 byte
	Length	2 byte
CHK	XX	

Data domain

Offset: The start address the data for reading, 2 bytes
Length: Data length of the data, 2 bytes

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Data	XX

Example

→ AA 00 00 08 00 00 10 82 00 00 00 04 9E
← AA 00 00 09 00 00 10 82 00 01 02 03 04 9F

CMD_SEL_ANT

Describe

This command apply to some special modules which have multi-ant, the antenna will active after been select.

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 05	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: 90	
DATA	INX_ANT	1byte
CHK	XX	

Data domain

INX_ANT: The index of antenna , valid value from 1 to 255

Response data domain

None

Example

//Select antenna 1
→ AA 00 00 05 00 00 10 90 01 84
← AA 00 00 05 00 00 10 90 00 85

CMD_UHF_INVENTORY

Describe

Reader detect tags by inventory operation, it will retrieve EPC of tags.

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 06	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: A0	
DATA	SCAN_TIME	2byte
CHK	XX	

Data domain

SCAN_TIME: Set a 16bit integer to define a time duration of scan tags, it'll not return until the time up, Unit MS.
Note: SCAN_TIME can by adjust by the actual environment of application, it shall be bigger if there are more tags. Otherwise shall be smaller if less tags for testing.

Response data domain

The data returned successfully are as follows:

Explain	Data Type	Length (bytes)
List of EPC	LEN1+EPC1+LEN2+EPC2+…	n

Example

→ AA 00 00 06 00 00 10 A0 00 32 84
← AA 00 00 1C 00 00 10 A0 00 04 00 00 00 09 0C 01 02 03 04 05 06 07 08 09 0A 0B 0C 04 00 00 00 17 B2

CMD_UHF_SEL_TAG

Describe

Select one from tags found, so can access this one specially.

Command message

Domain	Value
STX	AA

INX	XX	
LEN	LH: XX LL: XX	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: A3	
DATA	Mode	1byte
	EPC	nbyte
CHK	XX	

Data domain

Mode: Select/Unselect one tag, set 1 to select , 0 to unselect
EPC: the content of the tag's EPC.

Response data domain

None

Example

→ AA 00 00 0D 00 00 10 A3 01 01 02 03 04 05 06 07 08 B7
← AA 00 00 05 00 00 10 A3 00 B6

CMD_UHF_READ_TAG

Describe

Read bank data of tag, the bank which can set from EPC/TID/User specified by user.

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 0F
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: A1

DATA	Tag_Bank	1byte
	RAddr_W	4byte
	RLen_W	2byte
	PWD	4byte
CHK	XX	

Data domain

Tag_Bank: Which bank wanted to read, Values see to appendix.
RAddr_W: The start address of the bank, Unit: Word (2-byte).
RLen_W: The length of the bank been read, Unit: Word (2-byte).
PWD: the access-password used when reading, default value: 00000000h

Response data domain

The data returned successfully are as follows:

Explain	Length (bytes)
Bank Data	2*RLen_W

Example

→ AA 00 00 0F 00 00 10 A1 02 00 00 00 00 00 04 00 00 00 00 B8
← AA 00 00 0D 00 00 10 A1 00 E2 80 68 90 20 00 50 04 52

CMD_UHF_WRITE_TAG

Describe

Write data of tag, the bank which can set from EPC/TID/User specified by user.

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 0F	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: A2	
DATA	Tag_Bank	1byte

	WAddr_W	4byte
	WLen_W	2byte
	PWD	4byte
	WData	nbyte
CHK	XX	

Data domain

Tag_Bank: Which bank wanted to write, values see to appendix.
WAddr_W: The start address of the bank, Unit: Word (2-byte).
WLen_W: The length of the bank want to write, Unit: Word (2-byte).
PWD: the access-password used when writting, default value: 00000000h
WData: the data for write.

Response data domain

None

Example

→ AA 00 00 17 00 00 10 A2 01 00 00 00 02 00 04 00 00 00 00 01 02 03 04 05 06 07 08 AA
← AA 00 00 05 00 00 10 A2 00 B7

CMD_UHF_LOCK_TAG

Describe

Lock tag

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 0A	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: A9	
DATA	Tag_Bank	1byte
	Lock_Type	1byte

	PWD	4byte
CHK	XX	

Data domain

Tag_Bank: Which bank wanted to lock, values see to appendix.
Lock_Type: the lock type, 1 byte, value can be:

- ✧ 0x00, Open -Temporary
- ✧ 0x01, Lock -Temporary
- ✧ 0x02, Open-Permanent
- ✧ 0x03, Lock-Permanent

PWD: the access-password used when locking, default value: 00000000h

Response data domain

None

Example

→ AA 00 00 0A 00 00 10 A9 01 01 00 00 00 00 B3
← AA 00 00 05 00 00 10 A9 00 BC

CMD_UHF_KILL_TAG

Describe

Kill operation to make tag unchangeable

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 08	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: AA	
DATA	PWD	4byte
CHK	XX	

Data domain

PWD: the access-password used when killing tag, default value: 00000000h

Response data domain

None

Example

→ AA 00 00 08 00 00 10 AA 00 00 00 00 B2
← AA 00 00 05 00 00 10 AA 00 BF

CMD_UHF_SET_LINK_CONFIG

Describe

Set UHF RF's link configuration, which contains link communicate rate, type of modulation, and code mode. There is different appearance when set different kind of values when identifying tags.

Command message

Domain	Value	
STX	AA	
INX	XX	
LEN	LH: 00 LL: 05	
DEVICE	DH:XX DL: XX	
CMD	CH: 10 CL: AB	
DATA	Config_Mode	1byte
CHK	XX	

Data domain

Config_Mode: Configuration value, which defined bellows:
0xD0: Miller 40KHz tari 25us
0xD1: FM0 200Khz tari 6.25us
0xD2: FM0 200Khz tari 12.5us
0xD3: FM0 200KHz tari 25us

0xD4: Miller4 200KHz tari 6.25us
0xD5: Miller4 200KHz tari 12.5us
0xD6: Miller4 200KHz tari 25us (Default value)
0xD7: Miller4 250KHz tari 6.25us
0xD8: FM0 640KHz tari 6.25us
0xD9: FM0 40KHz tari 25us
0xDA: GB FM0 64KHz
0xDB: GB Miller 128KHz
0xDC: GB FM0 128KHz

Response data domain

None

Example

→ AA 00 00 05 00 00 10 AB D6 68
← AA 00 00 05 00 00 10 AA 00 BF

CMD_UHF_GET_LINK_CONFIG

Describe

Get UHF RF's link configuration, which contains link communicate rate, type of modulation, and code mode.

Command message

Domain	Value
STX	AA
INX	XX
LEN	LH: 00 LL: 04
DEVICE	DH:XX DL: XX
CMD	CH: 10 CL: AC
DATA	None
CHK	XX

Data domain

None

Response data domain

Config_Mode: Configuration value, defines see command: CMD_UHF_SET_LINK_CONFIG

Example

→ AA 00 00 04 00 00 10 AC B8
← AA 00 00 06 00 00 10 AC 00 D6 6C

Appendix

Verification card mode

60: Verify A password
61: Verify B password

The Bank Of UHF Tag

00: Reserved Bank
01: EPC Bank
02: TID Bank
03: User Bank
04: Access Password
05: Kill Password