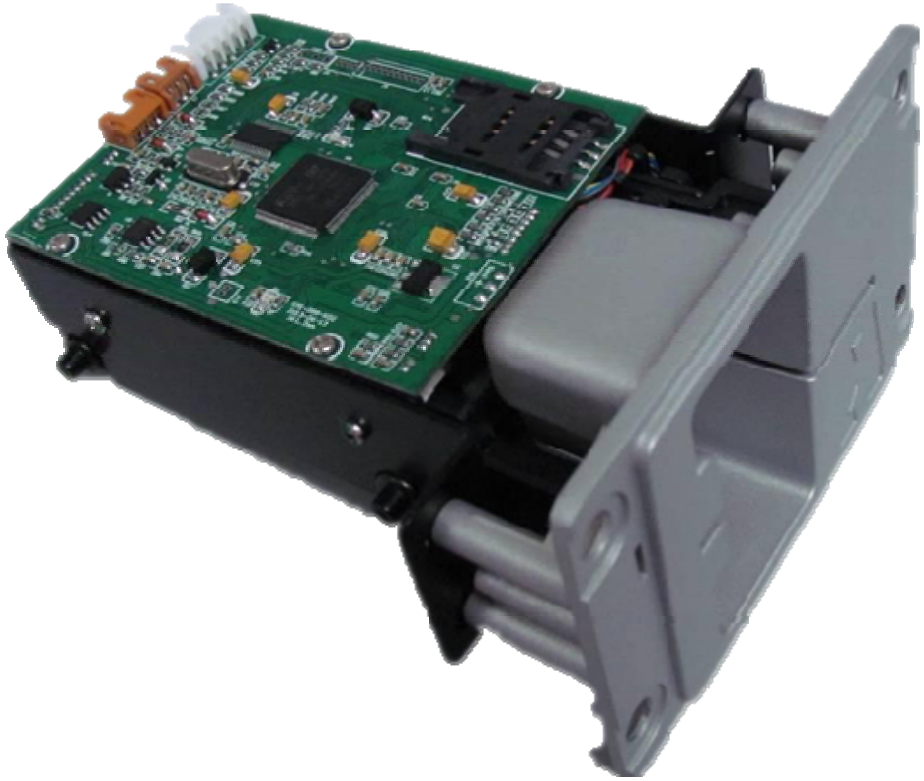
CRT-288-K001

MANUAL CARD READER

COMMUNICATION PROTOCOL



CREATOR (CHINA) TECH CO., LTD

·Add: 2F, M-10 Building, Center Area, Hi-tech Industrial Park, Shenzhen, China

·TEL: +86 755 26710691 FAX: +86 755 26710105

·Http://www.china-creator.com/

Revisions

Version	Date	Content
1.0	2013.6.23	Initial Release

Table of Contents

1. Communication Format

1.1 RS232 Communication

Baud rate (BPS): 9600/19200/38400/57600/115200 BPS （Support auto-identification）

Communication type: Asynchronous communication

Transmit type: Half duplex

Data Frame Structure:

Start bit	D0	D1	D2	D3	D4	D5	D6	D7	Stop bit

Start bit: 1 bit

Data bit: 8 bit

Stop bit: 1 bit

Coding scheme: ASCII 8 bit

1.2 USB Communication

1. Interface Mode: USB 2.0 full-speed (12M/S）
2. Driver: HID（Human interface device），comply with USB HID protocol, VID is 23D8H, PID is 0285H
3. Communication Speed: Adopt USB 2.0 full-speed and USB HID protocol, therefore interruption interval is 1ms, Description report is 65 bytes, Maximum byte per second is 65000 bytes.
4. Frame separate and reform: The data must separate and reformed because the description report is only 65 bytes long, data and command separate and reform base on the following format.

4-1 HID protocol, Report ID Value: 0x00

Frame format: User-defined

Report ID(1 byte)	Data0.....Data63(64Byte)

Frame Format for USB HID Protocol

4-2 The maximum capacity for USB 2.0 is 64 bytes, the frame separation and reform are requested

4-3 Report ID is invariably 00H, Data0-Data63 is data, if the data is larger than 64 bytes, it needs another frame to transmit the rest.

Example 1:

Send data=F2H, 00H, 01H, 05H, F4H (Need only one frame)

Report ID=00H,

' ……..' means the rest of data which is zero

FrameE1: 00H, [F2H, 00H, 01H, 05H, F4H]……..

Example 2:

Send data= F2H, 00H, 21H, 01H, 02H, 03H……,20H, 21H, BCC (Need two frames)

Data length: 67byte

FrameE1: 00H, [F2H, 00H, 21H, 01H, 02H, 03H…….]

FrameE2: 00H, [20H, 21H, BCC]……

Example 3:

Send data= F2H, 00H, 03H,'C', 30H, 30H, BCC (Need only one frame)

FrameE1: 00H, [F2H, 00H, 03H, 'C', 30H, 30H, BCC] ……

4-4 Data length information is contained in the beginning frame of data. The transmission process will be concluded, when the data which length is defined by the beginning frame have been transmitted, .

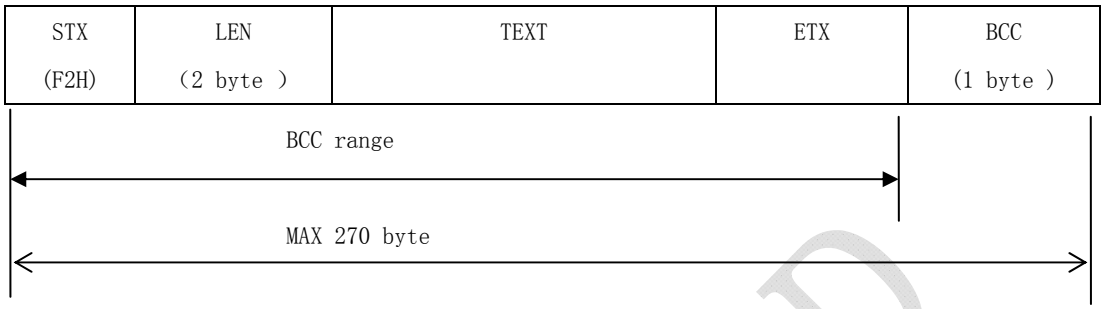
Notes: For USB communication mode, the start-up phase (Initialization phase) is 6 seconds, therefore please manipulate the reader after 6 seconds

2. Communication Control Method

Reader is a driven part and manipulated by valid command

3. Communication Format and Control Characters

3.1 Communication Format



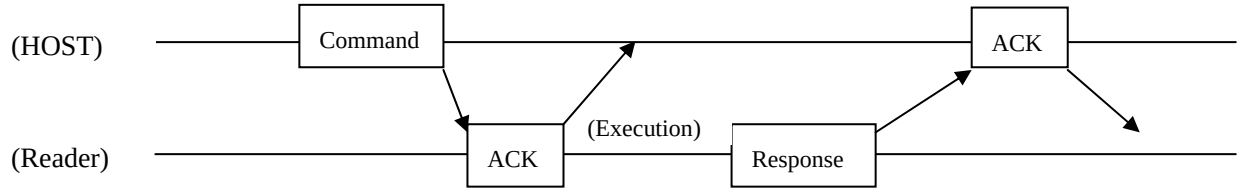
STX (F2H)	Start bit
LEN（2 bytes）	Length of data, high byte before low byte
TEXT	Data (Command or response)
BCC	Exclusive-or verify

3.2 Control Character

ACK (06H)	Communication acknowledge character
NAK (15H)	Communication negative acknowledge character
EOT (04H)	Communication Cancel Character

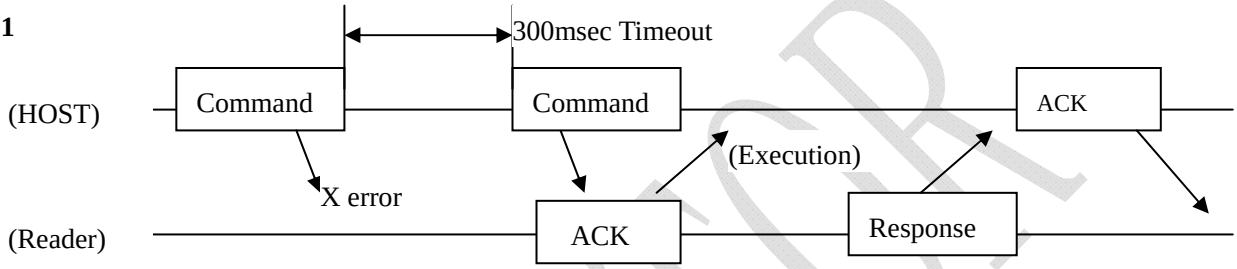
4. Communication Process Descriptions

4.1 Ordinary Communication Process

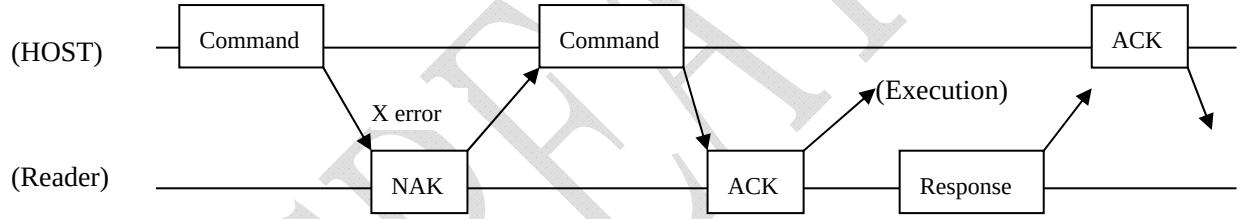


4.2 Irregular Communication Process (Command and response)

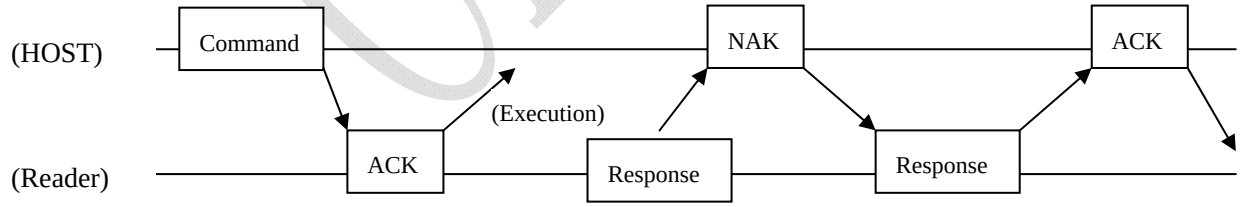
Case 1



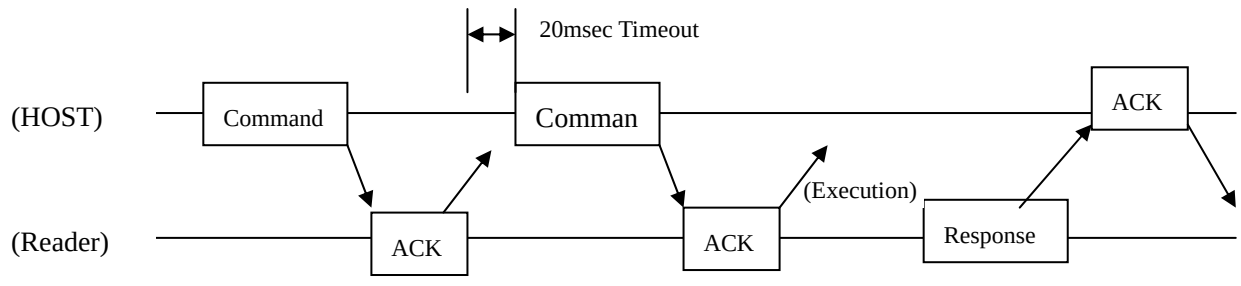
Case 2



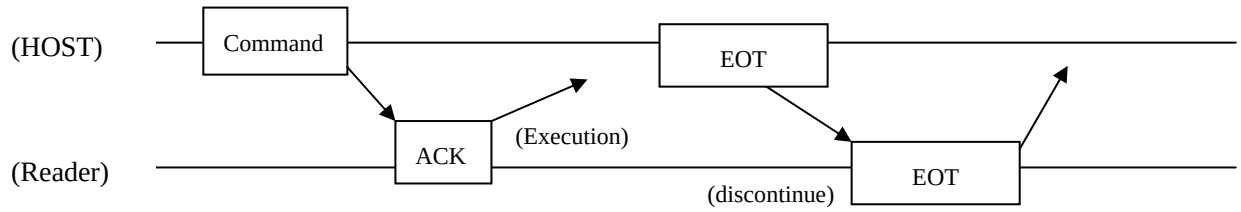
Case 3



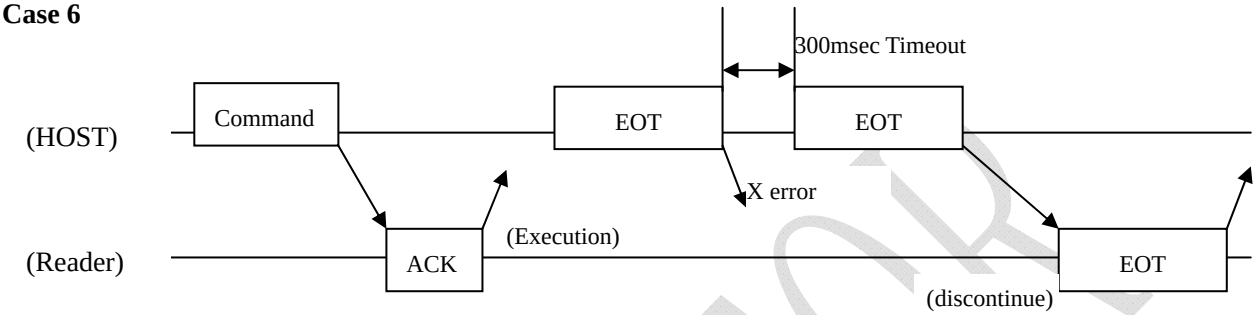
Case 4



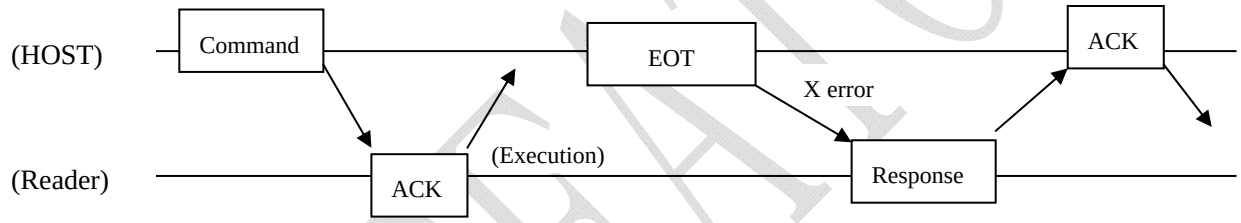
Case 5



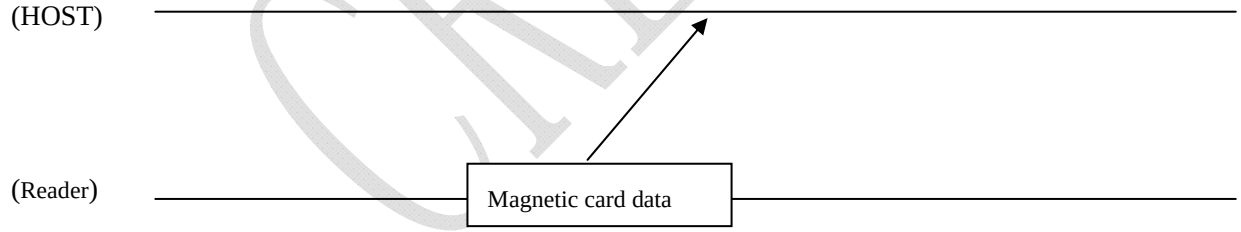
Case 6



Case 7



Case 8



Notes:

1. Case 8 is active uploading mode for magnetic card operation
2. The reader will not accept HOST command in the writing EEPROM process

5 Control Package (TEXT Package) Format

5.1 Command （HOST–> READER）

"C"	CM	PM	DATA

"C"= 43H

CM: Command character

PM: Parameter character

DATA: Transmission data

5.2 Ordinary Return （READER–> HOST）

"P"	CM	PM	ST1	ST0	DATA

"P"= 50H

CM&PM is the same as command (Except IC card control operation)

STO&ST1: Status Character

DATA: Transmission data

5. 3 Irregular Return（READER–> HOST）

"N"	CM	PM	E1	E0	DATA

"N"= 4EH

CM&PM is the same as command (5.1) (Except IC card control operation)

E0&E1: Error Code

DATA: Transmission data

Notes: Command must be sent 5ms after the response of the last command

6 Status Code and Error Code

6.1 Status Code ST1&ST0

ST1	Meaning	ST0	Meaning
“0”	Latch Lock	“0”	No Card inside and inserting
“1”	Latch Release	“1”	Card is not in place of card latch switch, but there is a card inside
		“2”	Card is in place of card latch switch

6.2 Error Code E1 & E0

E1 & E0	CONTENTS
“00”	CM (Command Character) Error
“01”	PM (Parameter Character) Error
“02”	Command can not be executed
“03”	Out of hardware support
“04”	Command data error
“05”--“10”	Preserve
“11”	Card latch operation failure
“12”--“14”	Preserve
“15”	EEPROM error
“16” --“19”	Preserve
“20”	Read magnetic card error（Exclusive-or bit error）
“21”	Read magnetic card error
“22”-“29”	Preserve
“30”	Power down
“31”-“40”	Preserve
“41”	IC card module operation failure
“42” -- “59”	Preserve
“60”	Short circuit of IC card power supply
“61”	IC card initialization failure
“62”	Out of IC card support command
“63”	IC card does not response
“64”	Other than”63”
“65”	Non-initialized of IC card
“66”	Card type out of reader support
“67”--“68”	Preserve
“69”	Not support EMV mode
“70”--“F9”	Preserve

7 Command List

Chapter	Command	Functions	CM	PM	Description
8.1	Initialize	Initialize CRT-288-K001	30H	30H	Initialized and release the lock
				31H	Initialized and keep lock up
8.2	Latch	Latch Operation	B0H	30H	Latch lock up
				31H	Latch release
				32H	Auto-Lock when card insert
				33H	Non-Lock when card insert
8.3	Serial Number	Read reader's serial number	A2H	30H	Read serial number
8.4	Status request	Inquire the current status of reader	31H	30H	Obtain status code ST0, ST1
8.5	LED Indicator	Control of two LED indicators	80H	30H	LED indicator on/off control
				31H	LED indicator flicker control
8.6	Auto Test Card Type		50H	30H	Auto test IC card type
				31H	Auto test RF card type
8.7	Magnetic Stripe Card Operation	Magnetic Stripe Card Application	36H	30H	Reading method (Pulling / Withdraw)
				31H	Read magnetic stripe card data buffer
				32H	Actively uploading magnetic stripe data
				39H	Clear magnetic stripe card buffer
8.8	CPU Card Operation	CPU card application	51H	30H	CPU Card Reset (Initialization)
				31H	CPU card power down
				32H	CPU card status inquiry
				33H	T=0 CPU Card APDU operation
				34H	T=1 CPU Card APDU operation
				38H	CPU card warm reset
				39H	Auto select T=0/T=1 CPU card APDU operation
8.9	SAM Card Operation	SAM Card application	52H	30H	SAM Card reset (Initialization)
				31H	SAM Card power down
				32H	SAM Card status inquiry
				33H	T=0 SAM Card APDU Operation
				34H	T=1 SAM Card APDU Operation
				38H	SAM Card warm reset
				39H	Auto Select T=0/T=1 SAM Card APDU Operation
				40H	Select SAM Card stand

8.10	SLE4442/4428 Card Operation		53H	30H	SLE4442/4428 reset (Initialization)
				31H	SLE4442/4428 power down (Release)
				32H	Inquire SLE4442/4428 status
				33H	Operate SLE4442 card
				34H	Operate SLE4428 card
8.11	I²C Memory Card Operation	24C01—24C256 card application	54H	30H	I²C card reset (Initialization)
				31H	I² C card power down(Release)
				32H	Inquire I² C card status
				33H	Read I²C card data
				34H	Write I²C card data
8.12	Contactless IC Card Operation (13.56 MHZ)	Mifare one Type A & B T=CL protocol	60H	30H	RF card reset (Initialization)
				31H	RF card power down
				32H	Inquire RF card status
				33H	Mifare card operation
				34H	Type A RF card communication
				35H	Type B RF card communication

8. Command Specification

8.1 Reset

HOST Send:

"C"	30H	PM

PM= 30H: Initialize and release the lock

PM= 31H: Initialize and keep the lock up

Positive Return:

"P"	30H	PM	ST1	ST0	Version information byte SV

Version information byte: CRT-288-K001 Reader SV= “CRT 288 K001”

Negative Return:

"N"	30H	PM	E1	E0

8.2 Latch Operation

HOST Send:

"C"	B0H	PM

PM= 30H: Lock the latch

PM= 31H: Lock Release

PM= 32H: Auto-lock when card insert

PM= 33H: Non-lock when card insert

Positive Return

"P"	B0H	PM	ST1	ST0

Negative Return:

"N"	B0H	PM	E1	E0

8.3 Read Serial Number of Machine

HOST Send:

"C"	A2H	30H

Positive Return

"P"	A2H	30H	ST1	ST0	Serial number package (n byte)

Serial number package:

Reserve as ASCII

Example:

ASCII text file of “CRT-288” is “43H, 52H, 54H, 2DH, 32H, 038H, 35H”

The maximum length of serial number package is 13 byte

Negative Return:

"N"	A2H	30H	E1	E0

8.4 Check Reader's Status

HOST Send:

"C"	31H	30H

Positive Return:

"P"	31H	30H	ST1	ST0

Negative Return:

"N"	31H	30H	E1	E0

8.5 LED Indicator Control

Control two LED indicators on main PCB board (one is red, the other is blue), the flicker cycle and on/off status of these two LED indicators can be controlled.

8.5.1 LED On/Off Control

HOST Send:

"C"	80H	30H	PM1	PM 2

PM1=30H Control Red LED

PM1=31H Control Blue LED

PM2=30H LED Off

PM2=31H LED On

Positive Return:

"P"	80H	30H	ST1	ST0

8.5.2 LED Flicker Control

HOST Send:

"C"	80H	31H	PM1	PM2	PM3

Communication length: N=4

PM1=30H Control Red LED

PM1=31H Control Blue LED

PM2, PM3 Control the flicker of LED, PM2 control the cycle time of light on status, PM3 control the cycle time of light off status

PM2: Cycle time of light on status

（The value range of PM2 is 00-FFH，Cycle time is 0.25 second × PM2）

PM3: Cycle time of light off status

（The value range of PM3 is 00-FFH, Cycle time is 0.25 second ×PM3）

LED flicker cycle time period = PM2 + PM3. The minimum cycle time period is 0.5 second

（PM1=01H, PM2=01H）

PM2=00H, PM3 is random value, LED will be ever extinguished

PM3=00H,PM2=01-FFH， LED will be ever bright

Notes: After cold reset (Power on/off) or warm reset (Reset command), the red LED indicator will be ever bright and the blue indicator will be extinguished

Positive Return:

"P"	80H	31H	ST1	ST0

8.6 Auto-Identify Card Type

8.6.1 Auto-Identify IC Card Type

HOST Send:

"C"	50H	30H

Reader executes auto-identify card type command and returns the card type information

Positive Return:

"P"	50H	30H	ST1	ST0	Card Type Status Byte S1	Card Type Status Byte S2

Card Type Status Byte S1, S2：

S1	S2	Description
’0’	‘0’	Unknown IC card type
‘1’	‘0’	T=0 CPU
	‘1’	T=1 CPU
‘2’	‘0’	SL4442
	‘1’	SL4428
‘3’	‘0’	AT24C01
	‘1’	AT24C02
	‘2’	AT24C04
	‘3’	AT24C08
	‘4’	AT24C16
	‘5’	AT24C32
	‘6’	AT24C64
	‘7’	AT24C128
	‘8’	AT24C256

Negative Return:

"N"	50H	30H	E1	E0

8.6.2 Auto-Identify RF Card Type

HOST Send:

"C"	50H	31H

Reader executes auto-identify card type command and returns the card type information

Positive Return:

"P"	50H	31H	ST1	ST0	Card Type Status S1	Card Type Status S2

Card Type Status Byte S1, S2

S1	S2	Description
‘0’	‘0’	Unknown Card Type
‘1’	‘0’	Mifare one S50
	‘1’	Mifare one S70
	’2’	Mifare one UL
’2’	‘0’	Type A CPU
’3’	‘0’	Type B CPU

Negative Return:

"N"	50H	31H	E1	E0

8.7 Magnetic Stripe Card Operation

Initialization status for coded format of magnetic stripe card data is ASCII for three tracks. Once execute reset command, the reader will switch back to initialization status. Magnetic stripe card operation is including reading mode selection, buffer reading/clearance, data uploading method selection;

the detail description is the following:

Setting magnetic card reading mode: CM=36H，PM=30H；

This command is to set coded format of magnetic stripe card (ASCII or binary) and data uploading method (Active or passive)

Read buffer for magnetic stripe card: CM=36H，PM=31H；

This command is to set reading of buffer and coded format for buffer. The data uploading is controlled by HOST and reader response according to the command

Active data uploading method: CM=36H，PM=32H；

This command is to set parameter of data active uploading method. The data uploading is automatically done by reader and HOST will passively receive the data of magnetic stripe card.

Clear magnetic stripe card data buffer: CM=36H，PM=39H；

This command is to set clearance of data in magnetic stripe card data buffer. And once the reading when insertion method is set, the buffer will automatically clear by reader when card is pulling out of the reader.

8.7.1 Setting Magnetic Card Reading Method

HOST Send：

"C"	36H	30H	Reading Method	Data Uploading Method	Tracks	Data Valid Mode (Pulling /Insertion)

Parameter Description:

Reading Method: 30H Read in ASCII coded mode（The default setting is ASCII coded mode）

31H Read in binary coded mode

Data Uploading Control: 30H Active data uploading method

（Need not to execute any other command to obtain magnetic card data）

31H Prohibit data active uploading (Data passive uploading)

(Need to execute other command to obtain magnetic card data)

Track 1: Maximum capability is 79 characters and each character is combined 7 bit, for example: b0,b1,b2,b3,b4,b5,P（Exclusive-or parity）

Track 2, Track 3: Maximum capability for track 2 is 40 characters，and for track 3 is 109 characters，each character is combined 5 bit，for example b0,b1,b2 b3,P (Exclusive-or parity）

Defined track number: 30H Read no track

31H Read track 1

32H Read track 2

33H Read track 3

34H Read track 1,2

35H Read track 1,3

36H Read track 2,3

37H Read track 1, 2, 3 (Default setting)

Data Valid Mode: 30H Data valid when inserting the card, when card pulling out of reader, the buffer will be clean

31H Data valid when pulling the card (Default Setting)，the data in the buffer will be clean by command or by inserting card

Positive return:

"P"	36H	30H	ST1	ST0

Negative return:

"N"	36H	30H	E1	E0

Notes: Once setting pulling the card valid, the card retention in reader for 1 second before pulling out is advised.

8.7.2 Read Magnetic Stripe Buffer

HOST Send

"C"	36H	31H	Reading Mode	Defined track number

Reading Mode: 30H ASCII Mode

31H Binary Mode

Defined track number: 30H Read no track

31H Read track 1

32H Read track 2

33H Read track 3

34H Read track 1, 2

35H Read track 1, 3

36H Read track 2, 3

37H Read track 1, 2, 3 (Default setting)

Positive Return:

"P"	36H	31H	ST1	ST0	Magnetic stripe card data（n byte）

Negative Return:

"N"	36H	31H	E1	E0	Magnetic stripe card data（n byte）

Reading Mode=30H ASCII Mode

=31H Binary Mode

ASCII Data Format

Track 1（IATA）: Maximum 79 Byte（6 bit Data +1bit CRC） Eg: b0,b1,b2,b3,b4, b5，P

Track 2（ABA）: Maximum 40 Byte（4 bit Data +1bit CRC） Eg: b0,b1,b2 b3，P

Track 3（MINTS）: Maximum 107 Byte（4 bit Data +1 bit CRC） Eg: b0,b1,b2 b3，P

Example:

ISO Track #1			ISO Track #2, #3		
bit	5 4 3 2 1 0	ASCII	bit	3 2 1 0	ASCII
data=0	0 1 0 0 0 0	30H	data=0	0 0 0 0	30H
data=A	1 0 0 0 0 1	41H	data=9	1 0 0 1	39H

Magnetic card data return format: ISO#1 + 7EH + ISO#2 + 7EH + ISO#3

ISO#N: Track Data (N=1,2,3)

Reading successful: “P” + Track Data（Excluded starting sentinel, ending sentinel and BCC bit）

Reading failure: “N2X” and “2X” is error code（“20”“23”“24”“26”“27”“28”）

Positive magnetic card data return:

Track Number =31H： "P" + ISO #1 data

Track Number =32H： "P" + ISO #2 data

Track Number =33H： "P" + ISO #3 data

Track Number =34H： "P" + ISO #1 data + 7EH + "P" + ISO #2 data

Track Number =35H： "P" + ISO #1 data + 7EH + "P" + ISO #3 data

Track Number =36H： "P" + ISO #2 data + 7EH + "P" + ISO #3 data

Track Number =37H： "P" + ISO #1 data + 7EH + "P" + ISO #2 data + 7EH + "P" + ISO #3 data

Reading failure:

E1,E0 is invariable "21"

E3,E2 is error code for ISO-1;

E5,E4 is error code for ISO-2

E7,E6 is error code for ISO-3

Track Number =31H： "N "+ E3,E2

Track Number =32H： "N" + E5,E4

Track Number =33H： "N" + E7,E6

Track Number =34H： "N "+ E3,E2 + 7EH + "N" + E5,E4

Track Number =35H： "N "+ E3,E2 + 7EH + "N" + E7,E6

Track Number =36H： "N "+ E5,E4 + 7EH + "N" + E7,E6

Track Number =37H： "N "+ E3,E2 + 7EH + "N" + E5,E4 + 7EH + "N" + E7,E6

E3\E2、E5\E4、E7\E6 Error Code Instruction:

E3\E2、E5\E4、E7\E6	CONTENTS
“20”	Exclusive-or parity error
“23”	Only have start sentinel, end sentinel and LRC bit
“24”	Blank Magnetic track
“26”	No start sentinel
“27”	No end sentinel
“28”	LRC error

Description:

1. E3\E2, E5\E4, E7\E6 is the error code for track 1, track 2, track 3 due to E1/E0 is “21”
2. If one track has an error, this track will return negative format and if one track has no error, this track will return positive format
3. The track number information is not contained in data

Binary Data format:

ISO#1 + 7EH + ISO#2 + 7EH + ISO#3

The binary data of magnetic card will transfer to ASCII code and upload it to HOST

The reader will ignore part of start/end sentinel 0 for there are too many sentinel 0

E.g. A track data: (HEX) = ‘0000 0000 0011 0111 1111 0000 0000 0011 0111 1111 0000 0000’

The uploading package ISO #N data(N=1,2,3)= 33H 37H 3FH 30H 30H 33H 37H 3FH

If there is no data on a track, this track will upload 0 byte package of ISO #N data (N=1,2,3) to HOST

Track Number =31H： ISO #1 data

Track Number =32H： ISO #2 data

Track Number =33H： ISO #3 data

Track Number =34H： ISO #1 data + 7EH + ISO #2 data

Track Number =35H： ISO #1 data + 7EH + ISO #3 data

Track Number =36H： ISO #2 data + 7EH + ISO #3 data

Track Number =37H： ISO #1 data + 7EH + ISO #2 data + 7EH + ISO #3 data

8.7.3 Active Data Uploading Method Setting

The data of magnetic stripe card will be automatically uploaded to HOST

Command Send:

“P”	36H	32H	ST1	ST0	ISO#1n byte + ISO#2 n byte + ISO#3 n byte

ASCII Data Format

Track 1（IATA）： Maximum 79 Byte（6 bit Data +1bit CRC） Eg: b0,b1,b2,b3,b4, b5，P

Track 2（ABA）： Maximum 40 Byte（4 bit Data +1bit CRC） Eg: b0,b1,b2 b3，P

Track 3（MINTS）： Maximum 107 Byte（4 bit Data +1 bit CRC） Eg: b0,b1,b2 b3，P

Example:

ISO Track #1			ISO Track #2, #3		
bit	5 4 3 2 1 0	ASCII	bit	3 2 1 0	ASCII
data=0	0 1 0 0 0 0	30H	data=0	0 0 0 0	30H
data=A	1 0 0 0 0 1	41H	data=9	1 0 0 1	39H

Magnetic card data return format: ISO#1 + 7EH + ISO#2 + 7EH + ISO#3

ISO#N: Track Data (N=1,2,3)

Reading successful: “P” + Track Data（Excluded starting sentinel, ending sentinel and BCC bit）

Reading failure: “N2X” and “2X” is error code（“20”“23”“24”“26”“27”“28”）

Positive magnetic card data return:

Track Number =31H： "P" + ISO #1 data

Track Number =32H： "P" + ISO #2 data

Track Number =33H： "P" + ISO #3 data

Track Number =34H： "P" + ISO #1 data + 7EH + "P" + ISO #2 data

Track Number =35H： "P" + ISO #1 data + 7EH + "P" + ISO #3 data

Track Number =36H： "P" + ISO #2 data + 7EH + "P" + ISO #3 data

Track Number =37H： "P" + ISO #1 data + 7EH + "P" + ISO #2 data + 7EH + "P" + ISO #3 data

Reading failure:

E1,E0 is invariable "21"

E3,E2 is error code for ISO-1;

E5,E4 is error code for ISO-2

E7,E6 is error code for ISO-3

Track Number =31H： "N "+ E3,E2

Track Number =32H： "N" + E5,E4

Track Number =33H： "N" + E7,E6

Track Number =34H： "N "+ E3,E2 + 7EH + "N" + E5,E4

Track Number =35H： "N "+ E3,E2 + 7EH + "N" + E7,E6

Track Number =36H： "N "+ E5,E4 + 7EH + "N" + E7,E6

Track Number =37H： "N "+ E3,E2 + 7EH + "N" + E5,E4 + 7EH + "N" + E7,E6

E3\E2、E5\E4、E7\E6 Error Code Instruction:

E3\E2、E5\E4、E7\E6	CONTENTS
“20”	Exclusive-or parity error
“23”	Only have start sentinel, end sentinel and LRC bit
“24”	Blank Magnetic track
“26”	No start sentinel
“27”	No end sentinel
“28”	LRC error

Description:

1. E3\E2, E5\E4, E7\E6 is the error code for track 1, track 2, track 3 due to E1/E0 is 21
2. If one track has an error, this track will return negative format and if one track has no error, this track will return positive format
3. The track number information is not contained in data

Binary Data format:

ISO#1 + 7EH + ISO#2 + 7EH + ISO#3

The binary data of magnetic card will transfer to ASCII code and upload it to HOST

The reader will ignore part of start/end sentinel 0 for there are too many sentinel 0

E.g. ISO#N = ‘0000 0000 0011 0111 1111 0000 0000 0011 0111 1111 0000 0000’

The uploading package ISO #N data(N=1,2,3)= 33H 37H 3FH 30H 30H 33H 37H 3FH

If there is no data on a track, this track will upload 0 byte package of ISO #N data (N=1,2,3) to HOST

Track Number =31H： ISO #1 data

Track Number =32H： ISO #2 data

Track Number =33H： ISO #3 data

Track Number =34H： ISO #1 data + 7EH + ISO #2 data

Track Number =35H： ISO #1 data + 7EH + ISO #3 data

Track Number =36H： ISO #2 data + 7EH + ISO #3 data

Track Number =37H： ISO #1 data + 7EH + ISO #2 data + 7EH + ISO #3 data

8.7.4 Clear Magnetic Stripe Card Buffer

HOST Send：

"C"	36H	39H

Positive Return:

"P"	36H	39H	ST1	ST0

Negative Return:

"N"	36H	39H	E1	E0

8.8 CPU Card Operation

8.8.1 CPU Card Reset (Initialization)

Command

“C”	51H	30H	Vcc

Positive response

“P”	51H	30H	ST1	ST0	Type	ATR

Negative response

“N”	51H	30H	E1	E0	Type	ATR

To reset IC card. The CRT-288-k supplies power (VCC) , clock (CLK), and Reset (RST) return ATR.

Vcc=30H: Supply +5V to CPU card and be initialized (active) in line with the EMV.

Vcc=33H: Supply +5V to CPU card and be initialized (active) in line with the ISO7816.

Vcc=35H: Supply +3V to CPU card and be initialized (active) in line with the ISO7816.

Vcc is optional parameter and If there is no Vcc in command, default Vcc=30H

If ATR is not compliant to EMV, return E1, E0=“69”

If IC card power is detected as error, return E0, E1=“60”

Type: CPU Card protocol Type

=30H T=0 protocol CPU Card

=31H T=1 protocol CPU Card

ATR Format:

TS	TO	TA1	TB1	…	TCK

8.8.2 Deactivate CPU Card

Command

“C”	51H	31H

Positive response

“P”	51H	31H	ST1	ST0

Negative response

“N”	51H	31H	E1	E0

This deactivates CPU card.

This command is to deactivate activated CPU card.

8.8.3 Inquire CPU Card Status

Command

“C”	51H	32H

Positive response

“P”	51H	32H	ST1	ST0	Sti

Negative response

“N”	51H	32H	E1	E0

The machine tells the status of IC card with sti.

Sti =30H Card not activated

=31H Card has activated, current CPU Card working frequency is 3.57 MHZ

=32H Card has activated, current CPU Card working frequency is 7.16 MHZ

If IC card power supply error, return E1,E0=“60”.

8.8.4 CPU Card APDU Operation T=0 Protocol

Command

"C"	51H	33H	C-APDU

Positive response

"P"	51H	33H	St1	St0	R-APDU

Negative response

"N"	51H	33H	E1	E0

This command specifies exchanges data in T=0 CPU card which has been successfully initialized

C-APDU from HOST ranges from 4 byte to 261 byte

CLA	INS	P1	P2	LC	Data1	……	Le

R-APDU to HOST ranges from 2 byte to 258 byte

Data1	…..	Data(n)	Sw1	Sw0

An E0, E1= "60" is returned when a power supply failure for IC card is detected.

If protocol type of IC card is not T=0. Error code E0, E1= "62" is sent.

If CPU card is out of Working Wait Time, CRT-288-K001 will deactivate IC card and E0, E1 ="63" is sent.

If any other protocol error occurs on CPU card, CRT-288-K001 will deactivate IC card and E0, E1= "64" is sent.

If HOST operates CPU card before CPU card activation (Reset), E0, E1= "65" is sent.

Note: Please refer to ISO/IEC7816-3 about T=0 APDU format, and specific C-APDU command, please refer to the COS command for the card

8.8.5 CPU Card APDU Operation T=1 Protocol

Command

"C"	51H	34H	C-APDU

Positive response

"P"	51H	34H	ST1	ST0	R-APDU

Negative response

"N"	51H	34H	E1	E0

This command specifies exchanges data in T=1 CPU card which is successfully initialized

CRT-288-K001 should follow T=1 protocol to combine C-APDU as I-block and send it to CPU card. CPU card should return R-APDU（extracted from I-block）to HOST.

A: Send C-APDU (Add block head, block end and C-APDU as I-block)

C-APDU

CLA	INS	P1	P2	Lc	Data1	…	Data(Lc)	Le

↓

I-block

NAD	PCB	LEN	CLA	INS	P1	P2	Lc	Data1	…	Data(Lc)	Le	EDC
Head block			Information block									End block

B: Receive R-APDU (extracted R-ADPU from I-block)

I-block

Head block			Information block									End block
NAD	PCB	LEN	CLA	INS	P1	P2	Lc	Data1	…	Data(Lc)	Le	EDC

↓

R-APDU

CLA	INS	P1	P2	Lc	Data1	…	Data(Lc)	Le

An E0, E1= "60" is returned when a CPU card power supply failure is detected.

If protocol type of CPU card is not T=0, E0, E1= "62"is sent.

If CPU card does not respond within Working Wait Time, CRT-288-K001 will deactivate CPU card and E0, E1= "63" is sent.

If any other protocol error occurs, CRT-288-K001 will deactivate CPU card and E0, E1= "64" is sent.

If HOST communicate before CPU card activation (Reset), E0, E1= "65" is sent.

Note: If you want to know more about T=0 APDU format. Please refer to ISO/IEC7816-3 and COS command of CPU card

8.8.6 CPU Warm Reset

Command

“C”	51H	38H

Positive response

“P”	51H	38H	ST1	ST0	Type	ATR

Negative response

“N”	51H	38H	E1	E0

Keeping the status of the CPU card contact activated, and then returns response upon receiving “ATR” again.

Type: CPU Card communication protocol

=30H T=0 Protocol

=31H T=1 Protocol

8.8.7 Auto Select T=0/T=1 Protocol of CPU Card APDU Operation

Command

“C”	51H	39H	C-APDU

Positive response

“P”	51H	39H	ST1	ST0	R-APDU

Negative response

“N”	51H	39H	E1	E0

Protocol is recognized automatically. CRT-288-K001 will automatically select protocol.

E0, E1= “60” is returned when a CPU card power supply failure is detected.

If protocol type of CPU card is not T=0/T=1, E0, E1= “62”is sent.

If CPU card does not respond within Working Wait Time, CRT-288-K001 will deactivate CPU card and E0, E1= “63” is sent.

If any other protocol error occurs, CRT-288-K001 will deactivate a CPU card and E0, E1= “64” is sent.

If HOST communicate before a CPU card activation (Reset), E0, E1= “65” is sent.

8.9 SAM Card Operation

8.9.1 SAM Card Reset(Initialization)

Command

“C”	52H	30H	Vcc

Positive response

“P”	52H	30H	ST1	ST0	Type	ATR

Negative response

“N”	52H	30H	E1	E0	Type	ATR

The CRT-288-K001 supplies power (VCC) and clock (CLK), and then reset (RST) release.

Type: SAM protocol type

=30H T=0 protocol

=31H T=1 protocol

ATR (Answer to Reset) format:

TS	TO	TA1	TB1	…	TCK

Vcc=30H: CRT-288-K001 supplies SAM card with +5V to VCC and activates in line with the EMV.

Vcc=33H: CRT-288-k supplies SAM card with +5V to VCC and activates in line with the ISO7816.

Vcc=35H: CRT-288-k supplies SAM card with +3V to VCC and activates in line with the ISO7816.

Vcc is optional parameter. In case there is no Vcc parameter, Vcc=30H

If ATR of SAM is not compliance to EMV, return E1,E0= “69”

If IC card power is failure, return E1, E0= “ 60”

8.9.2 Deactivate SAM Command

Command

“C”	52H	31H	

Positive response

“P”	52H	31H	ST1	ST0

Negative response

“N”	52H	31H	E1	E0

This command deactivates SAM card

8.9.3 Inquire SAM Status Command

Command

“C”	52H	32H

Positive response

“P”	52H	32H	ST1	ST0	Sti	Stj

Negative response

“N”	52H	32H	E1	E0

Inquire SAM status and CRT-288-k returns the status of SAM with sti. stj

Sti =30H SAM is deactivated

Sti =31H SAM is activated, working frequency is 3.57 MHZ

Sti =32H SAM is activated, working frequency is 7.16 MHZ

Stj =30H No.1 SAM card stand

Stj =31H No.2 SAM card stand (Optional)

Stj =32H No.3 SAM card stand (Optional)

Stj =33H No.4 SAM card stand (Optional)

E0, E1=“60” is returned when a power supply failure of SAM card is detected.

8.9.4 SAM T=0 Communication APDU Operation

Command

“C”	52H	33H	C-APDU

Positive response

“P”	52H	33H	ST1	ST0	R-APDU

Negative response

“N”	52H	33H	E1	E0

This command is for exchanging data in SAM by protocol T=0

If power supply of SAM card is failure, E0, E1= “60” is return.

If protocol type of SAM card is not T=0, E0, E1= “62”is return.

If SAM card does not respond within Working Wait Time, CRT-288-k will deactivate SAM card and E0, E1= “63” is sent.

If any other protocol error occurs, CRT-288-k will deactivate SAM card and E0, E1= “64” is sent.

If HOST communicate before SAM card activation (Reset), E0, E1= “65” is sent.

Note: Please refer to ISO/IEC7816-3 about T=0 APDU format and for specific C-APDU command, please refer to the COS of the SAM card

8.9.5 SAM T=1 Communication APDU Operation

Command

"C"	52H	34H	C-APDU

Positive response

"P"	52H	34H	ST1	ST0	R-APDU

Negative response

"N"	52H	44H	E1	E0

This command is for exchanging data in SAM card by protocol T=1

If power supply of SAM card is failure, E0, E1= "60" is return.

If protocol type of SAM card is not T=1, E0, E1= "62"is return.

If SAM card is out of Working Wait Time, CRT-288-K001 will deactivate SAM card and E0, E1= "63" is sent.

If any other protocol error occurs, CRT-288-K001 will deactivate SAM card and E0, E1= "64" is sent.

If HOST communicate before SAM card activation (Reset), E0, E1= "65" is sent.

Note: Please refer to ISO/IEC7816-3 about T=0 APDU format and for specific C-APDU command please refer to the COS of the card.

8.9.6 SAM Warm Reset

Command

"C"	52H	38H

Positive response

"P"	52H	38H	ST1	ST0	Type	ATR

Negative response

"N"	52H	38H	E1	E0

Keeping the status of the SAM activated, and then returns ATR response.

Type: SAM protocol type

=30H T=0 Protocol

=31H T=1 Protocol

8.9.7 Auto-Select SAM Card T=0/T=1 Protocol

Command

“C”	52H	39H	C-APDU

Positive response

“P”	52H	39H	ST1	ST0	R-APDU

Negative response

“N”	52H	39H	E1	E0

Automatically choose corresponding C-APDU operation according to T=0/T=1 protocol of SAM and return R-APDU.

If power supply of SAM card is failure, E0, E1= “60” is return.

If protocol type of SAM card is not T=0/T=1, E0, E1= “62” is return.

If SAM card is out of Working Wait Time, CRT-288-K001 will deactivate SAM card and E0, E1= “63” is sent.

If any other protocol error occurs, CRT-288-K001 will deactivate SAM card and E0, E1= “64” is sent.

If HOST communicate before SAM card activation (Reset), E0, E1= “65” is sent.

8.9.8 Select SAM

Command

“C”	52H	40H	SAMn

Positive response

“P”	52H	40H	St1	St0

Negative response

“N”	52H	40H	E1	E0

This command is to select SAM stand.

SAMn = 30H: SAM 1.

SAMn = 31H: SAM 2.

SAMn = 32H: SAM 3.

SAMn = 33H: SAM 4.

This SAM select command is only available for reader with PSAM board. (This command is only for one SAM stand)

8.10 SLE4442/4428 Card Operation

8.10.1 SLE4442/4428 Card Reset（Initialization）

Command

“C”	53H	30H

Positive response

“P”	53H	30H	ST1	ST0	ATR (4 byte)

Negative response

“N”	53H	30H	E1	E0

The CRT-288-K001 supplies power (VCC) and clock (CLK), and then reset (RST) release. After reset, return ATR.

ATR: SLE4442 Card ATR=“A2H，13H，10H，91H”

SLE4442 Card ATR=“92H，23H，10H，91H”

8.10.2 Deactivate SLE4442/4428

Command

“C”	53H	31H

Positive response

“P”	53H	31H	St1	St0

Negative response

“N”	53H	31H	E1	E0

The CRT-288-K001 stop supplying power (VCC) and clock (CLK) then reset (RST) release.

8.10.3 Inquire Status of SLE4442/4428

Command

“C”	53H	32H

Positive response

“P”	53H	32H	St1	St0	Sti

Negative response

“N”	53H	32H	E1	E0

CRT-288-K001 returns the status of SLE4442/4428 with Sti after the command successfully execute.

Sti= 30H SLE4442/4428 Deactivated

Sti= 31H SLE4442 Activated

Sti= 32H SLE4428 Activated

8.10.4 SLE4442 Card Operation

These functions are specified by a command data form like C-APDU which format is based on T=0 standard. Please see the following:

"C"	CM	PM	CLA	INS	P1	P2	……

After the command was executed properly, CRT-288-K001 returns a positive response with response data 9000H. When an error occurs during the communication with SLE4442, CRT-288-K001 returns a positive response with status information in response data "sw1+sw2" which is based on ISO/IEC 7816-3

Sw1	Sw2	Description
90H	00H	Operation Success
6FH	00H	Operation Failure
6FH	01H	Key Validation error
6FH	02H	Key Validation error and dead lock
67H	00H	Address overflow
6BH	00H	Operation length overflow
6DH	00H	INS Error
6EH	00H	CLA Error

8.10.4.1 Data Read From Main Memory on SLE4442

Command

"C"	53H	33H	00H	B0H	00H	abH	cdH

Positive response

"P"	53H	33H	ST1	ST0	data

Negative response

"N"	53H	33H	E1	E0

Notes: ab H: the start address of data that needs to read in the main memory
cd H: the length of bytes that needs to read

CRT-288-K001 reads data from the main memory of SLE4442, and transmits data on cdH bytes from the address abH.

The capacity of the main memory is 256 bytes.

All the contents of the main memory can be read with the following command.

Ex). "CS3"+00B0000000

8.10.4.2 Read Protection Bits on SLE4442

Command

“C”	53H	33H	00H	B0H	01H	abH	cdH

Positive response

“P”	53H	33H	ST1	ST0	Data(n byte)

Negative response

“N”	53H	33H	E1	E0

Notes: ab H: the start address of protection bit

cd H : the length of data to read

32 protection bit status is indicated by 4 bytes data. Protection bit address is 00H-1FH

The contents (4 byte) of the protection memory can be read with the following command.

Ex). "CS3"+00B0010004

8.10.4.3 Data Read From Security Memory on SLE4442

Command

“C”	53H	33H	00H	B0H	02H	abH	cdH	efH…

Positive response

“P”	53H	33H	ST1	ST0	data

Negative response

“N”	53H	33H	E1	E0

Notes: ab H: the start address of security area.

cd H : the length of security data to read

SLE4442 has 4 byte of security data

CRT-288-K001 handles the 4 byte.

1 of 4byte is data of error counter + 3 of 4 byte are key data.

The all contents (4 byte) of the security memory can be read with the following command.

Ex). "CS3"+00B0020004

8.10.4.4 Data Write to Main Memory on SLE4442

Command

“C”	53H	33H	00H	D0H	00H	abH	cdH	efH…

Positive response

“P”	53H	33H	ST1	ST0	data

Negative response

“N”	53H	33H	E1	E0

Notes: ab H: the start address to write data in the main memory

cd H: the length of bytes to write

ef H: the data to write first (cd H bytes)

Write data to main memory on SLE4442 and return result.

Before write to main memory, the validation of key is must.

The capacity of the main memory is 256 bytes. When cd=00H, the whole 256byte can be written.

The example that data is written in the whole area of the main memory is shown in the following.

Ex). "CS3"+ 00D0000000 + Write Data (256byte)

After the command execution, the reader will return 9000H (Successful) or SW1&SW2 (Failure)

The data can not be written into bit protection block.

8.10.4.5 Data Write with Protection Bit on SLE4442

Command

“C”	53H	33H	00H	D0H	01H	abH	cdH	efH…

Positive response

“P”	53H	33H	ST1	ST0	data

Negative response

“N”	53H	33H	E1	E0

Notes: ab H: the start address to write data in the main memory

cd H: the length of bytes to write

ef H: the data to write first (cd H bytes)

Before write to the memory, the validation of key is must.

The address of the protection memory is 00-1FH.The data of 00H-1FH is controlled by 32 bit of protection status bit. For example, if bit0=1 in byteE0, data on the address 00H on the main memory is protected.

The content of protect status can not be changed once setting protection.

For example: write 20H data to 10H address and set up protection

Ex). “CS3”+00D001100120

After command execution, CRT-288-K001 returns with 9000H (Successful) or sw1+sw2 (Failure) as the result.

CRT-288-K001 reads data first from the protection block, and it is compared with the value that it was received. When they are different, writing operation isn’t executed.

Protection condition can be set only one time in the main memory.

8.10.4.6 Data write to security memory on SLE4442 (Modify password)

Command

“C”	53H	33H	00H	D0H	02H	abH	cdH	efH…

Positive response

“P”	53H	33H	ST1	ST0	data

Negative response

“N”	53H	33H	E1	E0

Notes: ab H : the start address to write data in the main memory
cd H: the length of bytes to write
ef H : the data to write first (cd H bytes)

After a password check is finished normally, 3byte of password in security memory can be changed.
Change the password though command and the example is shown as following.
(Change password as 123456H)
Ex). "CS3"+ 00D0020103123456
After command execution, CRT-288-k returns response with 9000H (Successful) or sw1+sw2 (Fail) in the result.
Notes: Better not to write error counter for the key, because the Error-counter is always allowed to write and easily make a mistake. Error-Counter is controlled when password is checked.

8.10.4.7 Verification key of SLE4442

Command

“C”	53H	33H	00H	20H	03H	01H	03H	efH…

Positive response

“P”	53H	33H	ST1	ST0	data

Negative response

“N”	53H	33H	E1	E0

Notes: ef H: Key data (3 bytes)

Before changing data, password must be checked

Because this command is necessary for execute next command.

Ex). “CS3”+0020030103xxxxxx (xxxx: security code 3bytes)

Reader will verify password between card and password in the command.

Password must be known at least when a user wants to rewrite the data on SLE4442 card. If the password is given to wrong, the counter will reduce from 2 or less to 0 and when the error- counter reduce to 0, the card is scraped.

8.10.5 SLE4428 Card Operation

These functions are specified by a command data form like C-APDU which format is based on ISO/IEC 7816 T=0 standard.

Please see the following:

"C"	CM	PM	CLA	INS	P1	P2	……

After the command was executed properly, CRT-288-K001 returns a positive response with response data 9000H. When an error occurs during the communication with SLE4448, CRT-288-K001 returns a positive response with status information in response data "sw1+sw2" which is based on ISO/IEC 7816-3

Sw1	Sw2	Description
90H	00H	Operation Success
6FH	00H	Operation Failure
6FH	01H	Key Validation error
6FH	02H	Key Validation error and dead lock
6BH	00H	Address overflow
67H	00H	Operation length overflow
6DH	00H	PM Error
6EH	00H	CM Error

8.10.5.1 Data Reading of Main-Memory of SLE4428

Command

"C"	53H	34H	00H	B0H	0aH	bcH	deH

Positive response

"P"	53H	34H	ST1	ST0	data

Negative response

"N"	53H	34H	E1	E0

Notes: abc H: the start address to be read data in the main memory

de H: the number of bytes to be read

CRT-288-K001 read data from main memory of SLE4428 through abcH and deH

The capacity of the main memory is 1024bytes.

If De="00" Read 256byte data.

The data of SLE4428 can be read with the following command.

ex). "CS3"+00B0000000

8.10.5.2 Reading of protection-bit of SLE4428

Command

“C”	53H	34H	00H	B0H	10H	abH	cdH

Positive response

“P”	53H	34H	ST1	ST0	data

Negative response

“N”	53H	34H	E1	E0

Notes: ab H : the start address (0000H-007FH)

cd H : the length of data to read (01H-80H)

SLE4428 has 1024byte in main memory and correspondingly 1024 protection bit. The reader will handle 8 bit as byte. Every protection bit present corresponding protects status for each byte on SLE4428.

Bit=0 have already protect, can not write anything

Bit=1 not yet protect, data writing is available

The protection bit is start from 000H – 007H, and combined as 1 byte protection data.

The command to read all protection bit of SLE4428

Ex). "CS4"+00B0100080

The abH specifies the starting address of reading and cdH the length of reading

8.10.5.3 Data Writing to Main-Memory of SLE4428

Command

“C”	53H	34H	00H	D0H	0aH	bcH	deH	fgH…

Positive response

“P”	53H	34H	ST1	ST0	data

Negative response

“N”	53H	34H	E1	E0

Notes: abc H: the start address to write data in the main memory

de H : the number of bytes to write

fg H : the data to write first (de H bytes)

Write data in the main memory and return a result after written data are checked.

Before doing this operation, password check must be done

The capacity of the main memory is 1024 bytes.

The example command that 256 byte of main memory data is written

Ex). "CS4"+ 00D0000000 + Write Data (256byte)

After command execution, CRT-288-K001 returns response with 9000H or sw1+sw2 as the result.

If the addressed data on main memory is in protected status, the write operation is not available.

Notes: Last three units (abc=0x03FD, 0x03FE, 0x03FF) of SLE=4428 is password verification error counter for password1 and password2. Please don’t write any data to these units, otherwise the card will be easily scraped.

8.10.5.4 Written with protection-bit

Command

“C”	53H	34H	00H	D0H	2aH	bcH	deH	fgH…

Positive response

“P”	53H	34H	ST1	ST0	data

Negative response

“N”	53H	34H	E1	E0

Notes: abc H: the start address to write data in the main memory
de H: the number of bytes to write
fg H: the data to write first (de H bytes)

Before doing this operation that writing data with protection-bit, password check must be done

After command execution, CRT-288-K001 returns response with 9000H (Successful) or sw1+sw2 (Fail) as the result.

CRT-288-K001 reads data first from the main memory, and it is compared with the data that it was received.

When comparison is wrong, writing operation isn't executed. The protection only available when the data of written and data in the card is the same.

8.10.5.5 Verification of Password present to SLE4428

Command

“C”	53H	34H	00H	20H	00H	00H	02H	efH…

Positive response

“P”	53H	34H	ST1	ST0	data

Negative response

“N”	53H	34H	E1	E0

Notes: ef H: key data (2bytes)

Before changing data, Password must be checked properly with SLE4428.

The command is necessary for issuance of next command.

Ex). "CR3"+ 0020000002xxxx (xxxx: security code 2bytes)

The presented data are compared with internal data in SLE4428 card itself.

User should know the password of card if they want to modify data in SLE4442, Error-Counter can be reduce from 7 or less to 0. When error-counter reduces to zero, the card will lock and scrap.

8.11 I² C Memory Card Operation

8. 11. 1 Activate I² C memory card

Command

"C"	54H	30H	Wrd	Vcc

Positive response

"P"	54H	30H	ST1	ST0	Sti

Negative response

"N"	54H	30H	E1	E0

To activate I² C (24C01, 24C02, 24C04, 24C08, 24C16, 24C32, 24C64, 24C128, 24C256) card

CRT-288-K001 supplies a power supply (Vcc), Clock (CLK), Reset (RST) and return card type

Including:

Wrd set I² C type

Wrd =30 H To activate(24C01,24C02,24C04,24C08,24C16,24C32,24C64,24C128,24C256) card

Vcc choose voltage to card

Vcc=30H 5V

Vcc=31H 3V

Sti return I² C card type when operate successfully

Sti =31 H To activate 24C01card

Sti =32 H To activate 24C02 card

Sti =33 H To activate 24C04 card

Sti =34 H To activate 24C08 card

Sti =35 H To activate 24C16 card

Sti =36 H To activate 24C32 card

Sti =37 H To activate 24C64 card

Sti =38 H To activate 24C128 card

Sti =39 H To activate 24C256 card

Vcc is optional parameter, without setting parameter in command is equal to Set=30H

8.11.2 Deactivate I^2C memory card

Command

"C"	54H	31H

Positive response

"P"	54H	31H	ST1	ST0

Negative response

"N"	54H	31H	E1	E0

CRT-288-K001 halts supplying a power supply (Vcc), Clock (CLK), Reset (RST).

8.11.3 Inquire Status of I^2C Memory Card

Command

"C"	54H	32H

Positive response

"P"	54H	32H	ST1	ST0	Sti

Negative response

"N"	54H	32H	E1	E0

This command is used to inquire status of I^2C card and return status by Sti.

Sti Description:

Sti=30 H No I^2C be activated
Sti=31 H Activated 24C01
Sti=32 H Activated 24C02
Sti=33 H Activated 24C04
Sti=34 H Activated 24C08
Sti=35 H Activated 24C16
Sti=36 H Activated 24C32
Sti=37 H Activated 24C64
Sti=38 H Activated 24C128
Sti=39 H Activated 24C256

8.11.4 I² C Card Operation

These functions are specified by a command data form like C-APDU which format is based on ISO/IEC 7816 T=0 standard.

"C"	CM	PM	CLA	INS	P1	P2	……

In this case, CRT-288-K001 recognizes the meaning of the command data, and executes the treatment related to the card by controlling hardware.

After the command was executed properly, CRT-288-K001 returns a positive response 9000H like from the IC card. When an error occurs during the communication with I2C, CRT-288-K001 returns a positive response with status information "sw1+sw2" which is based on ISO/IEC 7816-3 T=0

Sw1	Sw2	Specification
90H	00H	Success
6FH	00H	Fail
6FH	01H	Password verification fail
6FH	02H	Password verification fail, card locked
6BH	00H	Address overflow
67H	00H	Operation length overflow
6DH	00H	PM error
6EH	00H	CM error

Write/Read I² C and Address scope is showed below:

Card_type	ab,cd
24C01	0000H ~ 007FH
24C02	0000H ~ 00FFH
24C04	0000H ~ 01FFH
24C08	0000H ~ 03FFH
24C16	0000H ~ 07FFH
24C32	0000H ~ 0FFFH
24C64	0000H ~ 1FFFH
24C128	0000H ~ 3FFFH
24C256	0000H ~ 7FFFH

8.11.4.1 Read data from I² C

Command

"C"	54H	33H	00H	B0H	abH	cdH	efH

Positive response

"P"	54H	33H	ST1	ST0	Data

Negative response

"N"	54H	33H	E1	E0

Value:

ab H : The upper address of head address which begins to read data

cd H : The lower address of head address which begins to read data

ef H : The number of bytes to read

Data: Data to read

CRT-288-K001 reads efH length and returns to HOST according to address specified by abH, cdH. The length of efH can not surpass the length of I² C address up-limit.

When the following command is transmitted, data can be read from the I²C memory card.

Ex). "CT3"+00B0000008

8.11.4.2 Write data to I² C

Command

"C"	54H	34H	00H	D0H	abH	cdH	efH	Data…

Positive response

"P"	54H	34H	ST1	ST0	Data

Negative response

"N"	54H	34H	E1	E0

This command is recognized as follows.

ab H : The upper address of head address which begins to write data

cd H : The lower address of head address which begins to write data

ef H : The number of bytes of data to write

Data: Data to write (Length is efH byte) and return SW1 and SW2

CRT-288-K001 read efH length and return to HOST according to address specified by abH, cdH. The Length of efH can not be surpassing the length of I² C address up limit.

The example which data on 8bytes are written into I² C

ex). "CT3"+ 00D0000008 + Write Data (8bytes)

After command execution, CRT-288-K001 returns response with 9000H or sw1+sw2 as the result.

8.12 Contactless IC Card Operation

8.12.1 Activated Contactless IC Card

Command

"C"	60H	30H	Set1	Set2

(1) Mifare One Card Positive Response

"P"	60H	30H	st0	st1	Rtype	ATQA	UID_len	UID_data	SAK

Mifare One Card Negative Response

"N"	60H	30H	E1	E0	Rtype	ATQA	UID_len	UID_data	SAK

(2) 14443 Type A Card Positive Response

"P"	60H	30H	st0	st1	Rtype	ATQA	UID_len	UID_data	SAK	ATS

14443 Type A Card Negative Response

"N"	60H	30H	E0	E1	Rtype	ATQA	UID_len	UID_data	SAK	ATS

(3) 14443 Type B Card Positive Response

"P"	60H	30H	st0	st1	Rtype	ATQB

14443 Type b Card Negative Response

"N"	60H	30H	E0	E1	Rtype	ATQB

Activate RFID card

CRT-288-K001 support activated IEC/ISO14443 Type A and IEC/ISO 14443 Type B

The process is show as below:

1).Mifare one card:

1. Request A (REQ A) / Answer Request A (ATQ A).
2. Anti-collision
3. Select (SEL) / Unique Identifier (UID) & Select Acknowledge (SAK)

When Mifare card successfully activates, CRT-288-K001 returns:

ATQA(2 byte), UID_data (4—10 byte) and SAK(1 byte).

2).ISO/IEC 14443 Type A:

1. Request A(REQ A) / Answer Request A (ATQ A).
2. Anti-collision
3. Select (SEL) / Unique Identifier (UID) & Select Acknowledge (SAK)

4. Request for answer to select (RATS) / Answer to Select (ATS)

8.┌.┐ Protocol and parameter selection request (PPSR) / PPS start (PPSS)

When ISO/IEC 14443 Type A card successfully activated, CRT-288-K001 return:

Mifare card return value increase (ATS (1-254 byte) and protocol parameter (1 byte))

3).ISO/IEC 14443 Type B: 1. Request B(REQ B) / Answer Request B (ATQ B).

2. Attribute (A TTRIB) / Answer to ATTRIB

When ISO/IEC 14443 Type B card successfully activated, CRT-288-K001 return ATQB 12 byte (including following information):

50H, PUPI (4 byte), App. Data (4 byte), Protocol info (3 byte)

Notes:

Set1, Set2 set sequence of operation for different type of protocol

Valid value: 41H (‘A’= Type A)，42H(‘B’= Type B), 30H(‘0’= Do not use)

Ex1：Set1=‘A’，Set2 =‘B’ (default)

Activate sequence： Type A protocol (first sequence), Type B protocol (second sequence)

Ex2：Set1=‘B’，Set2 =‘A’

Activate sequence： Type B protocol (first sequence), Type A protocol (second sequence)

Ex3：Set1=‘A’，Set2 =‘0’

Activate sequence： Type A protocol (first sequence), Type B protocol (Deactivated)

Ex4：Set1=‘B’，Set2 =‘0’,

Activate sequence： Type B protocol (first sequence), Type A protocol (Deactivated)

Rtype: Protocol

= 41H (‘A’) In line with ISO/IEC 14443 Type A protocol

= 42H (‘B’) In line with ISO/IEC 14443 Type B protocol

= 4DH (‘M’) In line with Philips Mifare one card protocol

When Rtype=4DH (‘M’)

ATQA= 0044H Mifare Ultralight Card

ATQA= 0004H Mifare S50 1K Card

ATQA= 0002H Mifare S70 4K Card

Mifare one, ISO/IEC 14443 Type A return UID (The length of UID_data)

UID_len=4 the length of UID_data is 4 byte

UID_len=7 the length of UID_data is 7 byte

UID_len=10 the length of UID_data is10 byte

8.12.2 Deactivate RF Card

Command

“C”	60H	31H

Positive response

“P”	60H	31H	ST1	ST0

Negative response

“N”	60H	31H	E1	E0

Deactivate RF card and Output signal to antenna is closed.

8.12.3 Inquire Status of RF Card

Command

“C”	60H	32H

Positive response

“P”	60H	32H	ST1	ST0	sti	stj

Negative response

“N”	60H	32H	E1	E0

Inquire status of RFID sti,stj：

sti	stj	Specification
‘0’	‘0’	Deactivated RF
‘1’	‘0’	Mifare one S50 card
	‘1’	Mifare one S70 card
	‘2’	Mifare one UL card
‘2’	‘0’	Type A CPU card
‘3’	‘0’	Type B CPU card

8.12.4 Mifare Card Operation

These functions are specified by a command data form like C-APDU which format is based on T=0 standard.

"C"	CM	PM	CLA	INS	P1	P2	……

In this case, CRT-288-K001 recognizes the meaning of the command data, and executes the treatment related to the card by controlling hardware.

After the command was executed properly, CRT-288-K001 returns a positive response with response data 9000H like from the IC card. When an error occurs during the communication with Mifare 1 card CRT-288-K001 returns a positive response with status information in response data "sw1+sw2" which is base on ISO/IEC 7816-3.

Sw1	Sw2	Specification
90H	00H	Success
6FH	00H	Fail
6FH	01H	Key Verification Error
6FH	02H	Key Verification Error, Card Locked
6BH	00H	Address overflow
67H	00H	Operation length overflow

8.12.4.1 Key Verification

Command

"C"	60H	33H	00H	20H	ks	sn	lc	pdata

Positive response

"P"	60H	33H	ST1	ST0	rdata

Negative response

"N"	60H	33H	E1	E0

Download key to CRT-288-K001 and verify the key directly

ks(1byte): key select (Key A=00H，Key B=01H)

sn(1byte): sector number (S50 card sn=00H-0FH, S70 card sn=00H-27H)

lc(1byte): password length lc=06H

pdata(6 byte): password data

rdata(2 byte): return data(positive response with data 9000H, and negative response with " sw1+sw2")

8.12.4.2 Verify Key From EEPROM

Command

"C"	60H	33H	00H	21H	ks	sn

Positive response

"P"	60H	33H	ST1	ST0	rdata

Negative response

"N"	60H	33H	E1	E0

Read key from EEPROM of RFID module and verify the sector key

Download key via command mentioned in 8.11.4.4

EEPROM can preserve 32 groups of key data

ks(1byte): key type select (Key A=00H，Key B=01H)

sn(1byte): sector number (sn=00H-0FH)

rdata(2 byte): return data (positive response with 9000H)

8.12.4.3 Modify Sector Key (KEY A)

Command

"C"	60H	33H	00H	D5H	00H	sn	lc	pdata

Positive response

"P"	60H	33H	ST1	ST0	rdata

Negative response

"N"	60H	33H	E1	E0

Modify sector key (key A)

This command only can modify KEY A, and modify KEY B as "0xFF, 0xFF, 0xFF,0xFF,0xFF,0xFF" in the mean time modify control words as"0xFF, 0x07, 0x80, 0x69" (ex-work default)

Use block command to modify Key A, Key B control word

sn(1byte): sector number (S50 card sn=00H-0FH, S70 card sn=00H-27H)

lc(1byte): password length lc=06H

pdata: password data 6 byte.

rdata(2 byte): return data

(Positive response with data 9000H, and negative response with " sw1+sw2")

8.12.4.4 Download Password to EEPROM

Command

“C”	60H	33H	00H	D0H	ks	sn	lc	pdata

Positive response

“P”	60H	33H	ST1	ST0	rdata

Negative response

“N”	60H	33H	E1	E0

Read key from EEPROM of RFID module and verify the sector key

EEPROM can preserve 32 groups of key data

ks(1byte): key select (Key A=00H， Key B=01H)

sn (1byte): sector number (sn=00H-0FH)

lc(1byte): password length lc=06H

pdata(6 byte): password data

rdata(2 byte): return data .

Positive response sw1+sw2=9000H.

Negative response sw1+sw2=6F00H

8.12.4.5 Read Sector Data

Command

“C”	60H	33H	00H	B0H	sn	bn	lc

Positive response

“P”	60H	33H	ST1	ST0	rdata

Negative response

“N”	60H	33H	E1	E0

Read block and sequence blocks from RFID card

sn(1 byte): sector number

bn(1 byte): Start block number

lc(1 byte): block number (le=01H read one block, le=03H read three blocks)

rdata(2 byte):return data

(Positive response with data 9000H, and negative response with “ sw1+sw2”)

Notes：

1.Ultralight Card only has one block in each sector，every block has 4 byte data. S50,S70 have16 byte data in each block.

2. Ultra light Card, Mifare 1k (S50), Mifare 4k (S70) card range of capacity is shown as below:

Ultra light Card: sn=00H-0FH, bn=00H, lc=01H-0FH

Mifare 1k (S50): sn=00H-0FH,bn=00H-03H,lc=01H-04H

Mifare 4k (S70): sn=00H-20H,bn=00H-03H,lc=01H-04H

sn=21H-27H, bn=00H-0FH,lc=01H-10H (the last 8 sector of S70 card have 16 blocks each)

8.12.4.6 Write Sector Data

Command

“C”	60H	33H	00H	D1H	sn	bn	lc	wdata

Positive response

“P”	60H	33H	ST1	ST0	rdata

Negative response

“N”	60H	33H	E1	E0

Read block and sequence blocks from RFID card

sn(1 byte): sector number

bn(1 byte): Start block number

lc(1 byte): block number (lc=01H write 1 block, lc=3H, write 3 block)

wdata: block to write (n byte)

rdata(2 byte): return data

(Positive response with data 9000H, and negative response with “ sw1+sw2”)

Notes:

1. Ultra light Card only has one block in each sector，every block has 4 byte data. S50,S70 has16 byte data in each block

2. Ultra light Card, Mifare 1k(S50), Mifare 4k (S70) card card range of capacity is shown as below:

Ultra light Card: sn=00H-0FH, bn=00H-03H,lc=01H-03H

Mifare 1k (S50): sn=00H-0FH, bn=00H, lc=01H-03H

Mifare 4k (S70): sn=00H-20H, bn=00H-03H,lc=01H-03H

sn=21H-27H,bn=00H-0FH, lc=01H-0FH

(the last 8 sectors of S70 card have 16 blocks each)

3. S50, S70 card last block of each sector is control sector to preserve Key A, read/write control words, Key B.

Cautions: Do not write last block and CRT-288-K001 also will prohibit writing last block.

8.12.4.7 Initialization (S50, S70)

Command

“C”	60H	33H	00H	D2H	sn	bn	lc	wdata

Positive response

“P”	60H	33H	ST1	ST0	rdata

Negative response

“N”	60H	33H	E1	E0

Initialization operation to RFID card

sn(1 byte): sector number

bn(1 byte): block number

lc(1byte): length of initialized data lc=04H

wdata: data of initialize (4 byte)

rdata(2 byte): return data

(Positive response with data 9000H, and negative response with “ sw1+sw2”)

Notes：Mifare 1k (S50), Mifare 4k (S70) card operation sector can not be out of range and last block can not be operated.

Mifare 1k (S50): sn=00H-0FH, bn=00H-03H,

Mifare 4k (S70): sn=00H-20H, bn=00H-03H,

sn=20H-27H, bn=00H-0EH,

(S70 card the last 8 sector has 16 blocks each)

8.12.4.8 Read Value (S50, S70)

Command

“C”	60H	33H	00H	B1H	sn	bn

Positive response

“P”	60H	33H	ST1	ST0	rdata

Negative response

“N”	60H	33H	E1	E0

Read value operations to RFID card

sn(1 byte): sector number

bn(1 byte): block number

rdata(2 byte): return data

(Positive response with data 9000H, and negatives response with “ sw1+sw2”)

Notes：Mifare 1k (S50), Mifare 4k (S70) card operation sector can not be out of range and last block can not be operated

Mifare 1k (S50): sn=00H-0FH, bn=00H-03H,

Mifare 4k (S70): sn=00H-20H, bn=00H-03H,

sn=20H-27H, bn=00H-0EH,

(S70 card last 8 sector has 16 blocks)

8.12.4.9 Increment (S50, S70)

Command

"C"	60H	33H	00H	D3H	sn	bn	lc	wdata

Positive response

"P"	60H	33H	ST1	ST0	rdata

Negative response

"N"	60H	33H	E1	E0

Increment operation to RFID card

sn(1 byte): sector number

bn(1 byte): block number

lc(1byte): increment data length lc=04H

wdata: increment data (4 byte)

rdata : return data

(Positive response with data 9000 H and negative response with "sw1 + sw2"

Notes：Mifare 1k (S50), Mifare 4k (S70) card operation sector can not be out of range and last block can not be operated

Mifare 1k (S50): sn=00H-0FH, bn=00H-03H,

Mifare 4k (S70): sn=00H-20H, bn=00H-03H,

sn=20H-27H, bn=00H-0EH,

(S70 card last 8 sector have 16 blocks)

8.12.4.10 Decrement (S50, S70)

Command

“C”	60H	33H	00H	D4H	sn	bn	lc	wdata

Positive response

“P”	60H	33H	ST1	ST0	rdata

Negative response

“N”	60H	33H	E1	E0

Decrement operation to RFID sector

sn(1 byte): sector number

bn(1 byte): block number

lc(1byte): Decrement data length lc=04H

wdata: Decrement data(4 byte)

rdata(2 byte): return data

(Positive response with data 9000 H and negative response with “sw1 + sw2”

Notes：Mifare 1k (S50), Mifare 4k (S70) card operation sector can not be out of range and last block can not be operated

Mifare 1k (S50): sn=00H-0FH, bn=00H-03H,

Mifare 4k (S70): sn=00H-20H, bn=00H-03H,

sn=20H-27H, bn=00H-0EH,

(S70 card last 8 sector have 16 blocks)

8.12.5 Type A RFID Card Communication

Command

“C”	60H	34H	C-APDU

Positive response

“P”	60H	34H	ST1	ST0	R-APDU

Negative response

“N”	60H	34H	E1	E0

This exchanges data between RFID card by protocol RFID Type A T=CL according to ISO/IEC 14443-4

Notes: The max. Length of C-APDU is 261 byte, the max. Length of R-APDU is 258 byte.

8.12.6 Type B RFID Card Communication

Command

“C”	60H	35H	C-APDU

Positive response

“P”	60H	35H	ST1	ST0	R-APDU

Negative response

“N”	60H	35H	E1	E0

This exchanges data between RFID card by protocol RFID Type B T=CL according to ISO/IEC 14443-4

Notes: The max. Length of C-APDU is 261 byte, the max. Length of R-APDU is 258 byte.