COMMUNICATION PROTOCOL

CRT-310 V4.0 USB Interface

Motorized card reader

CREATOR (CHINA) TECH CO., LTD.

ADD: 2F，M-10 building Centre area

Hi-tech industrial park Shenzhen China

TEL: +86 755 26710691

FAX: +86 755 26710105

EMAIL:Sales@china-creator.com

Http://www.china-creator.com

Contents

1 . Communication Specification 6

1.1 Communication Interface Specification 6

1.2 Communication Control 6

1.3 Transmission package format and characters 7

1.4 Successful responsive package format and character 8

1.5 Failed responsive package format and character 9

1.6 Normal Communication Procedure 10

1.7 Abnormal Communication Procedure(Command and Respond) 10

2. CRT-310 Card Reader Operation Command 12

2.1 Operation Command List 12

2.2 Status Code st0, st1 15

2.3 Error code e0, e1 15

3. Command Specification 17

3.1 Reset (Initialization) 17

3.2 Status Request Command 18

3.3 Move Card Command 19

3.4 Entry Command 20

3.5 Magnetic Card Operation 21

3.5.1 Magnetic register Read Operation Command 21

3.5.2 Multi-MAG-Track read command 23

3.6 Auto-Check IC Card 26

3.7 Auto-Check RFID Card Type 27

3.8 CPU Card Operations 28

3.8.1 CPU Card Reset 28

3.8.2 Deactivate CPU Command 29

3.8.3 Inquire CPU Card Status 29

3.8.4 CPU Card Communication T=0 30

3.8.5 CPU Card Communication T=1 31

3.8.6 CPU Warm Reset 32

3.8.7 T=1, T=0 CPU Card Protocol Automatic Communication 32

3.9 SAM (Secure Application Module) Control Command 33

3.9.1 Active SAM Command 33

CREATOR

3.9.2 Deactivate SAM Command 34
3.9.3 Inquire SAM Status Command 35
3.9.4 CPU T=0 Communication APDU 36
3.9.5 CPU T=1 Communication APDU 37
3.9.6 SAM Warm Reset 38
3.9.7 Auto-Check SAM Card T=0/T=1 Protocol 38
3.9.8 Select SAM 39
3.10 SLE4442/4428 Control 40
3.10.1 SLE4442/4428 Reset 40
3.10.2 Deactivate SLE4442/4428 40
3.10.3 Inquire status of SLE4442/4428 41
3.10.4 SLE4442 Control 42
3.10.5 Data read from main memory on SLE4442 42
3.10.6 Read protection bits on SLE4442 43
3.10.7 Data read from security memory on SLE4442 44
3.10.8 Data write to main memory on SLE4442 44
3.10.9 Data write with protection bit on SLE4442 45
3.10.10 Data write to security memory on SLE4442 (Modify password) 46
3.10.11 Verification data present to SLE4442 47
3.10.12 SLE4428 Control 48
3.10.13 Data Reading of main-memory of SLE4428 48
3.10.14 Reading of protection-bit of SLE4428 49
3.10.15 Data writing to main-memory of SLE4428 50
3.10.16 Written with protection-bit 51
3.10.17 Verification of password present to SLE4428 51
3.10.18 Modify Password of SLE4428 52
3.11 I2C Memory Card Control Command 53
3.11.1 Activate I2C memory card 53
3.11.2 Deactivate I2C memory card 54
3.11.3 Inquire Status of I2C memory card 55
3.11.4 I2C Control 56
3.11.5 Read data from I2C 57
3.11.6 Write data to I2C 57
3.12 Contactless IC card Operation 58

CREATOR

3.12.1 Activated contactless IC card 58
3.12.2 Deactivate RFID card 60
3.12.3 Inquire status of RFID card 60
3.12.4 Mifare card control 61
3.12.5 Key verification 61
3.12.6 Verify key from EEPROM 62
3.12.7 Modify sector key (KEY A) 63
3.12.8 Download password to EEPROM 64
3.12.9 Read sector data 65
3.12.10 Write sector data 66
3.12.11 Initialization 67
3.12.12 Read value 68
3.12.13 Increment 69
3.12.14 Decrement 70
3.12.15 Type A RFID card communication 71
3.12.16 Type B RFID card communication 71
3.13 Shutter related operation 72
3.13.1 LED setting 72
3.14 Easy-damage Part Counter 73
3.14.1 Read Counter 73
3.14.2 Initialization Counter 73
3.15 Read Serial Number of CRT-310 74
3.15.1 Read serial number 74
3.16 Read CRT-310 configuration 75
3.17 Read CRT-310 version information 76
3.18 Capture Card Counter Control 77
3.18.1 Read Capture Card counter 77
3.18.2 Set initial value of capture card counter 77

CREATOR

Notes: Communication protocol for USB and RS232 is different

REVISION

Version	Date	Contents
4.0-USB	2010.6.29	First Release

CREATOR

1. Communication Specification

1.1 Communication Interface Specification

USB Version： USB 2.0
Full Speed： 12Mbps
End Point： EPO Control transfer 32byte
EP1： Interrupt out 64byte
EP2： Interrupt in 64byte
Vendor Identifier： 8848 (hex)
Product Identifier： 0310 (hex)
Manufacture String： “CREATOR (CHINA) TECH. CO., LTD”
Product String: “CRT-310”
Device Class: HID (Human Interface Device) 1.11

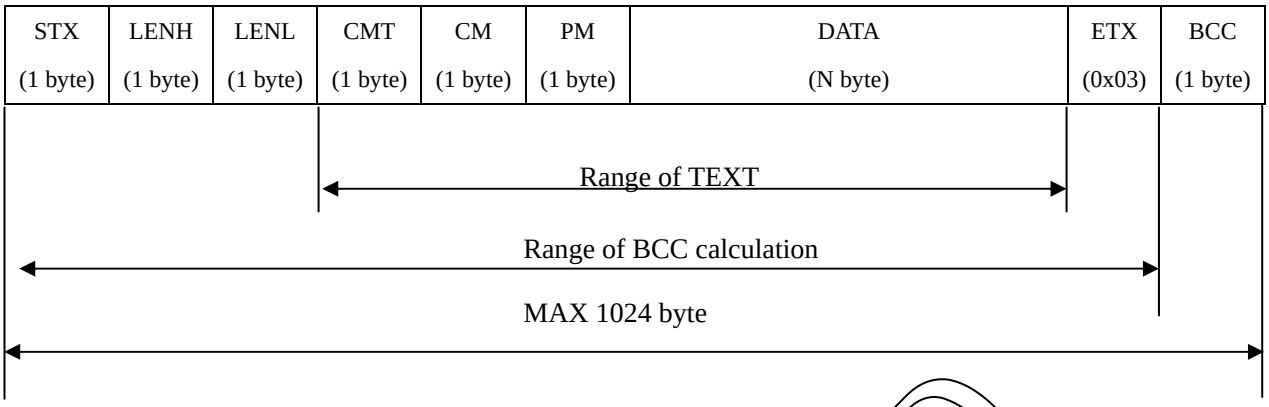
1.2 Communication Control

The machine is a driven part, operation after receive a legal command.

STX (F2H)	Start character of data package
ETX (03H)	End character of data package
ACK (06H)	Positive character(reader-host)
NAK (15H)	Negative character(reader-host)
EOT (04H)	Cancel character

CREATOR

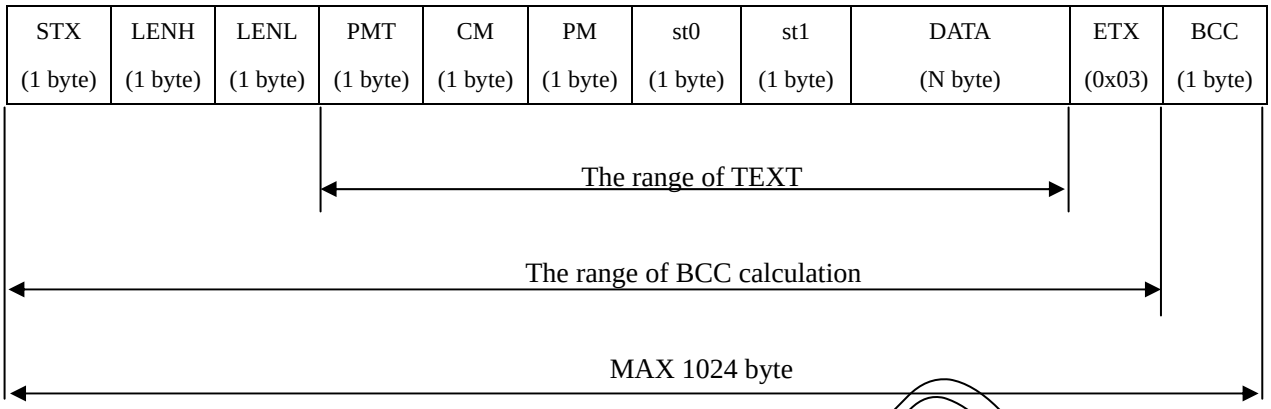
1.3 Transmission package format and characters



Code	Meaning
STX (F2H)	Representing the start of text in a command or a response.
LENH(1 byte)	Length of high byte of TEXT package
LENL(1 byte)	Length of low byte of TEXT package
CMT	Transmission Command Head ('C' , 43H)
CM	Transmission Command Character
PM	Transmission Command Parameter
DATA	Transmission command Data (N byte, N=0~512)
ETX (03H)	End of text
BCC(1byte)	CRC Parity

CREATOR

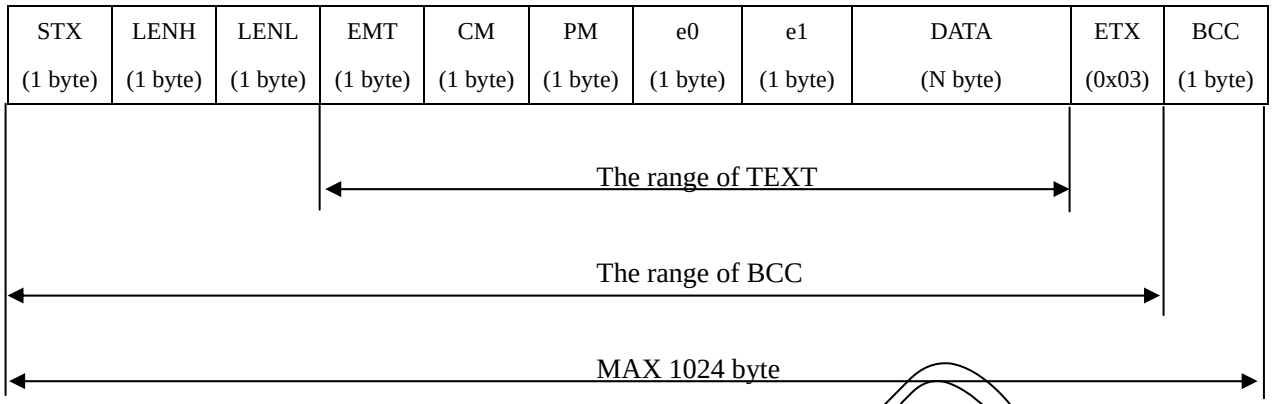
1.4 Successful responsive package format and character



Code	Meaning
STX (F2H)	Representing the start of text in a command or a response.
LENH(1 byte)	Length of high byte of return text
LENL(1 byte)	Length of low byte of return text
PMT	Return command head ('P', 50H)
CM	Return command character
PM	Return command parameter
st0,st1	Return command status code
DATA	Return command data (N byte, N=0~512)
ETX (03H)	End of text
BCC (1 byte)	CRC Parity

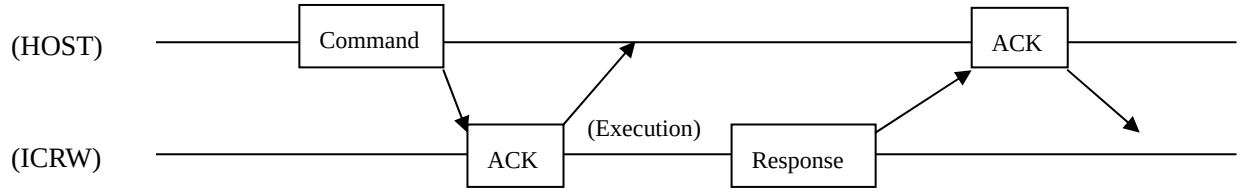
PRELIMINARY

1.5 Failed responsive package format and character



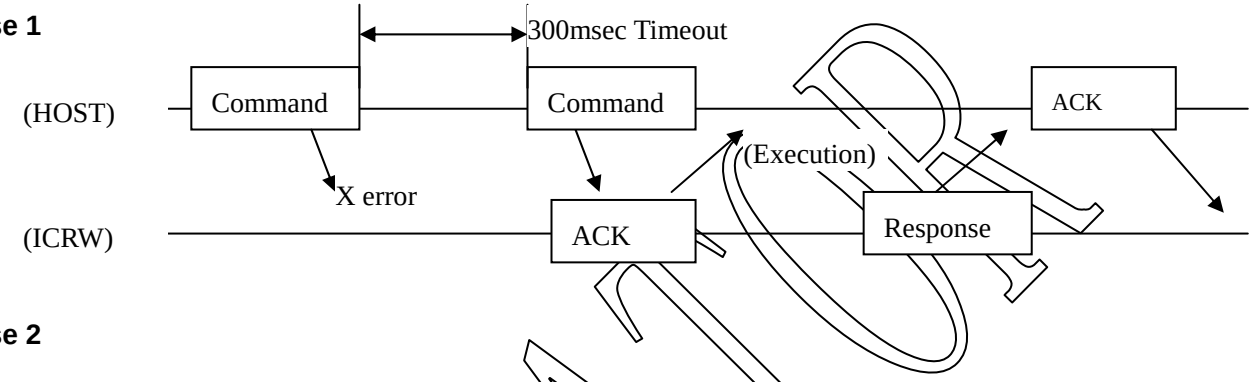
Code	Meaning
STX (F2H)	Representing the start of text in a command or a response.
LENH(1 byte)	Length of high byte of return text
LENL(1 byte)	Length of low byte of return text
EMT	Return command head ('N', 4EH)
CM	Return command character
e1,e0	Return command error status code
PM	Return command parameter
DATA	Return command data (N byte, N=0~512)
ETX (03H)	End of text
BCC (1 byte)	CRC Parity

1.6 Normal Communication Procedure

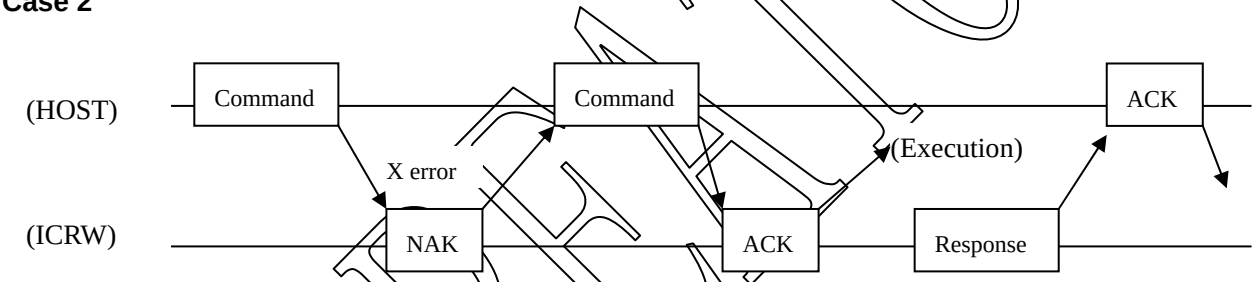


1.7 Abnormal Communication Procedure (Command and Respond)

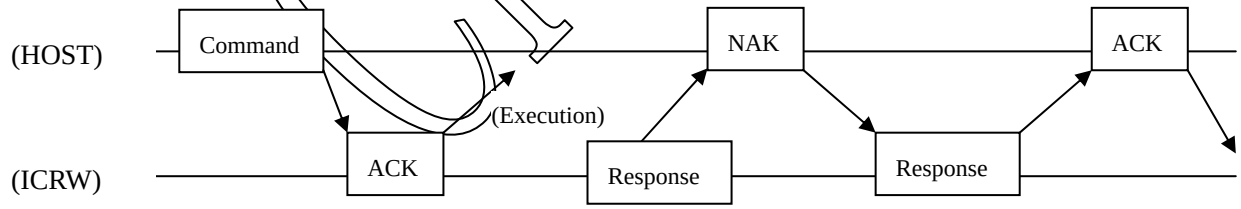
Case 1



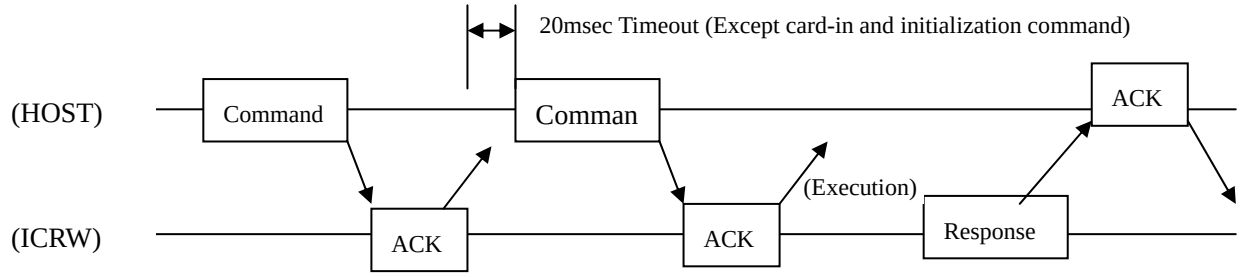
Case 2



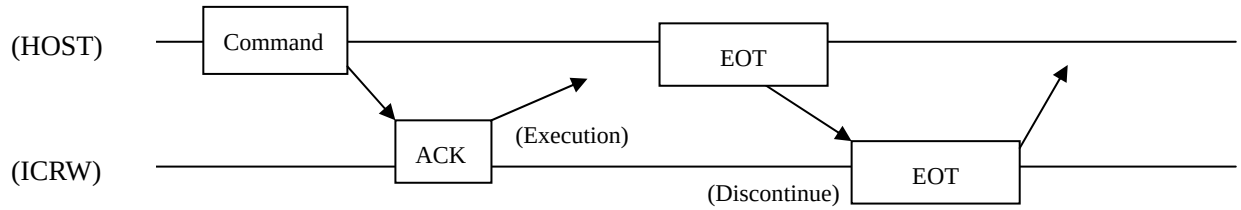
Case 3



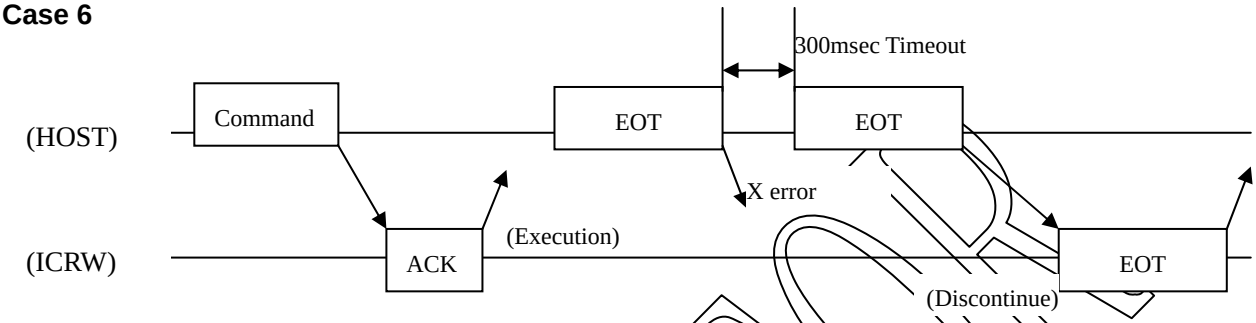
Case 4



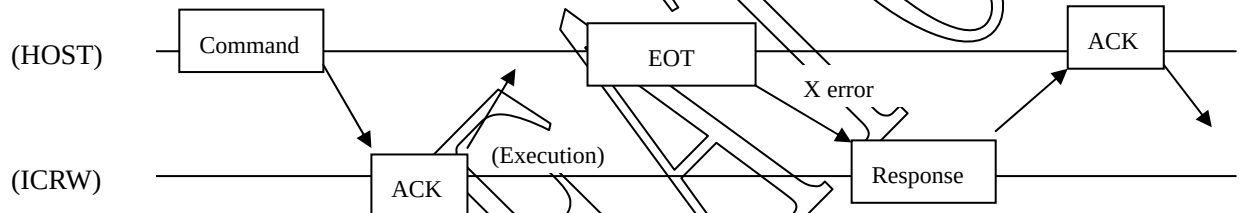
Case 5



Case 6



Case 7



CREATOR

2. CRT-310 Card Reader Operation Command

2.1 Operation Command List

CHAPTER	COMMAND	FUNCTION	CM	PM	DESCRIPTION
3.1	INITIALIZE	Initialize CRT-310	30H	30H	If card is inside, move card to card holding position
				31H	If card is inside, capture card to rear side without card holding position.
				32H	If card is inside, capture card to front side without card holding position.
				33H	If card is inside, does not move the card.
				34H	Same as 30H and capture card counter will work.
				35H	Same as 31H and capture card counter will work.
				36H	Same as 32H and capture card counter will work.
				37H	Same as 33H and capture card counter will work.
3.2	STATUS REQUEST	Inquire status	31H	30H	Report CRT-310 status
				31H	Report CRT-310status (With sensor status)
				32H	Report CRT-310 status (With sensor status)
3.3	CARD MOVE	Card movement	32H	30H	Move card to front side without card holding
				31H	Move card to rear side holding card position
				32H	Move card to RFID card operation position
				33H	Move card to IC card operation position
				34H	Move card rear side holding card position
				35H	Move card to rear side without

CREATOR

					holding card position.
3.4	CARD ENTRY		33H	30H	Prohibit entry from front
				31H	Enable entry by switch
				32H	Enable entry by magnetic signal
				40H	Prohibit entry from rear
				41H	Enable entry from rear
3.5.1	Magnetic card operation	Magnetic card register operation	35H	31H	Only upload ISO-1 track data
				32H	Only upload ISO-2 track data
				33H	Only upload ISO-3 track data
				36H	Clear the data in the magnetic register without moving the card.
				37H	Only check the data status of magnetic register
				51H	Read ISO-1 track data by binary mode
				52H	Read ISO-2 track data by binary mode
				53H	Read ISO-3 track data by binary mode
3.5.2	Combine the magnetic card operation	Combination of magnetic card operation	36H	31H	Only-read ISO-1 track
				32H	Only-read ISO-2 track
				33H	Only-read ISO-3 track
				34H	Only-read ISO-1, ISO-2 track data
				35H	Only-read ISO-1, ISO-3 track data
				36H	Only-read ISO-2, ISO-3 track data
				37H	Only-read ISO-1, ISO-2, ISO-3 track data
3.6	IC card Type		50H	30H	Auto check IC Card Type
3.7	RFID card Type		50H	31H	Auto check RFID Card Type
3.8	CPU CARD CONTROL	CPU Card Application Operation	51H	30H	CPU Card cold reset
				31H	CPU Card power down
				32H	CPU Card status check
				33H	T=0 CPU Card APDU data exchange
				34H	T=1 CPU Card APDU data exchange
				38H	CPU Card hot reset

CREATOR

				39H	Auto distinguish T=0/ T=1 CPU Card APDU data exchange
3.9	SAM CARD CONTROL	SAM Card Application Operation	52H	30H	SAM Card cold reset
				31H	SAM Card power off
				32H	SAM Card status check
				33H	T=0 SAM Card APDU data exchange
				34H	T=1 SAM Card APDU data exchange
				38H	SAM Card warm reset
				39H	Auto distinguish T=0/T=1 SAM Card APDU data exchange
				40H	Select SAM Card stand
3.10	SLE4442/4428CARD CONTROL		53H	30H	SLE4442/4428 Card reset
				31H	SLE4442/4428 Card power down
				32H	Browse SLE4442/4428 Card status
				33H	Operate SLE4442 Card
				34H	Operate SLE4428 Card
3.11	I2C MEMORYCARD	24C01—24C256 Card Operation	54H	30H	I2C Card reset
				31H	I2C Card power-off
				32H	Check I2C Card status
				33H	Read I2C Card
				34H	Write I2C Card
3.12	RFID CARD CONTROL (13.56 MHZ)	Mifare standard card Type A & B T=CL protocol operation	60H	30H	RFID Card startup
				31H	RFID Card down power
				32H	RFID Card operation status check
				33H	Mifare standard Card read/write
				34H	Type A standard T=CL Card APDU data exchange
				35H	Type B standard T=CL Card APDU data exchange
3. 13	LED Indicator operation		80H	30H	Red LED Operation
				31H	Green LED Operation
3.14	Easily damaged part lifetime		A1H	30H	Read counter of gate opening times
				31H	Read counter of Magnetic head reading times

CREATOR

				32H	Read counter of IC contact using times
3.15	Machine SERIAL NUMBER		A2H	30H	Read Machine Serial number
3.16	Read Machine CONFIG		A3H	30H	Read Machine configuration information
3.17	READ CRT-310 VERSION		A4H	30H	Read Card software version information
3.18	RECYCLEBIN COUNTER		A5H	30H	Read card retreat counter
				31H	Initiate card retreat counter

2.2 Status Code st0, st1

st0&st1	Content
“00”	No Card in CRT-310 (Including gate)
“01”	One Card in gate
“02”	One Card on RFID/IC Card Operation Position

2.3 Error code e0, e1

e0&e1	Content
“00”	Command Character Error
“01”	Command Parameter Error
“02”	Command Can Not Be Executed
“03”	Out of Hardware Support Command
“04”	Command Data Error
“05”--“09”	
“10”	Card Jam
“11”	Shutter error
“12”	
“13”	Too Long-Card in the machine
“14”	Too Short-Card in the machine
“15”	EEPROM Error
“16”	Card is pulled out by force
“17”	Card jam when insert
“18”	
“19”	Card not insert from rear
“20”	Read error (CRC error)

CREATOR

“21”	Read error
“22”	
“23”	Read Error (Only SS-ES-LRC)
“24”	Read Error (No data/blank)
“25”	
“26”	Read error (No SS)
“27”	Read error (No ES)
“28”	Read error (LRC error)
“29”	
“30”	Power Down
“31”	
“32”	Voltage is too high, more than 14.5V
“33”	Voltage is too low, more than 10.5V
“34-39”	
“40”	Card pulled out when retreating the card
“41”	Operation of IC Card Error
“42”	
“43”	Disable To Move Card To IC Card Position
“44”	
“45”	Card withdraw error
“46”--“49”	
“50”	Received Card Counter Overflow
“51”—“59”	
“60”	Abnormal condition was found on the power-line (Vcc) of IC card
“61”	ATR error
“62”	IC card type error
“63”	IC card does not respond
“64”	Other than “63”
“65”	Send CPU command by HOST before reception of ATR
“66”	Command Out Of IC Current Card Support
“67”—“68”	
“69”	IC card Non-Compliance To EMV Standard
“80”	
“81”	
“90”	Unknown card type
“B0”	Not Receive reset command

CREATOR

3. Command Specification

3.1 Reset (Initialization)

Command (TXET):

"C"	30H	Pm	Pd

Positive response (TXET):

"P"	30H	Pm	st0	st1	Rev_type

Negative response (TEXT):

"N"	30H	Pm	e0	e1

This should be the first command after power on, otherwise other command can not be executed, and then this command can be executed multiple times.

Once execute this command, the error status before will be cleaned, return software version information and machine will be in prohibit card-in status.

If no card in machine, the motor will rotate slightly (to adjust card position in the machine). If there is a card, the disposal is shown as below

Pm: Command parameter

30H: Move the card to front side holding card position

31H: Move the card to the rear side without holding card position (Retreat card)

32H: Move the card to the front side without holding card position.

33H: Without moving card

34H: Same as pm=30H, and Capture card counter will work.

35H: Same as pm=31H, and Capture card counter will work

36H: Same as pm=32H, and Capture card counter will work

37H: Same as pm=33H, and Capture card counter will work

Pd: Reject card when power off setting (Option parameter)

The operation will occur when the machine suddenly power-off, the card will be rejected

=30H when power-off suddenly, do not reject card

=31H when power-off suddenly, move the card to front side holding card position. (Base on the premise that the machine need to have stand-by power)

=32H when power-off, move the card to rear side holding card position. (Base on the premise that the machine need to have stand-by power)

Notes: Default setting Pd=30H, if no Pd parameter in reset command

Rev_type: software version, "CRT-310-U4.0"

3.2 Status Request Command

Command

"C"	31H	Pm

Positive response

"P"	31H	Pm	st0	st1	Sensor(8 byte)

Negative response

"N"	31H	Pm	e0	e1

Pm=30H: Report current status of st0, st1 (See 2.2)

Pm=31H: Report current status of st0 and st1 and status of sensor (8 byte)

Pm=32H, Error on machine, return current status of st0 and st1 and status of sensor (8byte)

The status of sensor is referred to appearance drawing.

Sensor		Status
DSS1 Gate sensor	30H	DSS1 No card
	31H	DSS1 Have card
	33H	No Shutter
DSS2 (Shutter sensor)	30H	Shutter close
	31H	Shutter open
	33H	No shutter
PSS 0	30H	PSS0 No card
	31H	PSS0 Have card
PSS1	30H	PSS1 No card
	31H	PSS1 Have card
PSS2	30H	PSS2 No card
	31H	PSS2 Have card
PSS3	30H	PSS3 No card
	31H	PSS3 Have card
PSS4	30H	PSS4 No card
	31H	PSS4 Have card
PSS5	30H	PSS5 No card
	31H	PSS5 Have card

SPECIMEN

3.3 Move Card Command

Command

"C"	32H	Pm

Positive response

"P"	32H	Pm	st0	st1

Negative response

"N"	32H	Pm	e0	e1

Carry the card to the different positions by command operation

Pm=30H Move card to front side without holding card position

Pm=31H Move card to front side holding card position

Pm=32H Move card to RFID card operation position

Pm=33H Capture card to IC card operation 1position

Pm=34H Move card to rear side holding card position

Pm=35H Move card to rear side without holding card position (Capture card)

If card can not move to specified position, CRT-310 will return Card jam error

Note:

1. Pm=35H, move card to rear side without holding card position, the retreat counter will work after initialization command which drive retreat card counter working.
2. Execute card move command when card is on IC card operation position and power on, the machine will power off the IC card first and execute move card operation.

CREATOR

3.4 Entry Command

Command

"C"	33H	Pm

Positive response

"P"	33H	Pm	st0	st1

Negative response

"N"	33H	Pm	e0	e1

After set card input from rear/front be available, if insert card from the gate, CRT-310 will carry the card to RFID card operation position. The end of the insertion can be detected by status inquiry command.

Pm=30H Disable card input from gate

Pm=31H Enable card input from gate by switch mode

Pm=32H Enable card input from gate by magnetic mode

Pm=40H Prohibit card in from rear

Pm=41H Allow card in from rear

CREATOR

3.5 Magnetic Card Operation

3.5.1 Magnetic register Read Operation Command

HOST Command:

"C"	35H	Pm

Positive return:

"P"	35H	Pm	st0	st1	Mag_Data (n byte)

Negative return:

"N"	35H	Pm	e0	e1

PM=31H： Read data on ISO Track #1

PM=32H： Read data on ISO Track #2

PM=33H： Read data on ISO Track #3

Upload data of register by ASCII mode to HOST, If the reading data is incorrect, it upload error status e0 and e1.

Data format of ISO ASCII code:

-Track#1(IATA): 79 characters max. (6bits+ 1parity) e.g. b0, b1, b2, b3, b4, b5，P

-Track#2(ABA): 40 characters max. (4bits+1 parity) e.g. b0, b1, b2 b3，P

-Track#3(MINTS): 107 characters max. (4bits+ 1parity) e.g. b0, b1, b2 b3，P

For examples:

ISO Track #1			ISO Track #2, #3		
bit	5 4 3 2 1 0		bit	3 2 1 0	
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

PM=36H: Clear the data of register (cleaning magnetic card memory)

PM=37H：Check if there are any data in the magnetic register.

Transmission Mag_Data data format:

Sn1	Sn2	Sn3

Snx =30H No data (The track is blank) (x=1, 2, 3)

Snx =31H Have data

Once execute magnetic register clean command"C56", Sn1=30H, Sn2=30H, Sn3=30H

PM=51H: Upload data on ISO Track #1 by binary without moving the card

PM=52H: Upload data on ISO Track #2 by binary without moving the card

PM=53H: Upload data on ISO Track #3 by binary without moving the card

Binary read card differs from other register; the data of register is not checked and decode by ASCII code. The data is original data.

The binary read card command ignores error or right, and which is transmitted in the form of converted ASCII code.

Every 4 bit as a group and transmit as ASCII Code

There are plenty of pre-load and suffix-load zeros in these sent data, so CRT-310 will ignores these zeros during sending data

For example: data in a track:

(HEX) = '0000 0000 0011 0111 1111 0000 0000 0011 0111 1111 0000 0000'

Data packet sent to HOST: 0x33 0x37 0x46 0x30 0x30 0x33 0x37 0X46

If there is no data in a track, then the length of Mag_Data is 0

CREATOR

3.5.2 Multi-MAG-Track read command

HOST Command:

"C"	36H	Pm	Mode

Positive Return:

"P"	36H	Pm	st0	st1	Mag_Data(n byte)

Negative Return:

"N"	36H	Pm	e0	e1	Mag_Data(n byte)

Mode=30H ASCII Mode

PM=31H： Read data on ISO Track #1

PM=32H： Read data on ISO Track #2

PM=33H： Read data on ISO Track #3

PM=34H： read data on ISO Track #1，ISO Track #2

PM=35H： read data on ISO Track #1，ISO Track #3

PM=36H： read data on ISO Track #2，ISO Track #3

PM=37H： read data on ISO Track #1，ISO Track #2，ISO Track #3

CRT-310 sends negative response and error code is 21. In case of card carrying, CRT-310 sends negative response too.

Data format of ISO ASCII code:

-Track#1(IATA): 79 characters max. (6bits+ 1parity) e.g. b0, b1, b2, b3, b4, b5，P

-Track#2(ABA): 40 characters max. (4bits+1 parity) e.g. b0, b1, b2 b3，P

-Track#3(MINTS): 107 characters max. (4bits+ 1parity) e.g. b0, b1, b2 b3，P

For example

ISO Track #1			ISO Track #2, #3		
bit	5 4 3 2 1 0		bit	3 2 1 0	
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

Response data format: ISO#1 data+7EH+ ISO#2 data+7EH+ ISO#3 data

ISO# n data (N=1, 2, and 3):

Positive read: "P"+ track data（ASCII code excludes SS-ES-LRC）

Negative read: "N2X" , "2X" error code （"20""23""24""26""27""28"）

Positive response:

PM=31H： "P" + ISO #1 data

PM=32H: "P" + ISO #2 data

PM=33H: "P" + ISO #3 data

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

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

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

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

All negative response and Mag_Data will be:

E1, E0: "21"

E3, E2: error code of ISO#1

E5, E4: error code of ISO#2

E7, E6: error code of ISO#3

PM=31H: "N "+ E3, E2

PM=32H: "N" + E5, E4

PM=33H: "N" + E7, E6

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

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

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

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

Mode=31H: Binary Mode

Read binary data from magnetic register, return Mag_Data format is following:

BIN#1data + 7EH + BIN#2 data +7EH + BIN#3 data

PM=31H BIN#1data

PM=32H BIN#2data

PM=33H BIN#3data

PM=34H BIN#1data + 7EH + BIN#2 data

PM=35H BIN#1data + 7EH + BIN#3 data

PM=36H BIN#2data + 7EH + BIN#3 data

PM=37H BIN#1data + 7EH + BIN#2 data +7EH + BIN#3 data

The binary read card command ignores error or right, and which is transmitted in the form of converted ASCII code.

CREATOR

Every 4 bit as a group and transmit as ASCII Code

There are plenty of pre-load and suffix-load zeros in these sent data, so CRT-310 will ignores these zeros during sending data

For example: data in a track:

(HEX) = '0000 0000 0011 0111 1111 0000 0000 0011 0111 1111 0000 0000'

Data packet sent to HOST: ISO#N data (N=1, 2, 3) 0x33 0x37 0x46 0x30 0x30 0x33 0x37 0X46

If there is no data in a track, then the length of ISO#N data is 0

CREATOR

3.6 Auto-Check IC Card

Command

“C”	50H	30H

Positive response

“P”	50H	30H	st0	st1	Card_type

Negative response

“N”	50H	30H	e0	e1

Auto-Check type of IC Card, and carry card to IC Card operation position, Auto Check IC Card Type, Return Card_type information.

Cart_type(2 byte)		Specification
‘0’	‘0’	Unknown IC Card Type
‘1’	‘0’	T=0 CPU Card
	‘1’	T=1 CPU Card
‘2’	‘0’	SLE4442 Card
	‘1’	SLE4428 Card
‘3’	‘0’	AT24C01 Card
	‘1’	AT24C02 Card
	‘2’	AT24C04 Card
	‘3’	AT24C08 Card
	‘4’	AT24C16 Card
	‘5’	AT24C32 Card
	‘6’	AT24C64 Card
	‘7’	AT24C128 Card
	‘8’	AT24C256 Card

SAMPLE

3.7 Auto-Check RFID Card Type

Command

“C”	50H	31H

Positive response

“P”	50H	31H	st0	st1	Card_type

Negative response

“N”	50H	31H	e0	e1

Auto-Check type of RFID card, carry card to RFID card operation position, Auto-Check RFID Card Type, Return Card_type information

Cart_type(2 byte)		Specification
‘0’	‘0’	Unknown RFID Card Type
‘1’	‘0’	Mifare one S50Card
	‘1’	Mifare one S70Card
	‘2’	Mifare one UL Card
‘2’	‘0’	Type A CPU Card
‘3’	‘0’	Type B CPU Card

CREATOR

3.8 CPU Card Operations

3.8.1 CPU Card Reset

Command

"C"	51H	30H	Vcc

Positive response

"P"	51H	30H	st0	st1	Type	ATR

Negative response

"N"	51H	30H	e0	e1	Type	ATR

To cold reset IC card. The CRT-310 supplies power (VCC) and clock (CLK), return ATR.

Vcc=30H: CRT-310 supplies with +5V to VCC and activates in line with the EMV2000 ver4.0.

Vcc=33H: CRT-310 supplies with +5V to VCC and activates in line with the ISO/IEC7816.

Vcc=35H: CRT-310 supplies with +3V to VCC and activates in line with the ISO/IEC7816.

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

If ATR is not compliance 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

Format of ATR

TS	TO	TA1	TB1	…	TCK

CREATOR

3.8.2 Deactivate CPU Command

Command

“C”	51H	31H

Positive response

“P”	51H	31H	st0	st1

Negative response

“N”	51H	31H	e0	e1

This deactivates CPU card.

This command is to deactivate activated CPU card.

CREATOR

3.8.3 Inquire CPU Card Status

Command

“C”	51H	32H

Positive response

“P”	51H	32H	st0	st1	Sti

Negative response

“N”	51H	32H	e0	e1

The machine tells the status of IC card with sti.

St i=30H Card not activated

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

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

If IC Card power error, return e1,e0=“60”.

3.8.4 CPU Card Communication T=0

Command

"C"	51H	33H	C-APDU

Positive response

"P"	51H	33H	st0	st1	R-APDU

Negative response

"N"	51H	33H	e0	e1

This exchanges data between CPU card by protocol T=0

C-APDU from HOST is range from 4 byte to 261 byte

CLA	INS	P1	P2	LC	Data1	.....	Le

R-APDU to HOST is range from 2 byte to 258 byte

Data1	.....	Data(n)	Sw1	Sw0

An e0, e1= "60" is returned when a power failure is detected.

If protocol type of IC card is not T=0, e0, e1= "62"is sent.

If ICC does not respond within Working Wait Time, CRT-310 deactivates an IC card and e0, e1 ="63" is sent.

If any other protocol error occurs, CRT-310 deactivates an IC card and e0, e1= "64" is sent.

If HOST tries to communicate before an IC card activation, e0, e1= "65" is sent.

Note: Please refer to ISO/IEC7816 about T=0 APDU format and specific C-APDU pleas refer to the COS of the card

CREATOR

3.8.5 CPU Card Communication T=1

Command

"C"	51H	34H	C-APDU

Positive response

"P"	51H	34H	st0	st1	R-APDU

Negative response

"N"	51H	34H	e0	e1

This exchanges data between CPU card by protocol T=1

CRT-310 should follow T=1 protocol to combination 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 power failure is detected.

If protocol type of IC card is not T=0, e0, e1= "62"is sent.

If ICC does not respond within Working Wait Time, CRT-310 deactivates an IC card and e0, e1= "63" is sent.

If any other protocol error occurs, CRT-310 deactivates an IC card and e0, e1= "64" is sent.

If HOST tries to communicate before an IC card activation, e0, e1= "65" is sent.

Note: If you want to more about T=0 APDU format. Please refer to ISO/IEC7816 and COS command

3.8.6 CPU Warm Reset

Command

“C”	51H	38H

Positive response

“P”	51H	38H	st0	st1	Type	ATR

Negative response

“N”	51H	38H	e0	e1

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

Type: CPU Card communication protocol

=30H T=0 Protocol

=31H T=1 Protocol

3.8.7 T=1, T=0 CPU Card Protocol Automatic Communication

Command

“C”	51H	39H	C-APDU

Positive response

“P”	51H	39H	st0	st1	R-APDU

Negative response

“N”	51H	39H	e0	e1

Protocol is recognized automatically. Set data to “C-APDU”. CRT-310 returns “R-APDU” data to HOST.

An e0, e1= “60” is returned when a power failure is detected.

If protocol type of IC card is not T=0, e0, e1= “62”is sent.

If ICC does not respond within Working Wait Time, CRT-310 deactivates an IC card and e0, e1= “63” is sent.

If any other protocol error occurs, CRT-310 deactivates an IC card and e0, e1= “64” is sent.

If HOST tries to communicate before an IC card activation, e0, e1= “65” is sent.

CREATOR

3.9 SAM (Secure Application Module) Control Command

3.9.1 Active SAM Command

Command

"C"	52H	30H	Vcc

Positive response

"P"	52H	30H	st0	st1	Type	ATR

Negative response

"N"	52H	30H	e0	e1	Type	ATR

The CRT-310 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-310 supplies with +5V to VCC and activates in line with the EMV2000 ver4.0.

Vcc=33H: CRT-310 supplies with +5V to VCC and activates in line with the ISO/IEC7816.

Vcc=35H: CRT-310 supplies with +3V to VCC and activates in line with the ISO/IEC7816.

Vcc is optional parameter. In case there is no Vcc parameter, it will have 30H as default value (Vcc =30H)

If ATR is not compliance to EMV, return e1,e0= "69"

CREATOR

3.9.2 Deactivate SAM Command

Command

“C”	52H	31H

Positive response

“P”	52H	31H	st0	st1

Negative response

“N”	52H	31H	e0	e1

This deactivates SAM

CREATOR

3.9.3 Inquire SAM Status Command

Command

"C"	52H	32H

Positive response

"P"	52H	32H	st0	st1	Sti	Stj

Negative response

"N"	52H	32H	e0	e1

CRT-310 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 First SAM card connector

Stj =31H Second SAM card connector (Optional)

Stj =32H Third SAM card connector (Optional)

Stj =33H Fourth SAM card connector (Optional)

Stj =34H Fifth SAM card connector (Optional)

e0, e1="60" is returned when a power failure is detected.

CREATOR

3.9.4 CPU T=0 Communication APDU

Command

"C"	52H	33H	C-APDU

Positive response

"P"	52H	33H	st0	st1	R-APDU

Negative response

"N"	52H	33H	e0	e1

This exchanges data between SAM by protocol T=0

If power supply of IC card is fail, e0, e1= "60" is return.

If protocol type of IC card is not T=0, e0, e1= "62"is return.

If ICC does not respond within Working Wait Time, CRT-310 deactivates an IC card and e0, e1= "63" is sent.

If any other protocol error occurs, CRT-310 deactivates an IC card and e0, e1= "64" is sent.

If HOST tries to communicate before an IC card activation, e0, e1= "65" is sent.

Note: Please refer to ISO/IEC7816 about T=0 APDU format and specific C-APDU pleas refer to the COS of the card

CREATOR

3.9.5 CPU T=1 Communication APDU

Command

"C"	52H	34H	C-APDU

Positive response

"P"	52H	34H	st0	st1	R-APDU

Negative response

"N"	52H	44H	e0	e1

This exchange data between SAM by protocol T=1

If power supply of IC is fail, e0, e1= "60" is return.

If protocol type of IC card is not T=0, e0, e1= "62"is return.

If ICC does not respond within Working Wait Time, CRT-310 deactivates an IC card and e0, e1= "63" is sent.

If any other protocol error occurs, CRT-310 deactivates an IC card and e0, e1= "64" is sent.

If HOST tries to communicate before an IC card activation, e0, e1= "65" is sent.

Note: Please refer to ISO/IEC7816 about T=0 APDU format and specific C-APDU pleas refer to the COS of the card

CREATOR

3.9.6 SAM Warm Reset

Command

“C”	52H	38H

Positive response

“P”	52H	38H	st0	st1	Type	ATR

Negative response

“N”	52H	38H	e0	e1

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

Type: SAM protocol type

=30H T=0 Protocol

=31H T=1 Protocol

3.9.7 Auto-Check SAM Card T=0/T=1 Protocol

Command

“C”	52H	39H	C-APDU

Positive response

“P”	52H	39H	st0	st1	R-APDU

Negative response

“N”	52H	39H	e0	e1

Automatically choose corresponding C-APDU according to auto check of T=0/T=1 of SAM and return R-APDU

If power supply of IC card is fail, e0, e1= “60” is return.

If protocol type of IC card is not T=0, e0, e1= “62”is return.

If ICC does not respond within Working Wait Time, CRT-310 deactivates an IC card and e0, e1= “63” is sent.

If any other protocol error occurs, CRT-310 deactivates an IC card and e0, e1= “64” is sent.

If HOST tries to communicate before IC card activation, e0, e1= “65” is sent.

CREATOR

3.9.8 Select SAM

Command

“C”	52H	40H	SAMn

Positive response

“P”	52H	40H	st0	st1

Negative response

“N”	52H	40H	e0	e1

HOST can select SAM stand.

SAMn = 30H: SAM 1.

SAMn = 31H: SAM 2. (Option)

SAMn = 32H: SAM 3. (Option)

SAMn = 33H: SAM 4. (Option)

SAMn = 34H: SAM 5. (Option)

SAM command is effective only in the module selection.

When Initialize command is executed, SAM 1 will be selected.

CREATOR

3.10 SLE4442/4428 Control

3.10.1 SLE4442/4428 Reset

Command

“C”	53H	30H

Positive response

“P”	53H	30H	st0	st1	ATR(4 byte)

Negative response

“N”	54H	30H	e0	e1

The CRT-310 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”

3.10.2 Deactivate SLE4442/4428

Command

“C”	53H	31H

Positive response

“P”	53H	31H	st0	st1

Negative response

“N”	53H	31H	e0	e1

The CRT-310 stop supplying power (VCC) and clock (CLK) then reset (RST) release.

CREATOR

3.10.3 Inquire status of SLE4442/4428

Command

“C”	53H	32H

Positive response

“P”	53H	32H	st0	st1	Sti

Negative response

“N”	54H	32H	e0	e1

CRT-310 tells 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

CREATOR

3.10.4 SLE4442 Control

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

In this case, CRT-310 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-310 returns a positive response with response data 9000H like from the IC card. When an error occurs during the communication with SLE4442, CRT-310 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 Validation error
6FH	02H	Key Validation error and Lock
67H	00H	Address overflow
6BH	00H	Operation length overflow

3.10.5 Data read from main memory on SLE4442

Command

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

Positive response

"P"	53H	33H	st0	st1	data

Negative response

"N"	53H	33H	e0	e1

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

cd H: the length of bytes of data to read

CRT-310 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

TRIAL

3.10.6 Read protection bits on SLE4442

Command

“C”	53H	33H	00H	B0H	01H	abH	cdH

Positive response

“P”	53H	33H	st0	st1	Data(n byte)

Negative response

“N”	53H	33H	e0	e1

Notes: ab H: the start address (00H—03H)

cd H : the length of bytes of data to read (01H—04H)

SLE 4442 have 32 bit protection address (00H-1FH), the address and length of protection bit is appoint by parameters. CRT-310 handle 8 bit of protection as a byte. Every protection bit corresponds to a byte of SLE4442.

Protection bit=0, already protected and can not write data any more

Protection bit=1, have no protection and can write data again

The contents (32bit) of the protection memory can be read with the following command.

Ex). "CS3"+00B0010004

CREATOR

3.10.7 Data read from security memory on SLE4442

Command

"C"	53H	33H	00H	B0H	02H	abH	cdH	efH…

Positive response

"P"	53H	33H	st0	st1	data

Negative response

"N"	53H	33H	e0	e1

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

cd H : the length of bytes of data to read

CRT-310 handles the data of all 32bits in the security memory as the data on 4bytes.

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

The contents (32bit) of the security memory can be read with the following command.

Ex). "CS3"+00B0020004

3.10.8 Data write to main memory on SLE4442

Command

"C"	53H	33H	00H	D0 H	00H	abH	cdH	efH…

Positive response

"P"	53H	33H	st0	st1	data

Negative response

"N"	53H	33H	e0	e1

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

cd H: the length of bytes of data 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 are written in the whole area of the main memory is shown in the following.

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

CREATOR

3.10.9 Data write with protection bit on SLE4442

Command

"C"	53H	33H	00H	D0H	01H	abH	cdH	efH…

Positive response

"P"	53H	33H	st0	st1	data

Negative response

"N"	53H	33H	e0	e1

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

cd H: the length of bytes of data 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 byte0, data on the address 00H on the main memory are protected.

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

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

Ex). "CS3"+00D001100120

After command execution, CRT-310 returns with 9000H (Successful) or sw1+sw2 (Fail) as the result.

CRT-310 reads data first from the main memory, and it is compared with the value that it was received. When they are different, writing protection isn't begun.

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

CREATOR

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

Command

"C"	53H	33H	00H	D0H	02H	abH	cdH	efH…

Positive response

"P"	53H	33H	st0	st1	data

Negative response

"N"	53H	33H	e0	e1

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

cd H: the length of bytes of data 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. All 32bits are handled as 4bytes. How to change the password is as the following. (Change password as 123456H)

Ex). "CS3"+ 00D0020103123456

After command execution, CRT-310 returns response with 9000H (Successful) or sw1+sw2 (Fail) in the result.

Notes: Better not to write, because the Error-counter is always allowed to write and easily make a failure. Error-Counter is controlled when password is checked.

CREATOR

3.10.11 Verification data present to SLE4442

Command

"C"	53H	33H	00H	20H	03H	01H	03H	efH…

Positive response

"P"	53H	33H	st0	st1	data

Negative response

"N"	53H	33H	e0	e1

Notes: ef H: the data to compare (3bytes)

Before changing data, password must be check

Because this function should be made effective, the issue of the next command is necessary.

Ex). "CS3"+0020030103xxxxxx (xxxxxx: security code 3bytes)

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

A user must know password at least when a user wants to rewrite the data on SLE4442 card. Error-Counter can be reset in the zero if password is given to SLE4442 card properly. 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.

CREATOR

3.10.12 SLE4428 Control

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

In this case, CRT-310 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-310 returns a positive response with response data 9000H like from the IC card. When an error occurs during the communication with SLE4442, CRT-310 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 Validation error
6FH	02H	Key Validation error and Lock
6BH	00H	Address overflow
67H	00H	Operation length overflow

3.10.13 Data Reading of main-memory of SLE4428

Command

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

Positive response

"P"	53H	34H	st0	st1	data

Negative response

"N"	53H	34H	e0	e1

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

de H: the number of bytes of data to read

CRT-310 read data from main memory of SLE4428 through abcH and deH

The capacity of the main memory is 1024bytes.

When De="00" Data to read means 256bytes.

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

ex). "CS4"+00B0000000

CREATOR

3.10.14 Reading of protection-bit of SLE4428

Command

“C”	53H	34H	00H	B0H	1aH	bcH	deH

Positive response

“P”	53H	34H	st0	st1	data

Negative response

“N”	53H	34H	e0	e1

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

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

SLE4428 have 1024byte in main memory and correspondingly have 1024bit of protection bit. The machine will read 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, can write data

The command to read all protection bit of SLE4428 is

Ex). "CS4"+00B0100080

CREATOR

3.10.15 Data writing to main-memory of SLE4428

Command

"C"	53H	34H	00H	D0H	0aH	bcH	deH	fgH…

Positive response

"P"	53H	34H	st0	st1	data

Negative response

"N"	53H	34H	e0	e1

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

de H : the number of bytes of data to write

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

Writes data in the main memory and returns 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 data are written is shown in the following.

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

After command execution, CRT-310 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, password1 and password2. Please don't write any data to these units, otherwise the card will be scraped.

CREATOR

3.10.16 Written with protection-bit

Command

"C"	53H	34H	00H	D0 H	2aH	bcH	deH	fgH…

Positive response

"P"	53H	34H	st0	st1	data

Negative response

"N"	53H	34H	e0	e1

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

de H: the number of bytes of data 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-310 returns response with 9000H (Successful) or sw1+sw2 (Fail) as the result.

CRT-310 reads data first from the main memory, and it is compared with the value that it was received.

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

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

3.10.17 Verification of password present to SLE4428

Command

"C"	53H	34H	00H	20H	00H	00H	02H	efH…

Positive response

"P"	53H	34H	st0	st1	data

Negative response

"N"	53H	34H	e0	e1

Notes: ef H: the data to compare (2bytes)

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

Because this function should be made effective, the issue of the next command is necessary.

Ex). "CR4"+ 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. When error-counter reduces to zero, the card will lock and scrap.

CREATOR

3.10.18 Modify Password of SLE4428

HOST Command:

"C"	53H	34H	00H	24H	00H	00H	02H	efH

Positive Response:

"P"	53H	34H	st0	st1	data

Negative Response:

"N"	53H	34H	e0	e1

Modify password of SLE4428

Notes ef: Password data that need to change(2 byte)

data: =9000H Modify successfully

data: =6F00H Fail to modify

Modify SLE4428 password as 55H，AAH

The command format is

Ex). "CS4"+002400000255AA

CREATOR

3.11 I2C Memory Card Control Command

3.11.1 Activate I2C memory card

Command

"C"	54H	30H	Wrd	Vcc

Positive response

"P"	54H	30H	st0	st1	Sti

Negative response

"N"	54H	30H	e0	e1

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

CRT-310 supplies a power supply (Vcc), Clock (CLK), Reset (RST).

Including:

Wrd set I2C 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 I2C card type when operation 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, no Set parameter in command is equal to Set=30H

CREATOR

3.11.2 Deactivate I2C memory card

Command

“C”	54H	31H

Positive response

“P”	54H	31H	st0	st1

Negative response

“N”	54H	31H	e0	e1

CRT-310 stops supplying a power supply (Vcc), Clock (CLK), Reset (RST).

CREATOR

3.11.3 Inquire Status of I2C memory card

Command

“C”	54H	32H

Positive response

“P”	54H	32H	st0	st1	Sti

Negative response

“N”	54H	32H	e0	e1

This command is used to inquire status of I2C card and return status by Sti.

Sti meanings:

Sti=30 H	No I2C 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

CREATOR

3.11.4 I2C Control

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

In this case, CRT-310 recognizes the meaning of the command data, and execute the treatment related to the card by controlling hardware.

After the command was executed properly, CRT-310 returns a positive response with response data 9000H like from the IC card. When an error occurs during the communication with I2C, CRT-310 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
6BH	00H	Address overflow
67H	00H	Operation length overflow

Write/Read I2C 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

CREATOR CONFIDENTIAL

3.11.5 Read data from I2C

Command

“C”	54H	33H	00H	B0H	abH	cdH	efH

Positive response

“P”	54H	33H	st0	st1	Data

Negative response

“N”	54H	33H	e0	e1

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 of data to read

CRT-310 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 I2C address up limit.

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

Ex). "CU3"+00B000000

3.11.6 Write data to I2C

Command

“C”	54H	34H	00H	D0H	abH	cdH	efH	ghH...

Positive response

“P”	54H	34H	st0	st1	Data

Negative response

“N”	54H	34H	e0	e1

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

gh H : the data to write first (the head data of the data on ef H bytes)

CRT-310 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 I2C address up limit.

The example which data on 8bytes are written into I2C

ex). "CU3"+ 00D0000008 + Write Data (8bytes)

After command execution, CRT-310 returns response with 9000H or sw1+sw2 as the result.

3.12 Contactless IC card Operation

3.12.1 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 Dard 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-310 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 activate, CRT-310return:

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

CREATOR

Select (ATS)

Protocol and parameter selection request (PPSR) / PPS start (PPSS)

When ISO/IEC 14443 Type A card successfully activated, CRT-310 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-310 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 Philps 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

CREATOR

3.12.2 Deactivate RFID card

Command

“C”	60H	31H

Positive response

“P”	60H	31H	st0	st1

Negative response

“N”	60H	31H	e0	e1

Deactivate RFID card and Output signal to antenna is closed.

3.12.3 Inquire status of RFID card

Command

“C”	60H	32H

Positive response

“P”	60H	32H	st0	st1	sti	stj

Negative response

“N”	60H	32H	e0	e1

Inquire status of RFID sti,stj:

sti	stj	Specification
‘0’	‘0’	Deactivated RFID
‘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

CREATOR

3.12.4 Mifare card control

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

In this case, CRT-310 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-310 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-310 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
6BH	00H	Address overflow
67H	00H	Operation length overflow

3.12.5 Key verification

Command

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

Positive response

"P"	60H	33H	st0	st1	rdata

Negative response

"N"	60H	33H	e0	e1

Download key to CRT-310 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 negtive response with " sw1+sw2")

CREATOR

3.12.6 Verify key from EEPROM

Command

“C”	60H	33H	00H	21H	ks	sn

Positive response

“P”	60H	33H	st0	st1	rdata

Negative response

“N”	60H	33H	e0	e1

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

Download key via command mentioned in 9.13.4.4

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)

CREATOR

3.12.7 Modify sector key (KEY A)

Command

“C”	60H	33H	00H	D5H	00H	sn	lc	pdata

Positive response

“P”	60H	33H	st0	st1	rdata

Negative response

“N”	60H	33H	e0	e1

Modify sector key (key A)

This command only can modify KEY A, an d 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 negatives response with “ sw1+sw2”)

CREATOR

3.12.8 Download password to EEPROM

Command

“C”	60H	33H	00H	D0H	ks	sn	lc	pdata

Positive response

“P”	60H	33H	st0	st1	rdata

Negative response

“N”	60H	33H	e0	e1

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

CREATOR

3.12.9 Read sector data

Command

"C"	60H	33H	00H	B0H	sn	bn	le

Positive response

"P"	60H	33H	st0	st1	rdata

Negative response

"N"	60H	33H	e0	e1

Read block and sequence blocks from RFID card

sn(1 byte): sector number

bn(1 byte): block number

le(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 have one block in each sector，every block have 4 byte data. S50,S70 have16 byte data in each block.

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

Ultralight Card: sn=00H-0FH, bn=00H, le=01H-0FH

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

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

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

CREATOR

3.12.10 Write sector data

Command

“C”	60H	33H	00H	D1H	sn	bn	lc	wdata

Positive response

“P”	60H	33H	st0	st1	rdata

Negative response

“N”	60H	33H	e0	e1

Read block and sequence blocks from RFID card

sn(1 byte): sector number

bn(1 byte): block number

le(1 byte): block number

wdata: block to write (n byte)

rdata(2 byte): return data

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

Notes：

1. Ultralight Card only have one block in each sector，every block have 4 byte data. S50,S70 have16 byte data in each block
2. Ultralight Card,Mifare 1k(S50), Mifare 4k (S70) card card range of capacity is shown as below:

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

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

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

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

   (S70 card the last 8 sector has 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 note write last block and CRT-310 also will prohibit writing last block.

3.12.11 Initialization

Command

"C"	60H	33H	00H	D2H	sn	bn	lc	wdata

Positive response

"P"	60H	33H	st0	st1	rdata

Negative response

"N"	60H	33H	e0	e1

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

(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 have 16 blocks each)

CREATOR

3.12.12 Read value

Command

“C”	60H	33H	00H	B1H	sn	bn

Positive response

“P”	60H	33H	st0	st1	rdata

Negative response

“N”	60H	33H	e0	e1

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

(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)

CREATOR

3.12.13 Increment

Command

"C"	60H	33H	00H	D3 H	sn	bn	lc	wdata

Positive response

"P"	60H	33H	st0	st1	rdata

Negative response

"N"	60H	33H	e0	e1

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(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

(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)

CREATOR

3.12.14 Decrement

Command

“C”	60H	33H	00H	D4H	sn	bn	lc	wdata

Positive response

“P”	60H	33H	st0	st1	rdata

Negative response

“N”	60H	33H	e0	e1

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

(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)

CREATOR

3.12.15 Type A RFID card communication

Command

"C"	60H	34H	C-APDU

Positive response

"P"	60H	34H	st0	st1	R-APDU

Negative response

"N"	60H	34H	e0	e1

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.

3.12.16 Type B RFID card communication

Command

"C"	60H	35H	C-APDU

Positive response

"P"	60H	35H	st0	st1	R-APDU

Negative response

"N"	60H	35H	e0	e1

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.

CREATOR

3.13 Shutter related operation

3.13.1 LED setting

HOST Command:

"C"	80H	Pm	LED

Positive Return:

"P"	80H	Pm	st0	st1

Negative Return:

"N"	80H	Pm	e0	e1

This is to control the lights (red and green) in entry to on or off

PM=31H： Red light control

PM=32H： Green light control

LED=30H： On

LED=31H： Off

LED=32H： glitter（cycle is 2sec. on for 1 sec., off for 1sec.）

CREATOR

3.14 Easy-damage Part Counter

3.14.1 Read Counter

Command

"C"	A1H	30H	Sc

Positive response

"P"	A1H	30H	st0	st1	ICRW_CNT(8 byte)

Negative response

"N"	A1H	30H	e0	e1

Read easy-damage part counter

Sc=30H Shutter open times

Sc=31H Magnetic head pass times

Sc=32H IC contact use times

ICRW_CNT (8 Byte), the time is presented by ASCII.

EX). 1000. ICRW_CNT="30 30 30 30 31 30 30 30"

3.14.2 Initialization Counter

Command

"C"	A1H	31H	Sc

Positive response

"P"	A1H	31H	st0	st1	ICRW_CNT(8 byte)

Negative response

"N"	A1H	31H	e0	e1

Read easy-damage part counter

Sc=30H Shutter open times

Sc=31H Magnetic head pass times

Sc=32H IC contact use times

ICRW_CNT (8 Byte), the time is presented by ASCII

EX). 1000. ICRW_CNT="30 30 30 30 31 30 30 30"

CREATOR

3.15 Read Serial Number of CRT-310

3.15.1 Read serial number

Command

"C"	A2H	30H

Positive response

"P"	A2H	30H	st0	st1	ICRW_SN

Negative response

"N"	A2H	30H	e0	e1

Length of CRT-310serial number (0-18byte)

ICRW_SN: CRT-310 serial number

CREATOR

3.16 Read CRT-310 configuration

Command

“C”	A3H	30H

Positive response

“P”	A3H	30H	st0	st1	ICRW_Config

Negative response

“N”	A3H	30H	e0	e1

CRT-310 configuration specification：ICRW_Config: Read machine configuration information

Address	Name	Value	Description
00H	S1		CRT Reader Type option
		“1”	S1 =“1”
01H~03H	S2/S3/S4 (3 Byte)		User Code option
		“V40”	CRT version
04H	S5		Card r/w type option
		“I”	IC card r/w
		“C”	RFID card r/w
		“M”	Mag card r/w
		“P”	Mag card r/w
		“E”	IC + RFID card r/w
		“F”	Mag + RFID card r/w
		“G”	Mag + IC card r/w
		“H”	Mag + IC + RFID card r/w
05H	S6		Interface type option
		“R”	RS-232Interface type
		“U”	USB Interface type
06H	S7		Mag card write type
		“R”	Mag card read only
		“L”	Low-Co mag card write
		“H”	High-Co mag card write
07H	S8		Shutter type option
		“0”	Not Shutter
		“D”	“D” type Shutter
		“E”	“E” type Shutter
		“F”	“F” type Shutter
08H	S9		SAM option
		“0”	Not SAM
		“1”	SAM 1
		“2”	SAM 2
		“3”	SAM 3
		“4”	SAM 4
		“5”	SAM 5

3.17 Read CRT-310 version information

HOST Command

“C”	A4H	30H

Positive response

“P”	A4H	30H	st0	st1	Rev

Negative response

“N”	A4H	30H	e0	e1

Read CRT-310 version information.

Pm=30H Read machine software information

Ex): Rev =“C310_V4.0_A_100629”

CREATOR

3.18 Capture Card Counter Control

3.18.1 Read Capture Card counter

Command

"C"	A5H	30H

Positive response

"P"	A5H	30H	st0	st1	Count(2 byte)

Negative response

"N"	A5H	30H	e0	e1

After reset capture card counter with initialization command, every time capture one card, counter plus one

Count= "00" ~ "99"

Counter overflow will return machine status (e1,e0= "50" Counter overflow error)

3.18.2 Set initial value of card counter

Command

"C"	A5H	31H	Count(2 byte)

Positive response

"P"	A5H	31H	st0	st1

Negative response

"N"	A5H	31H	e0	e1

Set initial value of capture card counter.

Count= "00" ~ "99"

Count value range (0-99)

Maximum is 99 pieces of card

CREATOR