CRT-591-M001 communication protocol

Catalog

1. SERIAL PORT CONTROL SPECIFICATION： 5

1.1.1 Communication format 5

1.1.2 Communication control method 5

1.2 COMMUNICATION FORMAT AND CONTROL CHARACTER 5

1.2.1 Send command package format 5

1.2.2 Successful responsive package format and character 6

1.2.3 Failed responsive package format and character 6

1.3 ADDRESS SET FOR MULTI-UNITS COMMUNICATION： 7

1.4 COMMUNICATION METHOD: 8

1.4.1 Ordinary Operation : (command and response) 8

1.4.2 Irregular operation : (command and response) 8

2. COMMAND LIST:（INCLUDING STATUS AND ERROR CODE） 10

2.1.1 Command list 10

2.1.2 Status code information format： 12

2.2 **E1, E0 ERROR CODE TABLE** 12

3. COMMAND SPECIFICATION: 15

3.1 CARD DISPENSER OPERATION 15

3.1.1 Reset (Initialization) 15

3.1.2 Status Request Command 15

3.1.3 Move card: 16

3.1.4 Entry Command: 16

3.2 CPU CARD OPERATION: 17

3.2.1 CPU Card Reset (Activate): 17

3.2.2 CPU Card Power off: 18

3.2.3 Inquire CPU Card Status 18

3.2.4 T=0 protocol CPU Card APDU Operation 18

3.2.5 T=1 Protocol CPU Card APDU Operation 19

3.2.6 CPU Card Warm Reset 20

3.2.7 T=1, T=0 CPU Card Protocol Automatic Communication 21

3.3 SAM(SECURE APPLICATION MODULE) CONTROL COMMAND 22

3.3.1 Active SAM Command: 22

3.3.2 Deactivate SAM Command 22

3.3.3 Inquire SAM Status Command 23

3.3.4 SAM Communication T=0 23

3.3.5 SAM Communication T=1 24

3.3.6 SAM Warm Reset 24

3.3.7 Auto-Check SAM Card T=0/T=1 Protocol 25

3.3.8 Select SAM *25*
3.4 SLE4442/4428 CARD OPERATION 26
3.4.1 SLE4442/4428 card reset (activation): *26*
3.4.2 Deactivate SLE4442/4428 : *26*
3.4.3 Inquire status of SLE4442/4428: *26*
3.4.4 SLE4442 Control: *27*
3.4.4.1 Data read from main memory on SLE4442： 27
3.4.4.2 Data read from protection memory on SLE4442： 27
3.4.4.3 Data read from security memory on SLE4442 28
3.4.4.4 Data write main memory on SLE4442: 28
3.4.4.5 Data write to security memory on SLE4442: 30
3.4.4.6 Verification data present to SLE4428: 30
3.4.5 SLE4428 control： *31*
3.4.5.1 Data Reading of main-memory of SLE4428： 31
3.4.5.2 Reading of protection-bit of SLE4428： 32
3.4.5.3 Data writing to main-memory of SLE4428： 32
3.4.5.4 Verification of SLE4428 with protecting： 33
3.4.5.5 Written with protection-bit： 34
3.4.5.6 Verification of password present to SLE4428: 34
3.5 I2C MEMORY CARD OPERATION： 35
3.5.1 Activate I2C memory card： *35*
3.5.2 Deactivate I2C memory card： *35*
3.5.3 Inquire Status of I2C memory card *36*
3.5.4 I2C operation： *36*
3.5.4.1 Read data from I2C: 37
3.5.4.2 Write data to I2C: 38
3.6 **CONTACTLESS IC CARD OPERATION：** 39
3.6.1 Activated contactless IC card： *39*
3.6.2 Deactivate RFID card： *41*
3.6.3 Inquire status of RFID card： *41*
3.6.4 MIFARE 1 CARD CONTROL 42
3.6.4.1 Key verification: 42
3.6.4.2 Verify key from EEPROM: 42
3.6.4.3 Modify sector key (KEY A): 43
3.6.4.4 Download password to EEPROM: 43
3.6.4.5 Read sector data: 44
3.6.4.6 Write sector data: 44
3.6.4.7 Initialization: 45
3.6.4.8 Read value 46
3.6.4.9 Increment: 46
3.6.4.10 Decrement: 47
3.6.5 Type A RF card communication: *48*
3.6.5.1 APDU Operate 48

3.6.6 Type B RFcard communication: *48*
3.6.6.1 APDU Operate 48
3.6.7 Serial number: *48*
3.6.8 Read CRT-591 configuration *49*
3.6.9 Error-card Bin Counter Control: *49*
3.6.9.1 Read error-card bin counter 49
3.6.9.2 Set initial value of error-card bin 49
3.6.10 Reset PC/SC reader *50*

Revisions record:

version	Date	content
1.0	02/07/2013	Initial release

1. Serial port control specification：

1.1.1 Communication format

Baud rate(BPS)： 9600/192000/38400/57600BPS (Automatically scan)

Communication method: Asynchronous

Transmission method： Half duplex, support multi-unit communication (16 units max)

Data frame structure：

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

Start bit: 1 bit

Data length: 8 bit

Check bit: none

Stop bit: 1 bit

Character code： ASCII 8 bit code

1.1.2 Communication control method

Dispenser is a slave component, executes operation according to text(command) received from HOST.

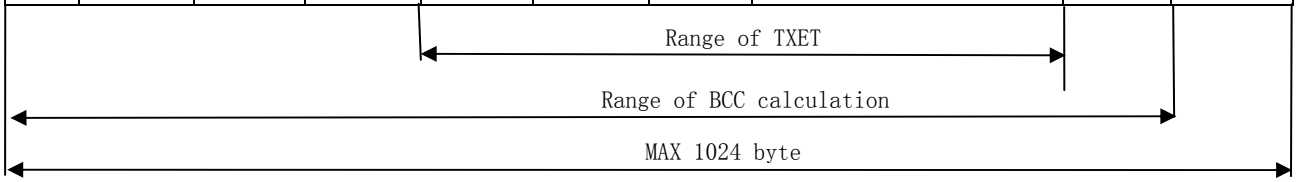
Character reference

STX (F2H)	Start of text
ETX (03H)	End of text
ACK (06H)	Acknowledge
NAK (15H)	Negative acknow
EOT (04H)	Clear the line
ADDR	Address character

1.2 Communication format and control character

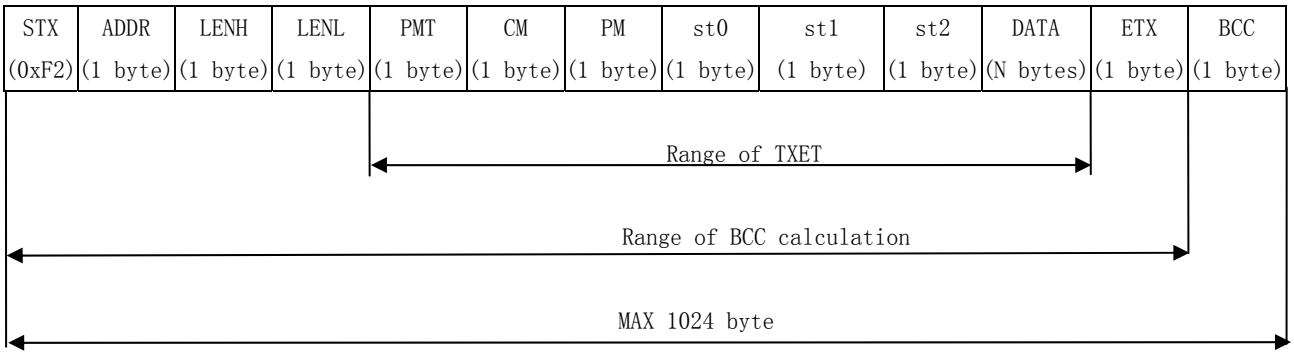
1.2.1 Send command package format

STX (0xF2)	ADDR (1 byte)	LENH (1 byte)	LENL (1 byte)	CMT (1 byte)	CM (1 byte)	PM (1 byte)	DATA (N bytes)	ETX (1 byte)	BCC (1 byte)



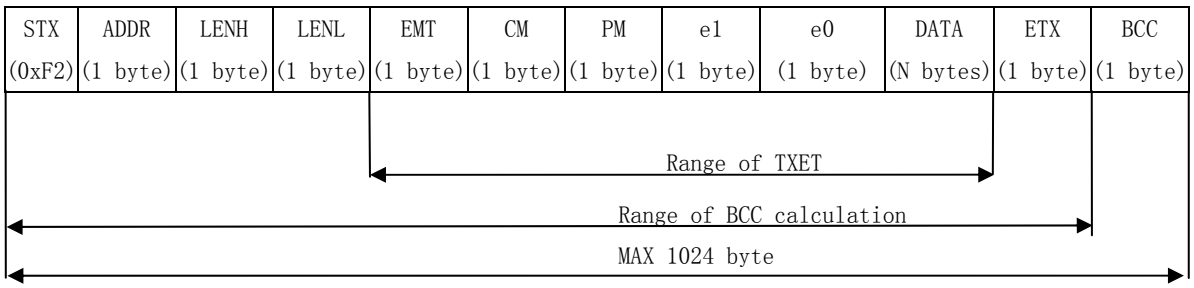
STX (F2H)	Start of text
LENH (1 byte)	Length of high byte of text
LENL (1 byte)	Length of low byte of text
CMT	Command head (‘C’ , 43H)
CM	Specify as command
PM	Command parameter
DATA	Transmission data (N byte, N=0 ~ 512)
ETX (03H)	End of text
BCC (1 bytes)	XOR

1.2.2 Successful responsive package format and character



STX (F2H)	Start of text
LENH (1 byte)	Length of high byte of text
LENL (1 byte)	Length of low byte of text
PMT	Return command head ('P' , 50H)
CM	Specify as command
PM	Return command parameter
St0, st1, st2	Return dispenser status code
DATA	Return command data (N byte, N=0~512)
ETX (03H)	End of text
BCC (1 bytes)	XOR

1.2.3 Failed responsive package format and character



STX (F2H)	Start of text
LENH (1 byte)	Length of high byte of text
LENL (1 byte)	Length of low byte of text
EMT	Return command head (N' , 45H)
CM	Specify as command
PM	Return command parameter
e1, e0	Return dispenser error code
DATA	Return command data (N byte, N=0~512)
ETX (03H)	End of text
BCC (1 bytes)	XOR

1.3 Address set for multi-units communication：

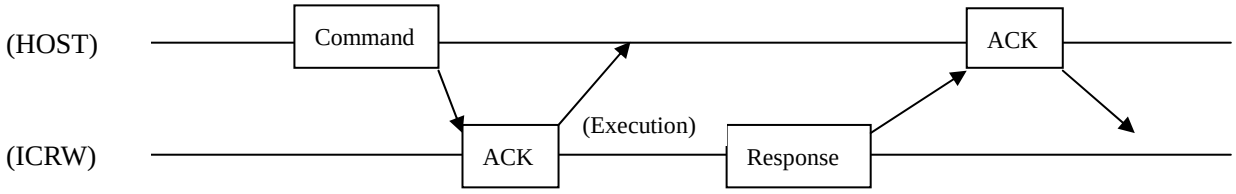
ADDR(multi-units communication)：Address every unit by 4 dip switch on the main board：

Address	DIP switch				ADDR
	4	3	2	1	
0#	ON	ON	ON	ON	00H
1#	ON	ON	ON	OFF	01H
2#	ON	ON	OFF	ON	02H
3#	ON	ON	OFF	OFF	03H
4#	ON	OFF	ON	ON	04H
5#	ON	OFF	ON	OFF	05H
6#	ON	OFF	OFF	ON	06H
7#	ON	OFF	OFF	OFF	07H
8#	OFF	ON	ON	ON	08H
9#	OFF	ON	ON	OFF	09H
10#	OFF	ON	OFF	ON	0AH
11#	OFF	ON	OFF	OFF	0BH
12#	OFF	OFF	ON	ON	0CH
13#	OFF	OFF	ON	OFF	0DH
14#	OFF	OFF	OFF	ON	0EH
15#	OFF	OFF	OFF	OFF	0FH

The default address for single device in ex-work is set as 00H, each device has unique address.

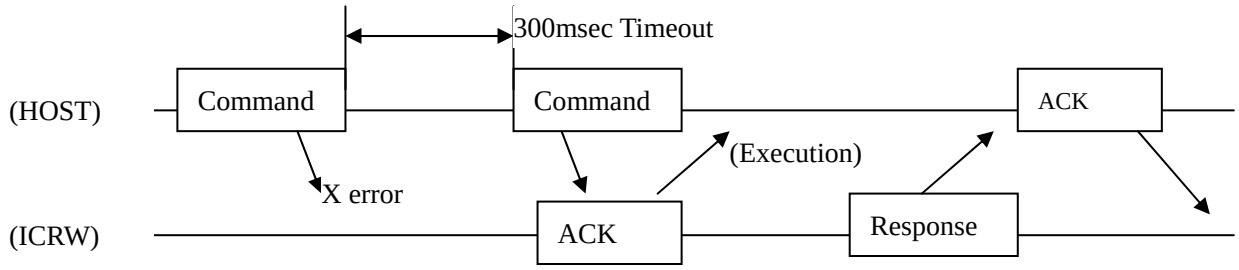
1.4 Communication method:

1.4.1 Ordinary Operation : (command and response)

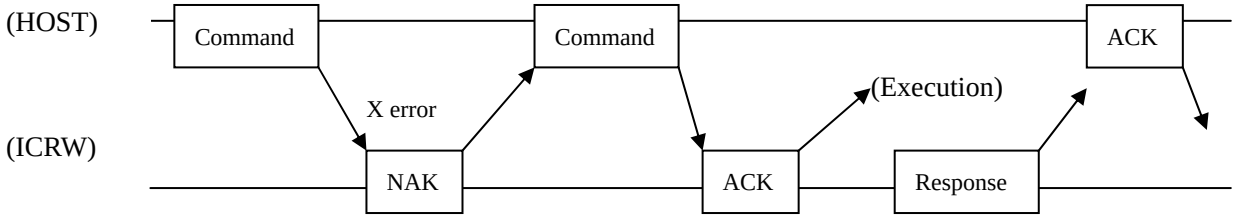


1.4.2 Irregular operation : (command and response)

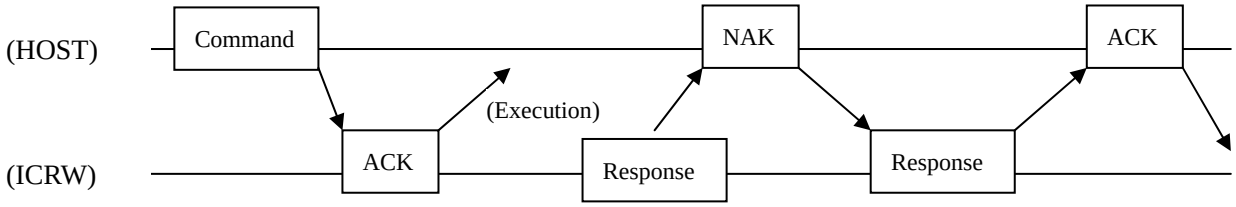
Case 1



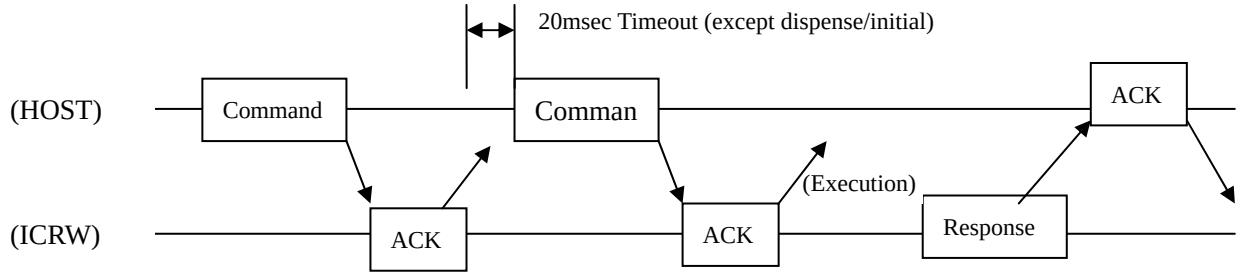
Case 2



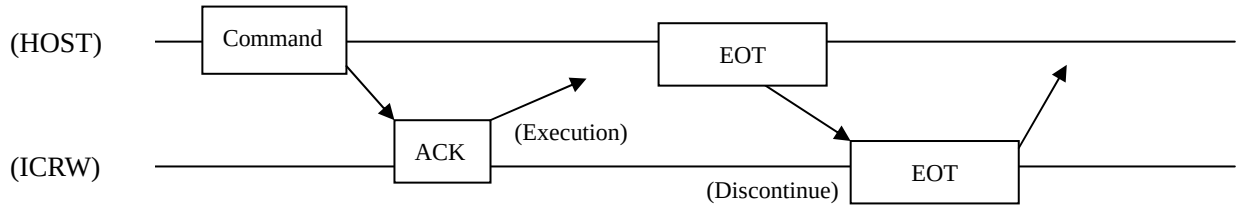
Case 3



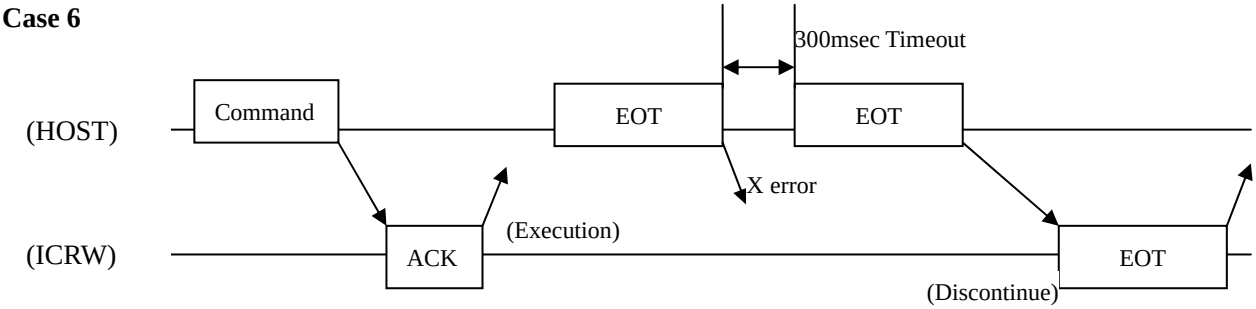
Case 4



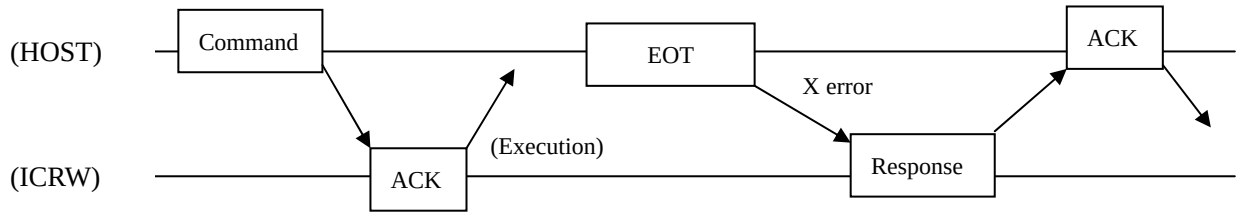
Case 5



Case 6



Case 7



2. command list:（including status and error code）

2.1.1 Command list

Chapter	Command	Function	CM	PM	description
9.1	INITIALIZE	Initialize CRT-591-M	30H	30H	If card is inside, move card to card holding position
				31H	If card is inside, capture card to error card bin
				33H	If card is inside, does not move the card.
				34H	Same as 30H and retract counter will work.
				35H	Same as 31H and retract counter will work.
				37H	Same as 33H and retract counter will work.
9.2	STATUS REQUEST	Inquire status	31H	30H	Report CRT-591M status
				31H	Report sensor status
9.3	CARD MOVE	Card movement	32H	30H	Move card to card holding positon
				31H	Move card to IC card position
				32H	Move card to RF card position
				33H	Move card to error card bin
				39H	Move card to gate
9.4	CARD ENTRY	From output gate	33H	30H	Enable card entry from output gate
				31H	Disable card entry from ouput gate
9.5	CARD TYPE	ICCard/RFCard TypeCheck	50H	30H	Autocheck ICCardType
				31H	Autocheck RFCardType
9.6	CPUCARD CONTROL	CPU Card Applicatio Opertion	51H	30H	CPUCard cold reset
				31H	CPUCard power down
				32H	CPUCard status check
				33H	T=0 CPUCard APDU data exchange
				34H	T=1 CPUCard APDU data exchange
				38H	CPUCard hot reset
				39H	Auto distinguish T=0/T=1 CPUCard APDU data exchange
9.7	SAM CARD CONTROL	SAMCard Application Operation	52H	30H	SAMCard cold reset
				31H	SAMCard down power
				32H	SAMCard status check
				33H	T=0 SAMCard APDU data

					exchange
				34H	T=1 SAMCardAPDU data exchange
				38H	SAMCard hot reset
				39H	Auto distinguish T=0/T=1 SAMCardAPDU data exchange
				40H	Choose SAMCard stand
9.8	SLE4442/4428CARD CONTROL		53H	30H	SLE4442/4428Card reset
				31H	SLE4442/4428Card power down
				32H	Browse SLE4442/4428Card status
				33H	Operate SLE4442Card
				34H	Operate SLE4428Card
9.9	IC MEMORY CARD	24C01—24C256Card Operation	54H	30H	ICCard reset
				31H	ICCard down power
				32H	Check ICCard status
				33H	Read ICCard
				34H	Write ICCard
9.10	RFCARD CONTROL (13.56 MHZ)	Mifare standard card Type A & B T=CL protocol operation	60H	30H	RF Card startup
				31H	RF Card down power
				32H	RF Card operation status check
				33H	Mifare standard Card read/write
				34H	Type A standard T=CLCard APDU data exchange
				35H	Type B standard T=CLCard APDU data exchange
				39H	RF Card enable/disable
9.11	Card SERIAL NUMBER		A2H	30H	Read Card Serial number
9.12	Read CARD CONFIG		A3H	30H	Read Card configuration information
9.13	READ CRT-591M VERSION		A4H	30H	Read Card software version information
9.14	RECYCLE BIN COUNTER		A5H	30H	Read number of counter of Card error card bin
				31H	Initiate card error card bin counter

2.1.2 Status code information format：

Card Status Code (st0,st1,st2）

st0	Content
“0”	No Card in CRT-591M
“1”	One Card in gate
“2”	One Card on RF/IC Card Position

st1	Content
“0”	No Card in stacker
“1”	Few Card in stacker
“2”	Enough Cards in card box

st2	Content
“0”	Error card bin not full
“1”	Error card bin full

2.2 e1, e0 Error Code Table

e1,e0 code	Content
“00”	Reception of Undefined Command
“01”	Command Parameter Error
“02”	Command Sequence Error
“03”	Out of Hardware Support Command
“04”	Command Data Error (error in communication package data)
“05”	IC Card Contact Not Release
“06”	
“07”	
“08”	
“09”	
“10”	Card Jam
“11”	
“12”	sensor error
“13”	Too Long-Card
“14”	Too Short-Card
“15”	
“16”	
“17”	
“18”	
“19”	

“20”	
“21”	
“22”	
“23”	
“24”	
“25”	
“26”	
“27”	
“28”	
“29”	
“30”	
“31”	
“32”	
“33”	
“34”	
“35”	
“36”	
“37”	
“38”	
“39”	
“40”	Disability of Recycling card
“41”	Magnet of IC Card Error
“42”	
“43”	Disable To Move Card To IC Card Position
“44”	
“45”	Manually Move Card
“46”	
“47”	
“48”	
“49”	
“50”	Received Card Counter Overflow
“51”	Motor error
“52”	
“53”	
“54”	
“55”	
“56”	
“57”	
“58”	
“59”	
“60”	Short Circuit of IC Card Supply Power

“61”	Activiation of Card failure
“62”	Command Out Of IC Card Support
“63”	
“64”	
“65”	Disablity of IC Card
“66”	Command Out Of IC Current Card Support
“67”	IC Card Transmittion Error
“68”	IC Card Transmittion Overtime
“69”	CPU/SAM Non-Compliance To EMV Standard
“A0”	Empty-Stacker
“A1”	Error card bin full
“A2”	
“A3”	
“A4”	
“A5”	
“A6”	
“A7”	
“A8”	
“A9”	
“B0”	Not Reset

3. Command Specification:

3.1 Card dispenser operation

3.1.1 Reset (Initialization)

HOST Command (TXET):

"C"	30H	Pm

Positive response (TXET):

"P"	30H	Pm	st0	st1	st2	Rev_type

Negative response (TEXT):

"N"	30H	Pm	e1	e0

This command should be received before any other command after card dispenser is power on, otherwise card dispenser can not execute any other commands; Card dispenser will auto detect ICRW and Host's BAUD and adapt corresponding BAUD when it receive this command for the first time. On receiving this command, card dispenser will clear all error code, Disable card entry from ouput gate and return FW version.

Pm: Command parameter

If there is no card in card dispenser, engine will rotate slightly to clear up card in stacker

If there are cards in card dispenser, the disposal is show as below:

=30H Move the card to Gate portion

=31H Capture card to reject-stacker

=33H If card is inside card dispenser, does not move the card

=34H Same as pm=30H, and Retract counter will work

=35H Same as pm=31H, and Retract counter will work

=37H Same as pm=33H, and Retract counter will work

Rev_type: FW version, "CRT-591-M001"

3.1.2 Status Request Command

HOST Command

"C"	31H	Pm

Positive response

"P"	31H	Pm	st0	st1	st2	Sensor(10 byte)

Negative response

"N"	31H	Pm	e1	e0

Pm=30H Report current status (see 2.2 for more detail)

Pm=31H Report current status and sensor status (8 Bytes) as following table:

Sensor	status	status
S1	30H No card	31H With card
S2	30H No card	31H With card
S3	30H No card	31H With card
S4	30H No card	31H With card
S5	30H No card	31H With card
S6	30H No card	31H With card
S7	30H No card	31H With card
S8	Reserve	

3.1.3 Move card:

HOST command:

“C”	32H	Pm

Positive response:

“P”	32H	Pm	st0	st1	st2

Negative response:

“N”	32H	Pm	e1	e0

Pm=30H move card to card holding position

Pm=31H move card to IC card read/write position (dispense from stacker)

Pm=32H move card to RF read/write position

Pm=33H retract card to error card bin

Pm=39H move card out of gate

If card can not move to specified position, CRT-591-M will return Card jam error

Note: When execute Capture card command, if error card bin is full, CRT-591M will return error card bin error

3.1.4 Entry Command:

HOST command:

“C”	33H	Pm

Positive response:

“P”	33H	Pm	st0	st1	st2

Negative response:

“N”	33H	Pm	e1	e0

After set card input from gate available, if insert card from gate, CRT-591-M will carry the card to RF

Card operation position.

Pm=30HEnable card input from gate

Pm=31HDisable card input from gate

Note: Execute reset command, CRT-591-M will disable card input from gate.

3.2 CPU card operation:

3.2.1 CPU Card Reset **(Activate):**

HOST Command:

"C"	51H	30H	Vcc

Positive response:

"P"	51H	30H	st0	st1	st2	Type	ATR

Negative response:

"N"	51H	30H	e1	e0	Type	ATR

To cold reset IC card. The ICRW supplies power (VCC) and clock (CLK) , Card activated, return ATR.

Vcc=30H: CRT-591M supplies with +5V to VCC and activates in line with the EMV2000 ver4.0.

Vcc=33H: CRT-591M supplies with +5V to VCC and activates in line with the ISO/IEC7816-3.

Vcc=35H: CRT-591M supplies with +3V to VCC and activates in line with the ISO/IEC7816-3.

In case there is no Vcc word, it will have 30H as default value.

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

Type: CPU Card protocol Type

=30H T=0 protocol CPUCard

=31H T=1 protocol CPUCard

Format of ATR:

TS	TO	TA1	TB1	…	TCK

3.2.2 CPU Card Power off:

HOST Command:

“C”	51H	31H

Positive response:

“P”	51H	31H	st0	st1	st2

Negative response:

“N”	51H	31H	e1	e0

Power off operation to CPU Card.

Power off operation to power on and activated CPU card.

3.2.3 Inquire CPU Card Status

HOST Command:

“C”	51H	32H

Positive response:

“P”	51H	32H	st0	st1	st2	Sti

Negative response:

“N”	51H	32H	e1	e0

ICRW 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 ICCard power error, return e1,e0= “60”

3.2.4 T=0 protocol CPU Card APDU Operation

HOST Command:

“C”	51H	33H	C-APDU

Positive response:

“P”	51H	33H	st0	st1	st2	R-APDU

Negative response:

“N”	51H	33H	e1	e0

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 error “60” is returned when a power failure is detected.

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

If ICC does not respond within Working Wait Time, CRT-591M deactivates an IC card and error code “63” is sent.

If any other protocol error occurs, CRT-591M deactivates an IC card and error code “64” is sent.

If HOST tries to communicate before an IC card activation, error code “65” is sent.

Note: If you want to more about T=0 APDU format. Plese refer to ISO/IEC7816-3 and COS command

3.2.5 T=1 Protocol CPU Card APDU Operation

HOST Command:

“C”	51H	34H	C-APDU

Positive response:

“P”	51H	34H	st0	st1	st2	R-APDU

Negative response:

“N”	51H	34H	e1	e0

This exchanges data between CPU card by protocol T=1

CRT-591-M should following T=1 protocol to combinate C-APDU as I-block and send it to CPU card.CPU card should return R-APDU to HOST

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. CRT-591 returns “R-APDU” data to HOST

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 error “60” is returned when a power failure is detected.

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

If ICC does not respond within Working Wait Time, CRT-591M deactivates an IC card and error code “63” is sent.

If any other protocol error occurs, CRT-591M deactivates an IC card and error code “64” is sent.

If HOST tries to communicate before an IC card activation, error code “65” is sent.

Note: If you want to more about T=0 APDU format. Plese refer to ISO/IEC7816-3 and COS command

3.2.6 CPU Card Warm Reset

HOST Command:

“C”	51H	38H

Positive response:

“P”	51H	38H	st0	st1	st2	Type	ATR

Negaitive response:

“N”	51H	38H	e1	e0

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

Type: CPU Card communication protocol

=30H T=0 Protocol

=31H T=1 Protocol

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

HOST Command:

“C”	51H	39H	C-APDU

Positive response:

“P”	51H	39H	st0	st1	st2	R-APDU

Negative response:

“N”	51H	39H	e1	e0

Protocol is recognized automatically. Set Data to “C-APDU”. CRT-591M returns “R-APDU” data to HOST.

An error “60” is returned when a power failure is detected.

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

If ICC does not respond within Working Wait Time, CRT-591M deactivates an IC card and error code “63” is sent.

If any other protocol error occurs, CRT-591M deactivates an IC card and error code “64” is sent.

If HOST tries to communicate before an IC card activation, error code “65” is sent.

3.3 SAM(Secure Application Module) Control Command

3.3.1 Active SAM Command:

HOSTCommand:

"C"	52H	30H	Vcc

Positive response:

"P"	52H	30H	st0	st1	st2	Type	ATR

Negative response:

"N"	52H	30H	e1	e0	Type	ATR

The CRT-591 supplies power (VCC) and clock (CLK), 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: ICRW supplies with +5V to VCC and activates in line with the EMV2000 ver4.0.

Vcc=33H: ICRW supplies with +3V to VCC and activates in line with the ISO/IEC7816-3.

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

Incase there is no Vcc, it will have 30H as default value

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

Notes : There will be error and return ATR & Type when reset in line with EMV return

When a power failure is recognized while a power supply is supplied to the card, error code "60" is returned.

3.3.2 Deactivate SAM Command

HOST Command:

"C"	52H	31H

Positive response:

"P"	52H	31H	st0	st1	st2

Negative response:

"N"	52H	31H	e1	e0

This deactivates SAM

Power off operation to power on and activated SAM card.

3.3.3 ınquire SAM Status Command

HOST Command:

“C”	52H	32H

Positive response:

“P”	52H	32H	st0	st1	st2	Sti	Stj

Negatiive response:

“N”	52H	32H	e1	e0

CRT-591-M return 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)

An error “60” is returned when a power failure is detected.

3.3.4 SAM Communication T=0

Command

“C”	52H	33H	C-APDU

Positive response:

“P”	52H	33H	st0	st1	st2	R-APDU

Negative response:

“N”	52H	33H	e1	e0

This exchanges data between SAM by protocol T=0

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

If ICC does not respond within Working Wait Time, CRT-591-M deactivates an IC card and error code “63” is sent.

If any other protocol error occurs, CRT-591-M deactivates an IC card and error code “64” is sent.

If HOST tries to communicate before an IC card activation, error code “65” is sent.

Note: If you want to more about T=0 APDU format. Plese refer to ISO/IEC7816-3 and COS command

3.3.5 SAM Communication T=1

Command

“C”	52H	34H	C-APDU

Positive response:

“P”	52H	34H	st0	st1	st2	R-APDU

Negative response:

“N”	52H	44H	e1	e0

This exchange data between SAM by protocol T=1

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

If ICC does not respond within Working Wait Time, CRT-591-M deactivates an IC card and error code “63” is sent.

If any other protocol error occurs, CRT-591-M deactivates an IC card and error code “64” is sent.

If HOST tries to communicate before an IC card activation, error code “65” is sent.

Note: If you want to more about T=1 APDU format. Plese refer to ISO/IEC7816-3 and COS command

3.3.6 SAM Warm Reset

Command

“C”	52H	38H

Positive response:

“P”	52H	38H	st0	st1	st2	Type	ATR

Negative response:

“N”	52H	38H	e1	e0

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

Type: SAM protocol type

=30H T=0 Protocol

=31H T=1 Protocol

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

Command

“C”	52H	39H	C-APDU

Positive response

“P”	52H	39H	st0	st1	st2	R-APDU

Negative response

“N”	52H	39H	e1	e0

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

If ICC does not respond within Working Wait Time, CRT-591-M deactivates an IC card and error code “63” is sent.

If any other protocol error occurs, CRT-591-M deactivates an IC card and error code “64” is sent.

If HOST tries to communicate before an IC card activation, error code “65” is sent.

3.3.8 Select SAM

Command

“C”	52H	40H	SAMn

Positive response

“P”	52H	40H	st0	st1	st2

Negative response

“N”	52H	40H	e1	e0

HOST can select SAM 1,2,3,4 or 5.

Sel = 30H: SAM 1.

Sel = 31H: SAM 2. (option)

Sel = 32H: SAM 3. (option)

Sel = 33H: SAM 4. (option)

Sel = 34H: SAM 5. (option)

SAM command is effective only in the module selection.
When Initialize command is executed, SAM 1 will be selected.

3.4 SLE4442/4428 card operation

3.4.1 SLE4442/4428 card reset (activation):

HOST command:

“C”	53H	30H

Positive response:

“P”	53H	30H	st0	st1	st2	ATR(4 byte)

Negative response:

“N”	54H	30H	e1	e0

The CRT-591-M supplies power (VCC), clock(CLK), then reset(RST),after reset, return ATR.

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

SLE4442 Card ATR=“92H，23H，10H，91H”

3.4.2 Deactivate SLE4442/4428 :

HOST command :

“C”	53H	31H

Positive response :

“P”	53H	31H	st0	st1	st2

Negative response :

“N”	53H	31H	e1	e0

The CRT-591-M stop suppling power (VCC), clock(CLK), and then reset(RST) release.

3.4.3 Inquire status of SLE4442/4428:

HOST command :

“C”	53H	32H

Positive response :

“P”	53H	32H	st0	st1	st2	Sti

Negative response :

“N”	54H	32H	e1	e0

This command is used to inquire the status of card ,will return Sti after the command successfully execute.

Sti= 30H SLE4442/4428 Deactivated

Sti= 31H SLE4442 Activated

Sti= 32H SLE4428 Activated

3.4.4 SLE4442 Control:

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

In this case, the CRT-591-M 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-591-M returns a positive response with response data 9000H; When an error occurs during the communication ,the CRT-591-M returns a positive response with status information in response data "sw1+sw2" which is base on ISO/IEC 7816-3 T=0 standard.

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

3.4.4.1 Data read from main memory on SLE4442：

HOST command:

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

Positive response:

"P"	53H	33H	st0	st1	st2	data

Negative response:

"N"	53H	33H	e1	e0

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

cd: the length of bytes of data to read

CRT-591-M read data from the main memory of SLE4442,and transmits data on abH and cdH . The capacity of the main memory is 256 byte. All the contents of the main memory can be with the following commandEx). "CR3"+00B0000000

3.4.4.2 Data read from protection memory on SLE4442：

HOST command:

"C"	53H	33H	00H	B0H	01H	abH	cdH

Positive response:

"P"	53H	33H	st0	st1	st2	data

egative response:

"N"	53H	33H	e1	e0

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

cd: the length of bytes of data to read

SLE4442 card of all 32 bits data in the protection memory as the data on 4 bytes. Corresponding protection address is 00H—1FH。All the SLE442 of protection memory can be read with the following command Ex). "CR3"+00B0010004

3.4.4.3 Data read from security memory on SLE4442

HOST Command:

“C”	53H	33H	00H	B0H	02H	abH	cdH	efH…

Positive response:

“P”	53H	33H	st0	st1	st2	data

Negative response:

“N”	53H	33H	e1	e0

Note： ab: the start address to read data in the main memory

cd: the length of bytes of data to read

To read the security data of SLE4442 card.

SLE4442 card with 4bytes security area，1 byte code error data and 3 byte password values (the password data can be read after correct check password). All the SLE442 card security area data can be read with the following command

Ex). “CR3”+00B0020004

3.4.4.4 Data write main memory on SLE4442:

HOST command:

“C”	53H	33H	00H	D0H	00H	abH	cdH	efH…

Positive response:

“P”	53H	33H	st0	st1	st2	data

Negative response:

“N”	53H	33H	e1	e0

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

cd: the length of bytes of data to write

ef: the data to write first (cdH byte)

To read the data on SLE4442 main memory，write the appointed data in main memory，will return the operating results after the CRT-591-M has been wrote the date with validation. Before write the main memory,must validate the SLE442 password.

The capacity of the main memory is 256 byte, the byte number cd=00H of data to write means 256bytes.

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

Ex). “CR3”+00D000000+Write data(256 byte)

After command execution, CRT-591-M returns response with 9000H or sw1, sw2 as the result.

If the addressed data on main memory is protected by the protect status, data is not allow.

Data write to protection memory on SLE4442

HOST command:

“C”	53H	33H	00H	D0H	01H	abH	cdH	efH…

Positive response :

“P”	53H	33H	st0	st1	st2	data

Negative response:

“N”	53H	33H	e1	e0

notes： ab: The start address to write data in the main memory

cd: the length of bytes of data to write

ef: the data to write first (cdH byte)

TO write protect unit of memory for main memory of protection .Before execute the command，much to validate the SLE442 card password. The address of the main memory that the protection is possible is 00H—1FH。Each protection condition of the 00H—1FH main memory can be controlled with 32 bit in the protection memory. if byte0 of the protection memory byte0 is “1” ,data on the address 00H of the main memory are protected.

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

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

Ex). “CR3”+00D001100120

After command execution ,CRT-591-M return with 9000H (successful) or sw1,sw2(fail) as the result.

CRT-591-M readd data first from the main memory ,and it is compared with the value that it was received.When this is wrong ,writing is not begun.

Protection condition can be set up at one time in the data which continued in the main memory.

3.4.4.5 Data write to security memory on SLE4442:

Command

“C”	53H	33H	00H	D0H	02H	abH	cdH	efH…

Positive response

“P”	53H	33H	st0	st1	st2	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 of data to write

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

After a password check is finished normally, the Reference-Data area of 3byte can be changed.

All 32bits are handled as 4bytes. How to change the Reference-Data is as the following.

ex). "CR3"+ 00D0020103123456

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

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

3.4.4.6 Verification data present to SLE4428:

Command

“C”	53H	33H	00H	20H	03H	01H	03H	efH…

Positive response

“P”	53H	33H	st0	st1	st2	data

Negative response

“N”	53H	33H	e1	e0

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). “CR3”+0020030103xxxxxx (xxxxxx : security code 3bytes)

Card will verify password between card and 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 value of Error-Counter is 2 or less

3.4.5 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-591M 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-591M returns a positive response with response data 9000H like from the IC card. When an error occurs during the communication with SLE4442, CRT-591M 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

3.4.5.1 Data Reading of main-memory of SLE4428：

Command

“C”	53H	34H	00H	B0 H	0aH	bcH	deH

Positive response

“P”	53H	34H	st0	st1	st2	data

Negative response

“N”	53H	34H	e1	e0

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

de H : the number of bytes of data to read

CRT-591-M read data from main memory of SLE4428 through abcH and deH

The capacity of the main memory is 1024bytes.

De="00"

Data to read means 256bytes.

The head part of the main memory can be read with the following command.

ex). "CR4"+00B0000000

3.4.5.2 Reading of protection-bit of SLE4428：

Command

“C”	53H	34H	00H	B0 H	10H	abH	cdH

Positive response

“P”	53H	34H	st0	st1	st2	data

Negative response

“N”	53H	34H	e1	e0

Notes: ab H : read the start address to read the image of protection data of the main memory

cd H : read data operation length

The protection conditions of 1024bytes of main-memory are changed into the data on 1024bits, and it is read.

1024bits is equivalent to 128bytes. (1024 = 128 x 8)

Data to read first become protection information to address (000H-007H) of main-memory in the case of abH=00H.

The contents of the whole protection image can be read with the following command.

ex). "CR4"+00B0100080

The device read protection-bit of SLE4428 according to abH。

3.4.5.3 Data writing to main-memory of SLE4428：

Command

“C”	53H	34H	00H	D0H	0aH	bcH	deH	fgH…

Positive response

“P”	53H	34H	st0	st1	st2	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 of data to write

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

The device writes data in the main memory. it 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 that data are written in from the address 100H is shown in the following.

ex). "CR4"+ 00D0010000 + Write Data (256byte)

After command execution, ICRW returns response with 9000H or sw1+sw2 as the result. If the addressed data on main memory is protected, the write operation is not available。

3.4.5.4 Verification of SLE4428 with protecting：

Command

“C”	53H	34H	00H	D0 H	1aH	bcH	deH	fgH…

Positive response

“P”	53H	34H	st0	st1	st2	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 of data to write

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

The device writes data in the main memory. It returns a result after written data are checked Before doing this operation, password check must be done

3.4.5.5 Written with protection-bit:

Command

“C”	53H	34H	00H	D0 H	2aH	bcH	deH	fgH…

Positive response

“P”	53H	34H	st0	st1	st2	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 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, ICRW returns response with 9000H or sw1+sw2 as the result.

The device reads data first from the main memory, and it is compared with the value that it was received.

When this is wrong, writing isn't begun. Protection condition can be set up at a time in the data which continued in the main memory。

3.4.5.6 Verification of password present to SLE4428:

Command

“C”	53H	34H	00H	20H	00H	00H	02H	efH…

Positive response

“P”	53H	34H	st0	st1	st2	data

Negative response

“N”	53H	34H	e1	e0

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 cad if they want to change the data in SLE4442, Error-Counter can be reset in the zero from 7 or less than 7. when error-counter is reset as zero, lock the card

3.5 I2C Memory Card operation：

3.5.1 Activate I2C memory card：

Command

“C”	54H	30H	Wrd	Vcc

Positive response

“P”	54H	30H	st0	st1	st2

Negative response

“N”	54H	30H	e1	e0

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

Device 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

Wrd =31 H To activate 24C01card

Wrd =32 H To activate 24C02 card

Wrd =33 H To activate 24C04 card

Wrd =34 H To activate 24C08 card

Wrd =35 H To activate 24C16 card

Wrd =36 H To activate 24C32 card

Wrd =37 H To activate 24C64 card

Wrd =38 H To activate 24C128 card

Wrd =39 H To activate 24C256 card

Vcc choose voltage to card

Vcc=30H 5V

Vcc=31H 3V

Vcc is optional parameter, no Set parameter in command is equal to Set=30H

3.5.2 Deactivate I2C memory card：

Command

“C”	54H	31H

Positive response

“P”	54H	31H	st0	st1	st2

Negative response

“N”	54H	31H	e1	e0

The device stops supplying a power supply (Vcc), Clock(CLK), Reset(RST)

3.5.3 Inquire Status of I2C memory card

HOST Command

“C”	54H	32H

Positive response

“P”	54H	32H	st0	st1	st2	Sti

Negative response

“N”	54H	32H	e1	e0

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

3.5.4 I2C operation：

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

In this case, CRT-591 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-591 returns a positive response with response data 9000H like from the IC card. When an error occurs during the communication with I2C, CRT-591 returns a positive response with status information in response data "sw1+sw2” which is base on ISO/IEC 7816-3 T=0

Sw1	Sw2	说　明
90H	00H	操作成功 Success
6FH	00H	操作失败 Fail
6BH	00H	操作地址溢出 Address overflow
67H	00H	操作长度溢出 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

3.5.4.1 Read data from I2C:

HOST Command

“C”	54H	33H	00H	B0H	abH	cdH	efH

Positive response

“P”	54H	33H	st0	st1	st2	Data

Negative response

“N”	54H	33H	e1	e0

Value:

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

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

ef: The number of bytes of data to read

CRT-591 read efH length and return to HOST according to address specified by abH, cdH.

The length of efH can not be surpass the length of I2C address up limit.

When the following command is transmitted, data can be read from the I2C memory card. （read data on 8bytes from the card）

Ex). “CU3”+00B0000008

3.5.4.2 Write data to I2C:

HOST COMMAND:

"C"	54H	34H	00H	D0H	abH	cdH	efH	ghH…

Positive response:

"P"	54H	34H	st0	st1	st2	Data

Negative response:

"N"	54H	34H	e1	e0

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

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

ef: The number of bytes of data to write

gh: write data (efH byte)

CRT-591 write efH length and return to HOST according to address specified by abH, cdH.

The length of efH can not be surpass the length of I2C address up limit.

Ex). "CU3"+00B0000008+ write data(8 byte)

After command execute, return 9000H (operation success) or sw1,sw2(operation failure) result.

3.6 Contactless IC card Operation：

3.6.1 Activated contactless IC card：

HOST **Command**

“C”	60H	30H	Set1	Set2

(1) **Mifare One Card Positive Response**

“P”	60H	30H	st0	st1	st2	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	st2	Rtype	ATQA	UID_len	UID_data	SAK	ATS

14443 Type A Card Negative Response

“N”	60H	30H	e1	e0	Rtype	ATQA	UID_len	UID_data	SAK	ATS

(3) **14443 Type B Card Positive Response**

“P”	60H	30H	st0	st1	st2	Rtype	ATQB

14443 Type b Card B Negative Response

“N”	60H	30H	e1	e0	Rtype	ATQB

Activate RFID card

CRT-591-M 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. Anticollision
3. Select (SEL) / Unique Identifier (UID) & Select Acknowledge(SAK)

When Mifare card successfully activate, CRT-591return:

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. Anticollision
3. Select(SEL) / Unique Identifier(UID) & Select Acknowledge(SAK)
4. Request for answer to select (RATS) / Answer to Select(ATS)
5. Protcol and parameter selection request(PPSR) / PPS start(PPSS

When ISO/IEC 14443 Type A card successfully activated, CRT-591 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-591 return ATQB 12 byte(including following information):

50H, PUPI(4 byte) , App.data(4 byte), Protoclol info(3 byte)

Notes:

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

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

Rtype=4DH(‘M’) : 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

3.6.2 Deactivate RFID card：

HOST Command

“C”	60H	31H

Positive response

“P”	60H	31H	st0	st1	st2

Negative response

“N”	60H	31H	e1	e0

Deactivate RFIN card and Output signal to antenna is closed。

3.6.3 Inquire status of RFID card：

HOST Command

“C”	60H	32H

Positive response

“P”	60H	32H	st0	st1	st2	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

3.6.4 Mifare 1 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-591 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-591 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-591 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

3.6.4.1 Key verification:

HOST Command

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

Positive response

"P"	60H	33H	st0	st1	st2	rdata

Negative response

"N"	60H	33H	e1	e0

Download key to CRT-591 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

return data(positive response with data 9000H, and negtive response with " sw1+sw2").

3.6.4.2 Verify key from EEPROM:

HOST Command

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

Positive response

“P”	60H	33H	st0	st1	st2	rdata

Negative response

“N”	60H	33H	e1	e0

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

Download key via command mentioned in 9.10.4.4

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)

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

3.6.4.3 Modify sector key (KEY A):

HOST Command

“C”	60H	33H	00H	D5H	00H	sn	lc	pdata

Positive response

“P”	60H	33H	st0	st1	st2	rdata

Negative response

“N”	60H	33H	e1	e0

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 timemodify 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): positive response with data 9000H, and negtive response with “ sw1+sw2

3.6.4.4 Download password to EEPROM:

HOST Command

“C”	60H	33H	00H	D0H	ks	sn	lc	pdata

Positive response

“P”	60H	33H	st0	st1	st2	rdata

Negative response

“N”	60H	33H	e1	e0

Read key from EEPROM of RF 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.

negtive response sw1+sw2=6F00H

3.6.4.5 Read sector data:

HOST Command

“C”	60H	33H	00H	B0H	sn	bn	le

Positive response

“P”	60H	33H	st0	st1	st2	rdata

Negative response

“N”	60H	33H	e1	e0

Read block and sequence blocks from RF 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 negtive response with “ sw1+sw2

Notes：

1. Ultralight Card only have one block in one sector，every block have 4 byte data. S50, S70 have 16 byte data in one block.

2. Ultralight Card, Mifare 1k (S50), Mifare 1k (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 1k(S70): sn=00H-20H, bn=00H-03H, le=01H-04H

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

3.6.4.6 Write sector data:

HOST Command

“C”	60H	33H	00H	D1H	sn	bn	lc	wdata

Positive response

“P”	60H	33H	st0	st1	st2	rdata

Negative response

“N”	60H	33H	e1	e0

Read block and sequence blocks from RF 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 negtive response with " sw1+sw2

Notes：

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

2. Ultralight Card,Mifare 1k(S50), Mifare 1k (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 1k(S70): sn=00H-20H, bn=00H-03H, lc=01H-03H
sn=21H-27H, bn=00H-0FH, lc=01H-0FH
(S70 card last 8 sector have 16 blocks)

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-591M also will prohibid to write last block

3.6.4.7 Initialization:

HOST Command

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

Positive response

"P"	60H	33H	st0	st1	st2	rdata

Negative response

"N"	60H	33H	e1	e0

Initialization operation to RF card

sn(1 byte): sector number
bn(1 byte): block number
lc(1byte): lc=04H Initialization data length 1c=04H
wdata: Initialization data (4 byte)
rdata(2 byte): return data (positive response with data 9000H,and negative response with sw1+sw2(2 byte)

Notes：Mifare 1k(S50), Mifare 1k (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 1k(S70): sn=00H-20H, bn=00H-03H,
sn=20H-27H, bn=00H-0EH,
(S70 card last 8 sector have 16 blocks)

3.6.4.8 Read value

HOST Command

"C"	60H	33H	00H	B1H	sn	bn

Positive response

"P"	60H	33H	st0	st1	st2	rdata

Negative response

"N"	60H	33H	e1	e0

Read value operations to RF card

sn(1 byte): sector number

bn(1 byte): block number

rdata: return data (positive response with data (4 byte)+9000H, and negtive response with " sw1+sw2" (2 byte))

Notes: Mifare 1k(S50), Mifare 1k (S70) card operation sector

(Sector can not be out of range and last block can't be operated)

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

Mifare 1k(S70): sn=00H-20H, bn=00H-03H,

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

(S70 card last 8 sector have 16 blocks)

3.6.4.9 Increment:

HOST Command

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

Positive response

"P"	60H	33H	st0	st1	st2	rdata

Negative response

"N"	60H	33H	e1	e0

Increment operation to RF card

sn(1 byte): sector number

bn(1 byte): block number

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

wdata: increment data(4 byte)

rdata: return data

(positive response with data 9000H, and negtive response with " sw1+sw2")

Notes：Mifare 1k(S50), Mifare 1k (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 1k(S70): sn=00H-20H, bn=00H-03H,

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

(S70 card last 8 sector have 16 blocks)

3.6.4.10 Decrement:

HOST Command

“C”	60H	33H	00H	D4H	sn	bn	lc	wdata

Positive response

“P”	60H	33H	st0	st1	st2	rdata

Negative response

“N”	60H	33H	e1	e0

Decrement operation to RF sector

sn(1 byte): sector number

bn(1 byte): block number

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

wdata: Decrement data(4 byte)

rdata: return data

(positive response with data 9000H, and negtive response with “ sw1+sw2” (2 byte)

Notes：Mifare 1k(S50), Mifare 1k (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 1k(S70): sn=00H-20H, bn=00H-03H,

sn=20H-27H, bn=00H-0EH, (S70 card last 8 sector have 16 blocks)

3.6.5 Type A RF card communication:

3.6.5.1 APDU Operate

HOST Command

“C”	60H	34H	C-APDU

Positive response

“P”	60H	34H	st0	st1	st2	R-APDU

Negative response

“N”	60H	34H	e1	e0

This exchanges data between RF card by protocol RF 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.

3.6.6 Type B RFcard communication:

3.6.6.1 APDU Operate

HOST Command

“C”	60H	35H	C-APDU

Positive response

“P”	60H	35H	st0	st1	st2	R-APDU

Negative response

“N”	60H	35H	e1	e0

This exchanges data between RF card by protocol RF 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.

3.6.7 Serial number:

HOST Command

“C”	A2H	30H

Positive response

“P”	A2H	30H	st0	st1	st2	len	ICRW_SN

Negative response

“N”	A2H	30H	e1	e0

Len: read length of CRT-591serial number (0byte-18byte)

ICRW_SN: CRT-591 Serial number

3.6.8 Read CRT-591 configuration

HOST Command

“C”	A3H	30H

Positive response

“P”	A3H	30H	st0	st1	st2	ICRW_Config

Negative response

“N”	A3H	30H	e1	e0

3.6.9 Error-card Bin Counter Control:

3.6.9.1 Read error-card bin counter

HOST Command

“C”	A5H	30H

Positive response

“P”	A5H	30H	st0	st1	st2	Count(3 byte)

Negative response

“N”	A5H	30H	e1	e0

After reset error-card bin counter. Capture on card, counter one plus

Count= “000” ~ “999”

Counter overflow will return machine status (e1,e0= “50”)

3.6.9.2 Set initial value of error-card bin

HOST Command

“C”	A5H	31H	Count(3 byte)

Positive response

“P”	A5H	31H	st0	st1	st2

Negative response

“N”	A5H	31H	e1	e0

Set initial value of error-card bin.

Count= “000” ~ “999”

Count value range (0-999)

3.6.10 Reset PC/SC reader

HS Command

“C”	A6H	30H

Positive response

“P”	A6H	30H	st0	st1	st2

The command is to reset PC/SC reader。