Communication Protocol

CRT-711

Card Issuing/Collecting Machine

With RFID Card and Barcode Read/Write

VER 1.0

CREATOR (CHINA) TECH CO., LTD.

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

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

·Http://www.china-creator.com

Revision Log

Version	Revision Time	Content
1.0	2010.06.03	First Release

Contents

1. CRT-711 Com Port Control Principle

1. 1 Communication Character Format

1) Baud rate: 9,600/19200/38400/57600 BPS （Baud rate auto-identification）

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

3) Synchronous method: Asynchronous

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

Start bit: 1 bit

Data length: 8bit

Check bit: None

Stop bit: 1 bit

Character Code: ASCII 8 bit code

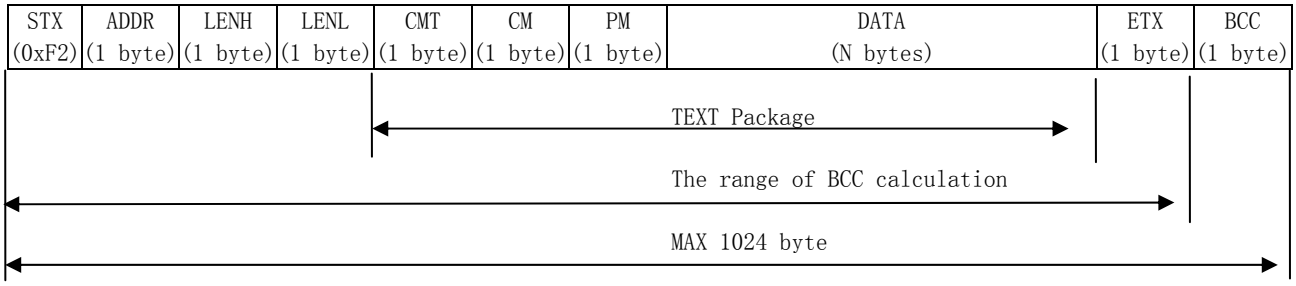
1.2 Transmission control method and characters

The machine is a driven part, operate after receive a valid command.
Reference control character:

STX (F2H)	Start character of data package
ETX (03H)	End character of data package
ACK (06H)	Acknowledge character
NAK (15H)	Negative character
EOT (04H)	Cancel character
ADDR	Machine address character

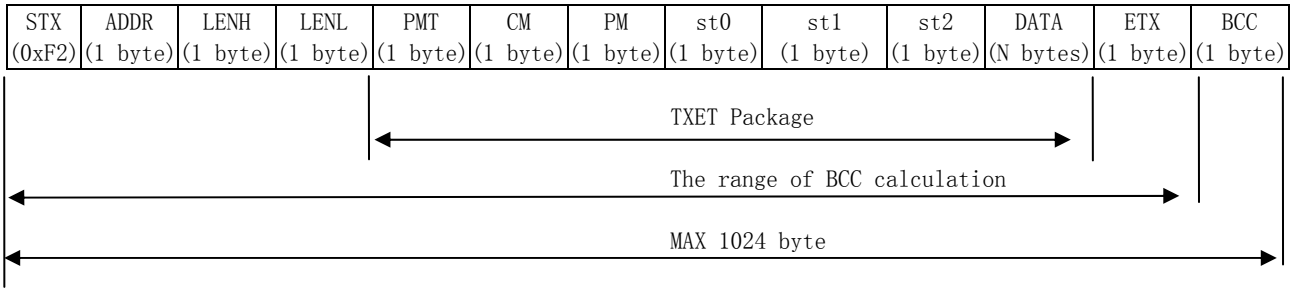
1.3 Communication Format and Control Character

1.3.1 Transmission package format and characters



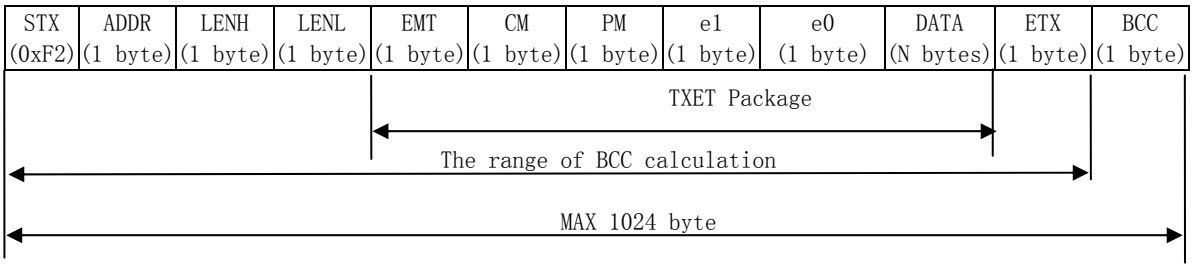
Code	Meaning
STX (F2H)	Start Character
LENH(1 byte)	Length of high byte of TEXT package
LENL(1 byte)	Length of low byte of TEXT package
CMT	Transmission Command Head (‘C’ , 43H)
CM	Transmission Command Character
PM	Transmission Command Parameter
DATA	Transmission command Data (N byte, N=0~512)
ETX (03H)	End Character
BCC(1byte)	BCC Parity

1.3.2 Successful responsive package format and character



Code	Meaning
STX (F2H)	Start Character
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, st2	Return command status code
DATA	Return command data (N byte, N=0~512)
ETX (03H)	End Character
BCC (1 byte)	BCC Parity

1.3.3 Negative responsive package format and character



Code	Meaning
STX (F2H)	Start Character
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', 45H)
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 Character
BCC (1 byte)	BCC Parity

1.3.4 Address according to Multi-unit communication

ADDR: Address word for each unit in multi-unit communication application

Unit	ADDR
0#	'0' (30H)
1#	'1' (31H)
2#	'2' (32H)
3#	'3' (33H)
4#	'4' (34H)
5#	'5' (35H)
6#	'6' (36H)
7#	'7' (37H)
8#	'8' (38H)
9#	'9' (39H)
10#	'A' (41H)
11#	'B' (42H)
12#	'C' (43H)
13#	'D' (44H)
14#	'E' (45H)
15#	'F' (46H)

1.3.5 DIP switch setting for multi-communication

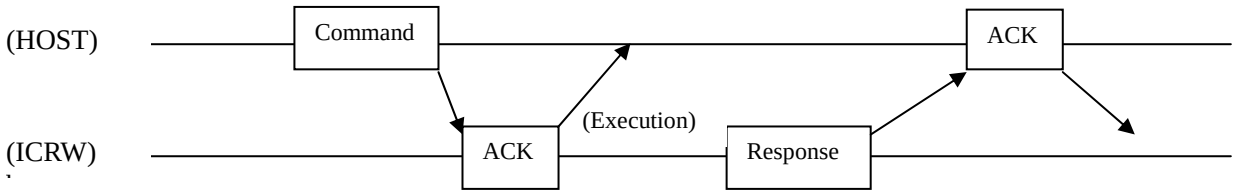
Setting address of each unit by dip switch

DIP Switch				Address
4	3	2	1	
ON	ON	ON	ON	0#
ON	ON	ON	OFF	1#
ON	ON	OFF	ON	2#
ON	ON	OFF	OFF	3#
ON	OFF	ON	ON	4#
ON	OFF	ON	OFF	5#
ON	OFF	OFF	ON	6#
ON	OFF	OFF	OFF	7#
OFF	ON	ON	ON	8#
OFF	ON	ON	OFF	9#
OFF	ON	OFF	ON	10#
OFF	ON	OFF	OFF	11#
OFF	OFF	ON	ON	12#
OFF	OFF	ON	OFF	13#
OFF	OFF	OFF	ON	14#
OFF	OFF	OFF	OFF	15#

The default address setting is #15 (Single-unit operation mode). For multi-unit operation mode, each unit must have unique address, the selection of each unit apply to its address word.

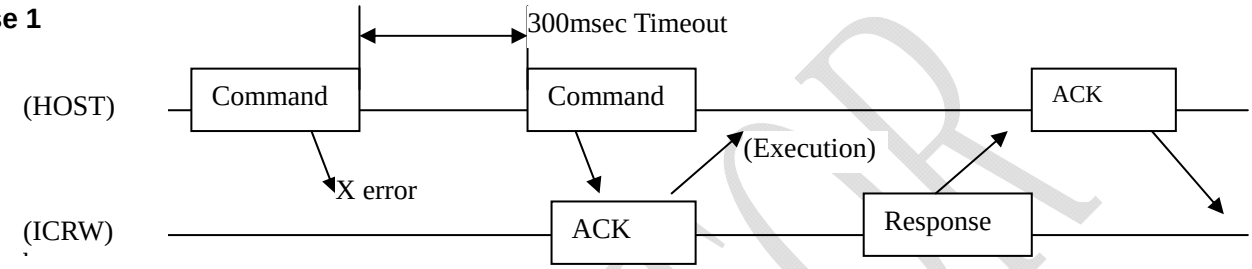
2. Communication Method

2.1 Ordinary operation

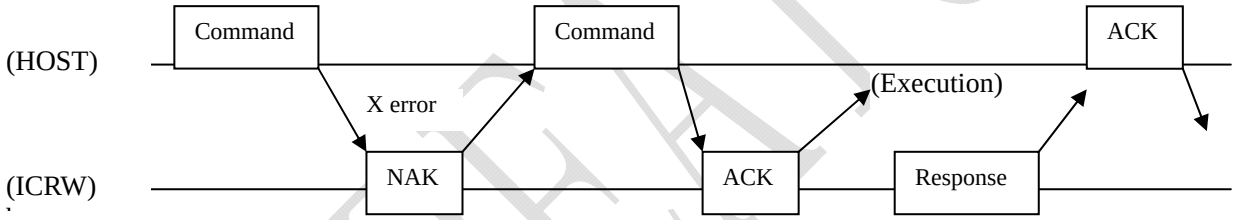


2.2 Irregular operation and back-up

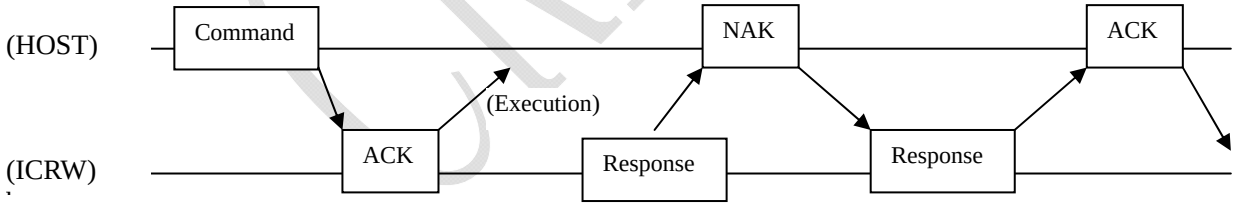
Case 1



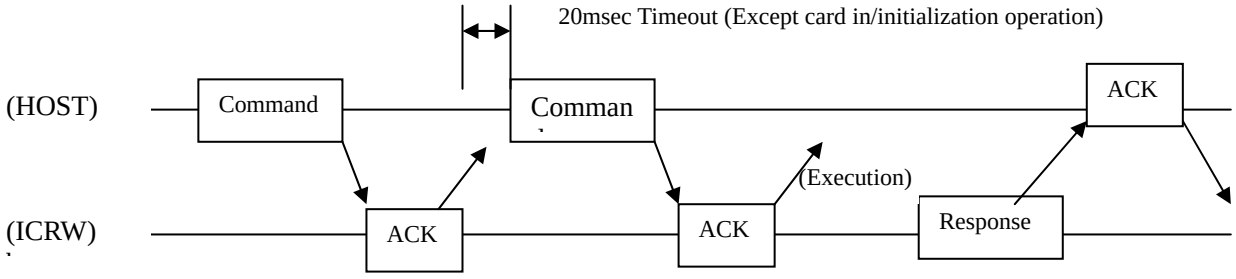
Case 2



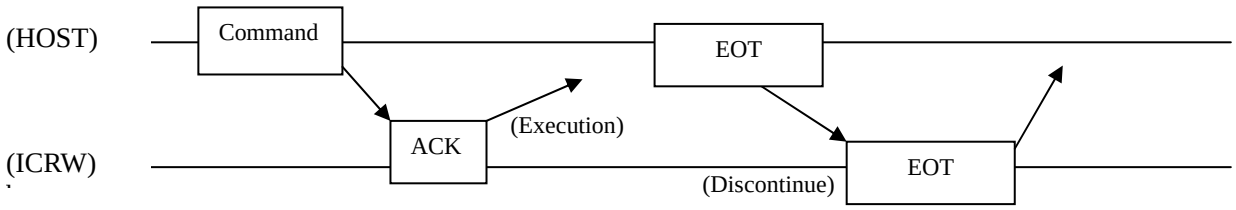
Case 3



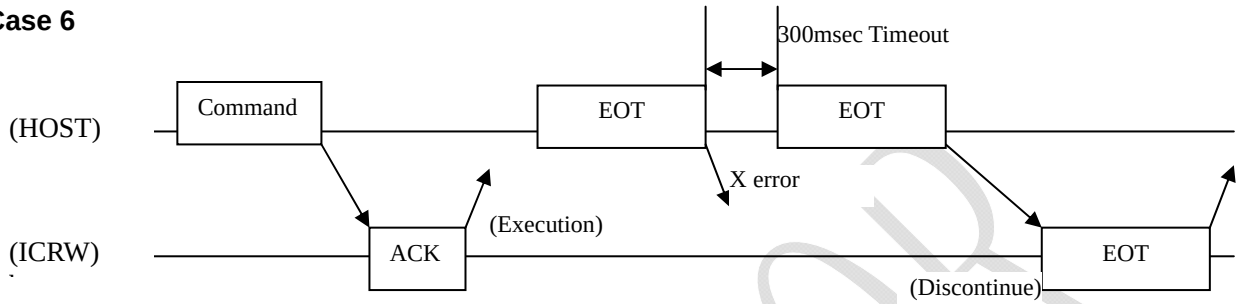
Case 4



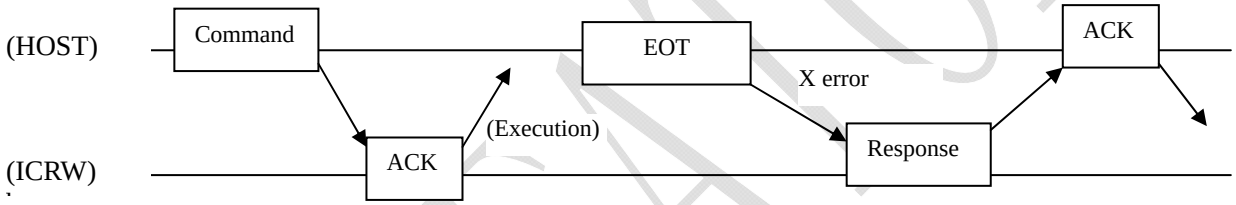
Case 5



Case 6



Case 7



3. Command List (Including status code and error status)

Chapter	Command	Function	CM	PM	Description
4.1	INITIALIZE	Initialize CRT-711	30H	30H	If card is inside, move card to front side card holding position
				31H	If card is inside, retract card to error card bin
				33H	If card is inside, does not move the card.
				34H	Same as 30H and eject card/error card bin counter will work.
				35H	Same as 31H and eject card/error card bin counter will work.
				37H	Same as 33H and eject card/error card bin counter will work.
4.2	STATUS REQUEST	Inquire status	31H	30H	Report machine status
				31H	Report sensor status
4.3	CARD MOVE	Card movement	32H	30H	Move card to front side card holding position
				33H	Move card to error card bin
				39H	Move card to front side without card holding position
4.4	CARD ENTRY		33H	30H	Enable card entry from front side
				31H	Disable card entry from front side
4.5	RFID CARD TYPE		50H	31H	Auto check RFID Card Type
4.6	SAM CARD CONTROL	SAM Card Operation	52H	30H	SAM Card cold reset
				31H	SAM Card power down
				32H	SAM Card status check
				33H	T=0 SAM Card APDU data exchange
				34H	T=1 SAM Card APDU data exchange
				38H	SAM Card hot reset
				39H	Auto distinguish T=0/T=1 SAM Card APDU data exchange
				40H	Select SAM card stand
4.7	RFID CARD CONTROL (13.56 MHz)	Mifare standard card Type A & B T=CL protocol operation	60H	30H	RFID Card initialization
				31H	RFID Card power down and release
				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
				39H	RFID card sleep/wake-up
4.8	Barcode Scan		70H	30H	Barcode Scan
4.9	Read Machine CONFIG information		A3H	30H	Read machine configuration information

4.10	READ machine VERSION		A4H	30H	Read machine software version information
4.11	Error card bin counter		A5H	30H	Read counter of error card bin
				31H	Initiate error card bin counter
4.12	Eject card counter		A6H	30H	Read counter of eject card
				31H	Initiate counter of eject card

3.1 Card Status Code

3.1.1 st0, st1, st2 status code

st0	Content
“0”	No Card in machine
“1”	One Card on bezel
“2”	One Card on RFID Card Position

st1	Content
“0”	No Card in error card bin
“1”	Cards in error card bin full

st2	Content
“0”	Reserve for extension function
“1”	Reserve for extension function

3.1.2 e1, e0 Error Code Table

e1,e0	Content
“00”	Undefined command
“01”	Command parameter error
“02”	Command execute sequence error
“03”	Command out of hardware support command
“04”	Command data error(TEXT content error)
“05”--“09”	
“10”	Card Jam in the machine
“11”-“49”	
“50”	Eject card / error card bin counter overflow
“51”-“59”	
“60”	Short circuit of SAM /RFID card power supply
“61”	Activation of SAM/RFID Card error
“62”	Command Out Of SAM/RFID Card Support
“63”	SAM/RFID card data error
“64”	
“65”	Card without initialization
“66”	Command out of IC card support
“67”	
“69”	SAM Non-Compliance To EMV Standard
“70”	Barcode scan error
“B0”	Machine haven’t reset yet
‘’A1”	Error card bin error

4. Command Specification

4.1 Reset (Initialization)

Command (TEXT):

“C”	30H	Pm

Positive response (TEXT):

“P”	30H	Pm	st0	st1	st2	Rev_type

Negative response (TEXT):

“N”	30H	Pm	e1	e0

This is the first command after power on, otherwise, other command can not be executed.

After it execute at first time, the machine will auto check and measure HOST baud rate.

CRT-711 is initialized in disable mode that card is not accepted by this command.

CRT-711 is in prohibit status and clear all error code before, and then return software version information.

Pm: Command parameter

If there is no card in CRT-711, engine will rotate slightly to clear up card in stacker.

If there are cards in CRT-711, the disposal is show as below:

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

31H: Retract card to error card bin

33H: If card is inside CRT-711, does not move the card.

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

35H: Same as pm=31H, and error card bin will work

37H: Same as pm=33H, and error card bin will work

Rev_type: software version, “CRT-711-V10”

4.2 Status Check Command

Command

"C"	31H	Pm

Positive response

"P"	31H	Pm	st0	st1	st2	Sensor(4 byte)

Negative response

"N"	31H	Pm	e1	e0

Pm=30H: Report current status about existence of card in the machine.

Pm=31H: Report current status about existence of card in the machine and also return information of sensor (4 byte)

The locations of sensor are referred to appearance drawing.

Sensor	Status
S1	30H No Card
	31H Have Card
S2	30H No Card
	31H Have Card
S3	30H No Card
	31H Have Card
S4	30H No Card
	31H Have Card

4.3 Carry Card Command

Command

"C"	32H	Pm	Set

Positive response

"P"	32H	Pm	st0	st1	st2

Negative response

"N"	32H	Pm	e1	e0

Pm=30H Move card to front side card holding position

Pm=33H Retract card to error card bin

(If there is sensor on error card bin, when error card bin is full, the machine will return error code 'A1')

Pm=39H Move card to the front side without card holding position

4.4 Front Entry Enable Command

Command

"C"	33H	Pm	Set

Positive response

"P"	33H	Pm	st0	st1	st2

Negative response

"N"	33H	Pm	e1	e0

Setting enable/disable of front entry

Pm=30H Enable card entry from front side

Pm=31H Disable card entry from front side

Set is optional parameter, if no set parameter, the entry setting is equal to Set=30H

Note: Execute reset command, CRT-711 will disable card entry from the front

4.5 Check RF Card Type

Command

“C”	50H	30H

Positive response

“P”	50H	30H	st0	st1	st2	Card_type

Negative response

“N”	50H	30H	e1	e0

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

Cart_type(2 byte)		Specification
‘0’	‘0’	Unknown RF 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

4.6 SAM Control Command

4.6.1 SAM Card Reset (Activation)

Command

"C"	52H	30H	Vcc

Positive response

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

Negative response

"N"	52H	30H	e1	e0	ATR

The CRT-711 supplies power (VCC) and clock (CLK) and reset (RST) signal to card. The card is activated and returns ATR.

Type: SAM protocol type

=30H T=0 SAM protocol

=31H T=1 SAM protocol

ATR(Answer To Reset) format:

TS	TO	TA1	TB1	...	TCK

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

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

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

Vcc is optional parameter. In case there is no Vcc, it will have Vcc=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.

4.6.2 Deactivate SAM Command

Command

"C"	52H	31H

Positive response

"P"	52H	31H	st0	st1	st2

Negative response

"N"	52H	31H	e1	e0

This deactivates SAM

4.6.3 Inquire SAM Status Command

Command

"C"	52H	32H

Positive response

"P"	52H	32H	st0	st1	st2	Sti	Stj

Negative response

"N"	52H	32H	e1	e0

The machine returns the SAM status 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 stand

Stj =31H Second SAM card stand (Optional)

Stj =32H Third SAM card stand (Optional)

Stj =33H Fourth SAM card stand (Optional)

Stj =34H Fifth SAM card stand (Optional)

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

4.6.4 SAM APDU operation T=0 protocol

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

The minimum length of C-APDU is 4 byte, the maximum is 261 byte, and the format is shown in the following:

CLA	INS	P1	P2	LC	Data1	……	Le

The minimum length of R-APDU is 2 byte, the maximum is 258 byte, and the format is shown in the following:

Data1	…..	Data(n)	Sw1	Sw0

If the power supply of IC card is failure, e1, e0="60"is sent.

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

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

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

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

Note: If you want to more about T=0 APDU format. Please refer to ISO/IEC7816-3, and for C-APDU command, please refer to COS command.

4.6.5 SAM APDU operation T=1 protocol

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.

The machine execute T=1 protocol C-APDU operation according to T=1 protocol standard. Integrate C-APDU as I-block and send it to SAM card, and SAM card retrieve R-ADPU from I-block and return to HOST.

A: Send C-APDU (Add block prologue, block epilogue, and block data as I-block to SAM card)

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
Block prologue			Block									Block epilogue

B: Return R-APDU (Retrieve I-block from SAM card and return block data to HOST)

I-block

Block prologue			Block									Block epilogue
NAD	PCB	LEN	CLA	INS	P1	P2	Lc	Data1	…	Data(Lc)	Le	EDC

R-APDU

CLA	INS	P1	P2	Lc	Data1	…	Data(Lc)	Le

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

If ICC does not respond within Working Wait Time, CRT-711 deactivates an IC card and e1, e0= "63" is sent.

If any other protocol error occurs, CRT-711 deactivates an IC card and e1, e0= "64" is sent.

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

Note: If you want to more about T=0 APDU format. Please refer to ISO/IEC7816-3, and for C-APDU command, please refer to COS command.

4.6.6 SAM Warm Reset

Command

"C"	52H	38H

Positive response

"P"	52H	38H	st0	st1	st2	Type	ATR

Negative response

"N"	52H	38H	e1	e0

The command executes in the case of IC card activation and return ATR

Type: SAM protocol type

=30H T=0 SAM Protocol

=31H T=1 SAM Protocol

If ATR information is not comply with protocol, the machine returns e1,e0="66" or "69"

4.6.7 Auto-Distinguish 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, "62"is sent.

If ICC does not respond within Working Wait Time, CRT-711 deactivates an IC card and e1, e0= "63" is sent.

If any other protocol error occurs, CRT-711 deactivates an IC card and e1, e0= "64" is sent.

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

4.6.8 Select SAM Stand

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.

SAMn = 30H: SAM 1.

SAMn = 31H: SAM 2. (Option)

SAMn = 32H: SAM 3. (Option)

SAMn = 33H: SAM 4. (Option)

SAM command is effective only in the PSAM module selection.

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

4.7 Contactless IC card Operation

4.7.1 Activated contactless IC card

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 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	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 Negative Response

“N”	60H	30H	e1	e0	Rtype	ATQB

Activate RFID card

CRT-711 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-711return:

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

2).ISO/IEC 14443 Type A:

1. Request A(REQ A) / Answer Request A (ATQ A).
2. Anti-collision
3. Select (SEL) / Unique Identifier (UID) & Select Acknowledge (SAK)
4. Request for answer to select (RATS) / Answer to Select (ATS)

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

When ISO/IEC 14443 Type A card successfully activated, CRT-711 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-711 return ATQB 12 byte (including following information):

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

Notes:

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

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

Ex1：Set1= 'A'，Set2 = 'B' (default)

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

Ex2：Set1= 'B'，Set2 = 'A'

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

Ex3：Set1= 'A'，Set2 = '0'

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

Ex4：Set1= 'B'，Set2 = '0'，

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

Rtype: Protocol

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

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

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

When Rtype=4DH ('M')

ATQA= 0044H Mifare Ultralight Card

ATQA= 0004H Mifare S50 1K Card

ATQA= 0002H Mifare S70 4K Card

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

UID_len=4 the length of UID_data is 4 byte

UID_len=7 the length of UID_data is 7 byte

UID_len=10 the length of UID_data is10 byte

4.7.2 Deactivate RFID card

Command

“C”	60H	31H

Positive response

“P”	60H	31H	st0	st1	st2

Negative response

“N”	60H	31H	e1	e0

Deactivate RFID card

4.7.3 Inquire status of RFID card

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

4.7.4 Mifare card control

The commands for Mifare card operation is based on ISO/IEC 7816 T=0 data exchange command （C-APDU）

After the command was executed properly, CRT-711 returns a positive response with response data 9000H. When an error occurs, the machine 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

4.7.4.1 Download password to EEPROM

Command

“C”	60H	33H	00H	D0H	ks	sn	pdata

Positive response

“P”	60H	33H	st0	st1	st2	rdata

Negative response

“N”	60H	33H	e1	e0

Download key to EEPROM of RFID module.

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)

pdata (6 byte): password data

rdata (2 byte): return data：

Positive response sw1+sw2=9000H.

Negative response sw1+sw2 （2 byte）

]

4.7.4.2 Read Key from EEPROM

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

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 (8 byte):	return data:	
	Positive response	Key data + (sw1+sw2=9000H)
	Negative response	sw1+sw2 （2 byte）

4.7.4.3 Key verification

Command

“C”	60H	33H	00H	20H	ks	sn	pdata

Positive response

“P”	60H	33H	st0	st1	st2	rdata

Negative response

“N”	60H	33H	e1	e0

Download key to the machine and verify the key of specific sector 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)

pdata (6 byte): password data

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

4.7.4.4 Upload key from EEPROM

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 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)

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

4.7.4.5 Read sector data

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 RFID sectors

Sn (1 byte): sector number

bn (1 byte): block number

le (1 byte): block number (le=01H read 1 block, le=03H read 3 blocks)

rdata (2 byte): return data

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

Notes：

1.Ultralight Card only have one block in one sector，every block have 4 byte data. And S50, S70 card have16 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 (Last 8 sector of S70 card have 16 blocks)

4.7.4.6 Write sector data

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 + 9000 H and negative 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 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

(Last 8 sector of S70 card 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 not write last block and the machine also will prohibit writing last block.

4.7.4.7 Initialization

Command

“C”	60H	33H	00H	D2H	sn	bn	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

wdata: 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 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,

(Last 8 sector of S70 card have 16 blocks)

4.7.4.8 Read value

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 from RFID sectors

Sn (1 byte): sector number

bn (1 byte): block number

rdata (2 byte): return data

(Positive response with data + 9000 H and negative 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,

(Last 8 sector of S70 card have 16 blocks)

4.7.4.9 Increment

Command

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

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 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,

(Last 8 sector of S70 card have 16 blocks)

4.7.4.10 Decrement

Command

“C”	60H	33H	00H	D4H	sn	bn	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

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 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,

(Last 8 sector of S70 card have 16 blocks)

4.7.5 Type A RF card communication

Command

"C"	60H	34H	C-APDU

Positive response

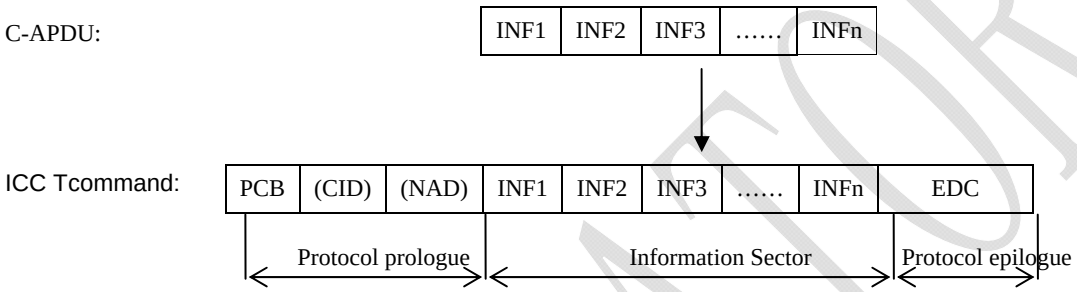
"P"	60H	34H	st0	st1	st2	R-APDU

Negative response

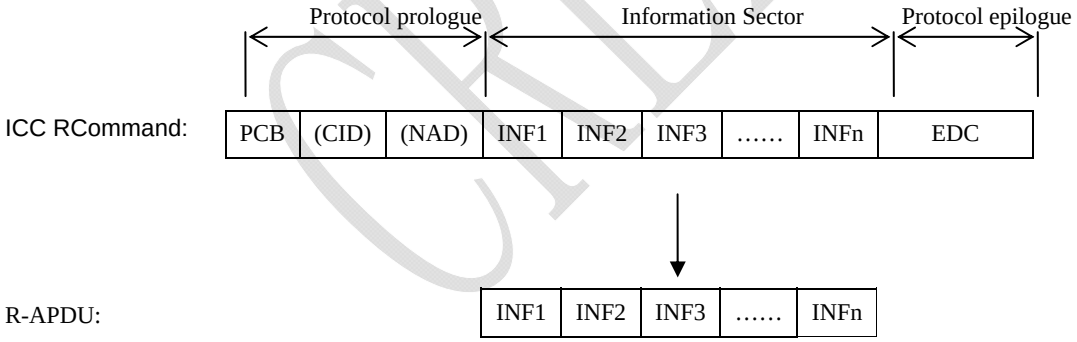
"N"	60H	34H	e1	e0

This command is complied with ISO/IEC 14443-4 standard to execute communication exchange for Type A T=CL protocol.

The C-APDU data to the card is complied with ICC Tcommand format.



The machine executes ICC Tcommand and then card will return ICC Rcommand to HOST as following format.



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

4.7.6 Type B RF card communication

Command

"C"	60H	35H	C-APDU

Positive response

"P"	60H	35H	st0	st1	st2	R-APDU

Negative response

"N"	60H	35H	e1	e0

This command is complied with ISO/IEC 14443-4 standard to execute communication exchange for Type A T=CL protocol.

The C-APDU data to the card is complied with ICC Tcommand format.

C-APDU:

INF1	INF2	INF3	……	INFn

ICC Tcommand:

PCB	(CID)	(NAD)	INF1	INF2	INF3	……	INFn	EDC

Protocol prologue | Information Sector | Protocol epilogue

The machine executes ICC Tcommand and then card will return ICC Rcommand to HOST as following format.

Protocol prologue | Information Sector | Protocol epilogue

ICC RCommand:

PCB	(CID)	(NAD)	INF1	INF2	INF3	……	INFn	EDC

R-APDU:

INF1	INF2	INF3	……	INFn

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

4.7.7 RFID card sleep and wake-up operation

Command:

"C"	60H	39H	Set

Positive response:

"P"	60H	39H	st0	st1	st2

Negative response:

"N"	60H	39H	e1	e0

This command for operation of RFID card sleep/wake-up

Set=30H RFID card sleep operation

Set=31H RFID card wake-up operation

4.8 Barcode scanning

Command:

"C"	70H	30H	

Positive response:

"P"	70H	30H	st0	st1	st2	Data

Negative response:

"N"	70H	30H	e1	e0

Data: Barcode data

Scanning failure, return e1，e0=70

4.9 Read CRT-711 configuration

Command

“C”	A3H	30H

Positive response

“P”	A3H	30H	st0	st1	st2	ICRW_Config

Negative response

“N”	A3H	30H	e1	e0

Read configuration of CRT-711

ICRW_Config: Read configuration information, max length is 16 byte

4.10 Read CRT-711 version information

Command

“C”	A4H	Pm

Positive response

“P”	A4H	30H	st0	st1	st2	Rev

Negative response

“N”	A4H	30H	e1	e0

Read CRT-711 version information

Pm=30H Read machine software information

Pm=31H Read IC Card software information

4.11 Error-card Bin Counter Control

4.11.1 Read error-card bin counter

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, retract one card, counter one plus

Count= “000” ~ “999”

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

4.11.2 Set initial value of error-card bin

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 counter.

Count= “000” ~ “999”

Count value range (0-999)

4.12 Eject card counter control

4.12.1 Read eject card counter

Command:

"C"	A6H	30H

Positive return:

"P"	A6H	30H	st0	st1	st2	Count

Negative return:

"N"	A6H	30H	e1	e0

After reset eject card counter, eject one card, counter one plus

Count= "000" ~ "999"

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

4.12.2 Set initial value of eject card bin

Command:

"C"	A6H	31H	Count

Positive return:

"P"	A6H	31H	st0	st1	st2

Negative return:

"N"	A6H	31H	e1	e0

Set initial value of eject card bin counter.

Count= "000" ~ "999"

Count value range (0-999)

5. TTL Specification

5.1 TTL status control

Pin No.	Signal	IN / OUT	Status	Valid Status
IN1	Eject Card	IN	High Level "5V"	Low Level Impulse (Width > 100ms)
IN2	Retract Card	IN	High Level"5V"	Low Level Impulse (Width > 100ms)
IN3	Entry Enable	IN	High Level"5V"	Low level"0V" (Enable)
OUT1	Machine Status	OUT	Low Level"0V" (No card)	High Level"5V" (Have card)
OUT2	Operation Successful	OUT	Low Level"0V"	High Level"5V" (Successful)
OUT3	Operation Error	OUT	Low level"0V"	High Level"5V" (Error)
GND	Ground	GND		Ground

Notes: Need reset or power-off when execute TTL and RS232 interchange

5.2 Error card bin status introduction (External interface)

Pin No	Signal	IN / OUT	Status	Valid Status
OUT4	Error card bin status	OUT	Low level"0V" (Not full)	High level"5V" (card Full)
GND	Ground		GND	Ground