

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1. 0
		Page	1/16

CRT-603-P1 COMMUNICATION PROTOCOL

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	2/16

CONTENT

CRT-603-P1 COMMUNICATION PROTOCOL	1
1. Communication Character format.....	4
2. Communication format and control characters.....	4
3. Communication Description	6
4. CONTROL DATA (TEXT) FORMAT	7
5.CRT-603-P1 status code and error bit lists.....	8
6. Operation command lists	10
7. Command Detailed Explanation.....	10
8. APDU operation.....	14

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	3/16

Version History

Version	date	content
1.0	2016.11.16	Create CRT-603-P1communication protocol

CREATOR

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	4/16

1. Communication Character format

Serial Port Communication

Baud rate (BPS): 115200BPS (fixed baud rate)

Communication type: asynchronous communication

Transmission type: Half-Duplex

Data frame structure:

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

Start bit: 1 bit

Data bit: 8 bits

Stop bit: 1 bit

Communication control method

Reader is a driven part and manipulated by valid command

2. Communication format and control characters

Communication frame structure:

B0 (1 byte)	B1 (1 byte)	B2 (1 byte)	LEN (2 byte)	TEXT (n byte)	BCC (1 byte)
(Header)	Reserved identifier	Encrypted mode bit	TEXT data length	Text data Packets	BCC XOR checkout

B0 : 0X02

B1 : 0X00

B2 :TEXT data plaintext identifier bit or ciphertext identifier bit

plaintext identifier bit is 0X01; 3DES ciphertext identifier bit is 0X00;

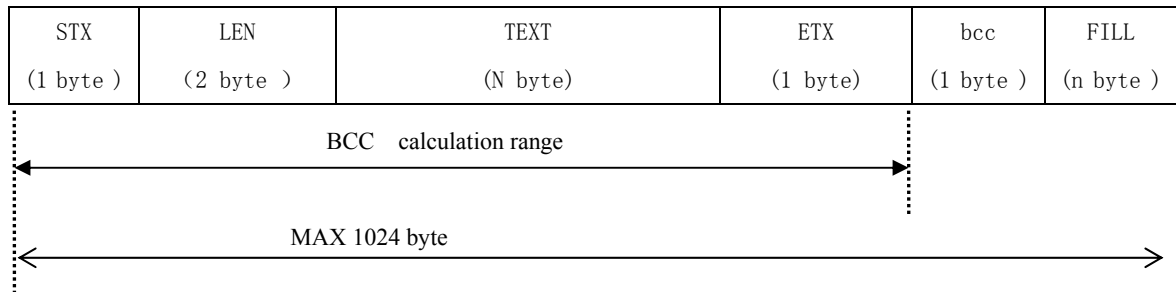
LEN :TEXT data length is 2 bytes. Max length is 1024 bytes. High byte before low byte.LEN should be divided by 8 without remainder. If not, random number needs to be added to fill the TEXT to be divided by 8 exactly.

TEXT: when data B2=0, data is 3 DES encrypted.

BCC: $B1 \oplus B2 \oplus LEN \oplus TEXT$ (XOR from B0 to previous one byte of BCC) .

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	5/16

TEXT Data Packet Format:



STX (F2H) Start bit
 LEN(2bytes) data length, high byte before low byte
 TEXT data (command or response)
 ETX: 03H
 bcc XOR checkout
 FILL Random number to fill-in

N : Max length 1024-5=1019 bytes;

n :when (N+5) divided by 8 without remainder, n =0; then FILL data no exist;

When (N+5) divided by 8 with remainder n+N+5; then n is between in 1-7. FILL data is random number.

ACK PACKET DATA FORMAT

TEXT ACK data format:

0XF2	0X00	0X03	0X43	0X06	0X00	0X03	BCC
------	------	------	------	------	------	------	-----

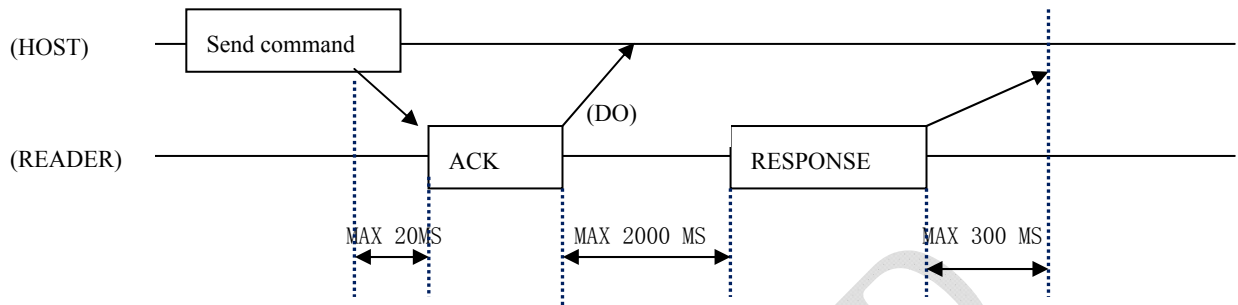
TEXT NAK data format:

0XF2	0X00	0X03	0X43	0X15	0X00	0X03	BCC
------	------	------	------	------	------	------	-----

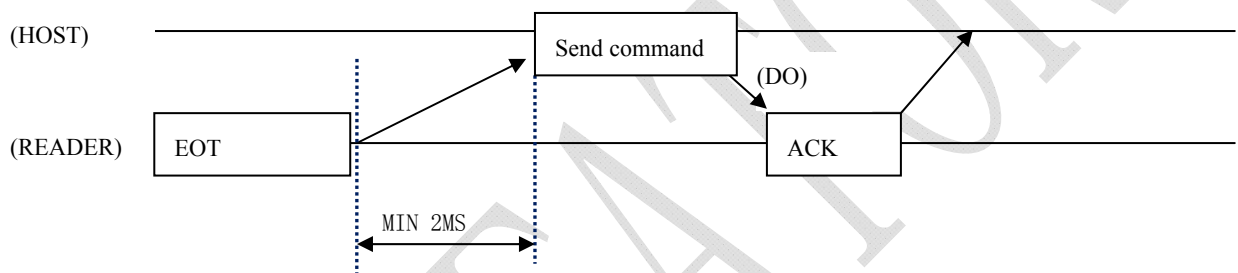
	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	6/16

3. Communication Description

ordinary communication:(command and response)



Send ACK timing:



	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	7/16

4. CONTROL DATA (TEXT) FORMAT

COMMAND (HOST→ READER)

"C"	PM	DATA	FILL DATA
-----	----	------	-----------

"C" = 43H

CM: Command word

PM: Command parameter

DATA: any

FILL: Random number to fill in. No actual meaning, only for data length can be divided by 8

Positive response (READER→ HOST)

"P"	CM	PM	ST1	ST0	DATA	FILL DATA
-----	----	----	-----	-----	------	-----------

"P" = 50H

CM and PM :same as command (except for IC card controlling)

ST0 和 ST1: status word

DATA: any

FILL: Random number to fill in. No actual meaning, only for data length can be divided by 8

Negative response (READER→ HOST)

"N"	CM	PM	E1	E0	DATA	FILL DATA
-----	----	----	----	----	------	-----------

"N" = 4EH

CM and PM :same as command (except for IC card control)

E0 and E1: error word

DATA: any

FILL: Random number to fill in. No actual meaning, only for data length can be divided by 8

Note: HOST can only send new command 2ms later after receiving return data

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	8/16

5. CRT-603-P1 status code and error words lists

Status code ST1 & ST0

ST1 & ST0 (HEX)	Status description
00 01	No card
00 02	Multiple cards
10 01	Canceling transaction
10 11	Requiring for patting card
10 12	Requiring for selecting application
10 13	Requiring for confirming account
10 14	Requiring for inputting password
10 15	Requiring for online
10 16	Requiring for off-line
20 01	Off-line approval
20 02	Off-line refuse
20 03	Off-line success
20 04	Off-line failure
20 05	Off-line to online
20 06	Online approval
20 07	Online refuse
20 08	Closing transaction
20 09	Transaction success
20 10	Transaction failure
20 11	Transaction refuse
30 01	Visa issuing script, requiring to remind patting card again
30 02	Visa APDU return timeout, resuming transaction
30 03	Script updating success
30 04	Script updating failure
30 05	Online approval, requiring for patting card again
30 06	Online refuse, requiring for patting card again
30 07	APDU timeout, requiring for seeking cards (delaying 2-3seconds and make transaction)

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	9/16

Error code E1 & E0

E1 & E0 (HEX)	Description
30 30	Command word error
30 31	Command parameter error
30 32	Not support command
30 33"	Hardware no supporting command
30 34	Command data error
31 35	EEPROM error

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	10/16

6. Operation command lists

Command	function	CM	PM	Description
Reset reader	Set initialization parameter	30H	30H	
Reader serial number	Checking reader serial number	A2H	30H	Reader serial number
Auto-test card type		50H	30H	Auto-test contact IC card type
CPU card operation	CPU Card operation	61H	30H	RF CPU card resetting(activation)
			31H	RF CPU card off-power
			39H	Auto-select T=0/T=1 protocol ,CPU card APDU operation
SAM card operation	SAM card operation	52H	30H	SAM card resetting(activation)
			31H	SAM card deactivate
			32H	SAM card status checking
			38H	SAM card warm resetting
			39H	Auto-select T=0/T=1 protocol SAM card APDU operation
			40H	Selecting SAM card slot

7. Command Detailed Explanation

7.1 Resetting reader

HOST send:

"C"	30H	PM
-----	-----	----

PM= 30H: clearing internal storage data;

READER positive response:

"P"	30H	PM	ST1	ST0	Reader version info word SV
-----	-----	----	-----	-----	-----------------------------

Reader version info: CRT-603-P001 reader SV= "CRT 603 P001"

READER negative response:

"N"	30H	PM	E1	E0
-----	-----	----	----	----

7.2 Reader serial number

HOST send:

"C"	A2H	30H
-----	-----	-----

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	11/16

READER positive response

"P"	A2H	30H	ST1	ST0	Reader serial number data packet (n byte)
-----	-----	-----	-----	-----	--

Reader serial number data packet: stored in A S C I I code:

If reader serial number is "CRT-603", reader serial number data packet:

"43H,52H,54H,2DH,36H,30H,33H"

Note : Be stored with max 13 bytes

READER negative response:

"N"	A2H	30H	E1	E0
-----	-----	-----	----	----

CREATOR

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	12/16

7.3 PSAM card operation:

SAM card resetting (activation):

HOST send command:

"C"	52H	30H	Vcc
-----	-----	-----	-----

READER positive return:

"P"	52H	30H	ST1	ST0	Type	ATR
-----	-----	-----	-----	-----	------	-----

READER negative return:

"N"	52H	30H	E1	E0	Type	ATR
-----	-----	-----	----	----	------	-----

Reader provides VCC, CLK, and RST to card for card activation and return ATR.

Type: SAM card protocol type

=30H T=0 protocol SAM card

=31H T=1 protocol SAM card

ATR: resetting response data format as below:

TS	TO	TA1	TB1	...	TCK
----	----	-----	-----	-----	-----

Vcc=30H supply 5V power, use EMV mode to reset SAM card (activation).

Vcc=33H supply 5V power, use ISO7816 mode to reset SAM card (activation).

Vcc=35H supply 3V power, use ISO7816 mode to reset SAM card (activation).

Vcc is parameter optional. If no Vcc parameter in command, then Vcc=30H.

During resetting, SAM card ATR info not complying with EMV, then returning E1,E0= "69" error.

During resetting, test IC card power failure, return E1,E0= "60" error.

SAM card deactivate:

HOST send command:

"C"	52H	31H
-----	-----	-----

READER positive response:

"P"	52H	31H	ST1	ST0
-----	-----	-----	-----	-----

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	13/16

READER negative response:

"N"	52H	31H	E1	E0
-----	-----	-----	----	----

SAM card deactivate operation

deactivate the activated SAM card

7.4 Auto-select T=0/T=1 protocol SAM card APDU operation

HOST sends command:

"C"	52H	39H	C-APDU
-----	-----	-----	--------

READER positive response:

"P"	52H	39H	ST1	ST0	R-APDU
-----	-----	-----	-----	-----	--------

READER negative response:

"N"	52H	39H	E1	E0
-----	-----	-----	----	----

Reader auto test SAM card T=0/T=1 protocol, auto-select protocol C-APDU operation, return R-APDU.

During operation, fail to test IC card power, return E1,E0= "60" error code;

If SAM card is not T=0/T=1 protocol, return E1,E0= "62" error code;

If SAM card timeout, deactivate SAM card firstly, then return E1,E0= "63" error code;

If other protocol error occur, deactivate SAM card firstly, then return E1,E0= "64" error code;

If HOST does not activate SAM card, return E1,E0= "65" error code

7.5 Select SAM card slot

HOST sends command:

"C"	52H	40H	SAMn
-----	-----	-----	------

READER positive response:

"P"	52H	40H	ST1	ST0
-----	-----	-----	-----	-----

READER negative response:

"N"	52H	40H	E1	E0
-----	-----	-----	----	----

Select SAM card in PSAM slot

SAMn=30H select SAM1

=31H select SAM2

This command is valid for reader with PSAM board, and for only one SAM card operation one time.

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	14/16

7.6 RF card operation:

Card activation

HOST sends command:

"C"	37H	30H	path type
-----	-----	-----	-----------

Path type: 30H activate contact card

31H activate contactless card

READER operation positive response:

"P"	37H	30H	ST1	ST0	ATR
-----	-----	-----	-----	-----	-----

READER operation negative response:

"N"	37H	30H	E1	E0
-----	-----	-----	----	----

8. APDU operation

HOST sends:

"C"	37H	31H	Path type	C-APDU
-----	-----	-----	-----------	--------

Path type: 30H contact card APDU operation

31H contactless card APDU operation

READER operation positive response:

"P"	37H	31H	ST1	ST0	R-APDU
-----	-----	-----	-----	-----	--------

READER operation negative response:

"N"	37H	31H	E1	E0
-----	-----	-----	----	----

C-APDU HOST sends to card data packet, min 4 bytes, max 261 bytes. Format is as below:

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

R-APDU card returns to HOST data packet, min 2 bytes, max 258 bytes. Format is as below:

Data1		Data(n)	SW1	SW2
-------	-------	---------	-----	-----

APDU format refer to ISO/IEC7816-3 relevant content, specific C-APDU command is subject to card COS command.

	SPECIFICATION		Model No.	CRT-603-P1
			Date	2017/04/20
	COMMUNICATION PROTOCOL		Ver.	1.0
			Page	15/16

9. LED and buzzer operation commands :

Buzzer control

HOST sends:

"C"	80H	30H	Cycle times	Start time	Close time
-----	-----	-----	-------------	------------	------------

Cycle times sets as 1 ---- 10 times

Start time 1 ----- 100 unit is n*10 ms

Close time 1 ----- 100 unit is n*10 ms

READER operation positive return:

"P"	80H	30H	ST1	ST0	ATR
-----	-----	-----	-----	-----	-----

READER operation negative return:

"N"	80H	30H	E1	E0
-----	-----	-----	----	----

E1 E0 error code status list

LED controlling operation

HOST sends:

"C"	80H	31H	LED position	LED switch status	LED flicker status	flicker period
-----	-----	-----	--------------	-------------------	--------------------	----------------

LED position: 31H blue lamp
32H yellow lamp
33H green lamp
34H red lamp

LED switch status: 00H switch off
01H switch on

LED flicker status: 00H switch off
01H switch on

Flicker period 0x01 ----- 0X0D unit is n* 25ms
0X0E Specific representation 83 ms
0X0F Specific representation 750 ms

	SPECIFICATION	Model No.	CRT-603-P1
		Date	2017/04/20
	COMMUNICATION PROTOCOL	Ver.	1.0
		Page	16/16

READER operation positive return:

"P"	80H	31H	ST1	ST0	R-APDU
-----	-----	-----	-----	-----	--------

READER operation negative return:

"N"	80H	31H	E1	E0
-----	-----	-----	----	----

E1 E0 error code status code list

For example: 43 80 31 31 01 01 0f

80 31 present command word

31 presents to operate LED to blue

01 presents LED is in switch on status

01 presents LED is in flicker status

0F presents LED is in flicker cycle with specific representation 750 ms.