CRT-603 Product Manual

CREATOR (CHINA) TECH CO., LTD

ADD: 2/F, M-10 Building, Center Area, High-tech Industrial Park

Shenzhen, Guangdong, China.

Tel: +86-755-26710345

Fax: +86-755-26710105

EMAIL: sales@china-creator.com

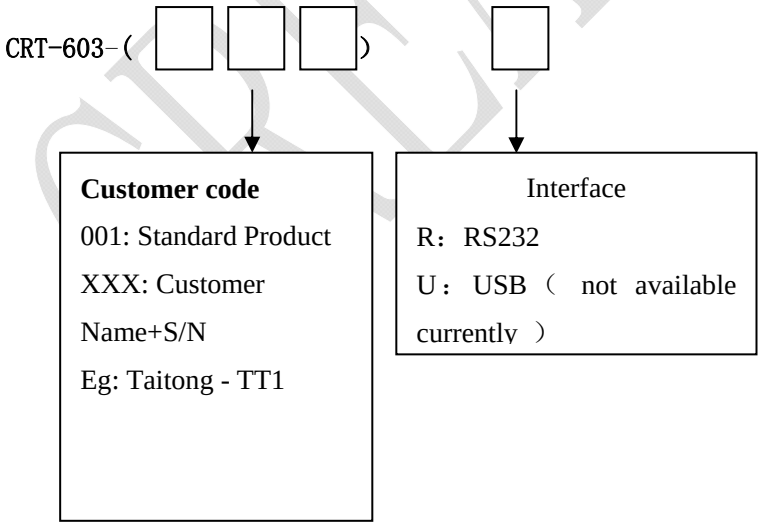
Http://www.china-creator.com

1. Specification

CRT-603 series product is a RFID card read/writing module with SIM slot option featuring:

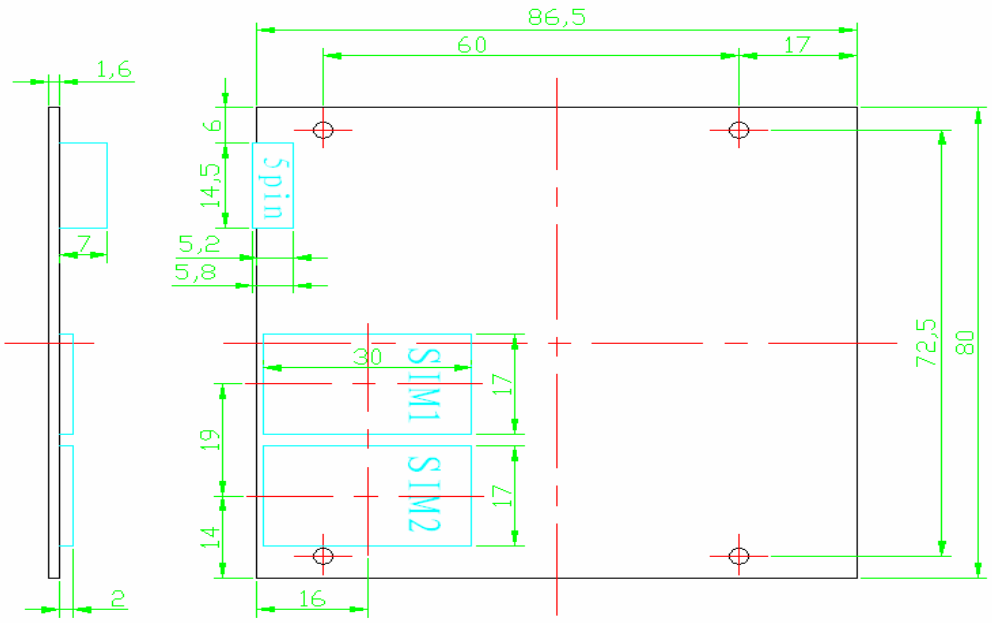
- Card type: Mifare 1K/4K; UltraLight; ISO14443-4 TYPE A&B; ISO7816
- Auto seek card: available, (default: disable)
- EEPROM: 512 byte
- Power: DC 5.0V ±5%
- Interface: 5V TTL / RS232
- Max power consumption: 150mA
- Distance: 70mm (Depending on Card quality)
- Dimension: 80mm*86.5mm
- Weight: Approximately 100g
- ISP: available
- Working temperature allowance: 0~+50℃
- Storage temperature allowance: -20 ~ +70℃;

2. Model NO.



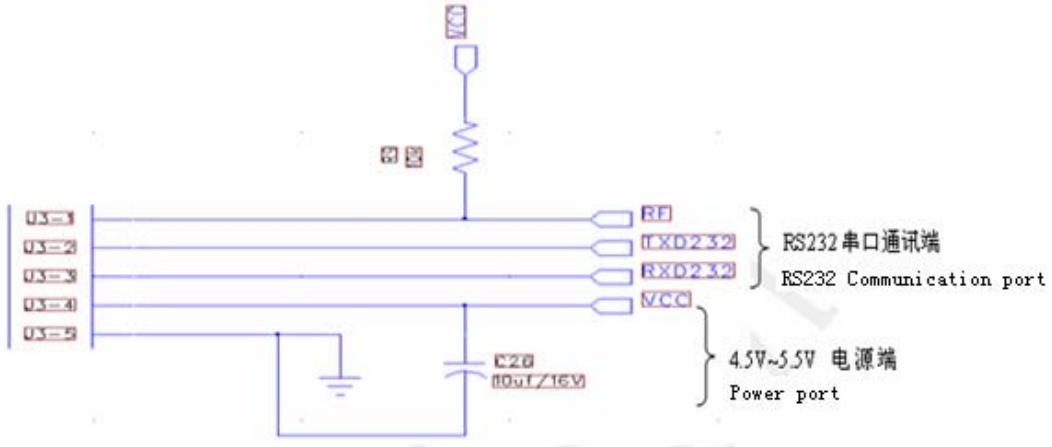
3. Installation drawing and pin definition

3.1 Installation drawing



3.2 Pin definition

Pin No.	Function	Type	Note
J3-1	RF	TTL	0：card existent；1：card inexistent
J3-2	TXD/SDA	RS232	UART TXD/IIC SDA
J3-3	RXD/SCL	RS232	UART RXD/IIC SCL
J3-4	VCC	Power	VCC
J3-5	GND	Power	GND



4. Communication protocol

4. 1 UART protocol

4.1.1 Communication format

Byte is the unit of communication, data sending and receiving adopt Hexadecimal System，communication Parameter is as following:

Baud rate：19200 bps

Data bit：8 bits

Stop bit：1 bit

Parity ： None

Flow control：None

4.1.2 Data format

Length byte	Command byte	Data	Parity byte

Length byte：Number of bytes is calculated from length Byte to the last byte of Data

Command byte：1 byte

Data：The length of Data depends on the Command Byte, it may be empty

Parity byte：Exclusive OR (XOR) result from Length Byte to the last byte of Data

4.1.3 UART data return format

Positive return：

Length byte	Command byte	Data	Parity byte

Negative return：

Length byte	CPL(~) Command byte	Parity byte

4. 2 Command list

Command byte	Note
0x10	Baud rate setting
0x11	Module working status
0x13	LED Indicator setting
0x14	Buzzer setting
0x20	Seek card
0x21	Read block
0x29	Read sector (4 blocks)
0x22	Write block
0x23	Value initialization
0x24	Read value
0x25	Increment operation
0x26	Decrement operation
0x27	Value backup
0x28	Mifare card halt
0x2D	Download secret key from module
0x15	EEPROM reading
0x16	EEPROM writing
0x30	ISO14443-4 TYPE A card reset
0x31	Send APDU to ISO14443-4 card
0x41	UltraLight reading
0x42	UltraLight writing
0x70	Card reading mode setting
0x60	ISO14443-4 TYPE B card reset
0x62	ISO14443-4 TYPEA,TYPE B card halt
0x51	SAM card 1reset
0x52	SAM card reset
0x53	Send APDU to SAM card 1
0x54	Send APDU to SAM card 2
0x68	Seek and reset ISO14443-4 card，both type A and B

5. Detail operation command list

5.1 Baud rate setting:

Host sends:

0x03	0x10	mode	Parity byte

Mode: 1 byte （default: 19200）

0x01: 9600 0x02: 19200

0x03: 38400 0x04: 115200

Module positive return:

0x02	0x10	Parity byte

Module negative return:

0x02	0xEF	Parity byte

5.2 Working mode setting

Host sends:

0x03	0x11	mode	Parity byte

Mode: 1 byte

Antenna status: BIT0=0 : disable BIT0=1 : Enable

Auto seek card: BIT1=0 : disable BIT1=1 : Enable

Module positive return:

0x02	0x11	Parity byte

Module negative return:

0x02	0xEE	Parity byte

Note: Setting is not store in the module, All setting will be invalidate when powered on next time.

5.3 LED indicator setting

Host sends:

0x03	0x13	LED status	Parity byte

status: 1 byte, 0: Disable; 1: Enable

Module positive return:

0x02	0x13	Parity byte

Module negative return:

0x02	0xEC	Parity byte

5.4 Buzzer setting

Host sends:

0x03	0x14	Time	Parity byte

Time: 1 byte, Unit is 10ms. If time is 0x0A then buzzer's time is 100 ms

Module positive return :

0x02	0x14	Parity byte

Module negative return:

0x02	0xEC	Parity byte

5.3 Seek card

Host sends:

0x03	0x20	mode	Parity byte

Mode: 1 byte, 0: WUPA (seek all cards); other value: REQA (Seek card only not halted)

Module positive return:

-	0x20	Data	Parity byte

Data: 4, 7 or 10 byte card S/N + 2 byte ATQA + 1 byte SAK

Module negative return:

0x02	0xDF	Parity byte

5.3 Read block

Host sends:

0x0A	0x21	Secret key ID	Block NO.	Secret key	Parity byte

Secret ID: 1 byte, Key identification

BIT0=0: Key A; BIT0=1: Key B ;

BIT1=0: use the following secret key; BIT1=1: use the secret key download by command 0x2D

Block No.: 1 byte, read block NO., S50: 0~ 0x3F; S70: 0 ~0xFF

Secret key: 6 bytes, card secret key

Module positive return:

0x12	0x21	Data	Parity byte

Data: 16 bytes card data

Module negative return:

0x02	0xDE	Parity byte

5.4 Read block

Host sends:

0x0A	0x29	Secret key ID	Sector No.	Secret key	Parity

Secret key ID: 1 byte, Key identification

Sector NO.: 1 byte, read Sector No., S50 card: 0 ~0x0F; S70 card 0 ~ 0x3F

Secret key: 6 bytes, card secret key

Module positive return:

0x42	0x29	data	Parity

Data: 64 bytes card's data

Module negative return:

0x02	0xD6	Parity

Note: There are 4 blocks in both S50 and S70'previous 32 blocks. Because there are 16 blocks in S70's 32~39 sectors, if you need to read the blocks in this sector, you need send 5 times the above commands to accomplish the operation.

5.5 Write block

Host sends:

0x1A	0x22	Secret key ID	Block NO.	Secret key	dada	Parity

Secret key ID: 1 byte, Key identification

Block NO.: 1 byte, read block NO., S50: 0 ~ 0x3F; S70: 0 ~ 0xFF

Secret key: 6 bytes, card's secret key

Data: write 16 bytes data

Module positive return:

0x02	0x22	Parity

Module negative return:

0x02	0xDD	Parity

5.6 Value initialization

Host sends:

0x0E	0x23	Secret key ID	Block NO.	Secret key	Value	Parity byte

Secret key ID: 1 byte, Secret key identification

Block NO: 1 byte, Block data initiation, S50: 0 ~ 0x3F; S70: 0 ~ 0xFF

Secret key: 6 bytes, card's secret key

Value: 4 bytes, initialized value, LSB first

Module positive return:

0x02	0x23	Parity byte

Module negative return:

0x02	0xDC	Parity byte

5.7 Read value

Host sends:

0x0A	0x24	Secret key ID	Block NO.	Secret key	Parity byte

Secret key ID: 1 byte, Secret key identification

Block No.: 1 byte, read block NO., S50: 0 ~ 0x3F; S70: 0 ~ 0xFF

Secret key: 6 bytes, card's secret key

Module positive return:

0x06	0x24	Value	Parity byte

Value: 4 Bytes value data, LSB first

Module negative return:

0x02	0xDB	Parity byte

Note: module will read the data in the block, and check if it is a Electronic Purse format。If yes, return 4 bytes value data; If no, return negative.

5.8 Increment operation

Host sends:

0x0E	0x25	Secret key ID	Block NO.	Secret key	Value	Parity byte

Secret key ID: 1 byte, Secret key identification

Block NO.: 1 byte, Block data initiation, S50: 0 ~ 0x3F; S70: 0 ~ 0xFF

Secret key: 6 bytes, card's Secret key

Value: 4 bytes, added value, LSB first

Module positive return:

0x02	0x25	Parity byte

Module negative return:

0x02	0xDA	Parity byte

5.9 Decrement operation

Host sends:

0x0E	0x26	Secret key ID	Block NO.	Secret key	Value	Parity byte

Secret key ID: 1 byte, Secret key identification

Block NO.: 1 byte, Block No. Initialization, S50: 0 ~ 0x3F; S70: 0 ~ 0xFF

Secret key: 6 bytes, card's secret key

Value: 4 bytes, reduced value, LSB first

Module returns success

0x02	0x26	Parity byte

Operation failure:

0x02	0XD9	Parity byte

5.10 Backup Value

Host sends:

0x0E	0x27	Secret key ID	origin	Target	Secret key	Parity byte

Secret key ID：1 byte，Secret key ID identification

Origin：1 byte，copy the number of Blocks，S50: 0 ~ 0x3F；S70: 0 ~ 0xFF

Target：1 byte，back up the value to the pointed block　(Origin and Target must be in Sector One)

Secret key：6 bytes, card's secret key

Operation success:

0x02	0x27	Parity byte

Operation failure:

0x02	0xD8	Parity byte

5.11 Mifare card Halt

Host sends:

0x02	0x28	Parity byte

Operation success

0x02	0x28	Parity byte

Operation failure:

0x02	0xD7	Parity byte

5.12 Download module's secret key

Host sends:

0x09	0x2D	Secret key index	Secret key	Parity byte

Secret key index：1 byte，store Secret key index in the module

Secret key：6 bytes, the secret key stored in module

Operation success

0x02	0x2D	Parity byte

Operation failure:

0x02	0xD2	Parity byte

5.13 Read EEPROM

Host sends:

0x05	0x15	Address	Bytes	Parity byte

Address：2 bytes，start address for reading （effective address is 0x00—0x7F,128bytes in total）

Bytes：1 byte，the number of bytes for reading，Max 16bytes.

Operation success:

-	0x15	Data	Parity byte

Data：Data obtained from the reading operation

Note：the byte length is “-”，it means the byte length is determined by the card’s actual returning information.

Operation failure:

0x02	0xEA	Parity byte

5.14 Write EEPROM

Host sends:

-	0x16	Address	Bytes	Data	Parity byte

Address：2 bytes，start address for writing（effective address is 0x00—0x7F,128bytes in total）

Byte：1 Byte，the number of bytes for writing，Max. 16 bytes

Data：data that will be written in

Note：the byte length is “-”，it means the byte length is determined by the card’s actual returning information.

Operation success:

0x02	0x16	Data	Parity byte

Operation failure:

0x02	0xE9	Parity byte

5.15 ISO14443-4 TYPE A card reset （ the Command need to be executed after seek card operation ）

Host sends:

0x02	0x30	Parity byte

Operation success:

-	0x30	Information	Parity byte

Information：card reset information，length is determined by card type

Note：the byte length is “-”，it means the byte length is determined by the card’s actual returning information.

Operation failure:

0x02	0xCF	Parity byte

5.16 Send APDU to card

Host sends:

-	0x31	APDU	Parity byte

APDU：APDU that you would like to send

Operation success:

-	0x31	Response	Parity byte

Response：card response，length is determined by specific command

Operation failure:

0x02	0xCE	Parity byte

5.17 Read UltraLight card

Host sends:

0x03	0x41	Block	Parity byte

Block：1 byte，start block number for reading

Operation success:

0x12	0x41	Data	Parity byte

Data：16 bytes data

Operation failure:

0x02	0xBE	Parity byte

5.18 Write UltraLight card

Host sends:

0x07	0x42	Block NO.	Data	Parity byte

Block No.：1 byte，the Block's NO. which will be written

Data：4 bytes data that will be written into the block

Operation success:

0x02	0x42	Parity byte

Operation failure:

0x02	0xBD	Parity byte

5.19 Card reading mode setting

Host sends:

0x03	0x70	mode	Parity byte

Mode：1 byte，0：ISO14443 TYPE A；1：ISO14443 TYPE B

Operation success:

0x02	0x70	Parity byte

Operation failure:

0x02	0x8F	Parity byte

5.20 ISO14443-4 TYPE B card reset

Host sends:

0x03	0x60	Model	Parity byte

Model：1 byte，0：WUPB (seek all cards)；1：All other data：ATQB (Seek card not halted only)

Operation success:

-	0x60	information	Parity byte

Information：12 bytes, card reset information

Operation failure:

0x02	0x9F	Parity byte

5.21 ISO14443-4 card halt，including Type A &B

Host sends:

0x02	0x62	Parity byte

Operation success:

0x02	0x62	Parity byte

Operation failure:

0x02	0x9D	Parity byte

5.22 SAM card 1 reset

Host sends:

0x02	0x51	Parity byte

Operation success:

-	0x51	Information	Parity byte

Information：card reset information，Byte length is determined by card type

Operation failure:

0x02	0xAE	Parity byte

5.23 SAM card 2 reset

Host sends:

0x02	0x52	Parity byte

Operation success:

-	0x52	Information	Parity byte

Information：card reset information，byte length is determined by card type

Operation failure:

0x02	0xAD	Parity byte

5.24 Send APDU to SAM card 1

Host sends:

-	0x53	APDU	Parity byte

APDU：APDU that you would like to send

Operation success:

-	0x53	Response	Parity byte

Response：SAM card response，length is determined by specific command

Operation failure:

0x02	0xAC	Parity byte

5.25 Send APDU to SAM card 2

Host sends:

-	0x54	APDU	Parity byte

APDU：APDU that you would like to send

Operation success:

-	0x54	Response	Parity byte

Response：SAM card response，length is determined by specific command

Operation failure:

0x02	0xAB	Parity byte

5.26 Seek and reset ISO14443-4 card，including both type A and B

Host sends：

0x02	0x68	Parity byte

Operation success:

-	0x68	Reset information	Parity byte

Reset information：The length of card reset information depends on card type

Operation failure:

0x02	0x97	Parity byte

6. The key identification

There is 1 byte key identification in card reading/writing etc operation commands, which suggest the way how it obtains the card's secret key。

Key Identification							
BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
0							

BIT0 = 0：Key A，To Verify Key A

BIT0 = 1：Key B，To Verify Key B

BIT1 = 0：Use the following 6bytes Key in Command

BIT1 = 1：Use download secret key

BIT6:BIT5:BIT4:BIT3:BIT2 ：The S/N of download the key（0～31）

If BIT1 is 0，then these 5BITs (BIT6 to BIT2) are unused. If BIT1 is 1，then use the key which has been downloaded. At the same time, the 6bytes Key in command will become unrelated data. But it is still a integral part of the command.