NFC-1901

Test Program Manual

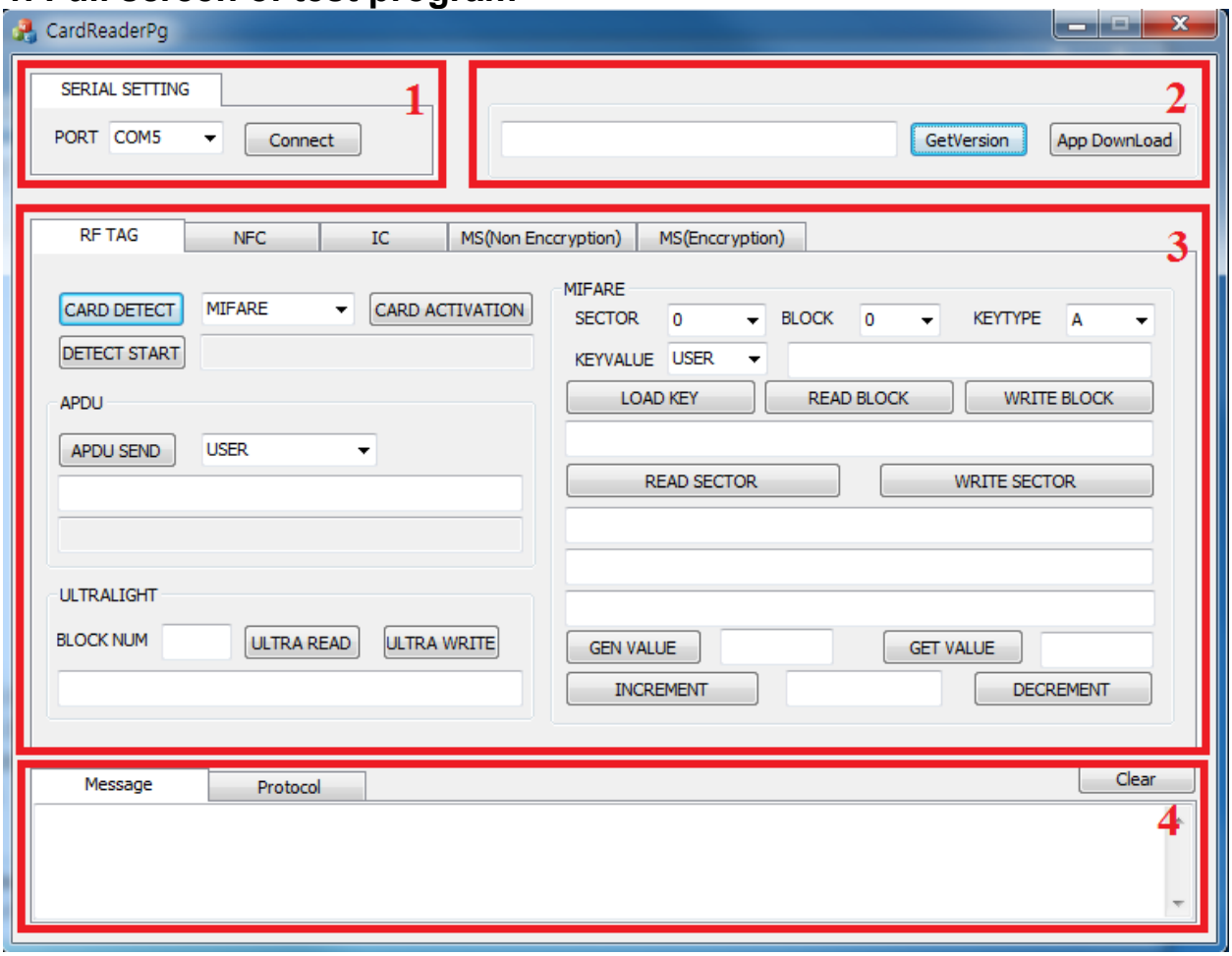
(REV. X01)

For Product information, application engineering assistance or pricing, contact us at:

Peripheral Dynamics Inc.
5150 Campus Drive
Plymouth Meeting, PA 19462-1123
Toll Free: 800-523-0253
Phone: 610-825-7090 Fax: 610-834-7708
Email: sales@pdiscan.com Internet: www.pdiscan.com

March 24, 2014

1. Full screen of test program

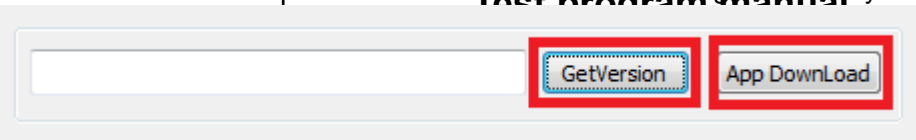


1-1. Serial port setting

First of all, provided USB driver installation is necessary.
Find the serial port using “Device manager” and connect it.

1-2. Get Version and App download

NFC-1901 Firmware version check or Firmware downloading if necessary.

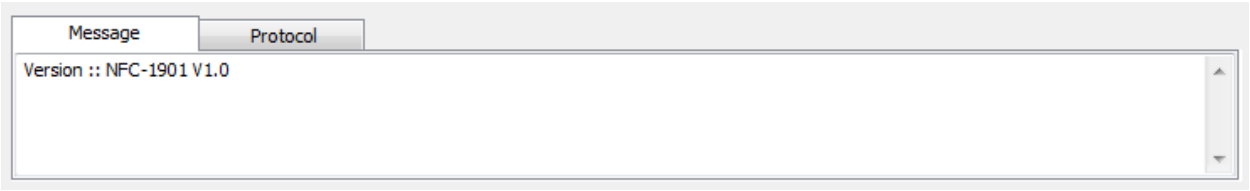


1-3. Test RF & NFC & IC & MS (Non encryption) & MS (encryption)

1-4. Display the Message & Protocol

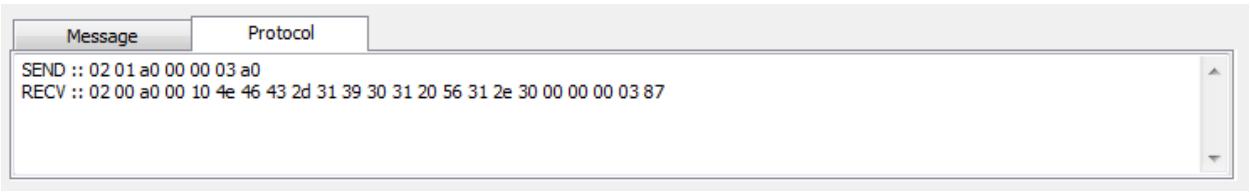
1-4.1. Message

You can see the test result of each command.

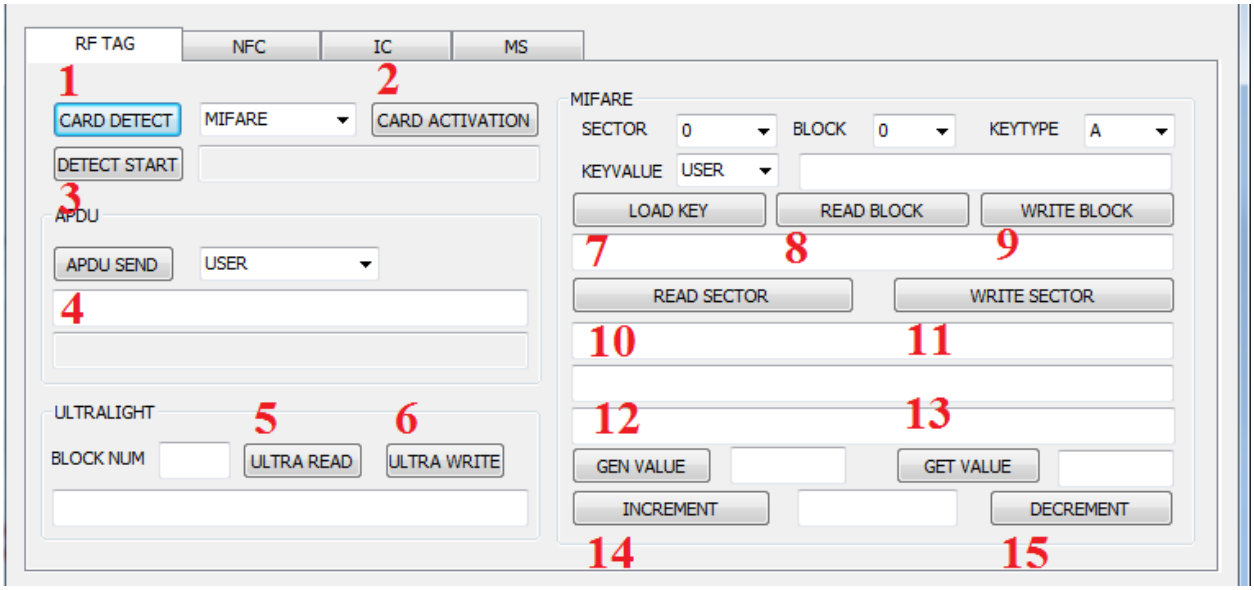


1-4.2 Protocol

You can see the each protocol status and data.



2-1. RF TAG



2-1.1 CARD DETECT

It detects the card exist or not.

♠ After success, the card information as;

- First byte (CardType)
0x41 : ISO-14443 TypeA
0x42 : ISO-14443 TypeB
0x46 : Felica

- Detect information per CardType

* ISO-14443 Type A
0x41 + SAK(1Byte) + UID

* ISO-14443 Type B
0x42 + PUPI

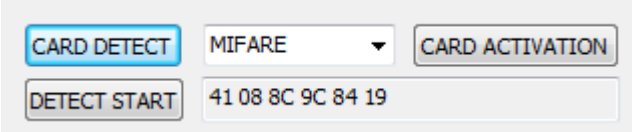
* Felica
0x46 + Felica Speed(0x01 : 212 kbps, 0x02 : 424 kbps) +
Len(1Byte) + response code(1Byte) + UID(8Byte) +
PAD(8Bytes) + system code(2Bytes)

- Type A

Mifare classic
41 08 8C 09 B7 94
Mifare Ultralight
41 00 04 82 9E D9 5B 02 80
ISO-14443-4 typeA
41 28 20 84 9D A3
NXP Desfire
41 20 04 76 89 DA 65 1E 80

- Type B
  42 80 78 A2 50

- FeliCa 212 kbps
  46 01 12 01 01 01 04 10 38 0F 4C 01 10 38 0F 4C 01 10 0B 4B 42 84 85 D0 FF



2-1.2 CARD ACTIVATION

It's for RF TAG Read and Write.

* After CARDTYPE selection, click the button (Mifare, TypeA, TypeB, Felica)

♠ After success, the card information as;

Mifare Card response

00 04 08 04 0B EC 5B 2A

00 04 → SENS_RES

08 → SAK

04 → UID Length

0B EC 5B 2A → UID

TYPEA Card response

00 04 20 04 08 47 91 BC 08 57 80 02 01 10 00 09

00 04 → SENS_RES

20 → SAK

04 → UID Length

08 47 91 BC → UID

08 57 80 02 01 10 00 09 → RATS

TYPE B Card response

50 71 23 47 BE 04 08 00 00 00 71 C1 01 41

50 71 23 47 BE 04 08 00 00 00 71 C1 → ATQB_RES(12 bytes)

01 → ATTRIB_RES Length

41 → ATTRIB_RES

0x46 → Card type, 0x01 → Felica212(0x02 → Felica 424)

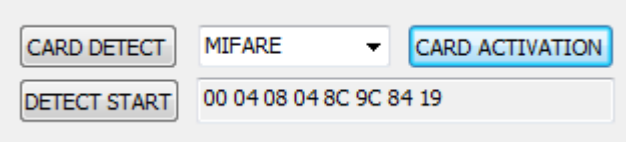
0x14 → Length

0x01 → response code byte

01 01 02 12 36 0E FF 08 → UID

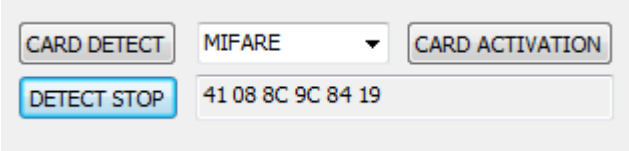
10 0B 4B 42 84 85 D0 FF → PAD

00 03 → System Code



2-1.3 DETECT START & STOP

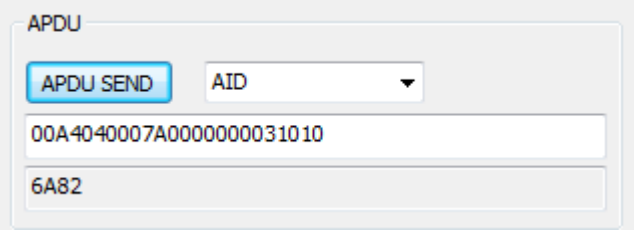
START means, send “CARD DETECT” command every 1 sec.



2-1.4 APDU SEND

This command is to send/receive the data with the card TYPE A and TYPE B.

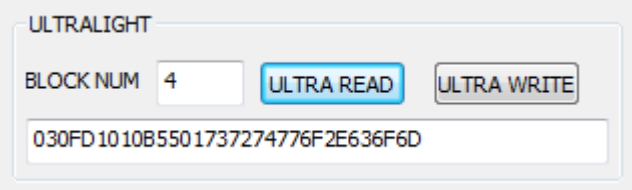
* You can choose APDU sample data.



♠ This command is only possible when the card is activated.

2-1.5 ULTRA READ

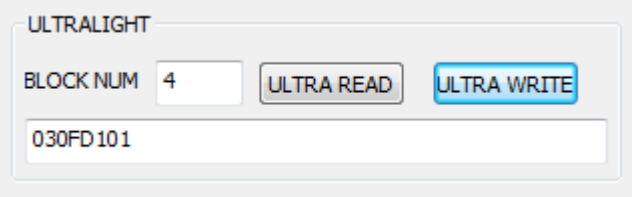
It's to read Ultra light card's 4block (16byte).



♠ This command is only possible when the card is activated.

2-1.6 ULTRA WRITE

It's to write Ultra light card's 1block (4byte).



♠ This command is only possible when the card is activated.

2-1.7 LOAD KEY

It's verification after using Mifare's key value.

* Select "SECTOR, KEY TYPE" and input KEYVALUE

- General KEY VALUE
NEW CARD : FFFFFFFFFFFF (NEW KEY)
NFC CARD_SECTOR0 : A0A1A2A3A4A5 (AID)
NFC CARD_SECTOR1~ : D3F7D3F7D3F7 (PUBLIC)

♠ This command is only possible when the card is activated.

2-1.8 READ BLOCK

It's to read Mifare card's 1block (16byte)

* Select the block after verification

♠ This command is only possible when the card is activated & verified.

2-1.9 WRITE BLOCK

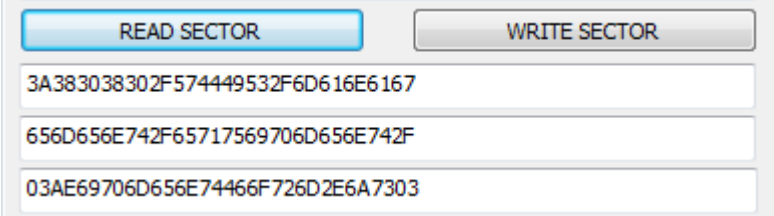
It's to write Mifare card's 1block (16byte)

* Select the block after verification

♠ This command is only possible when the card is activated & verified.

2-1.10 READ SECTOR

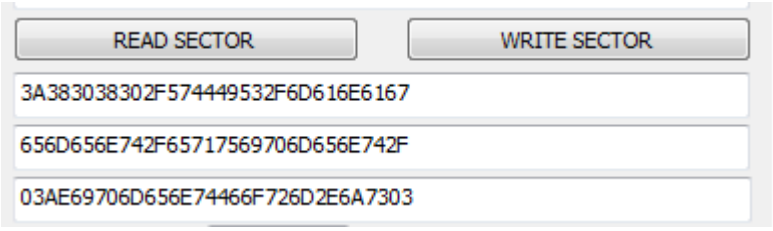
It's to read Mifare card's 1sector (48byte).



♠ This command is only possible when the card is activated & verified.

2-1.11 WRITE SECTOR

It's to write Mifare card's 1sector (48byte).



♠ This command is only possible when the card is activated & verified.

It's to write Mifare card's Value.

* Input VALUE and button click.

♠ This command is only possible when the card is activated & verified.

2-1.13 GET VALUE

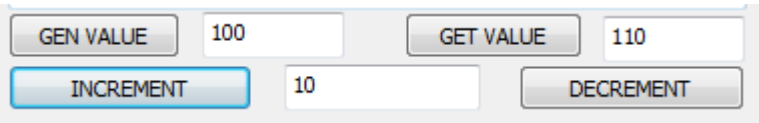
It's to read Mifare card's Value.

♠ This command is only possible when the card is activated & verified.

2-1.14 INCREMENT

It's for Mifare card's Value increment.

* Input the increment value and button click.

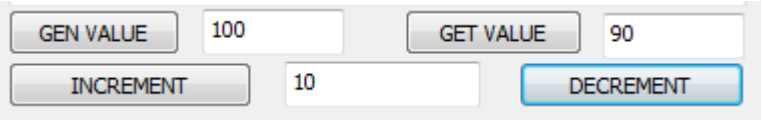


♠ This command is only possible when the card is activated & verified.

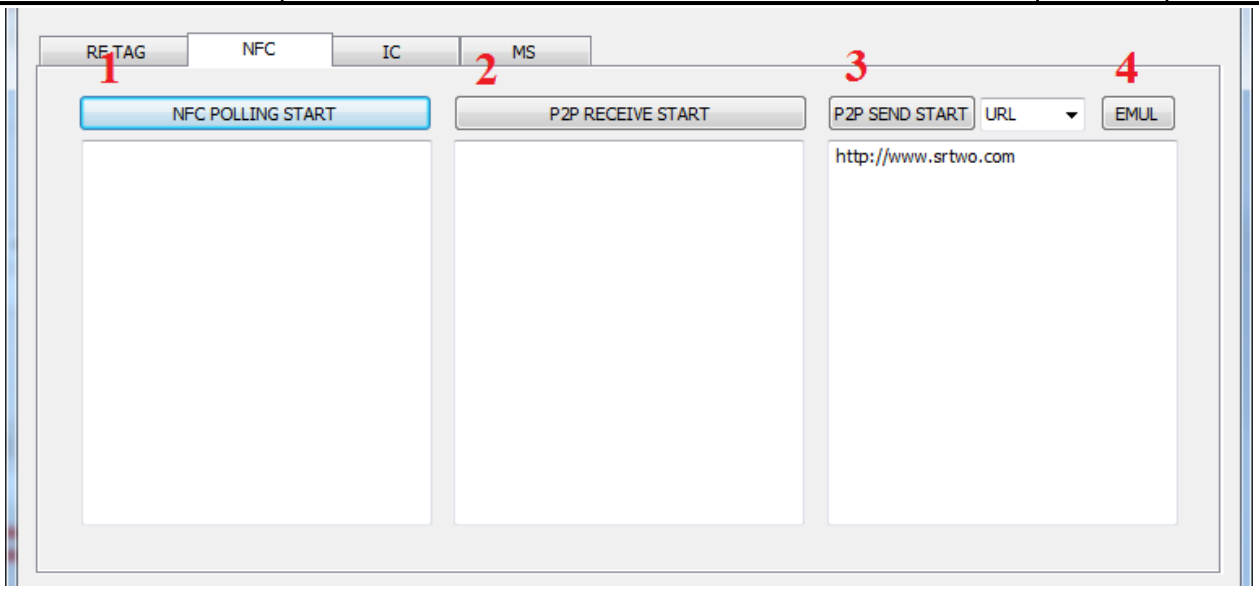
2-1.15 DECREMENT

It's for Mifare card's Value increment.

* Input the decrement value and button click.



♠ This command is only possible when the card is activated & verified.



2-2.1 NFC POLLING START

Read NFEF message and display the information of NFC tag.

* After button click, place the NFC tag on the module (NFC-1901).

2-2.2 P2P RECEIVE START

Read NFEF message and display the information of cell phone.

* After button click, place the cell phone on the module (NFC-1901).

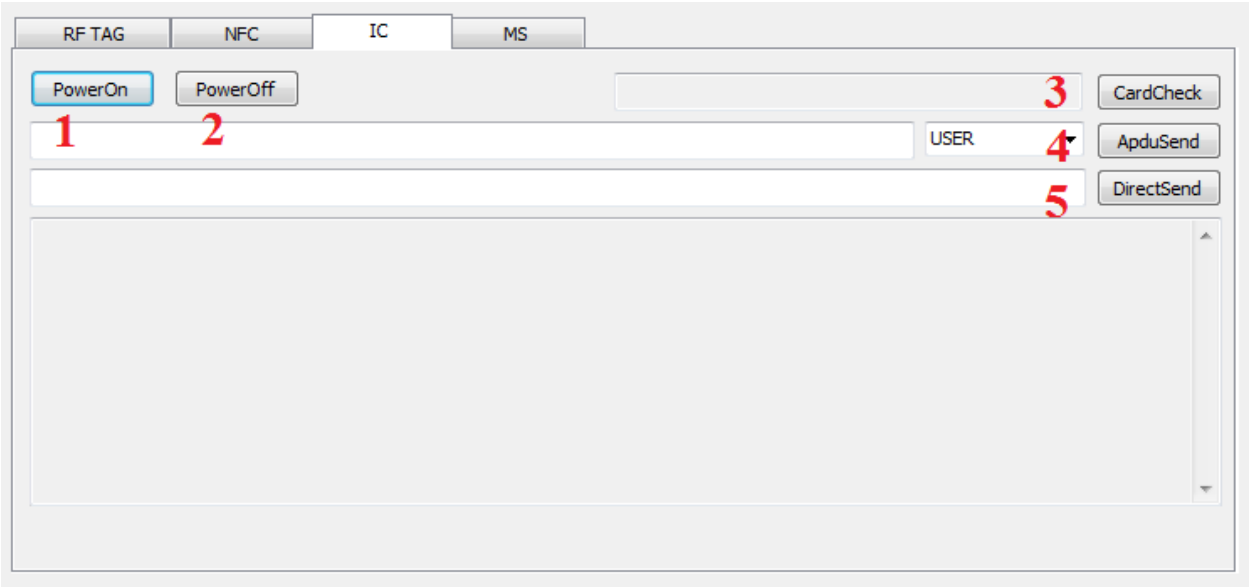
2-2.3 P2P SEND START

* Select the data type (URL, TEXT, VCARD) and input the data button click, (Please the cell phone on the module NFC-1901).

2-2.4 EMULATION

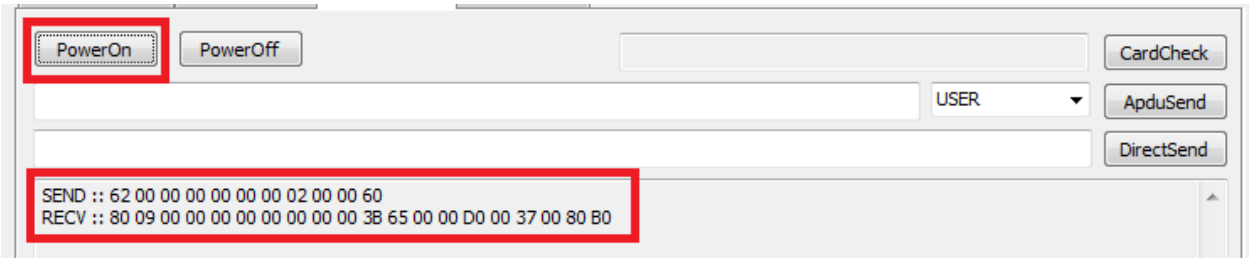
It's for emulation mode.

♠ For details, you can refer the protocol spec of EICM-1000.



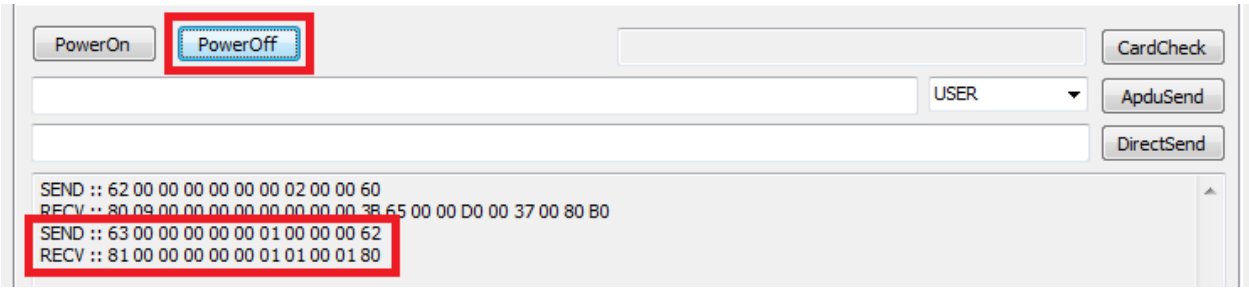
2-3.1 PowerOn

It's for IC card actiation.



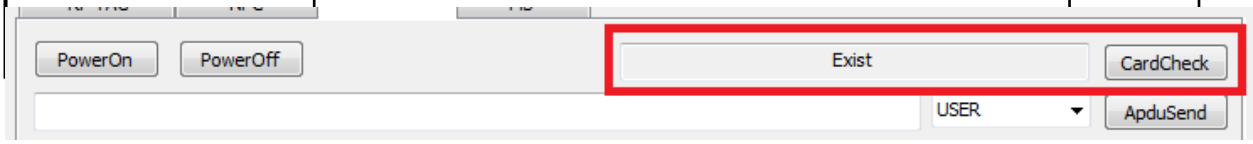
2-3.2 PowerOff

It's for IC card deactivation.



2-3.3 CardCheck

It's to check IC card is inserted.

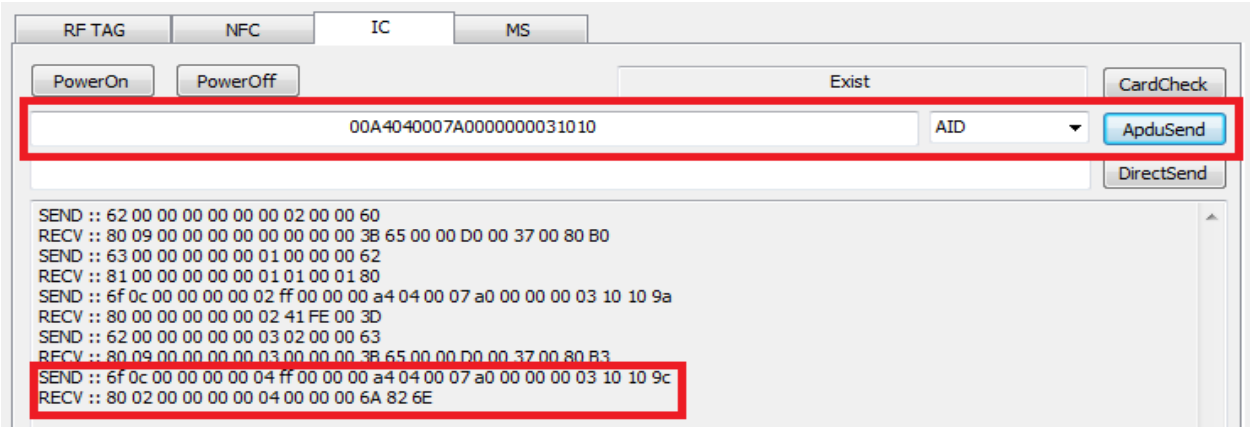


* Exist or No Exist

2-3.4 ApduSend

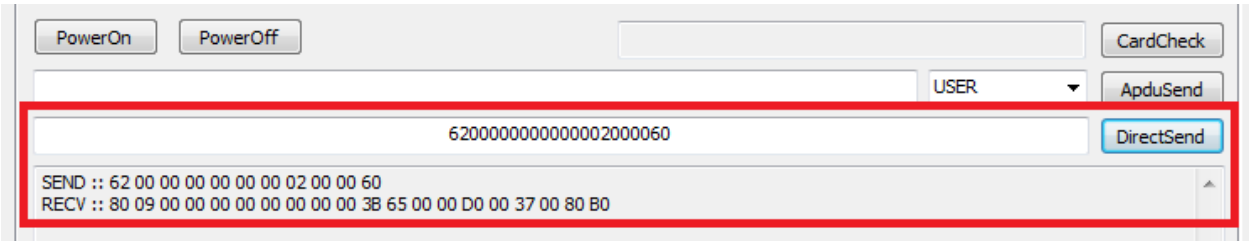
It's for APDU data transaction with inserted IC card.

* You can choose APDU sample data for the test.



♠ This command is only possible when the card is activated.

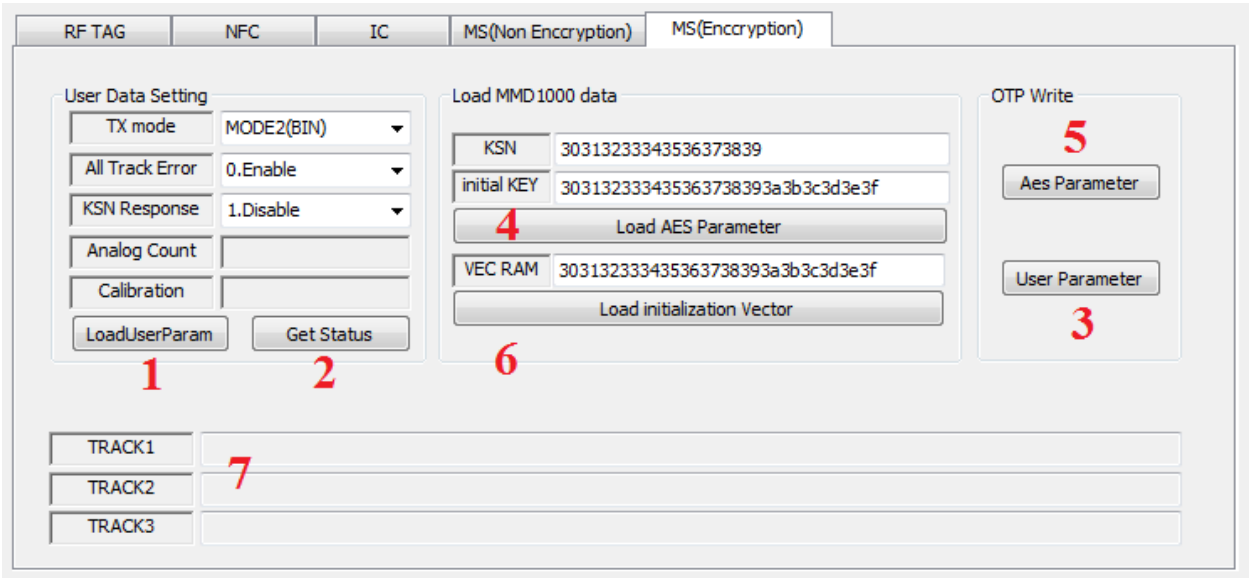
2-3.4 DirectSend



There are two tabs as;
MS (Non encryption) => card reader model “PDR-1689”.
MS (Encryption) => card reader model “MMD-1902”.

For details, you can refer the spec document of PDR-1689 (Non encryption) and MMD-1900 series (encryption).
Model name MMD-1902 is part of MMD-1900 series.

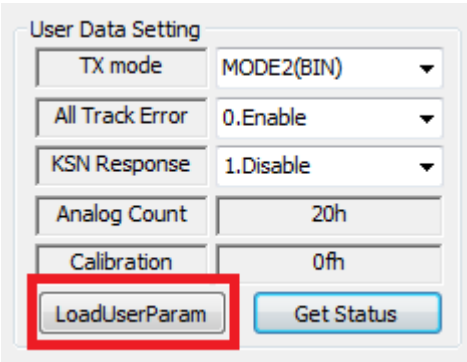
< Important>
For MS (Non encryption) test, TX MODE must be “MODE2”.
If you choose the mode 4, 6 which is for encryption mode, you cannot read MS track data.



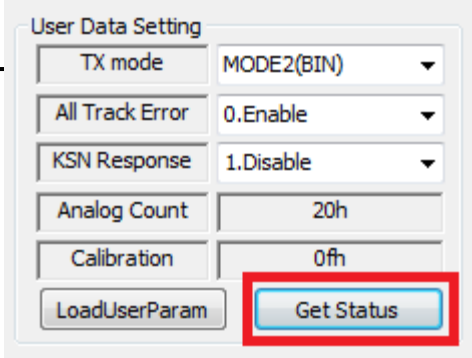
Following is the explanation about MS (Encryption) test, using card reader model “MMD-1902”.

2-4.1 LoadUserParam

<Important>
For security purpose, OTP Write is only possible maximum 2 times only.
If over 2times, OTP Write will not work any longer.
Therefore, please be careful with configuration before “OTP write” process.



2-4.2 Get Status

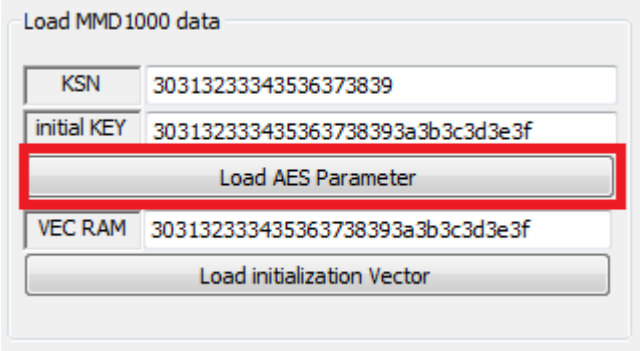


2-4.3 User Parameter OTP Write

You can do “OTP Write” maximum **2 times only**.

2-4.4 Load AES Parameter

Configurate KSN(Key Serial Number) & Initial Key.

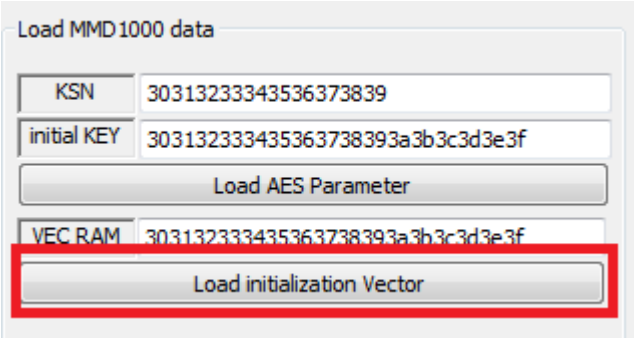


2-4.5 AES Parameter OTP Write

OTP Write Configurated AES Parameter.(OTP write is only possible maximum **2 times only**.)

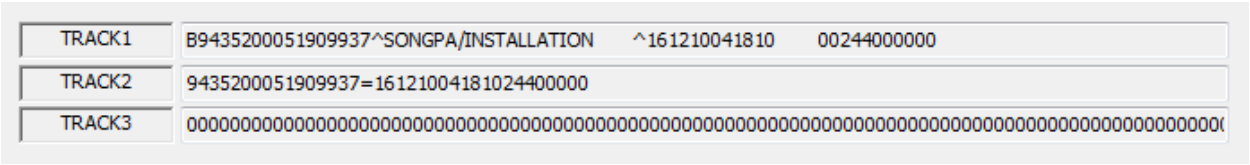
2-4.6 Load Initalization Vector

If Tx Mode is BINAES(IV:RAM), configurate “Initialization vector”.



2-4.7 Read MS Card Data

You can read MS card data.



<The contents can be changed without prior notice.>

Specification No. 3-1308-8755-Z1000