

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

	NFC-1901	REV.	
	Test program manual	X01	2 OF 17

March 24, 2014

1. Full screen of test program

The screenshot shows the CardReaderPg application window. It features a top menu bar with 'SERIAL SETTING' and 'GetVersion' buttons. Below this is a 'Connect' button and a 'GetVersion' button. The main area is divided into several sections: 'RF TAG' with tabs for 'NFC', 'IC', 'MS(Non Encryption)', and 'MS(Encryption)'; 'MIFARE' section with fields for 'SECTOR', 'BLOCK', 'KEYTYPE', and 'KEYVALUE'; 'APDU' section with 'APDU SEND' and 'USER' dropdown; 'ULTRALIGHT' section with 'BLOCK NUM' and 'ULTRA READ/WRITE' buttons; and a 'Message' section at the bottom with 'Protocol' and 'Clear' buttons. Red boxes and numbers 1 through 4 highlight specific areas: 1 points to the 'SERIAL SETTING' tab, 2 points to the 'GetVersion' button, 3 points to the 'MIFARE' section, and 4 points to the 'Message' section.

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	REV.	
NFC-1901 Firmware version check or Firmware downloading if necessary.	TEST APPLET MANIP	X01	3 OF 17

GetVersion

App DownLoad

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.

Message

Protocol

Version :: NFC-1901 V1.0

1-4.2 Protocol

You can see the each protocol status and data.

Message

Protocol

SEND :: 02 01 a0 00 00 03 a0
RECV :: 02 00 a0 00 10 4e 46 43 2d 31 39 30 31 20 56 31 2e 30 00 00 03 87

	NFC-1901	REV.	
2. Function explanation	Test program manual	X01	4 OF 17

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 + PUP1

* 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	NFC-1901	REV.	
	Test program manual	X01	5 OF 17

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

The screenshot shows a software interface for testing NFC cards. It includes a 'CARD DETECT' button, a dropdown menu currently set to 'MIFARE', a 'CARD ACTIVATION' button, and a 'DETECT START' button. Below these is a text field containing the hex value '41 08 8C 9C 84 19'.

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

FELICA 212 Card response 46 01 14 01 01 01 02 12 36 0E FF 08 10 0B 4B 42 84 85 D0 FF 00 03	NFC-1901	REV.	
	Test program manual	X01	6 OF 17

- 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

CARD DETECT

MIFARE

CARD ACTIVATION

DETECT START

00 04 08 04 8C 9C 84 19

2-1.3 DETECT START & STOP

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

CARD DETECT

MIFARE

CARD ACTIVATION

DETECT STOP

41 08 8C 9C 84 19

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.

APDU

APDU SEND

AID

00A4040007A0000000031010

6A82

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

2-1.5 ULTRA READ	NFC-1901	REV.	
	Test program manual	X01	7 OF 17

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

ULTRALIGHT

BLOCK NUM **ULTRA READ**

♣ 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).

ULTRALIGHT

BLOCK NUM **ULTRA WRITE**

♣ 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 : FFFFFFFFFF (NEW KEY)

NFC CARD_SECTOR0 : A0A1A2A3A4A5 (AID)

NFC CARD_SECTOR1~ : D3F7D3F7D3F7 (PUBLIC)

MIFARE

SECTOR BLOCK KEYTYPE

KEYVALUE

LOAD KEY

LoadKey Success

♣ 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

	NFC-1901	REV.	
		X01	8 OF 17

MIFARE

SECTOR

2

BLOCK

2

KEYTYPE

A

KEYVALUE

PUBLIC

D3F7D3F7D3F7

LOAD KEY

READ BLOCK

WRITE BLOCK

45717569706D656E74466F726D2E6A73

♣ 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

MIFARE

SECTOR

2

BLOCK

2

KEYTYPE

A

KEYVALUE

PUBLIC

D3F7D3F7D3F7

LOAD KEY

READ BLOCK

WRITE BLOCK

45717569706D656E74466F726D2E6A73

♣ 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).

READ SECTOR

WRITE SECTOR

3A383038302F574449532F6D616E6167

656D656E742F65717569706D656E742F

03AE69706D656E74466F726D2E6A7303

♣ 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).

READ SECTOR

WRITE SECTOR

3A383038302F574449532F6D616E6167

656D656E742F65717569706D656E742F

03AE69706D656E74466F726D2E6A7303

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

2-1.12 GEN VALUE	NFC-1901	REV.	
	Test program manual	X01	9 OF 17

It's to write Mifare card's Value.

* Input VALUE and button click.

A screenshot of a software interface showing a button labeled "GEN VALUE" in blue text on a light blue background, followed by a white text input field containing the number "100".

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

2-1.13 GET VALUE

It's to read Mifare card's Value.

A screenshot of a software interface showing a button labeled "GET VALUE" in blue text on a light blue background, followed by a white text input field containing the number "100".

♣ 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.

A screenshot of a software interface showing four buttons: "GEN VALUE" (light blue), "GET VALUE" (light blue), "INCREMENT" (blue), and "DECREMENT" (light blue). Each button is followed by a white text input field. The "GEN VALUE" field contains "100", the "GET VALUE" field contains "110", the "INCREMENT" field contains "10", and the "DECREMENT" field is empty.

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

2-1.15 DECREMENT

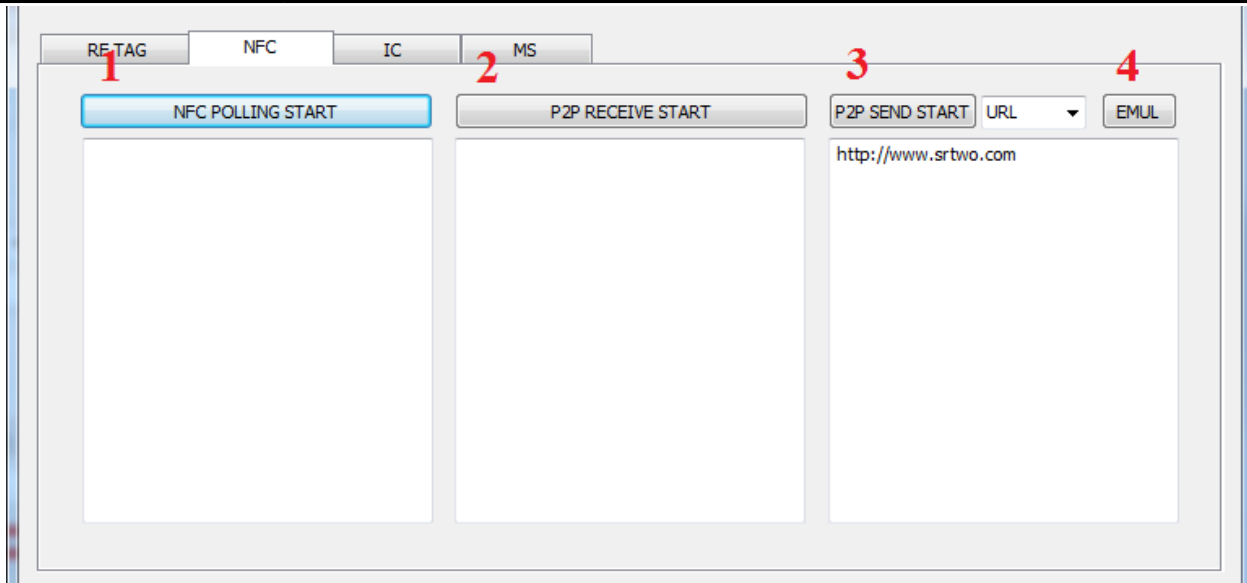
It's for Mifare card's Value increment.

* Input the decrement value and button click.

A screenshot of a software interface showing four buttons: "GEN VALUE" (light blue), "GET VALUE" (light blue), "INCREMENT" (light blue), and "DECREMENT" (blue). Each button is followed by a white text input field. The "GEN VALUE" field contains "100", the "GET VALUE" field contains "90", the "INCREMENT" field contains "10", and the "DECREMENT" field is empty.

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

2-2. NFC/P2P	NFC-1901	REV.	
	Test program manual	X01	10 OF 17



2-2.1 NFC POLLING START

Read NDEF 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 NDEF 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.

* Input the data and button click.	NFC-1901	REV.	
	Test program manual	X01	11 OF 17

2-3. IC	NFC-1901	REV.	
	Test program manual	X01	12 OF 17

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

RF TAGNFCICMS

PowerOn

PowerOff

3

CardCheck

1

2

USER

4

ApduSend

5

DirectSend

2-3.1 PowerOn

It's for IC card actiation.

PowerOn

PowerOff

CardCheck

USER

ApduSend

DirectSend

SEND :: 62 00 00 00 00 00 02 00 00 60

RECV :: 80 09 00 00 00 00 00 00 00 38 65 00 00 D0 00 37 00 80 80

2-3.2 PowerOff

It's for IC card deactivation.

PowerOn

PowerOff

CardCheck

USER

ApduSend

DirectSend

SEND :: 62 00 00 00 00 00 02 00 00 60

RECV :: 80 09 00 00 00 00 00 00 00 38 65 00 00 D0 00 37 00 80 80

SEND :: 63 00 00 00 00 00 01 00 00 62

RECV :: 81 00 00 00 00 00 01 01 00 01 80

2-3.3 CardCheck

It's to check IC card is inserted.

		NFC-1901		REV.	
<input type="button" value="PowerOn"/> <input type="button" value="PowerOff"/>		<input type="button" value="Exist"/>		<input type="button" value="CardCheck"/>	3 OF 17
		<input type="text" value="USER"/>		<input type="button" value="ApduSend"/>	

* 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.

RF TAG	NFC	IC	MS
<input type="button" value="PowerOn"/> <input type="button" value="PowerOff"/>		<input type="button" value="Exist"/>	<input type="button" value="CardCheck"/>
<input type="text" value="00A4040007A0000000031010"/>		<input type="button" value="AID"/>	<input type="button" value="ApduSend"/>
		<input type="button" value="DirectSend"/>	
<pre> SEND :: 62 00 00 00 00 00 02 00 00 60 RECV :: 80 09 00 00 00 00 00 00 00 3B 65 00 00 D0 00 37 00 80 B0 SEND :: 63 00 00 00 00 00 01 00 00 00 62 RECV :: 81 00 00 00 00 00 01 01 00 01 80 SEND :: 6F 0c 00 00 00 00 02 ff 00 00 00 a4 04 00 07 a0 00 00 03 10 10 9a RECV :: 80 00 00 00 00 00 02 41 FE 00 3D SEND :: 62 00 00 00 00 00 03 02 00 00 63 RECV :: 80 09 00 00 00 00 03 00 00 00 3B 65 00 00 D0 00 37 00 80 B3 SEND :: 6F 0c 00 00 00 00 04 ff 00 00 00 a4 04 00 07 a0 00 00 03 10 10 9c RECV :: 80 02 00 00 00 00 04 00 00 00 6A 82 6E </pre>			

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

2-3.4 DirectSend

<input type="button" value="PowerOn"/> <input type="button" value="PowerOff"/>		<input type="button" value="CardCheck"/>
<input type="text" value="USER"/>	<input type="button" value="ApduSend"/>	
<input type="text" value="62000000000000002000060"/>	<input type="button" value="DirectSend"/>	
<pre> SEND :: 62 00 00 00 00 00 02 00 00 60 RECV :: 80 09 00 00 00 00 00 00 00 3B 65 00 00 D0 00 37 00 80 B0 </pre>		

2-4. MS There are two tabs as;	NFC-1901	REV.	
	Test program manual	X01	14 OF 17

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.

The screenshot shows the 'MS(Non Encryption)' tab selected. The interface includes several sections:

- User Data Setting:** Contains dropdowns for TX mode (MODE2(BIN)), All Track Error (0.Enable), and KSN Response (1.Disable). It also has input fields for Analog Count and Calibration, and buttons for LoadUserParam (1) and Get Status (2).
- Load MMD 1000 data:** Contains input fields for KSN, initial KEY, and VEC RAM, all with the same hexadecimal value. It has buttons for Load AES Parameter (4) and Load initialization Vector (6).
- OTP Write:** Contains buttons for Aes Parameter (5) and User Parameter (3).
- TRACKS:** A section at the bottom with input fields for TRACK1, TRACK2, and TRACK3, highlighted by a red number 7.

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.

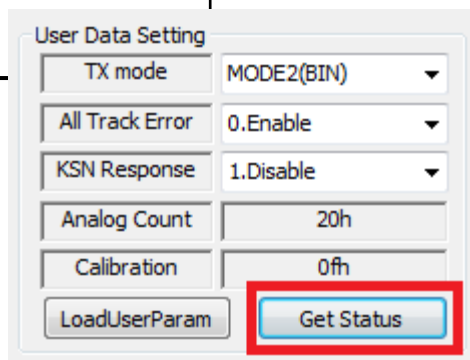
If over 2times, OTP Write will not work any longer.

Therefore, please be careful with configuration before "OTP write" process.

This close-up shows the 'User Data Setting' section. The 'LoadUserParam' button is highlighted with a red rectangle, indicating it is the focus of this section.

2-4.2 Get Status

	NFC-1901	REV.	
	program manual	X01	15 OF 17

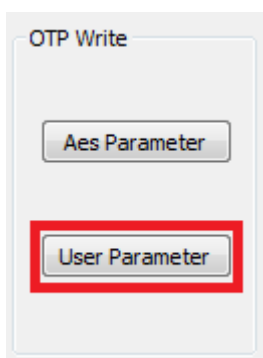


User Data Setting

TX mode	MODE2(BIN)
All Track Error	0.Enable
KSN Response	1.Disable
Analog Count	20h
Calibration	0fh
LoadUserParam	Get Status

2-4.3 User Parameter OTP Write

You can do "OTP Write" maximum **2 times only**.

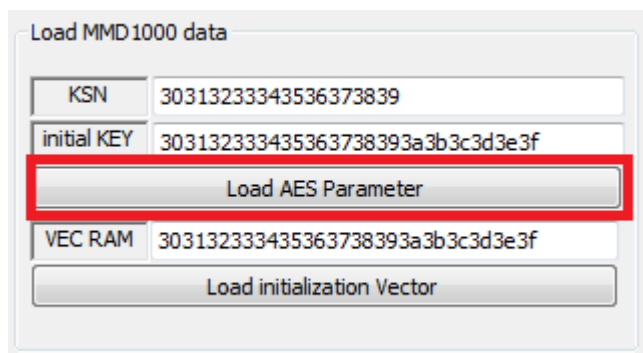


OTP Write

Aes Parameter
User Parameter

2-4.4 Load AES Parameter

Configure KSN(Key Serial Number) & Initial Key.



Load MMD1000 data

KSN	30313233343536373839
initial KEY	303132333435363738393a3b3c3d3e3f
Load AES Parameter	
VEC RAM	303132333435363738393a3b3c3d3e3f
Load initialization Vector	

2-4.5 AES Parameter OTP Write

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

Specification No. 3-1308-8755-Z1000