Software User Manual

HF Reader Testing Demo

(ISO14443A/B,MIFARE DESFire,ISO15693)

(Version 1.1)

*All rights reserved, and the contents may be revised without notice

Contents

1. Introduction

This testing demo is offered for the basic functions available to operate read/write and other functions of the HF series Modules and Reader products designed by CHIKEK, and it supports of UART-TTL, RS232, RS485 and USB(COM) port products.

This demo is programmed basing on C# language and run under WINDOWS system.

Any other specific function not showing in this demo, can be realized by customize if there need, please contact our sales persons for details requesting.

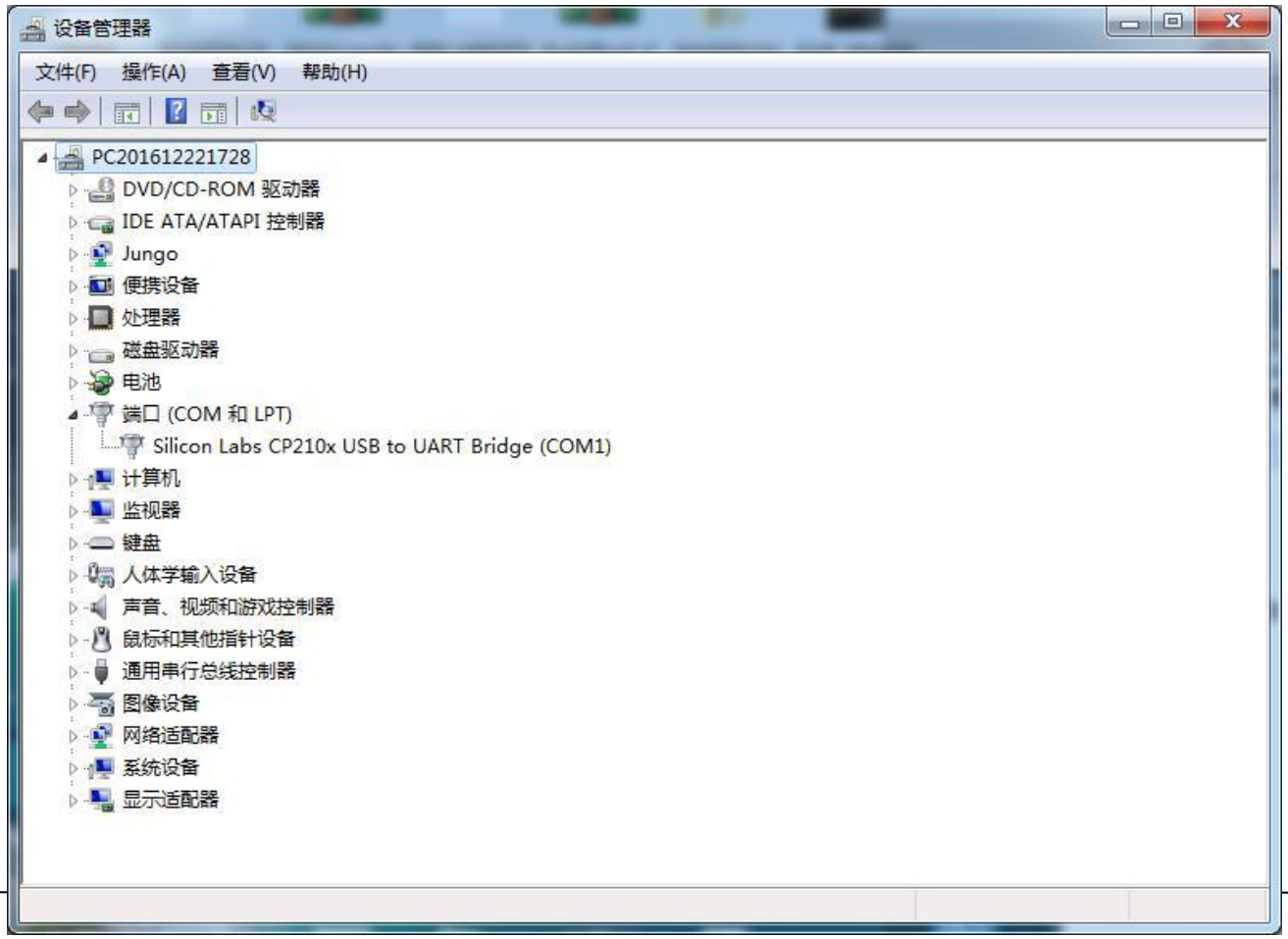
2. Operation Features

2.1 Hardware connection

For Modules series product, please firstly refer to datasheet of the specified Module using for their PIN definition and connect them with correspond mid-ware tool when testing with PC.

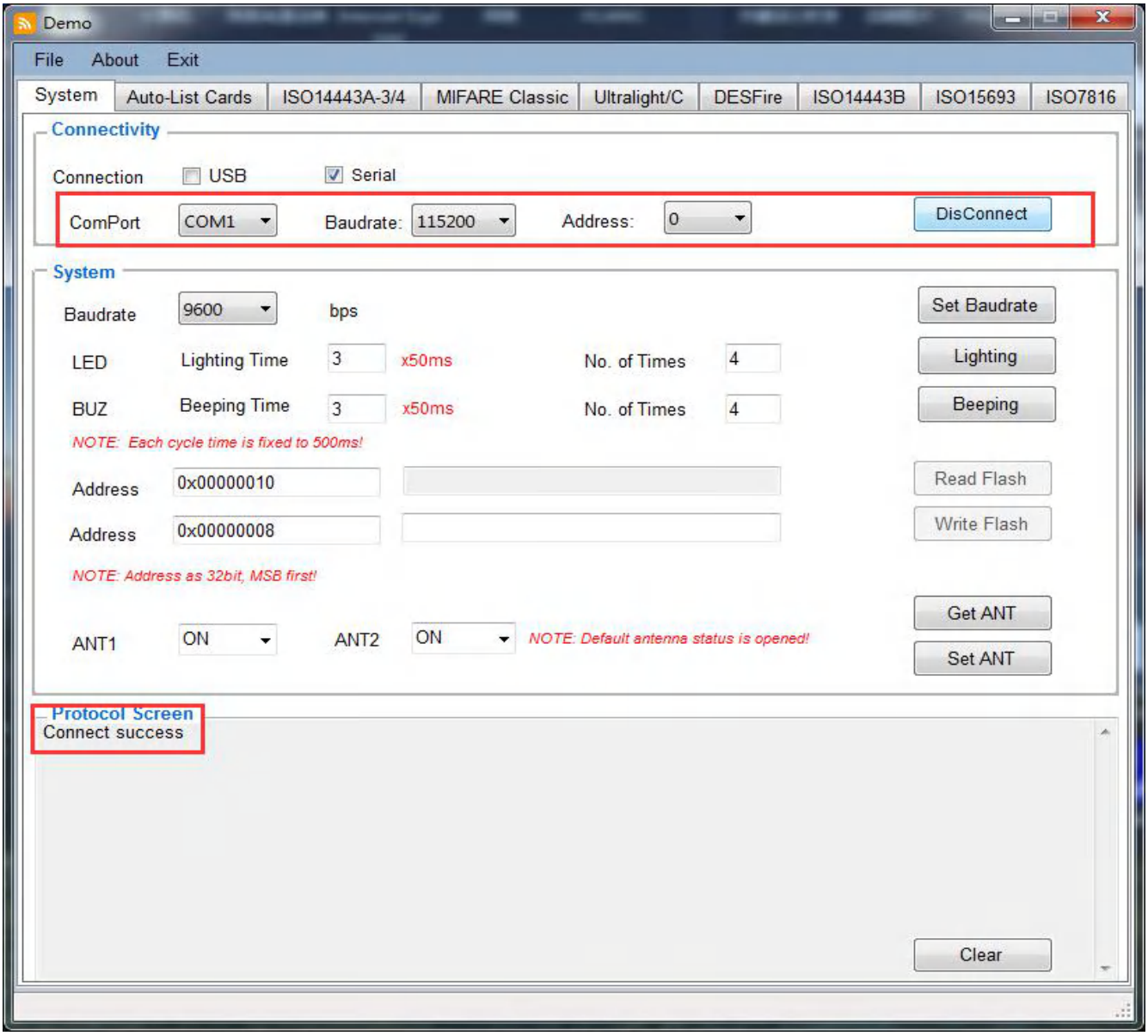
For Reader product with USB COM port, just plug USB connector to the PC side.

Then please check the COM port if be recognized in PC successfully, the way to check it is: Open Computer Manager--Device Manager--COM and LPT, as below :



2.2 Software connection

Firstly double click the DEMO EXE file to open demo software, and enter into connection interface as below:



Notes for Connectivity parameters:

Port number: Refer to Device Manager--COM&LPT, which on listing

Baudrate: Default as 115200bps, available from 9600bps ~ 115200bps;

Address: Not important

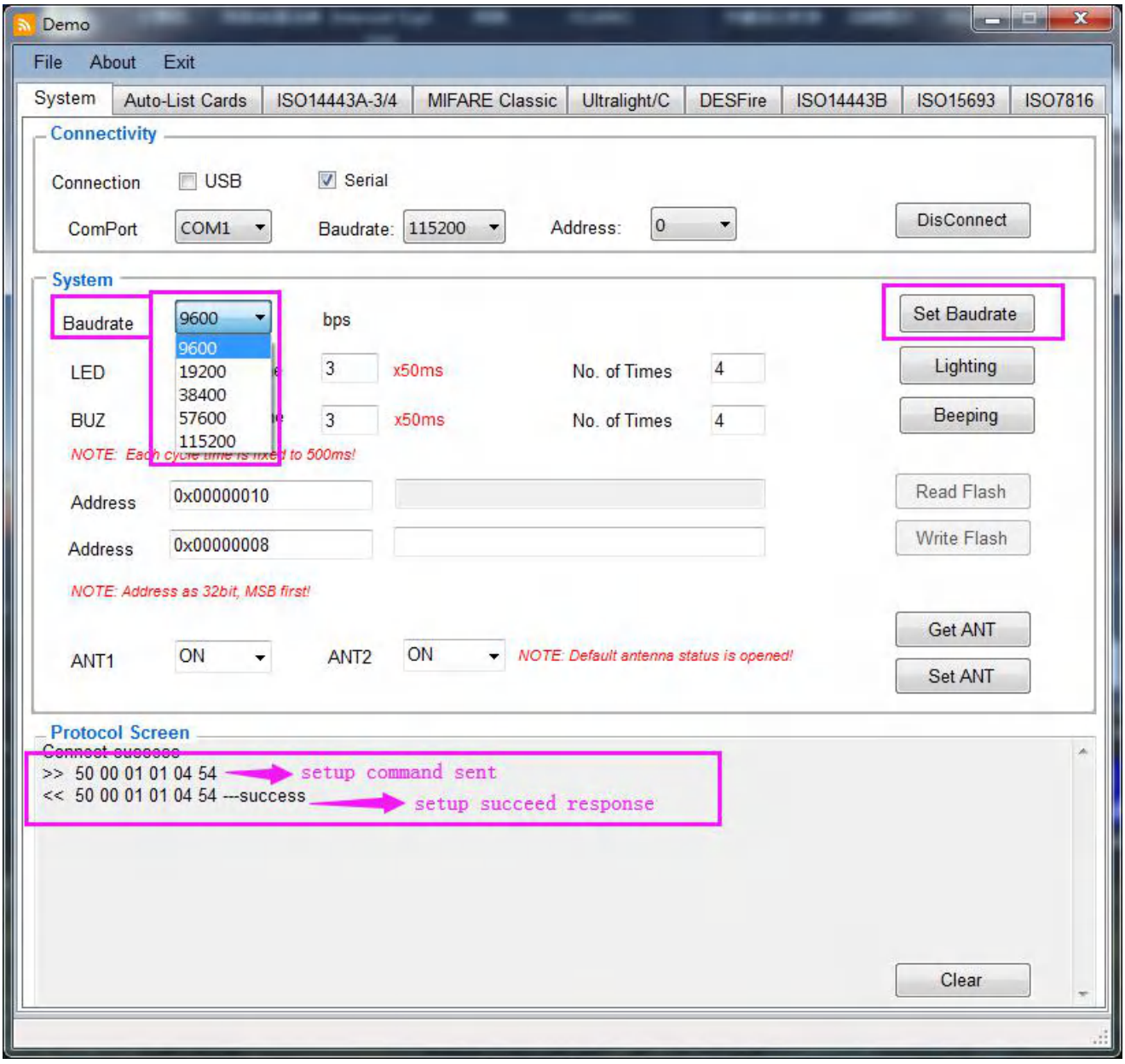
Make sure above parameters in right, then click Connect button to enter functions interface, and according response will be shown on “Protocol Screen” box.

2.3 System command

2.3.1 Set Baudrate

This function is to set according baudrate to be used in specific application. The available value is as listing and just select the right one to be set, as following show.

And in the Box of Protocol Screen, there will be showing according setup command and right succeed response.



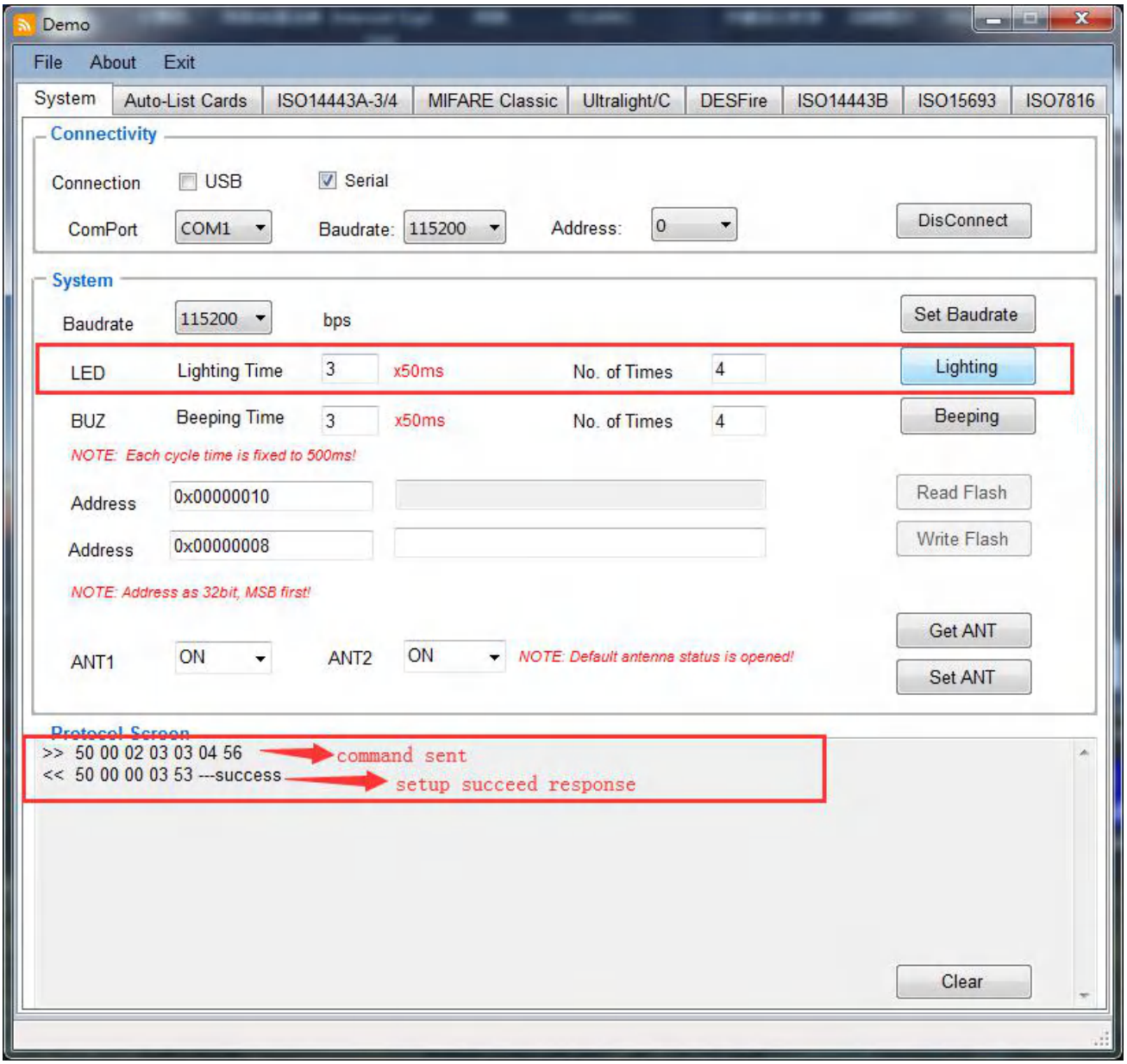
2.3.2 Set LED

This function is to set according LED's working way to be used in specific application. The available value including:

Lighting time: time length to be light, and the unit as 50ms

No. Of Times: time cycle, which means how many times to be light during whole length

And in the Box of Protocol Screen, there will be showing according setup command and right succeed response.



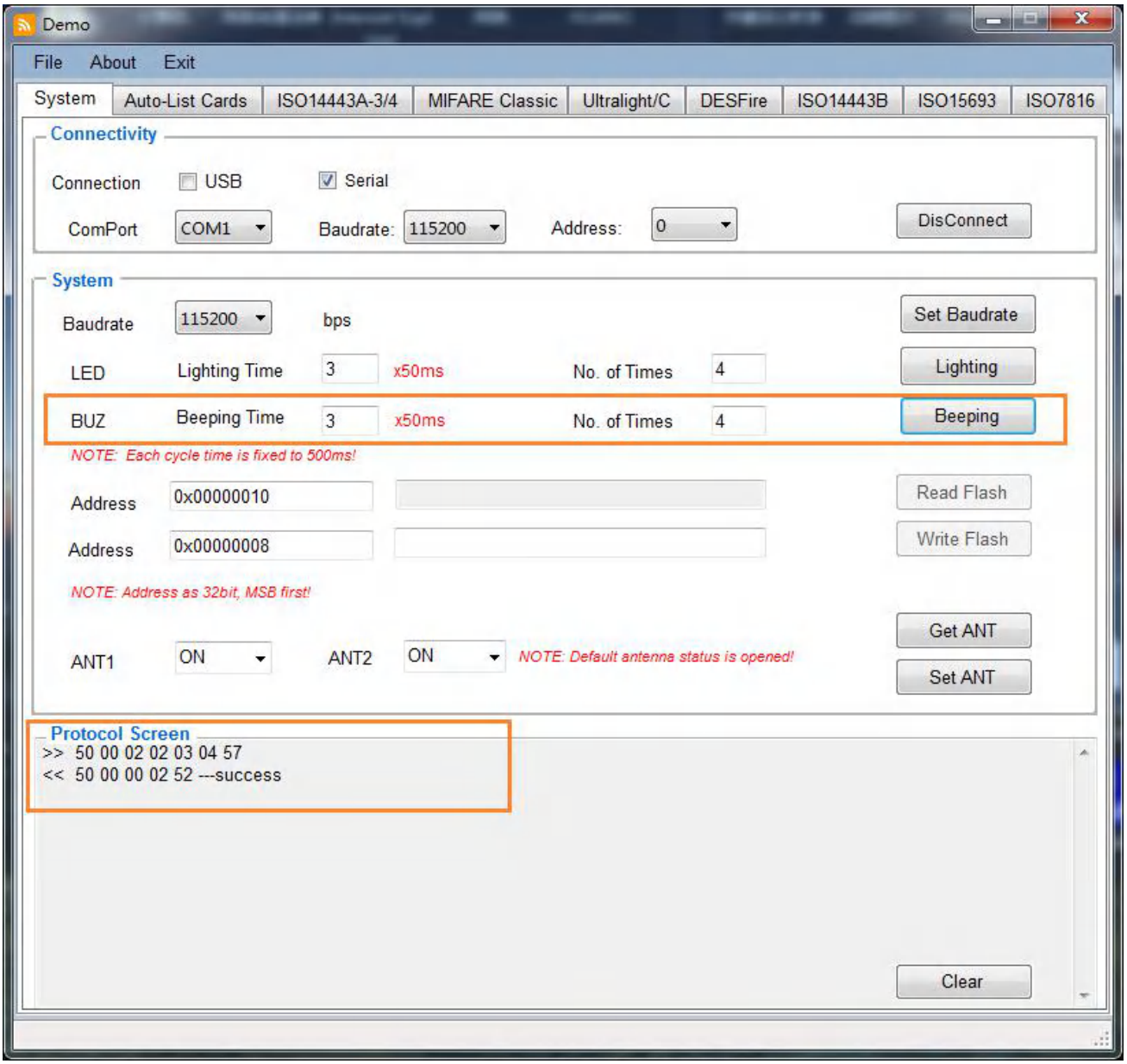
2.3.3 Set BUZ

This function is to set according buzzer's working way to be used in specific application. The available value including:

Beeping time: time length to be beeping, and the unit as 50ms

No. Of Times: time cycle, which means how many times to be beeping during whole length

And in the Box of Protocol Screen, there will be showing according setup command and right succeed response.

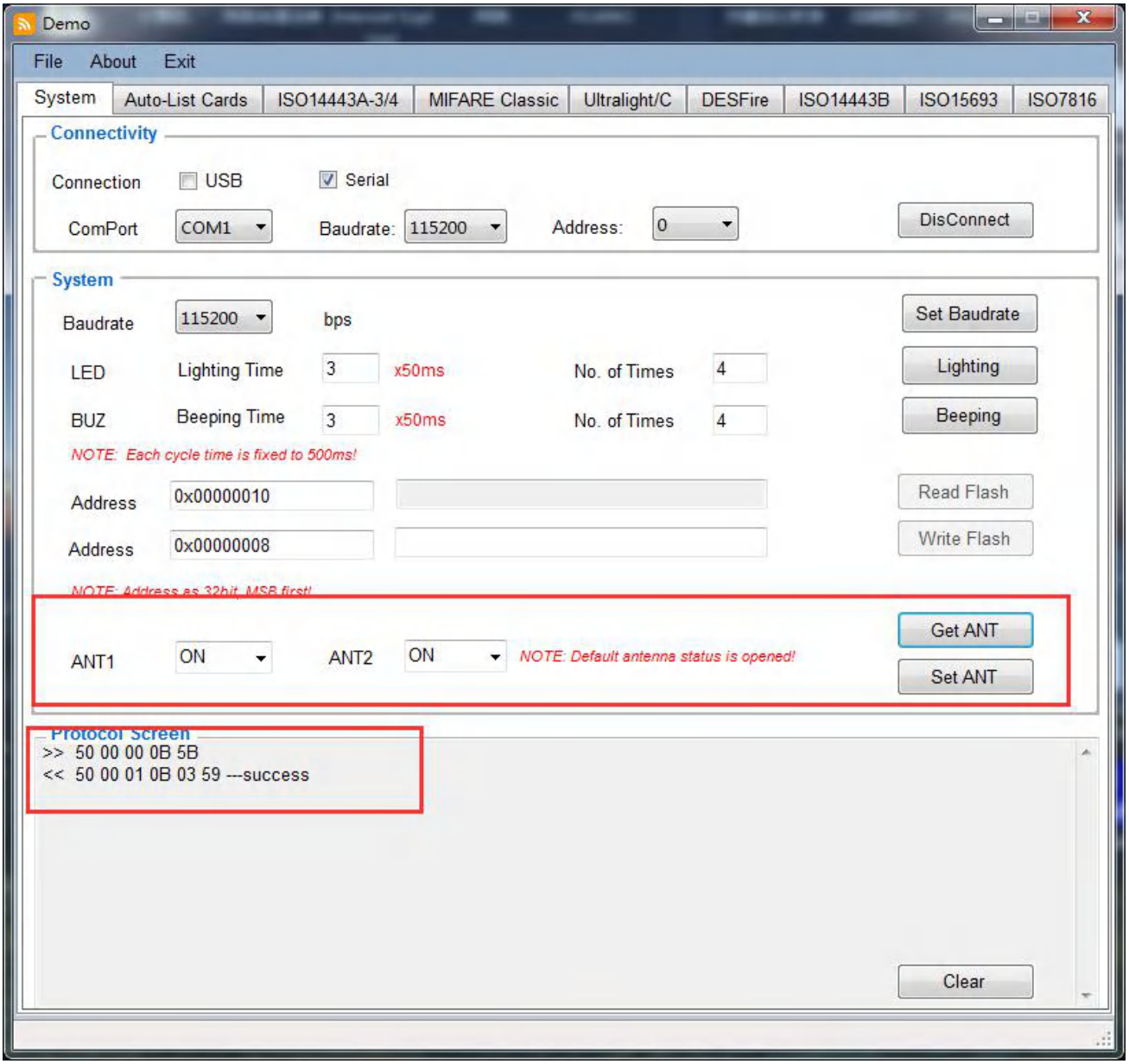


2.3.4 Set ANT

This function is to set which antenna to be ON or OFF when there are two antennas.

(Note: The antenna's default status is opened, and please refer to detail commands to do setup based on the Communication Protocol document for different product, or contact our technician for support)

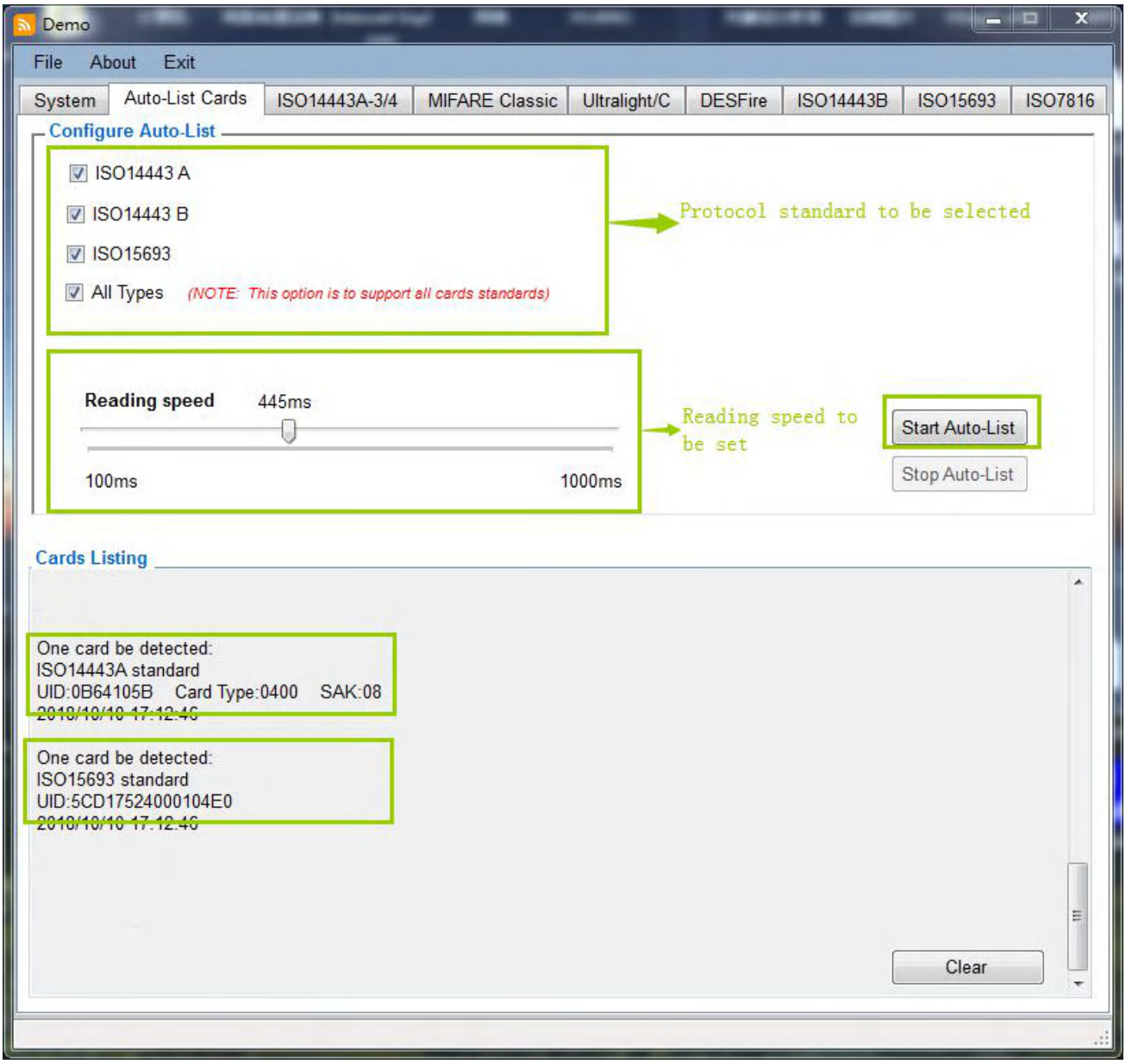
And in the Box of Protocol Screen, there will be showing according setup command and right succeed response.



This product uses an embedded PCB antenna, which is not removable and has a maximum antenna gain of 0.0dbi.

2.4 Auto-List Card

This TAB is available to do Read all cards under 13.56MHz frequency automatically, and the function can be configured Protocol standard and Reading speed as following shown, the cards information will be listing on Card Listing box:



2.5 ISO14443A-3/4

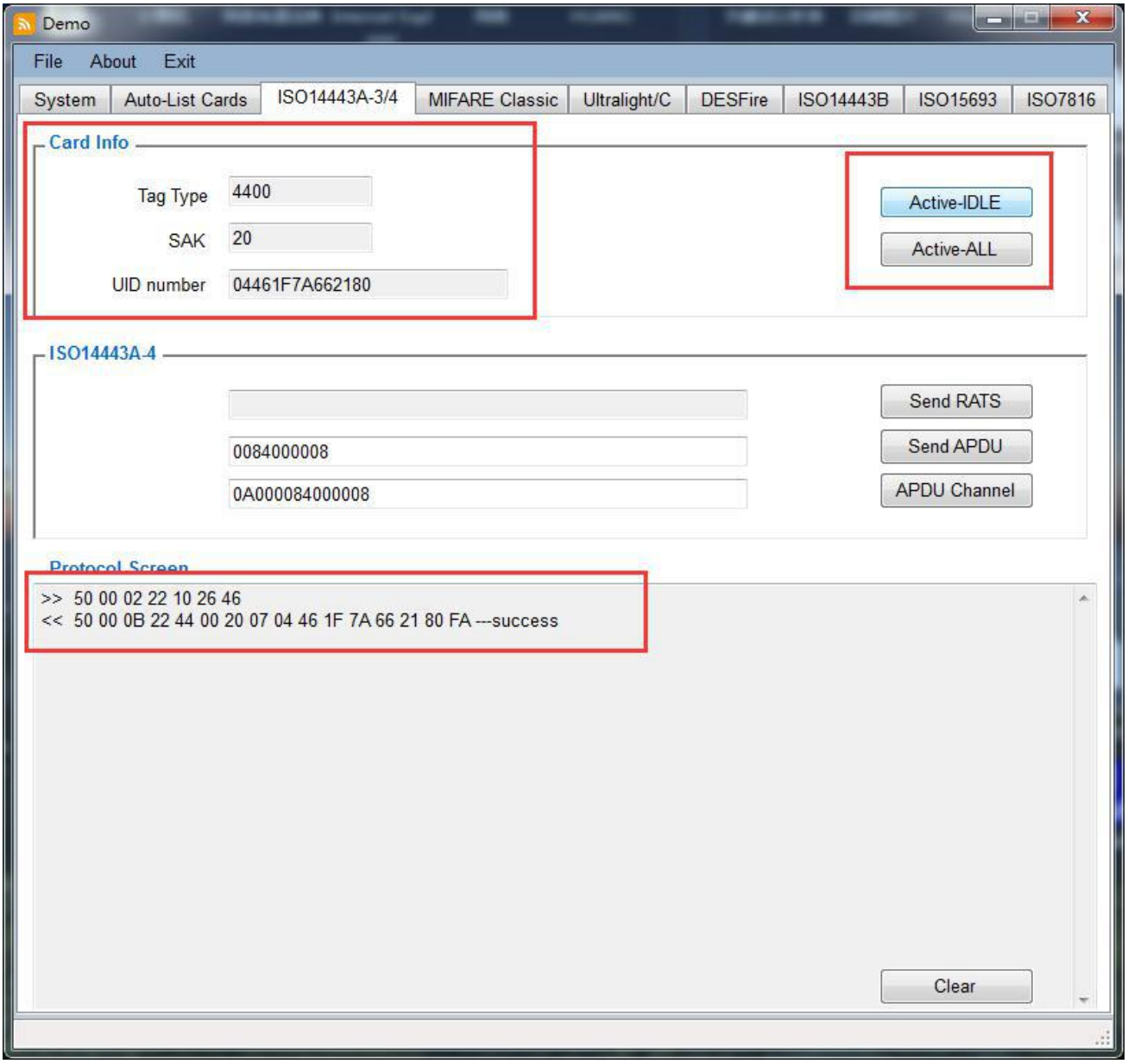
The interface is to enable ISO14443A-3 standard cards to enter into ISO14443A-4 standard and as a contactless CPU card.

2.5.1 Request card

The optional button including as below:

Active-IDLE: to request the cards not dormant

Active-ALL: Request cards including dormant cards

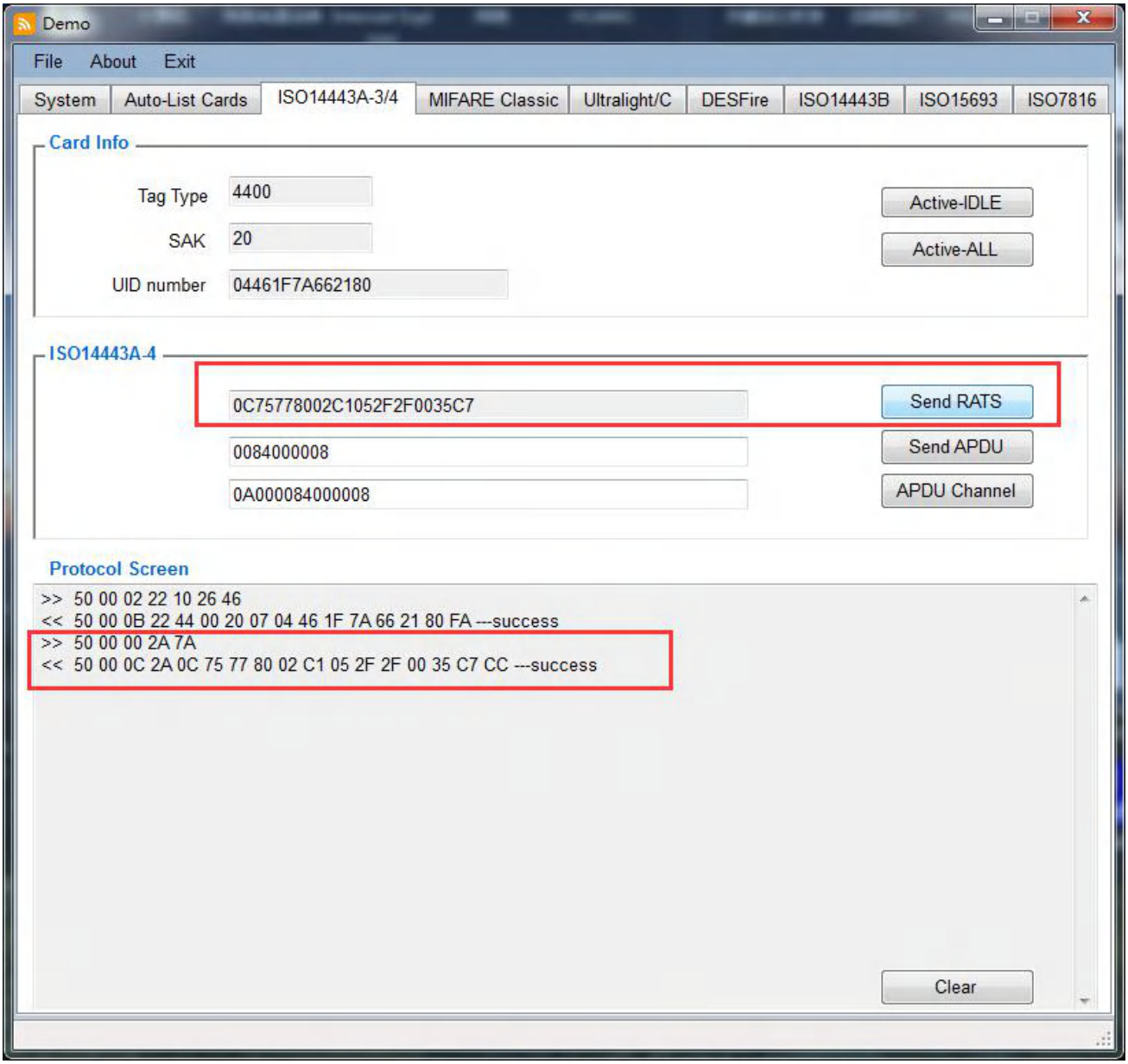


2.5.2 Send RATS

RATS= Request for Answer to Select

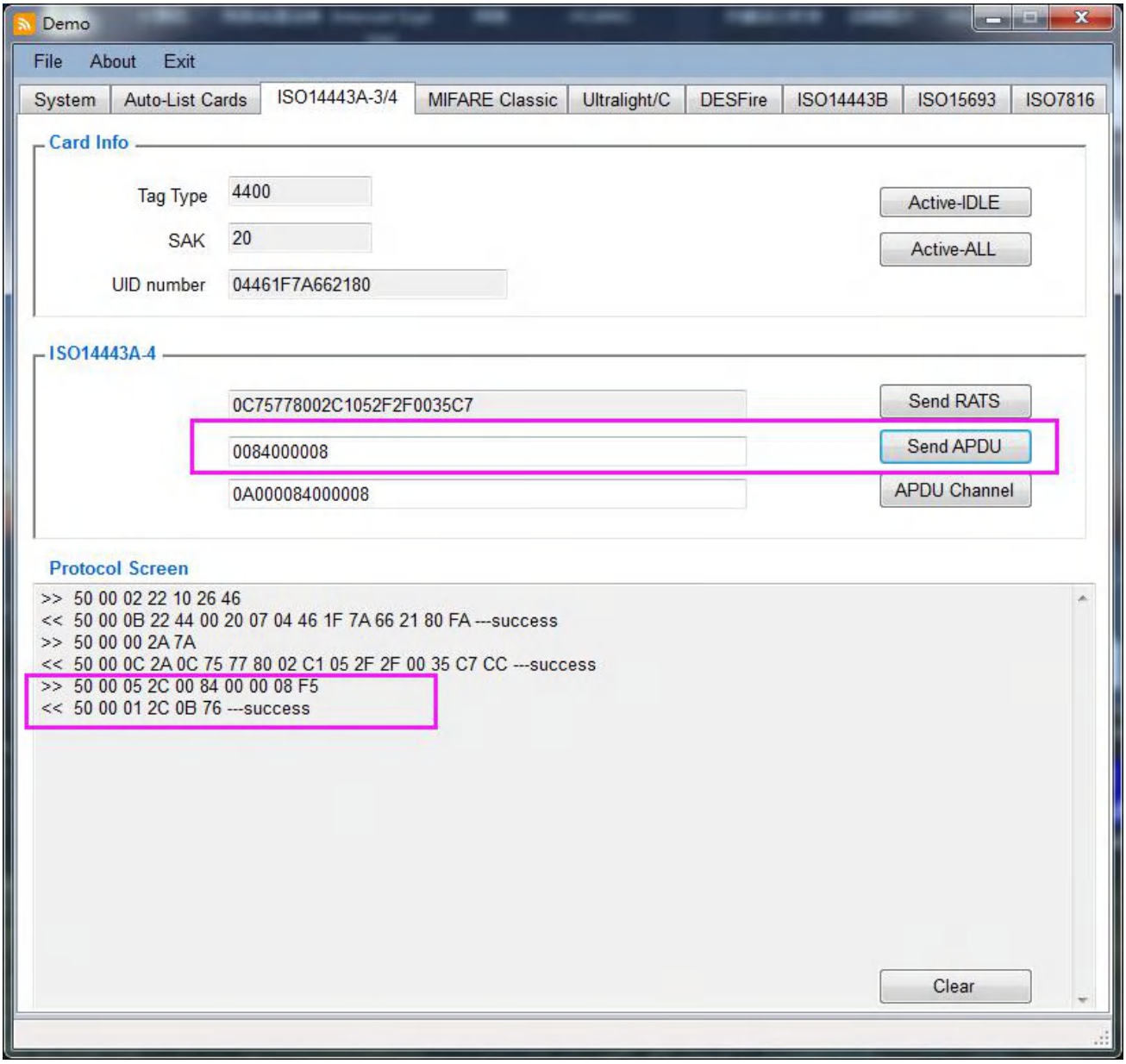
This function is to make the card quit from ISO14443A-3 enter into 14443A-4 standard, and the data returned after Send RATS, it includes the information of the testing card's.

And the response to RATS is the "Answer to Select" ATS, and the ATS consists of specified bytes for communicate between PICC capabilities and PCD. Details specific byte's meaning, please refer to datasheet of using card.



2.5.3 Send APDU

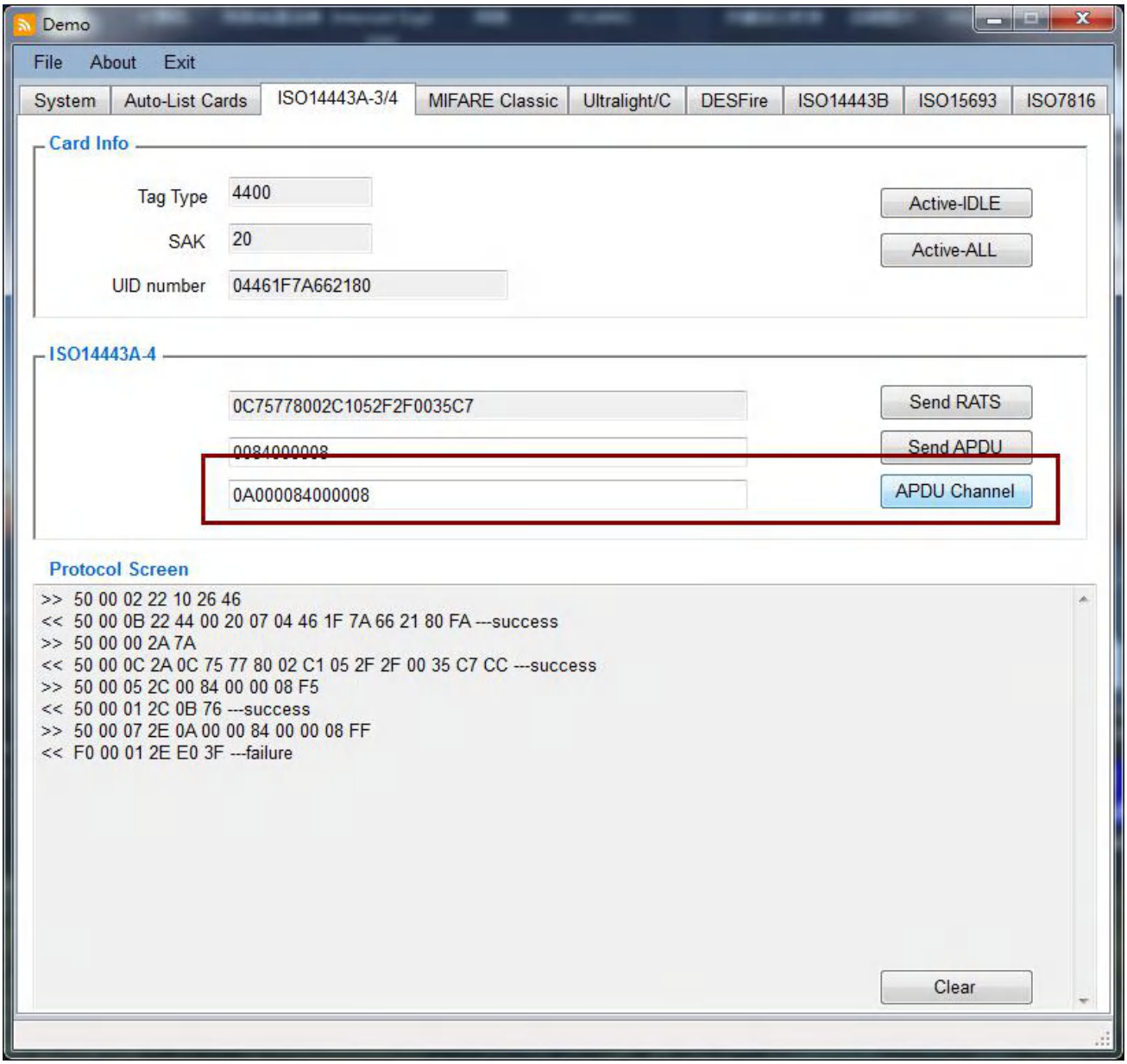
This function button is a channel opened for the APDU commands, which according to different compatible commands for different cards, and please refer to them based on the cards' datasheet.



2.5.4 APDU Channel

This is transfer channel to send any available commands to the card directly through RF chipset.

Details commands please refer to ISO14443A-4 Standard .



2.6 MIFARE Classic

This Interface is opened all available data operations specially for the MIFARE Classic series cards, including card type of MIFARE Classic 1K, MIFARE Classic 4K, etc,

The function is enable to get card details information, read and write block data, key authenticate, also the E-wallet, etc.

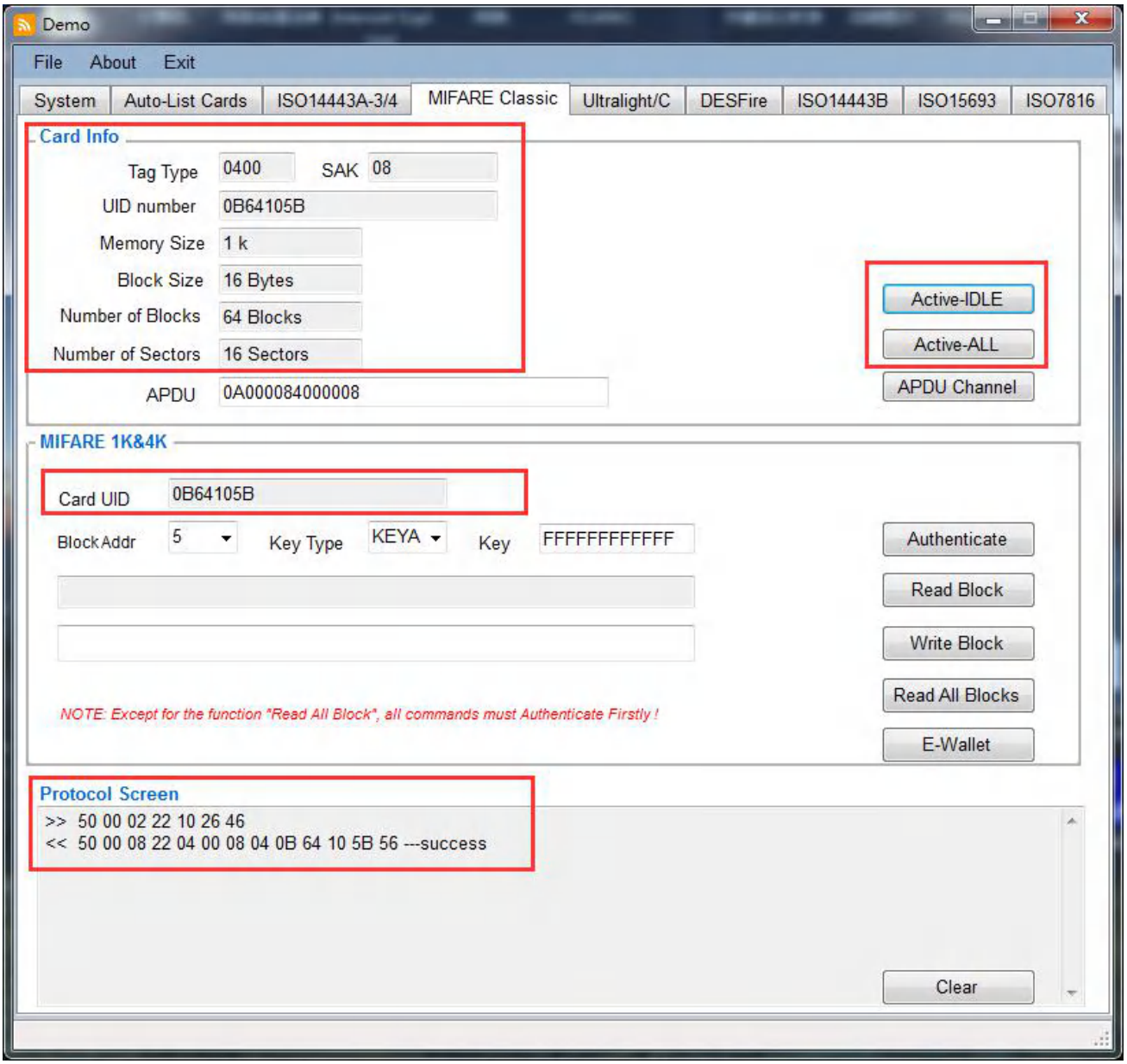
2.6.1 MIFARE Classic- Request card

The optional button including as below:

Active-IDLE: to request the cards not dormant

Active-ALL: Request cards including dormant cards

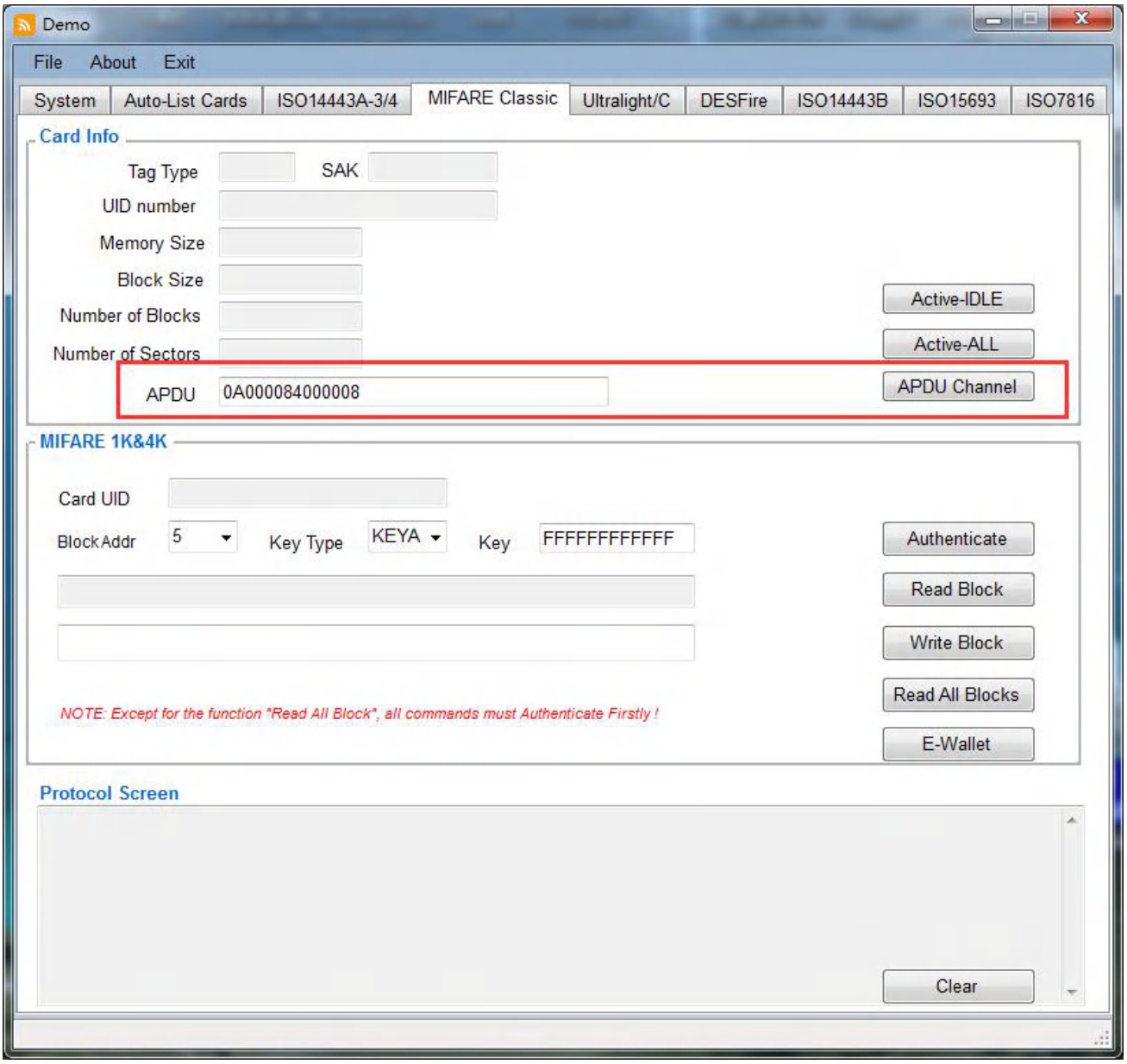
When succeeded request card, the card's details information including card type, SAK, UID number, memory sizes, etc will be shown as below:



2.6.2 MIFARE Classic-APDU Channel

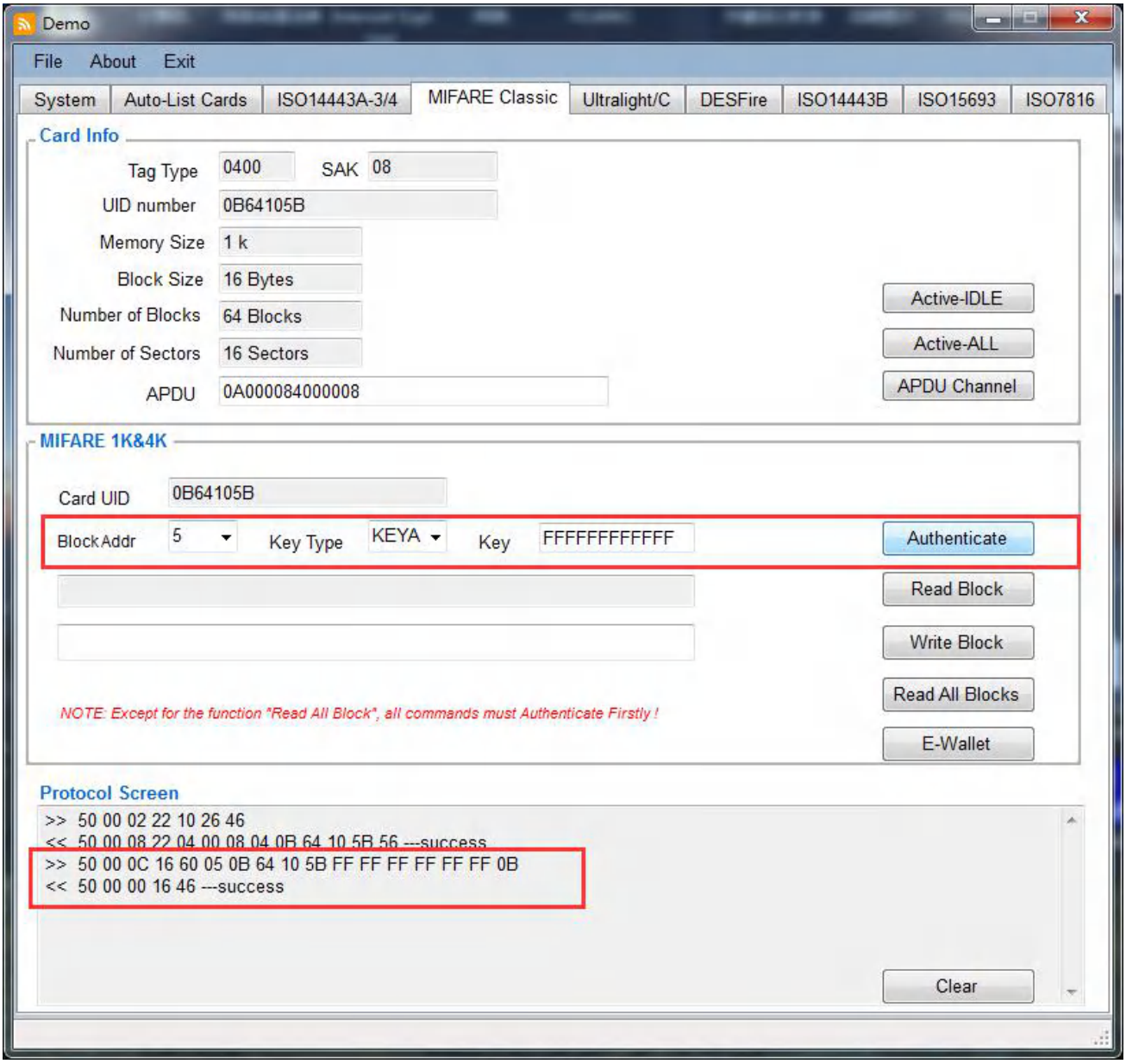
This is transfer channel to send any available commands to the card directly through RF chipset.

Details commands please refer to ISO14443A-3 Standard .



2.6.3 MIFARE Classic- Key Authenticate

This is to use according KEY to authenticate for any specific Block address, Key Type and Key value. Please select the according parameter need to be used.



Note:

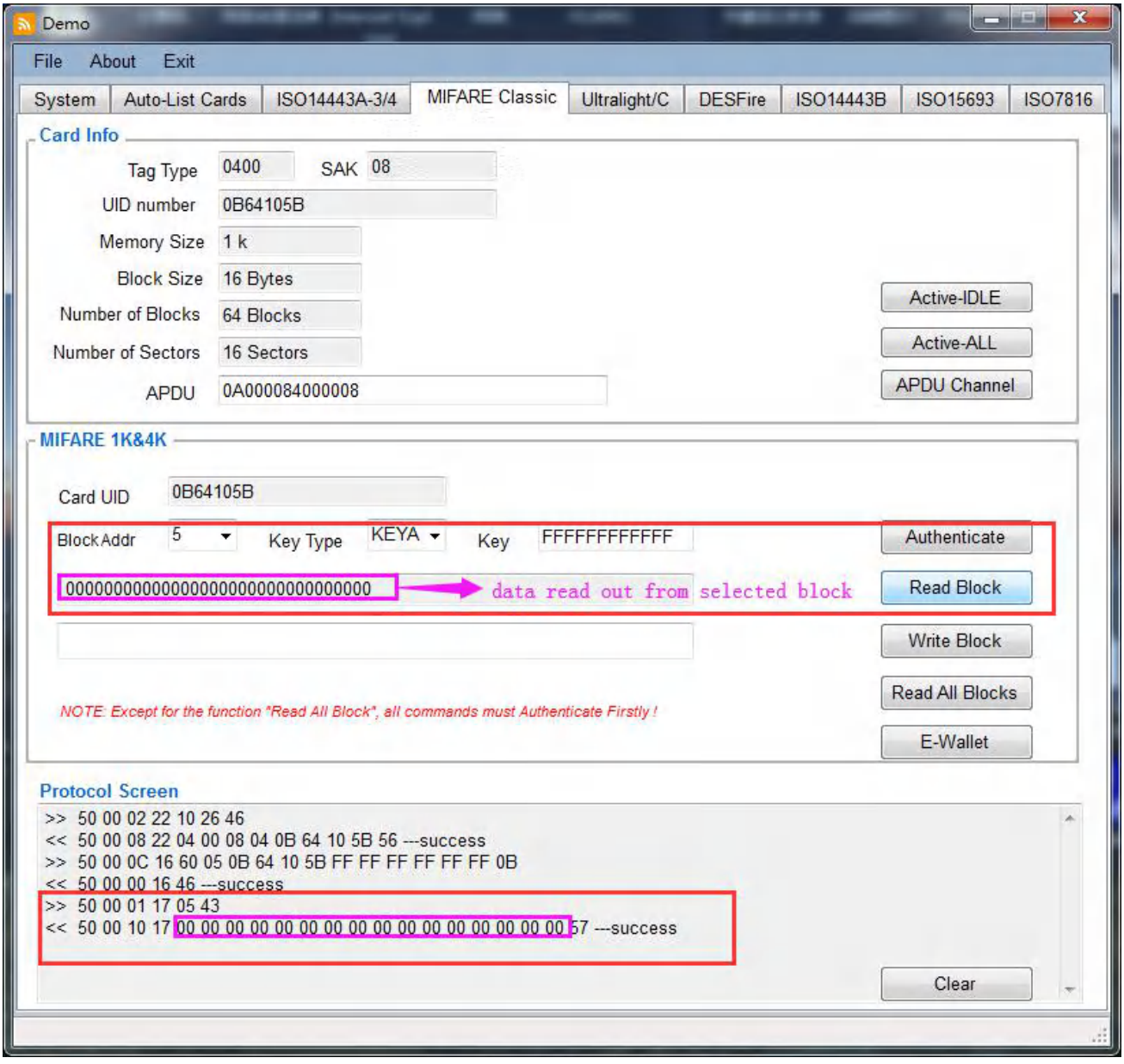
1. *The default Key value for a new MIFARE Classic 1K/4K card is FFFFFFFFFFFF when there is no change of it*
2. *Before each authenticate, it must to do Active card firstly and make sure without any remove card from antenna field.*

2.6.4 MIFARE Classic-Read Block

To get to read out the data stored in the according block address.

The parameters need to be selected including:
Block Addr: which block address to be read
Key Type: optional as KEYA or KEYB
Key: password of selected block (default value is FFFFFFFFFFFF for new card)

After Read Block, the data will be shown on the left side box also on Protocol Screen message box as below:



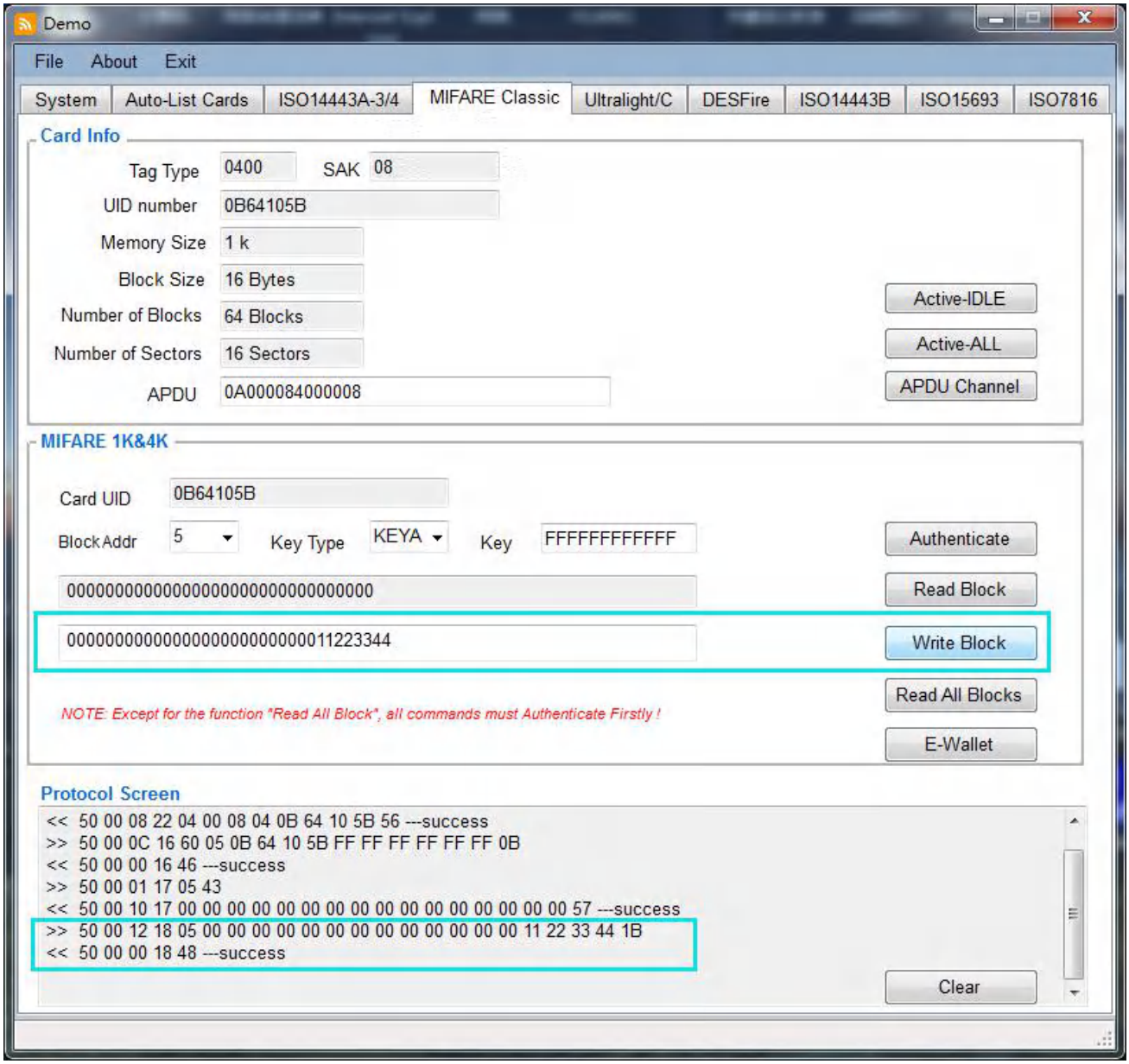
Note:

1) *Before Read Block, it must do Active card-->Authenticate firstly*
2) *Please input the right Key value for the card which changed before*

2.6.5 MIFARE Classic-Write Block

This function button is for writing data into according requested block, also for password changing operation, detail operations please refer to datasheet of MIFARE Classic cards

The parameters need to be selected including:
Block Addr: which block address to be written
Key Type: optional as KEYA or KEYB
Key: password of selected block (default value is FFFFFFFFFFFF for new card)
Data length: 16bytes



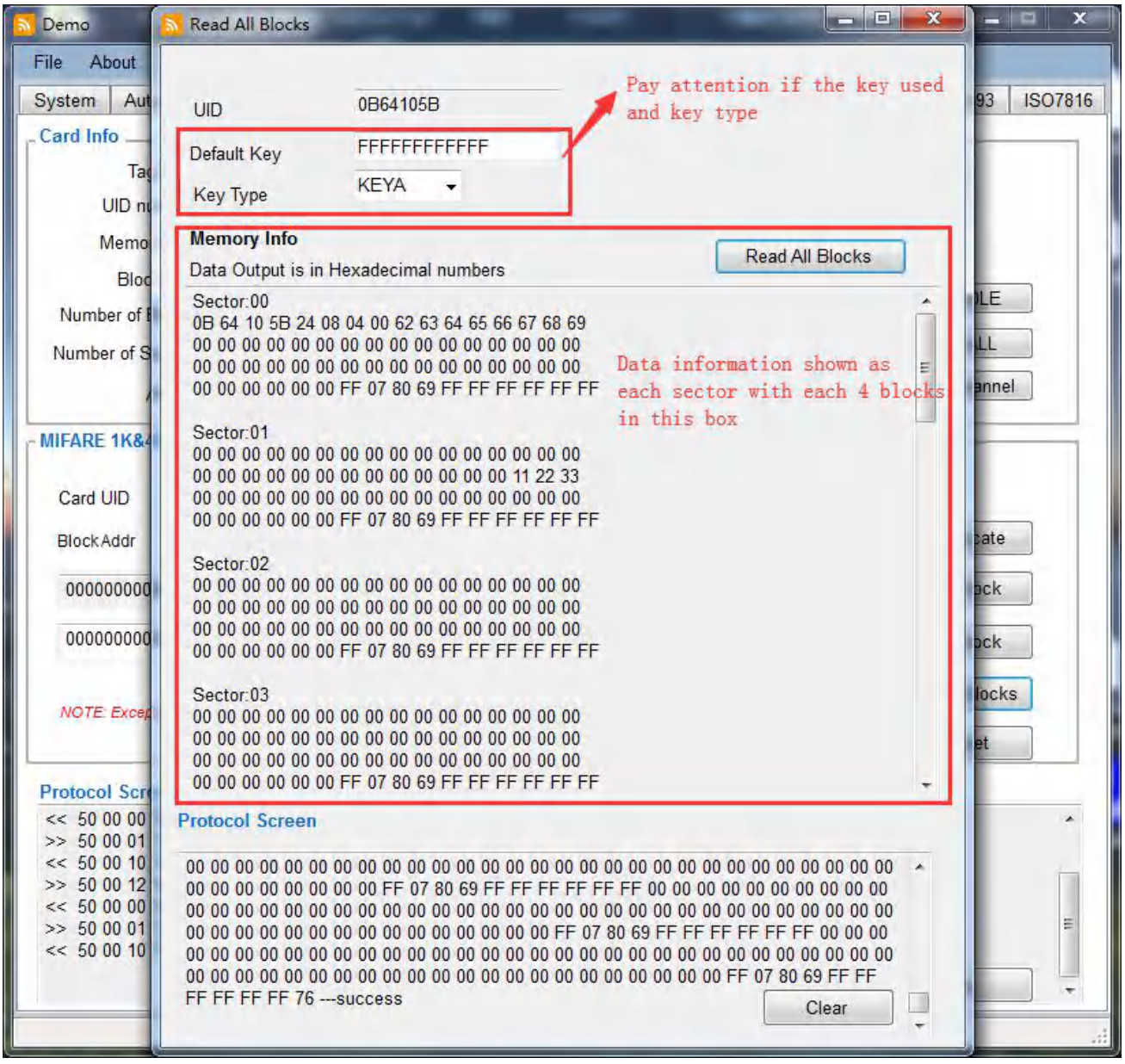
Note:

1) *Before Write Block, it must do Active card-->Authenticate firstly*
2) *Please input the right Key value for the card which changed before*
3) *Please input right data length to be written*
4) *For password writing operation, pls refer to using card's datasheet for more details*

2.6.6 MIFARE Classic-Read All Blocks

This is to get read out all blocks data in one time.

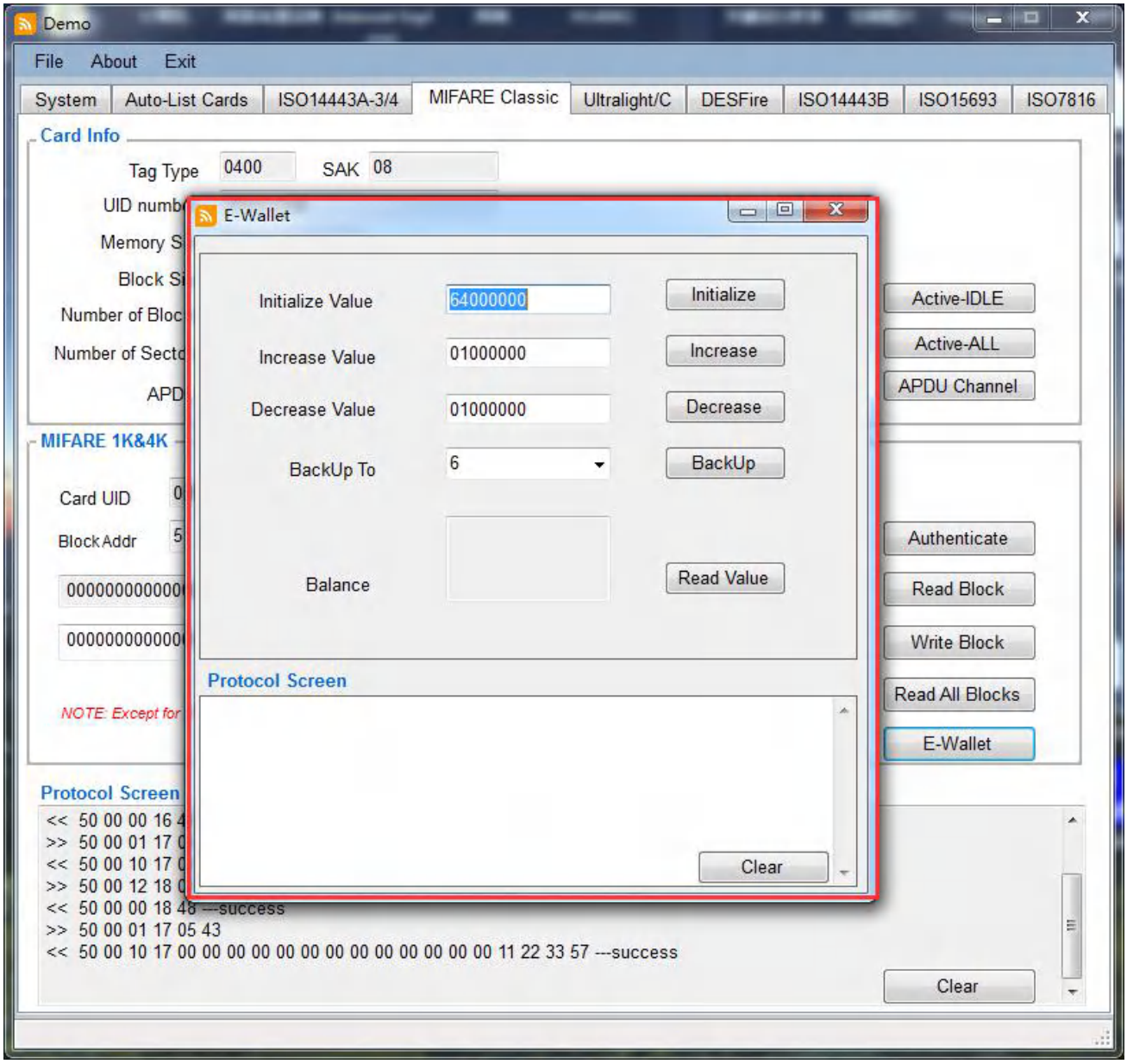
Before enter into Read All Blocks interface, it must do Active card firstly, but no need to do Authenticate. After entered Read All Blocks, please input right key value and Key Type to do Read, when succeed reading, all data information will be listing as each sector with each 4 blocks as following:



Note: When there are some sectors or blocks' key differed from others default key, their data will be failed to be read.

2.6.7 MIFARE Classic-E-wallet

This interface is available to do value operations directly for E-wallet function, please do according right setup for the values as below.



2.7 Ultralight/C

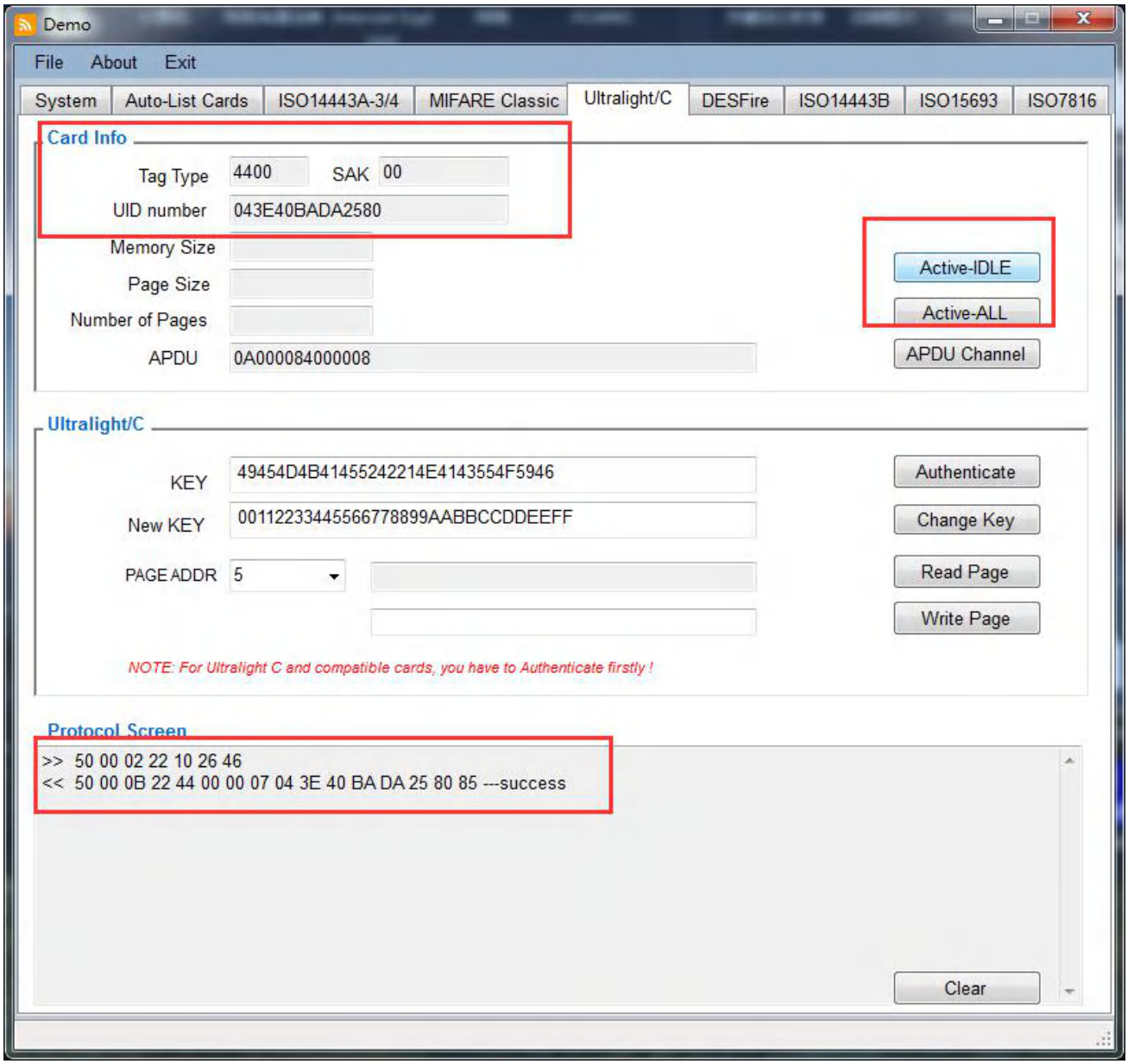
2.7.1 Ultralight/C-Active/Request Card

The optional button including as below:

Active-IDLE: to request the cards not dormant

Active-ALL: Request cards including dormant cards

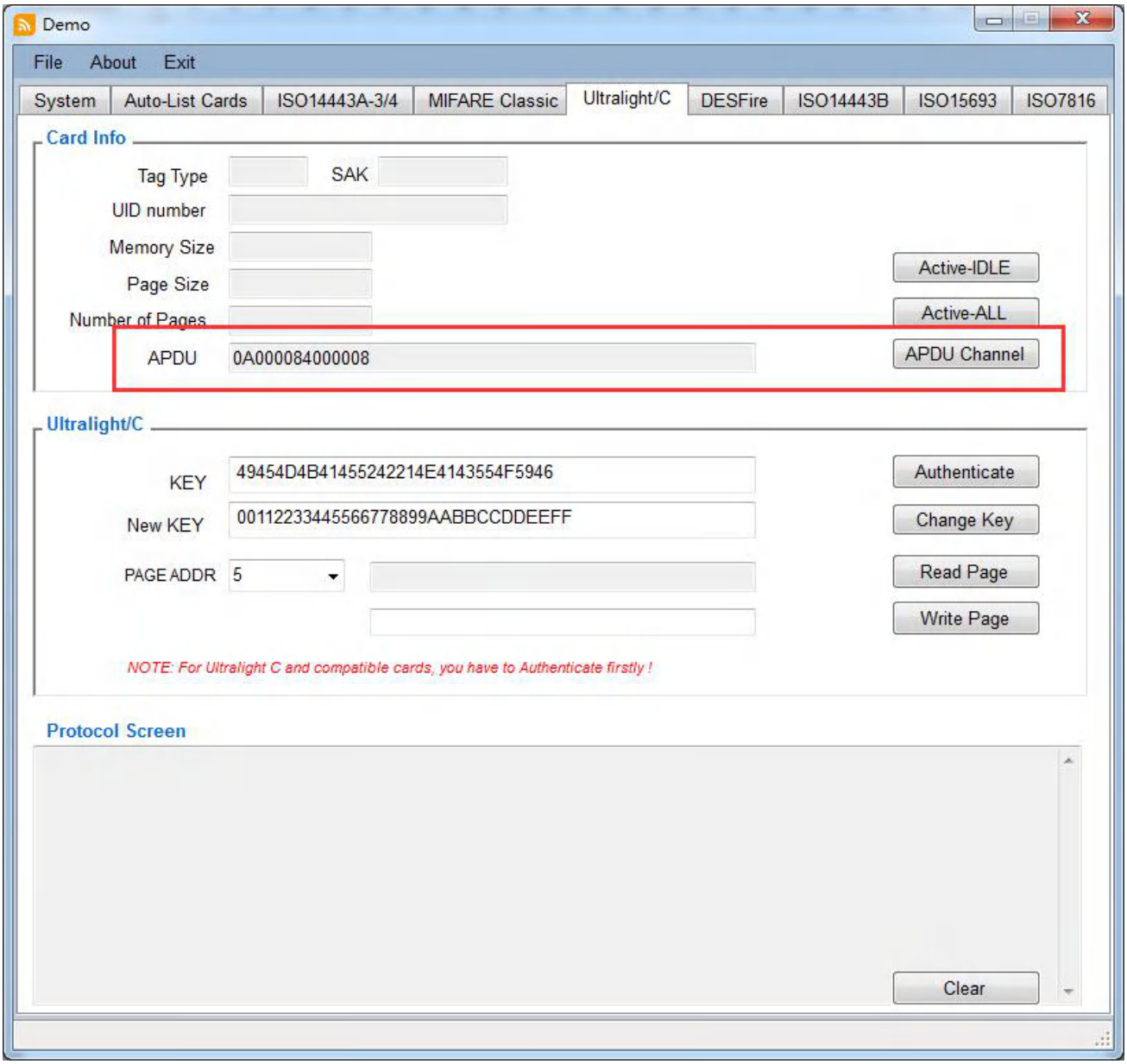
When succeeded request card, the card's details information including card type, SAK, UID number, memory sizes, etc will be shown as below:



2.7.2 Ultralight/C--APDU Channel

This is transfer channel to send any available commands to the card directly through RF chipset.

Details commands please refer to ISO14443A-4 Standard .

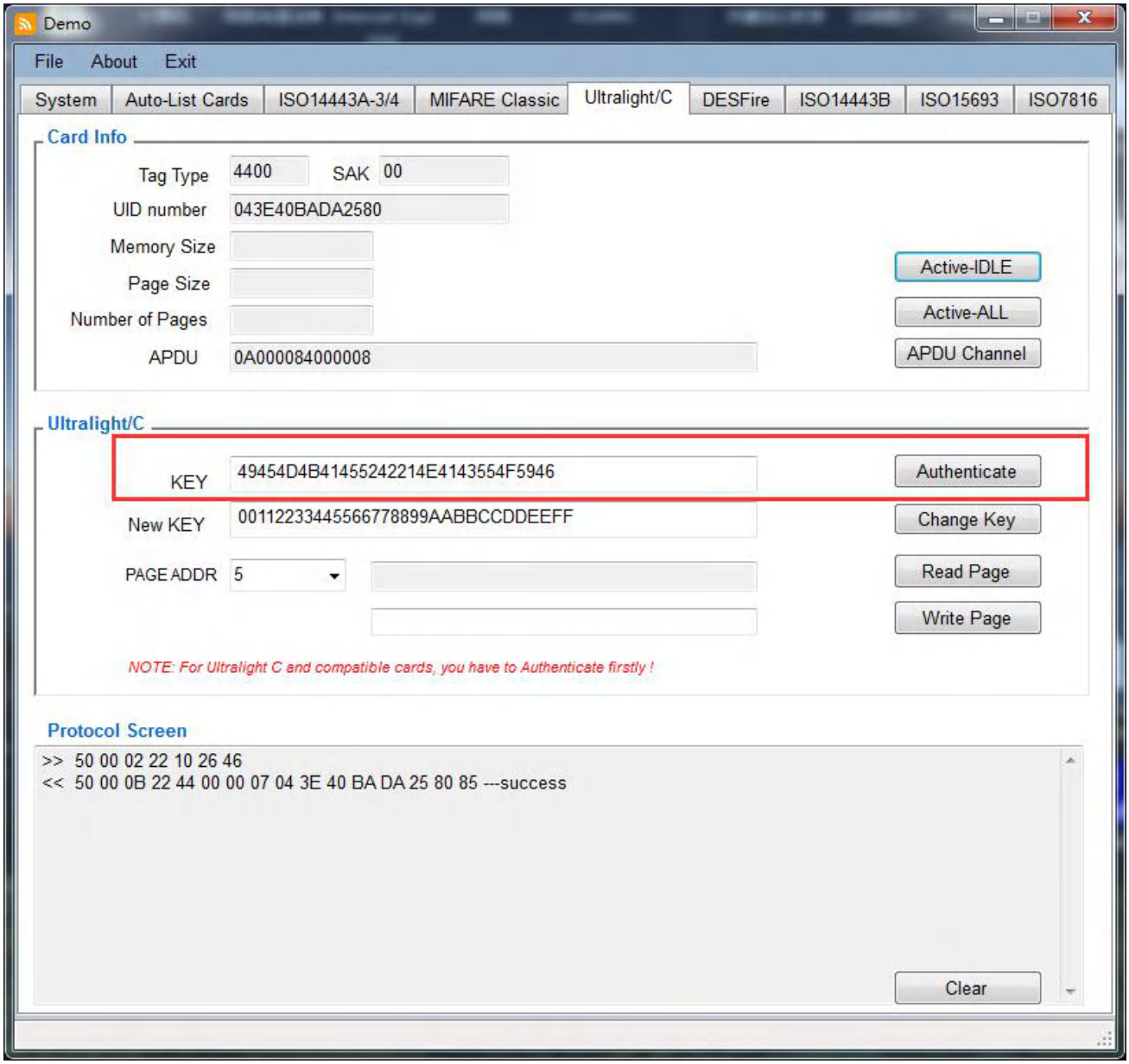


2.7.3 Ultralight C Authenticate

This is only opened for Ultralight C and its compatible cards which with password protected.

The common MIFARE Ultralight card/tag is without password protected and no need to do it.

Please input right KEY value to do authenticate for the card

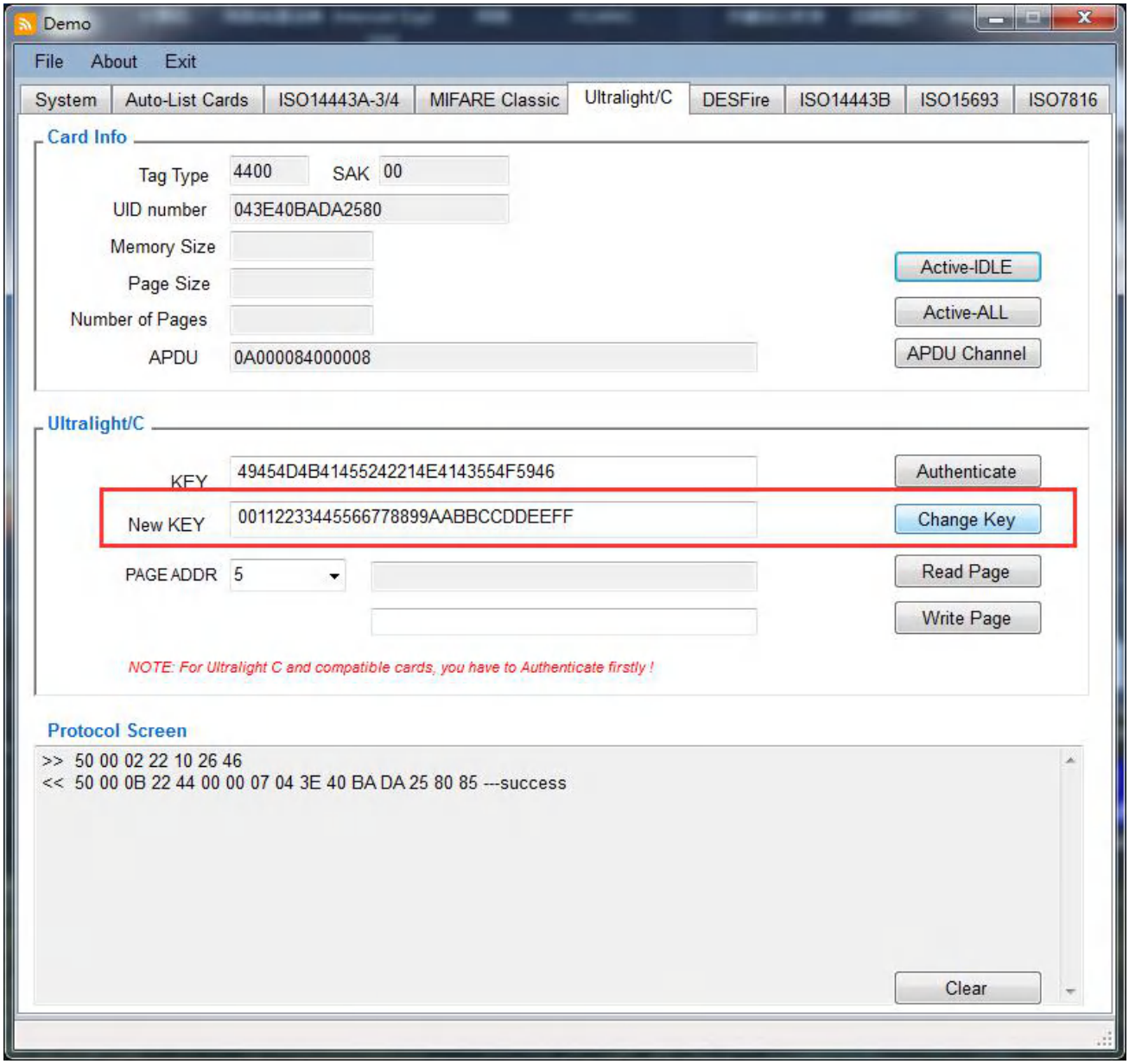


2.7.4 Ultralight C Change Key

This is only opened for Ultralight C and its compatible cards which with password protected.

And please do Authenticate with old KEY before Change Key.

The data length for the KEY value is 16bytes.



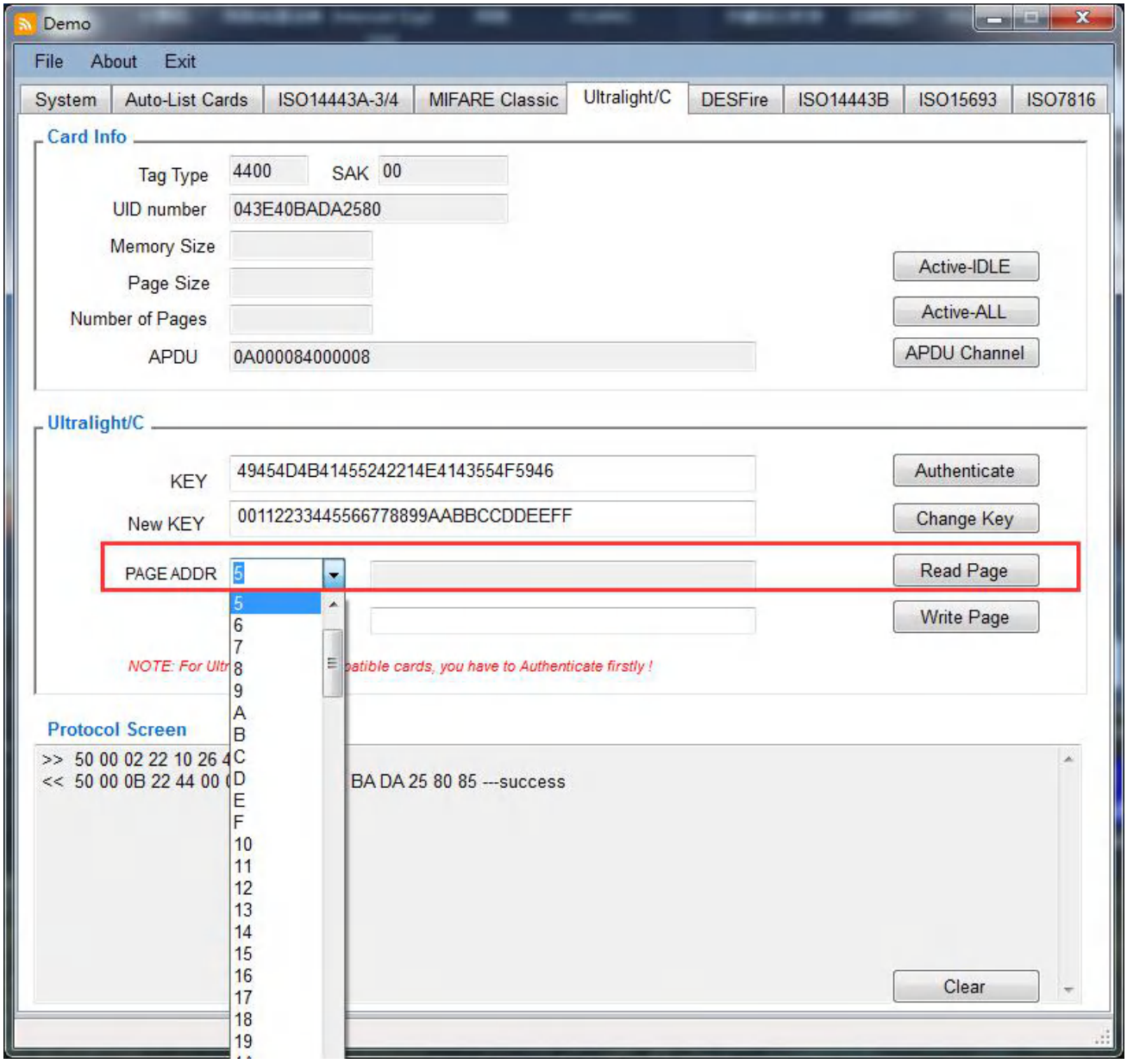
2.7.5 Ultralight /C Read Page

To get to read out the data stored in the according page address.

And For MIFARE Ultralight C and its compatible cards, And NTAG 2xx series card

before Read Page, Authenticate is needed firstly and make sure no remove of card after Active card. If there any remove, please again as Active-IDLE/Active-ALL --> Authenticate then Read Page with optional Page Address, as below:

For common MIFARE Ultralight card, Authenticate is no need.



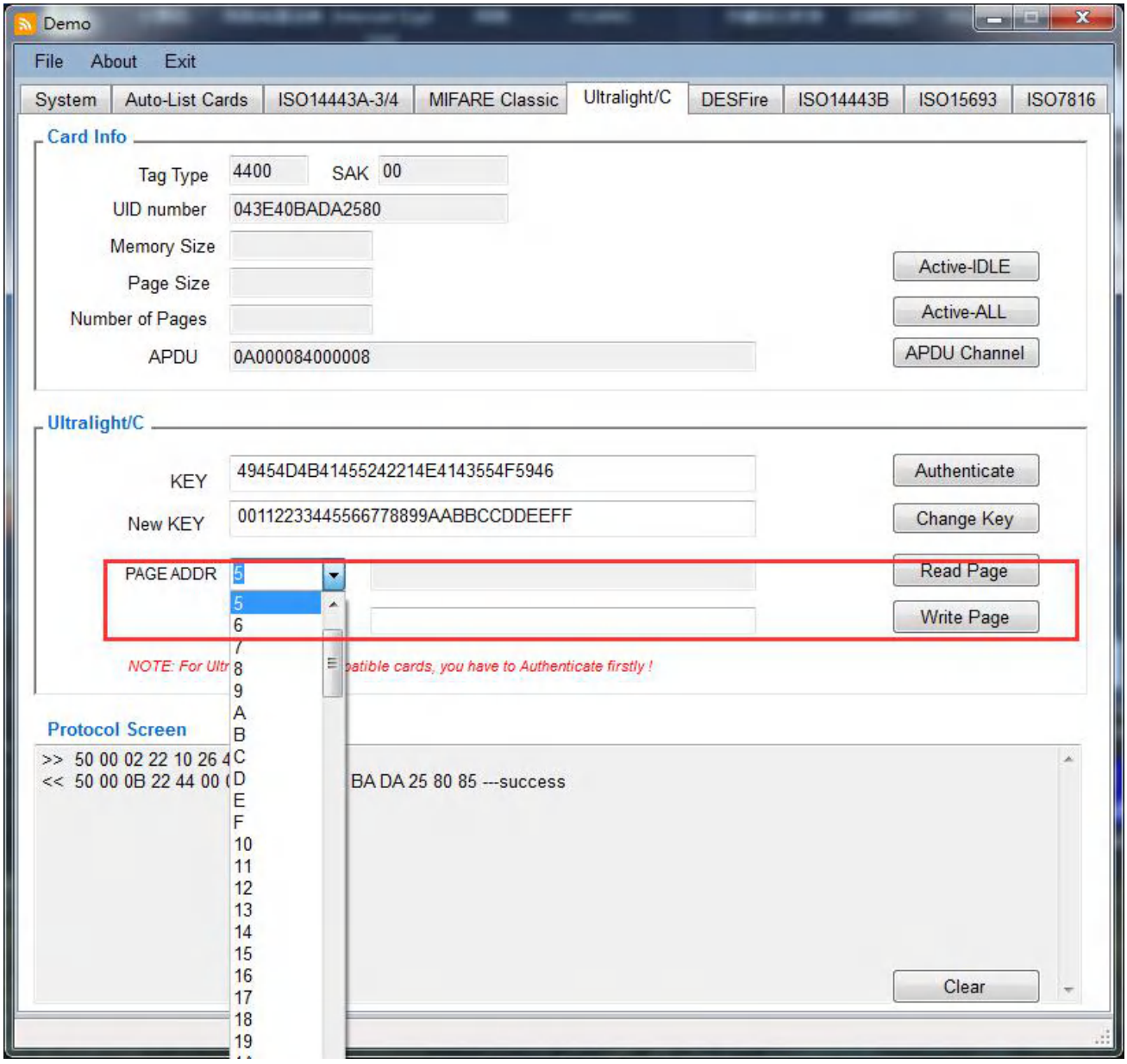
2.7.6 Ultralight /C Write Page

To Write the requested data into the according page address.

And For MIFARE Ultralight C and its compatible cards, And NTAG 2xx series card

Before Write Page, Authenticate is needed firstly and make sure no remove of card after Active card.
If there any remove, please again as Active-IDLE/Active-ALL --> Authenticate then Write Page to optional Page Address, as below:

For common MIFARE Ultralight card, Authenticate is no need.



Note: Some specific page cannot be written please refer to datasheet of using card/tag.

2.8 DESFire Interface

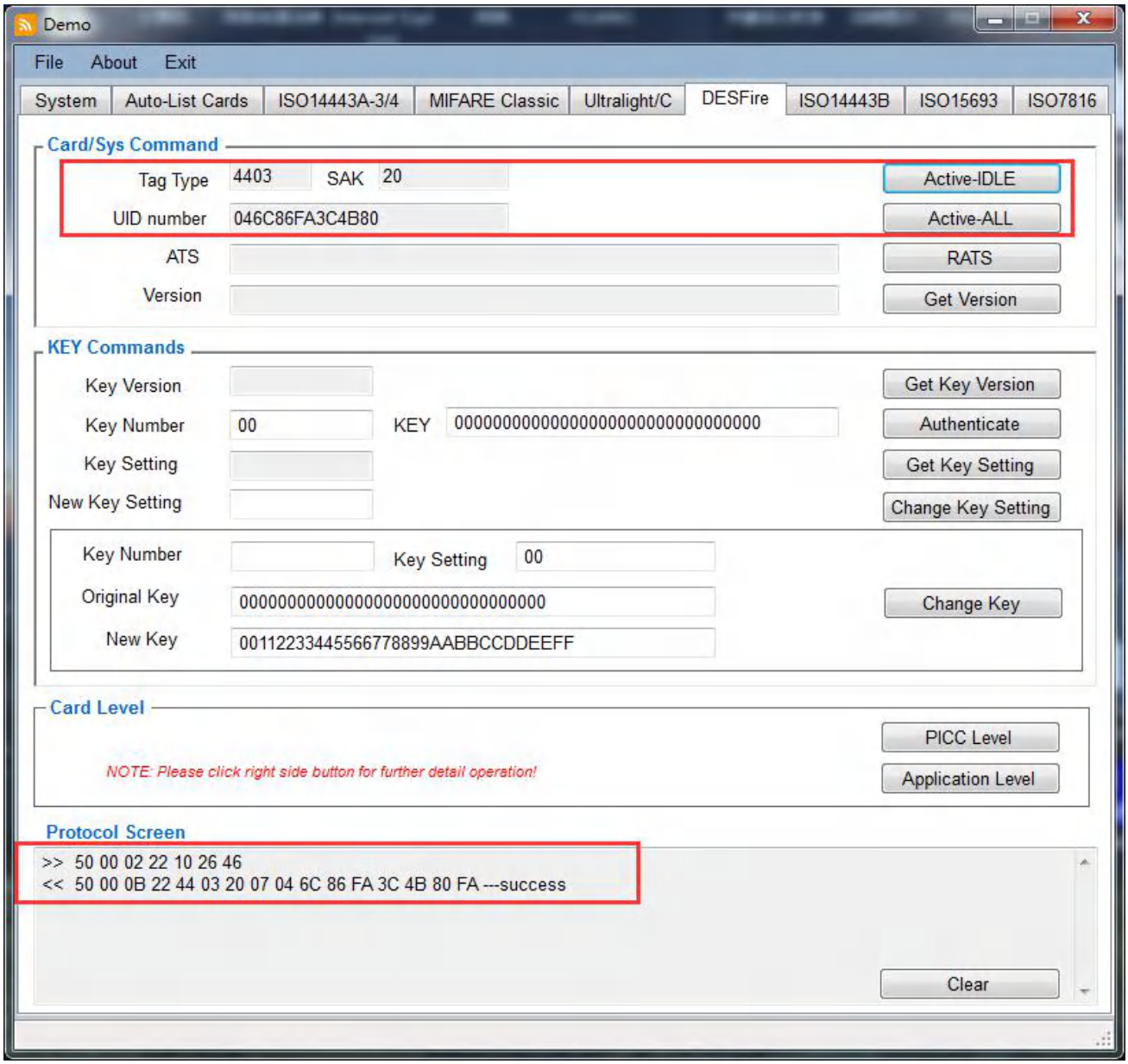
2.8.1 Active DESFire card

The optional button including as below:

Active-IDLE: to request the cards not dormant

Active-ALL: Request cards including dormant cards

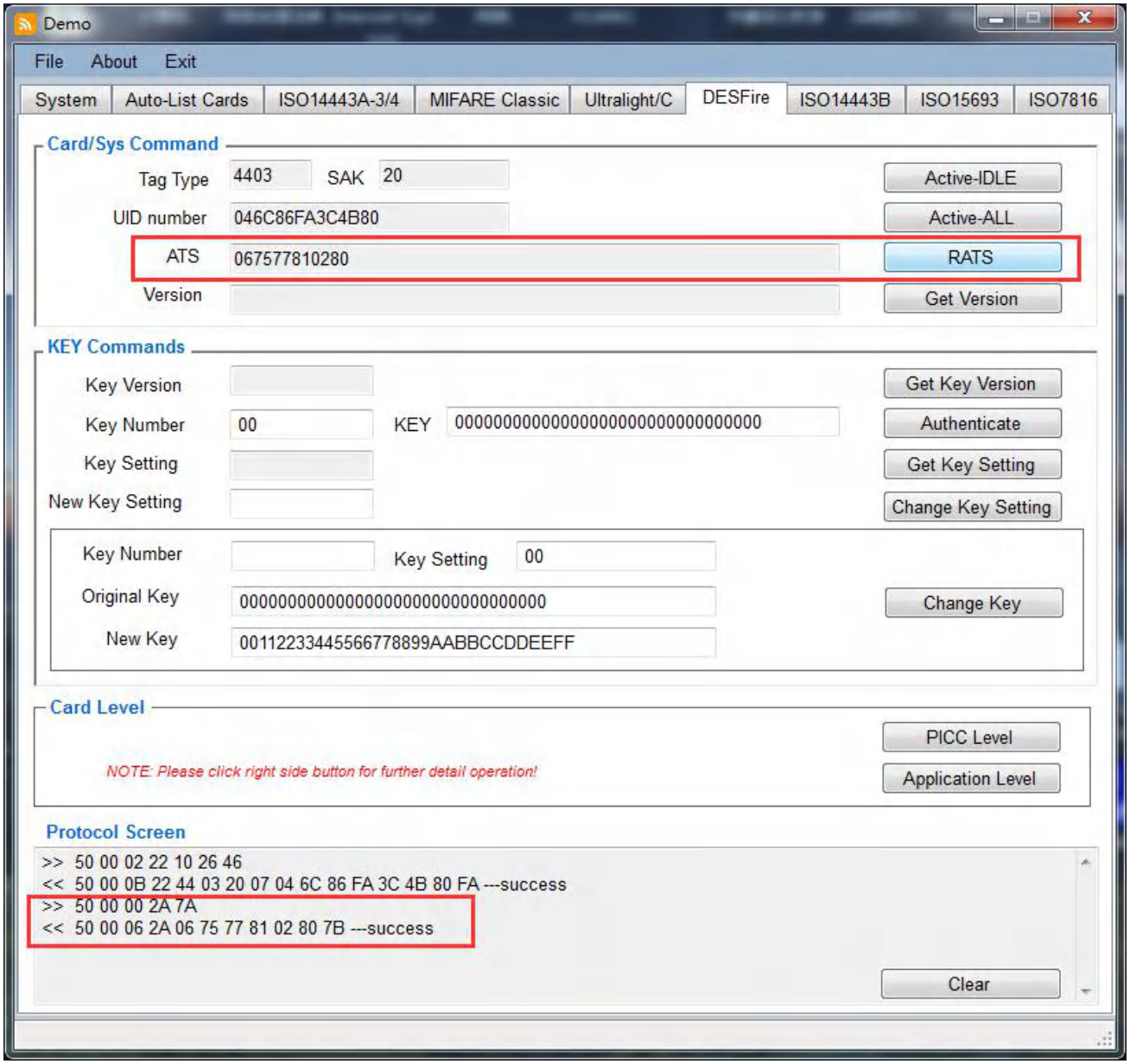
When succeeded request card, the card's detail information including card type, SAK, UID number will be shown as below:



2.8.2 DESFire Card-RATS

RATS= Request for Answer to Select

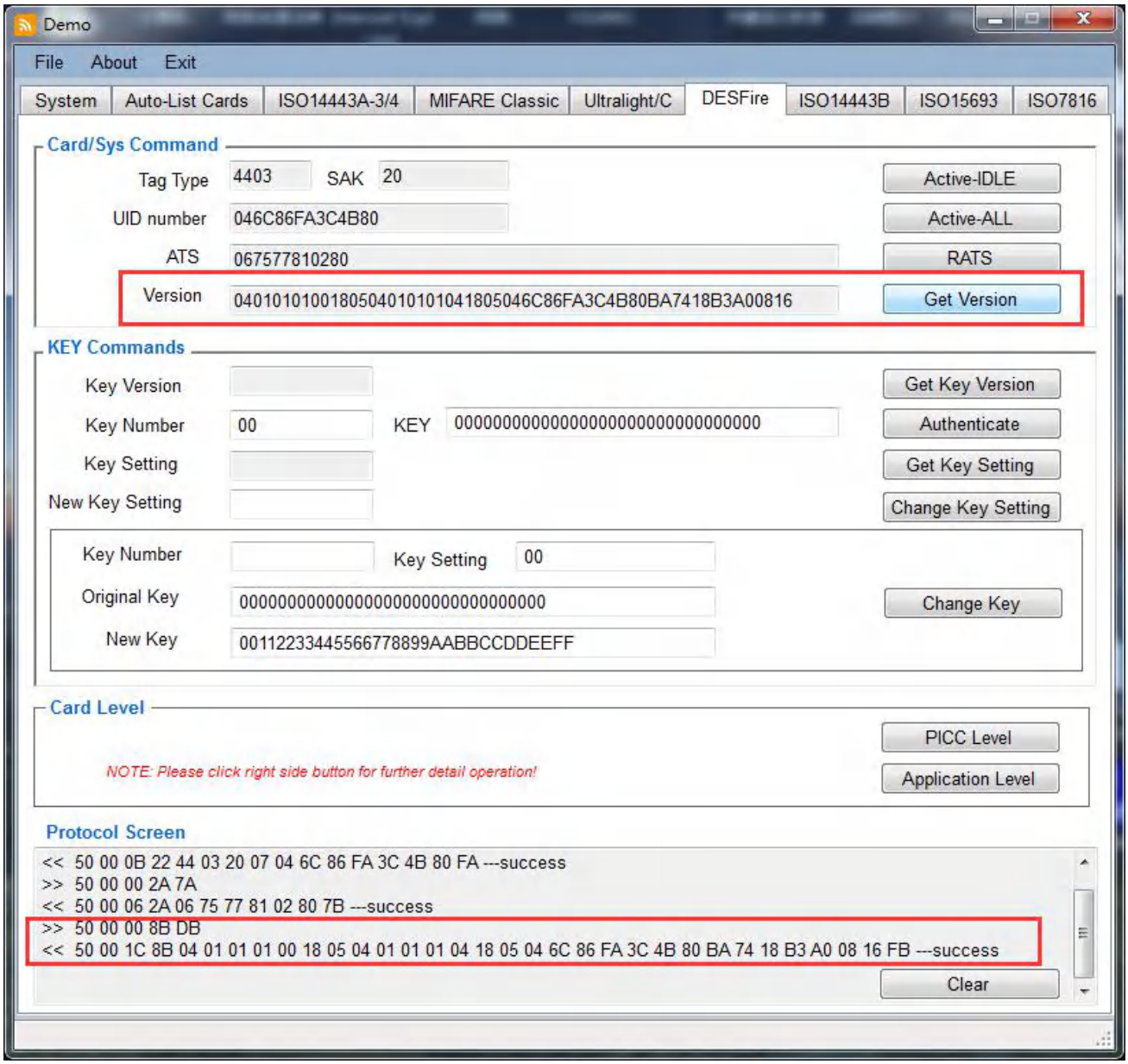
And the response to RATS is the “Answer to Select” ATS, and the ATS consists of specified bytes for communicate between PICC capabilities and PCD. Details specific byte’s meaning, please refer to datasheet of using card.



Note: Before RATS, Active-IDLE/Active-ALL is needed firstly.

2.8.3 DESFire Card-Get Version

To get the returned manufacturing related data of the DESFire cards



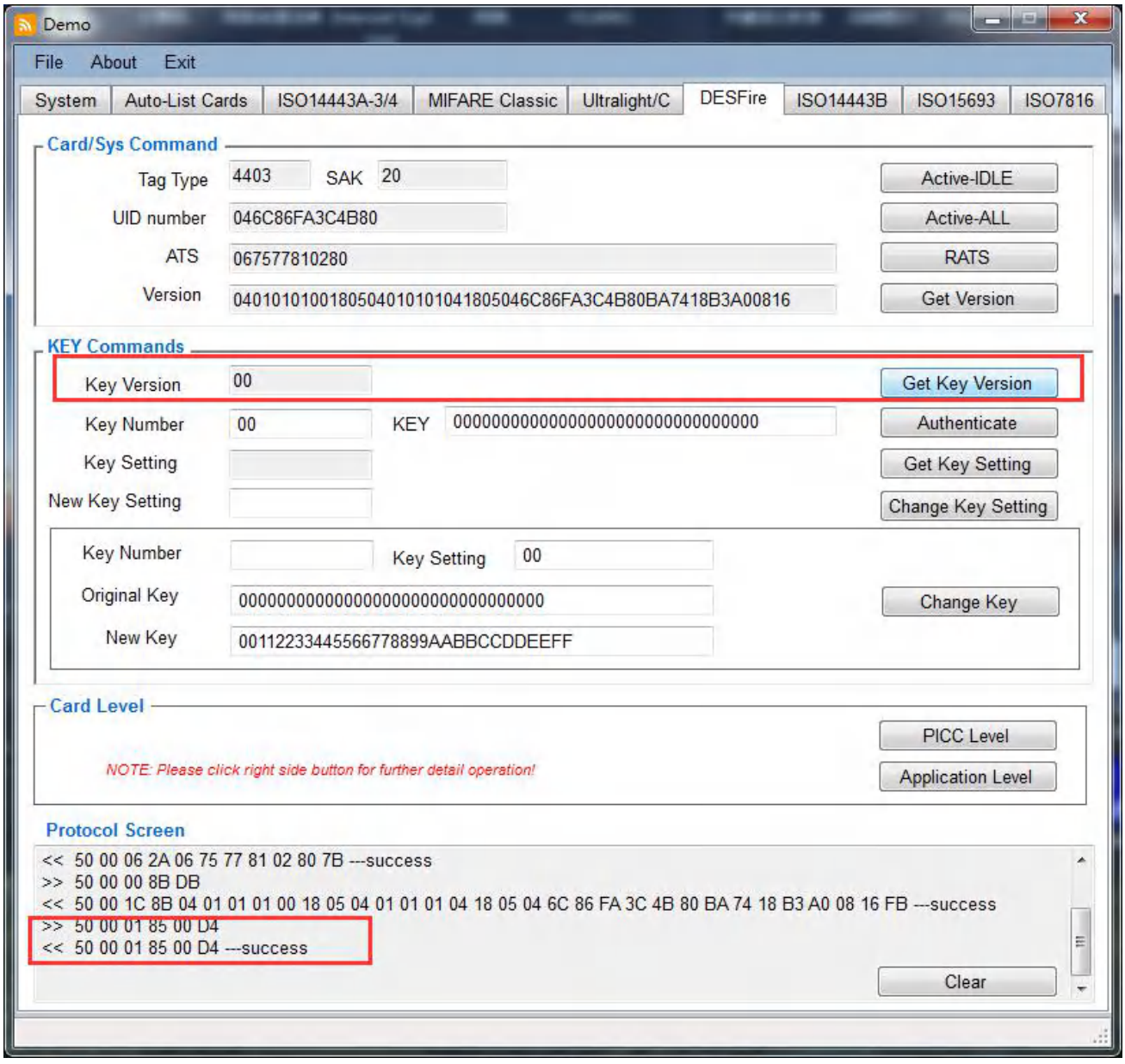
Note:

Active-IDLE/Active-ALL-->>RATS is needed before Get Version.

2.8.4 DESFire Card-Get Key Version

The Get Key Version command allows to read out the current key version of any key stored on the card.

Operation procedure: Active-IDLE/Active-ALL -->> RATS -->> Get Key Version

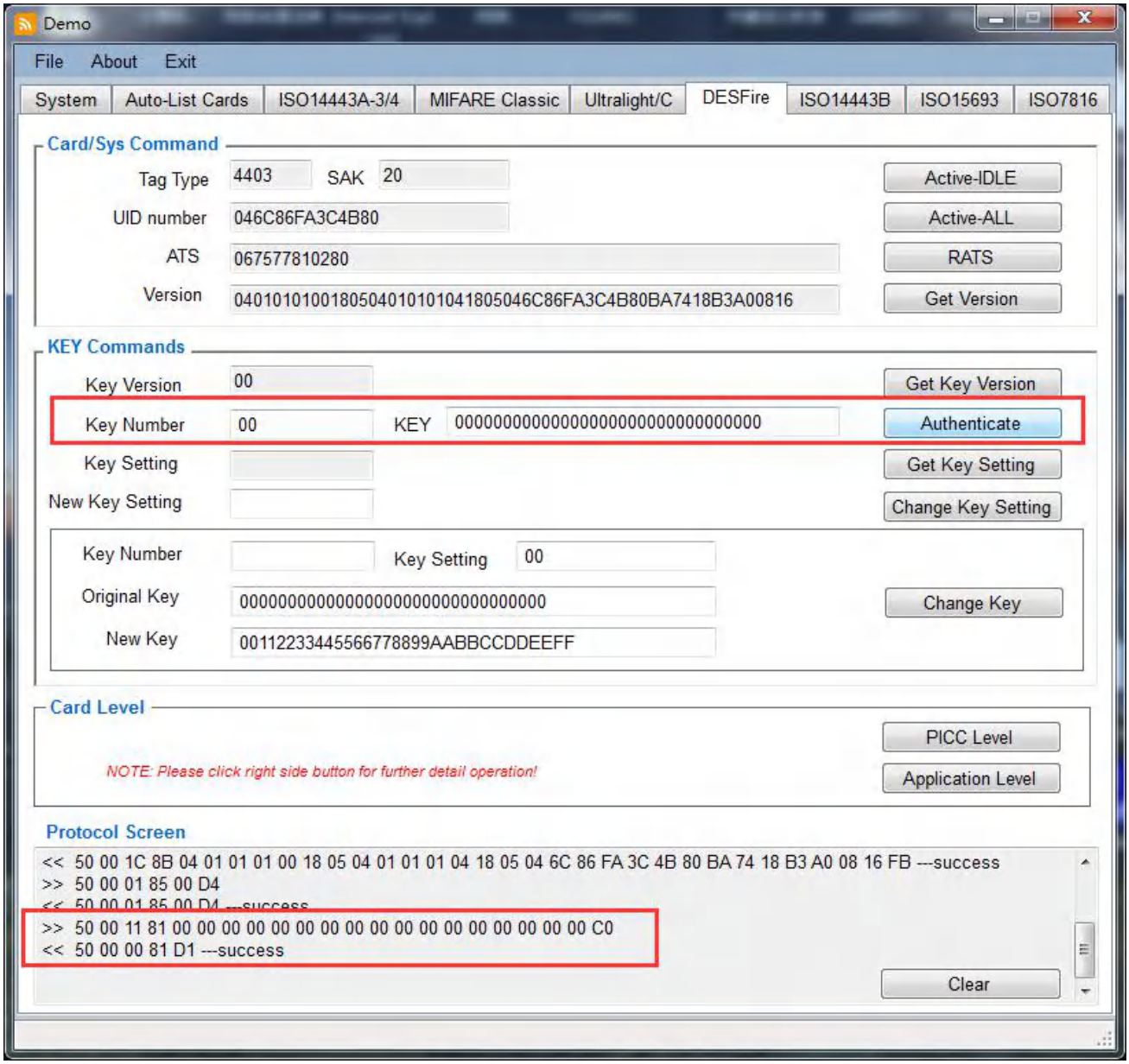


2.8.5 DESFire Card- Key Authenticate

This procedure is not only confirm that both card/tag and reader device can trust each other, but also generates a session key which can be used to keep the further communication path secure.

Note Master Keys are identified by their key number 0x00, this is valid on PICC level (selected AID=0x00) and on Application Level.

Operation procedure: Active-IDLE/Active-ALL -->> RATS -- >> Authenticate



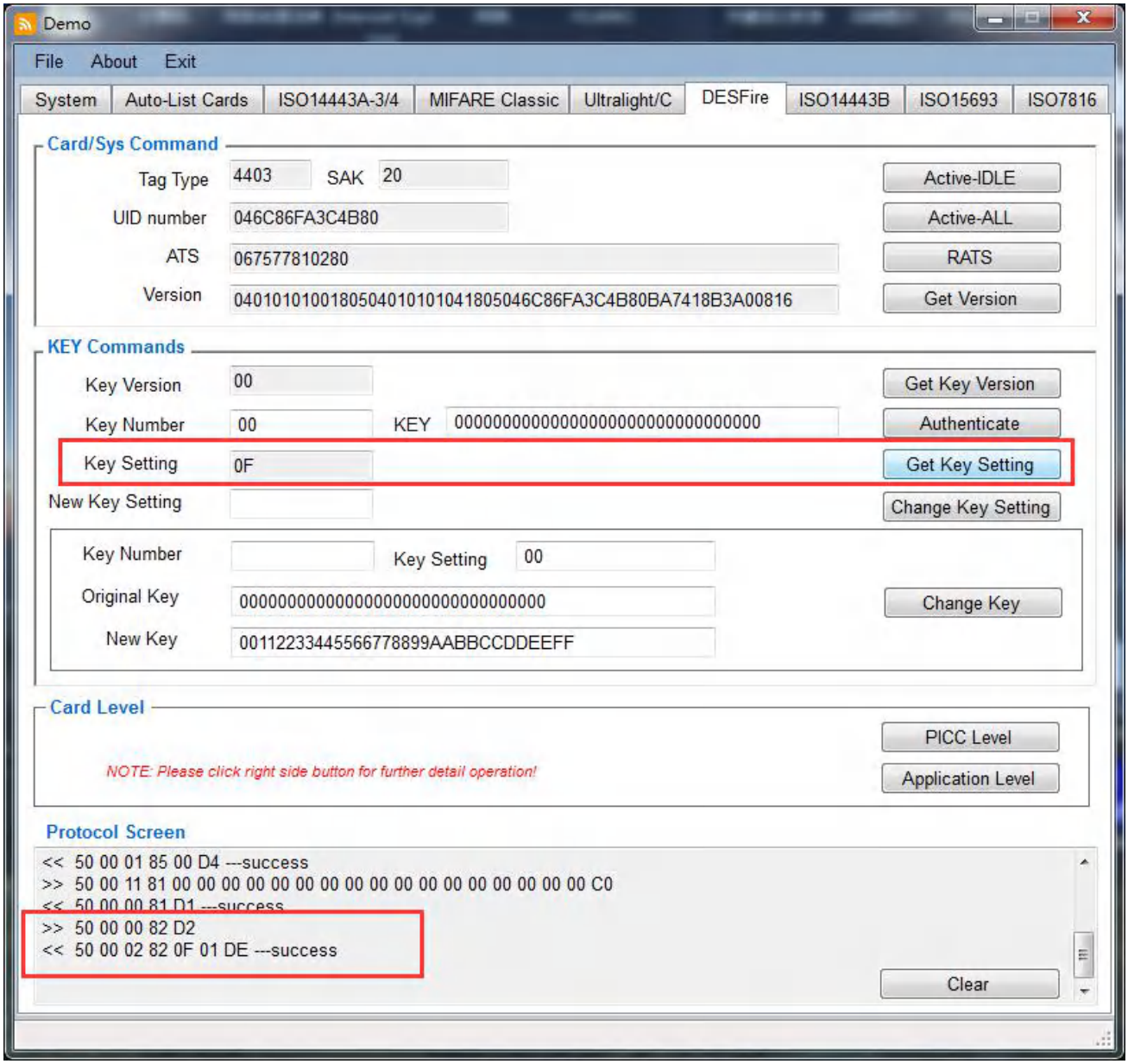
2.8.6 DESFire Card- Get Key Setting

This function command allows to get configuration information on the card/tag and application master key configuration setting.

It returns the maximum number of keys which can be stored within the selected application.

Before Get Key Setting, a proceeding authentication with the master key is required.

Operation procedure: Active-IDLE/Active-ALL -->> RATS -- >> Authenticate -->> Get Key Setting



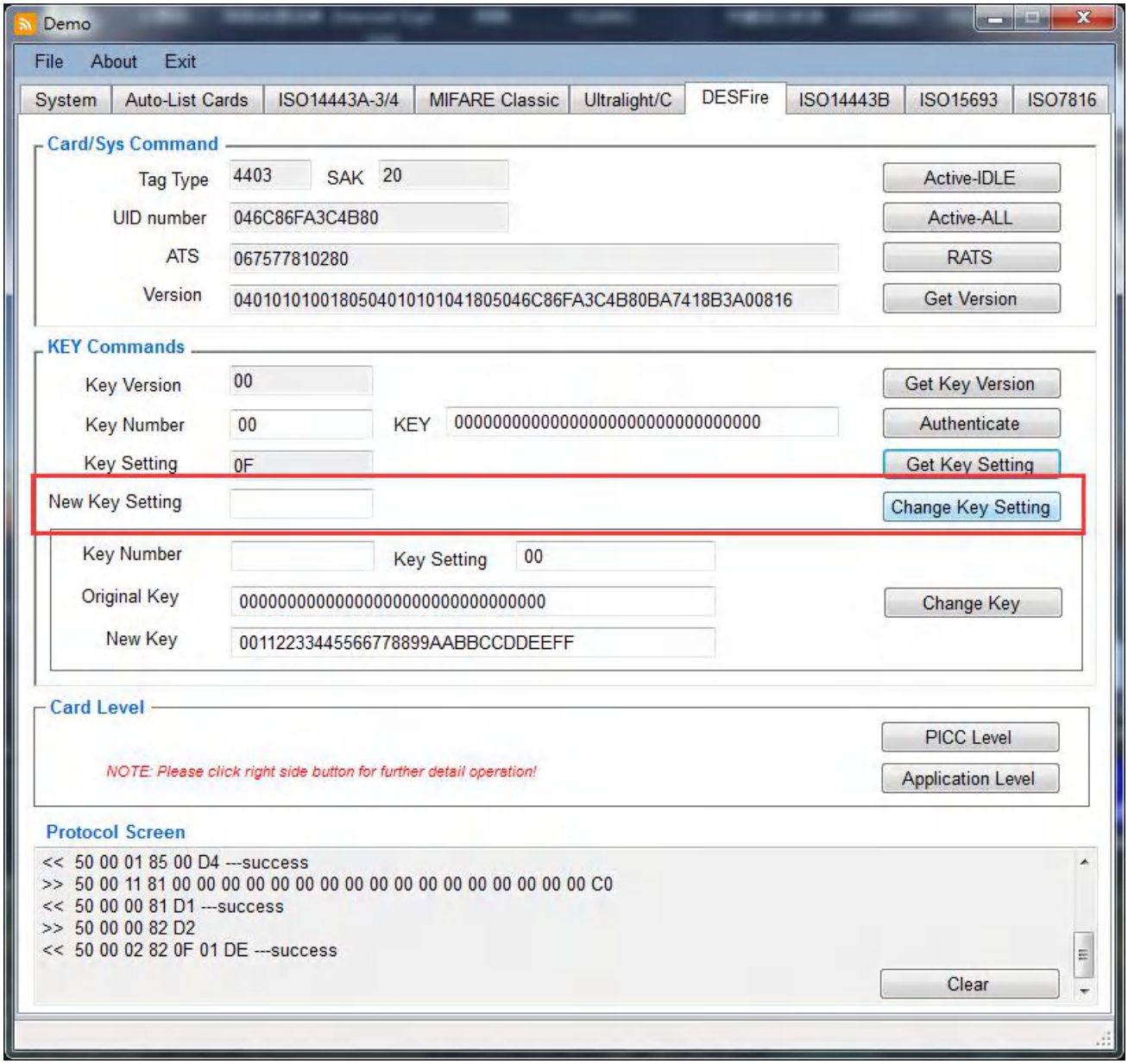
2.8.7 DESFire Card- Change Key Setting

This command changes the master key configuration setting depending on the currently selected AID.

This command takes one byte as parameter which codes the new master key settings., details configuration changeable bits, please refer to detail datasheet of using card.

Authenticate is needed before Change Key Setting.

Operation procedure: Active-IDLE/Active-ALL -->> RATS -- >> Authenticate -->> Change Key Setting



2.8.8 DESFire Card- Change Key

This command allows to change any key stored on the card/tag.

Parameter value to be changed:

Key Number: One byte length and has to be range from 0x00 to number of application key to 1

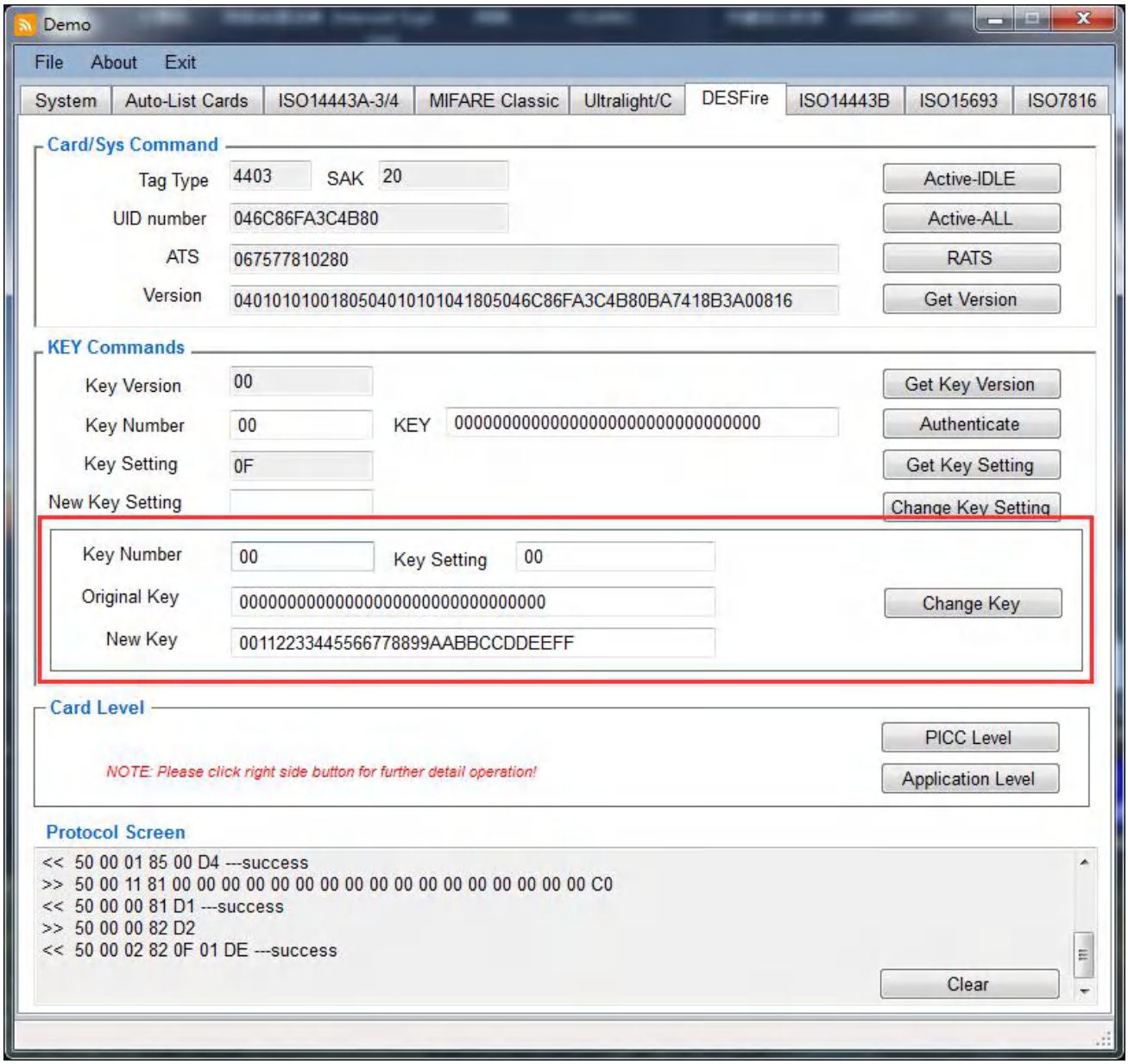
Key Setting: Whether a change of key is permit or not and show which key is need for Authenticate before the Change key command

Original Key: Old key

New Key: the key to be changed

To the Change Key Key or Master Key, Authenticate Master Key is necessary. Other details for specific operations, please refer to datasheet of using card.

Operation procedure: Active-IDLE/Active-ALL -->> RATS -- >> Authenticate -->> Change Key

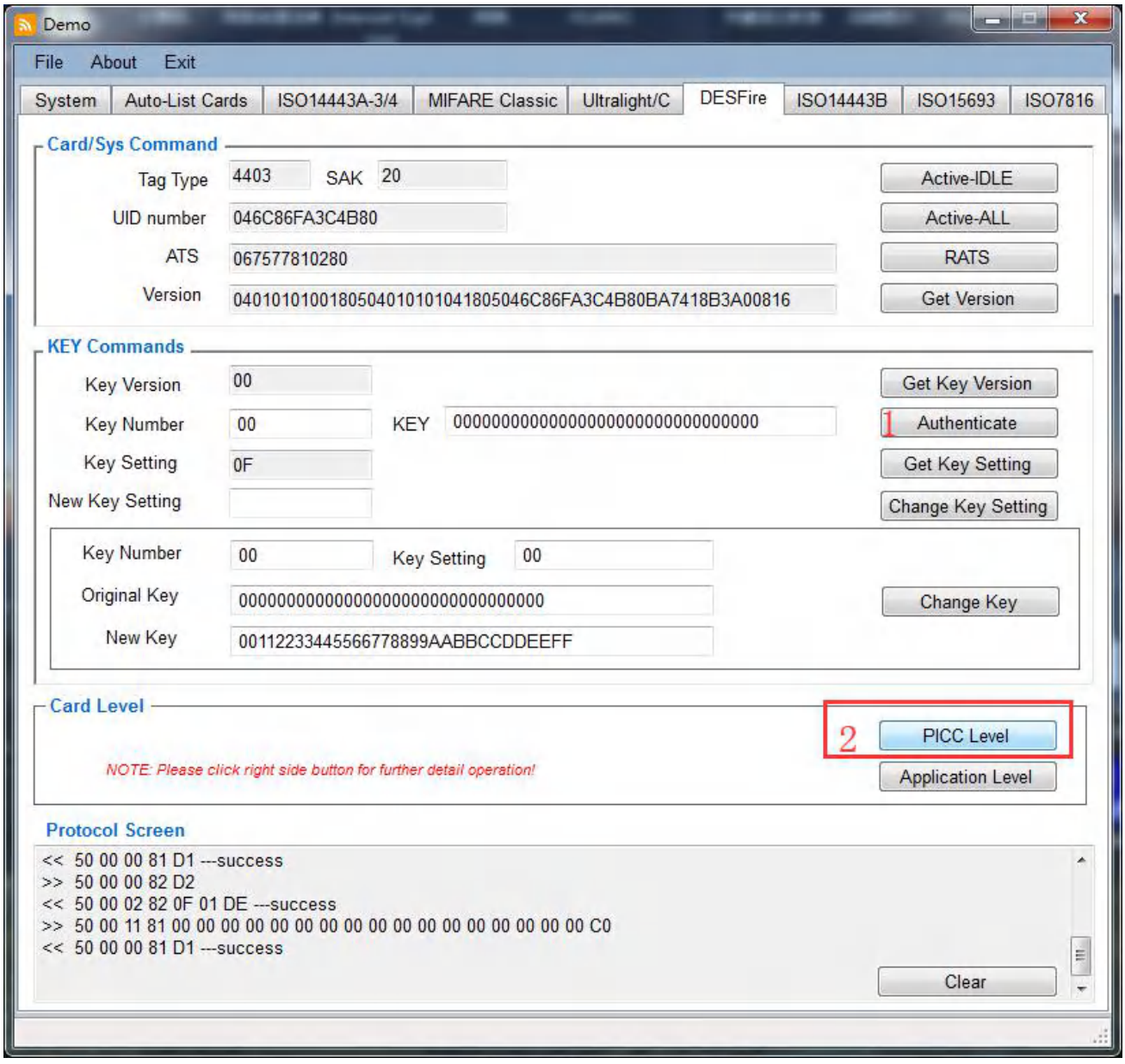


2.8.9 DESFire Card- PICC Level

This interface is for PICC application operations.

When enter into PICC Level interface,Authenticate Master Key is necessary

Operation procedure: Active-IDLE/Active-ALL -->> RATS -- >> Authenticate -->> PICC Level



2.8.9.1 PICC Level-Create Application

This command allows to create new application on the PICC

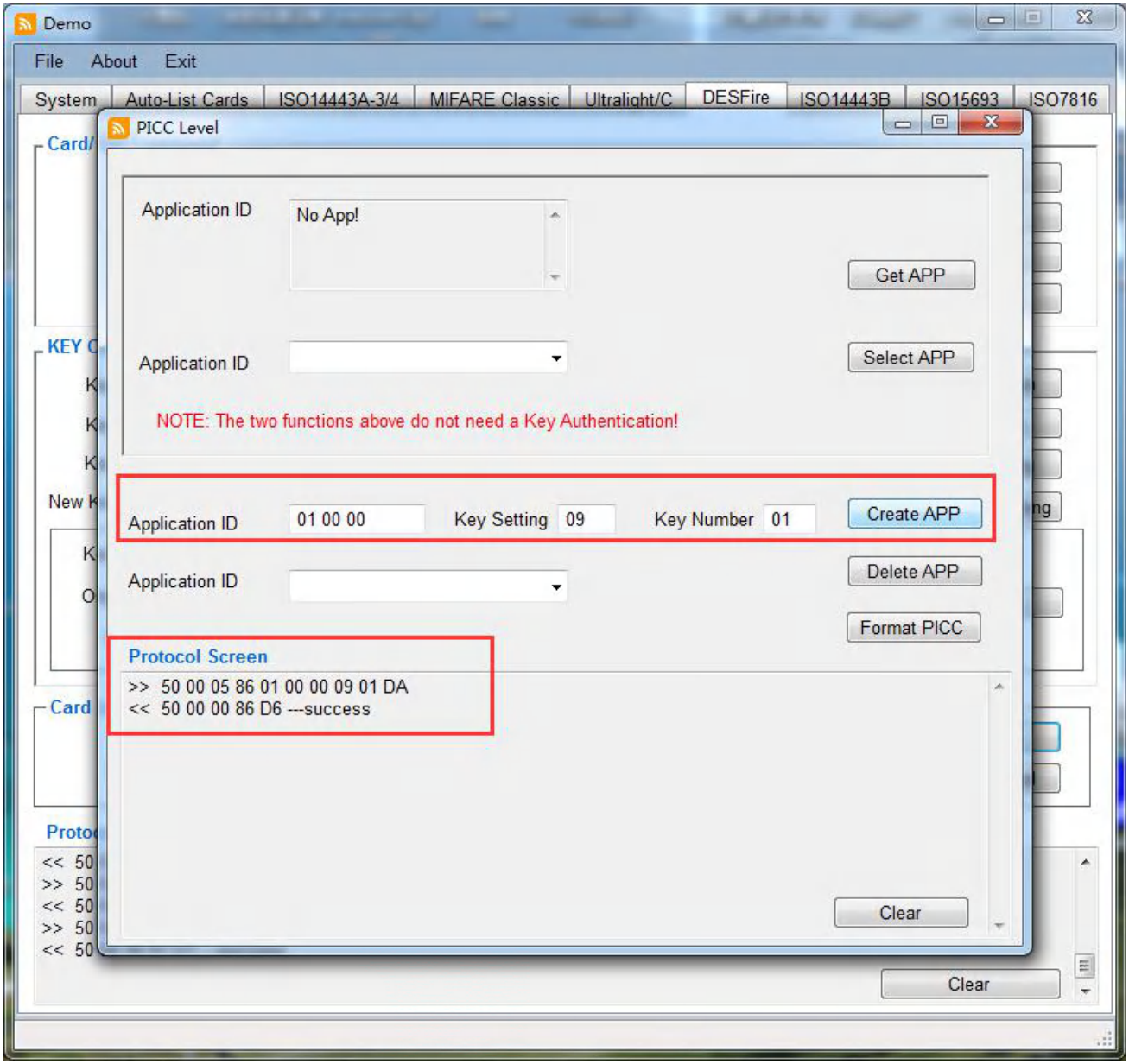
Parameters to be operated:

Application ID(AID): 24 bit number=0x00 00 00 and reserved as reference to the PICC itself

Key Setting: Application Master Key Setting as defined in Chapter 2.8.6

Key Number: Number of Keys defines how many keys can be stored within the application for cryptographic purposes

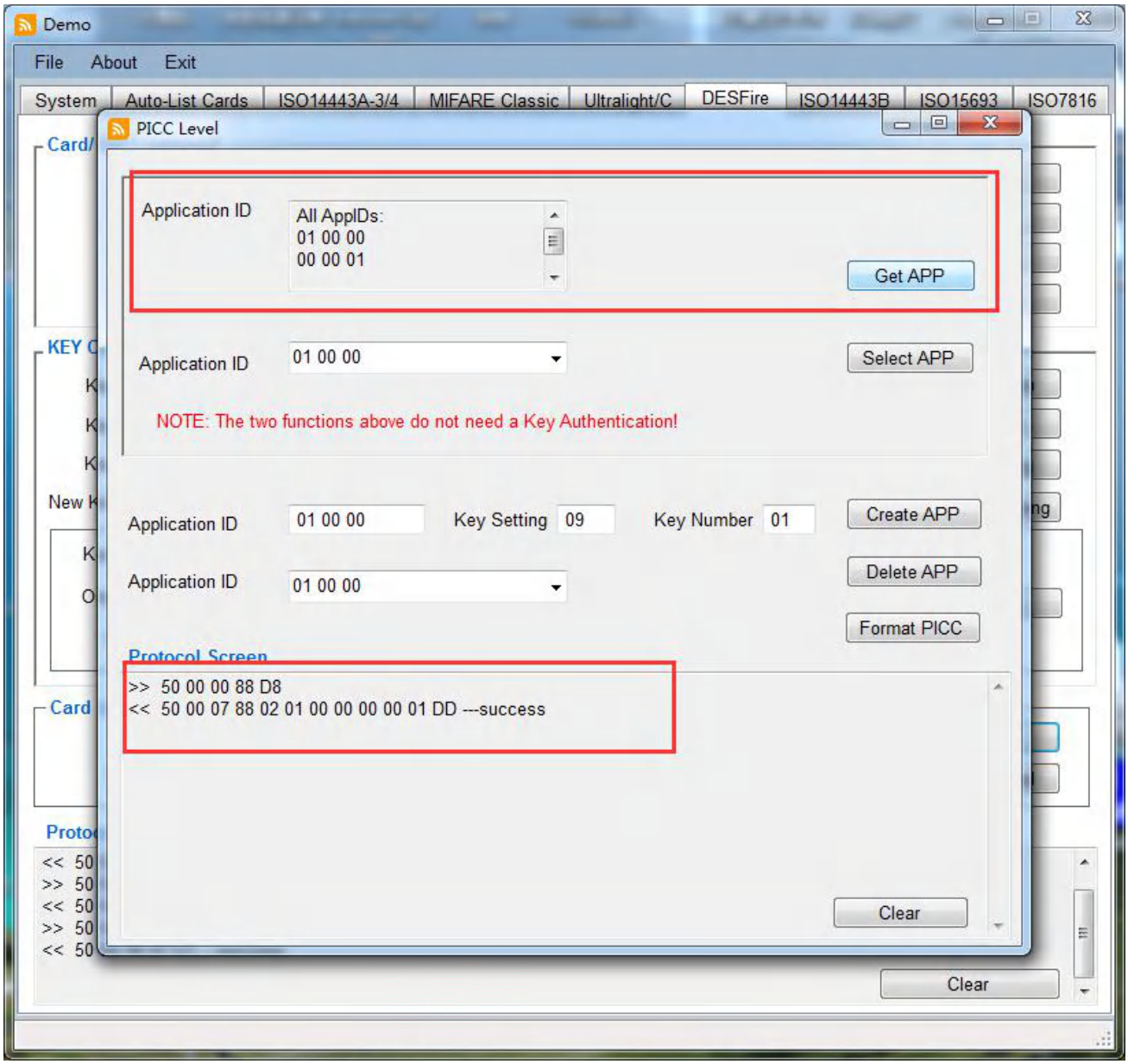
For example below:



Note: Proceeding PICC Master key authentication may be required

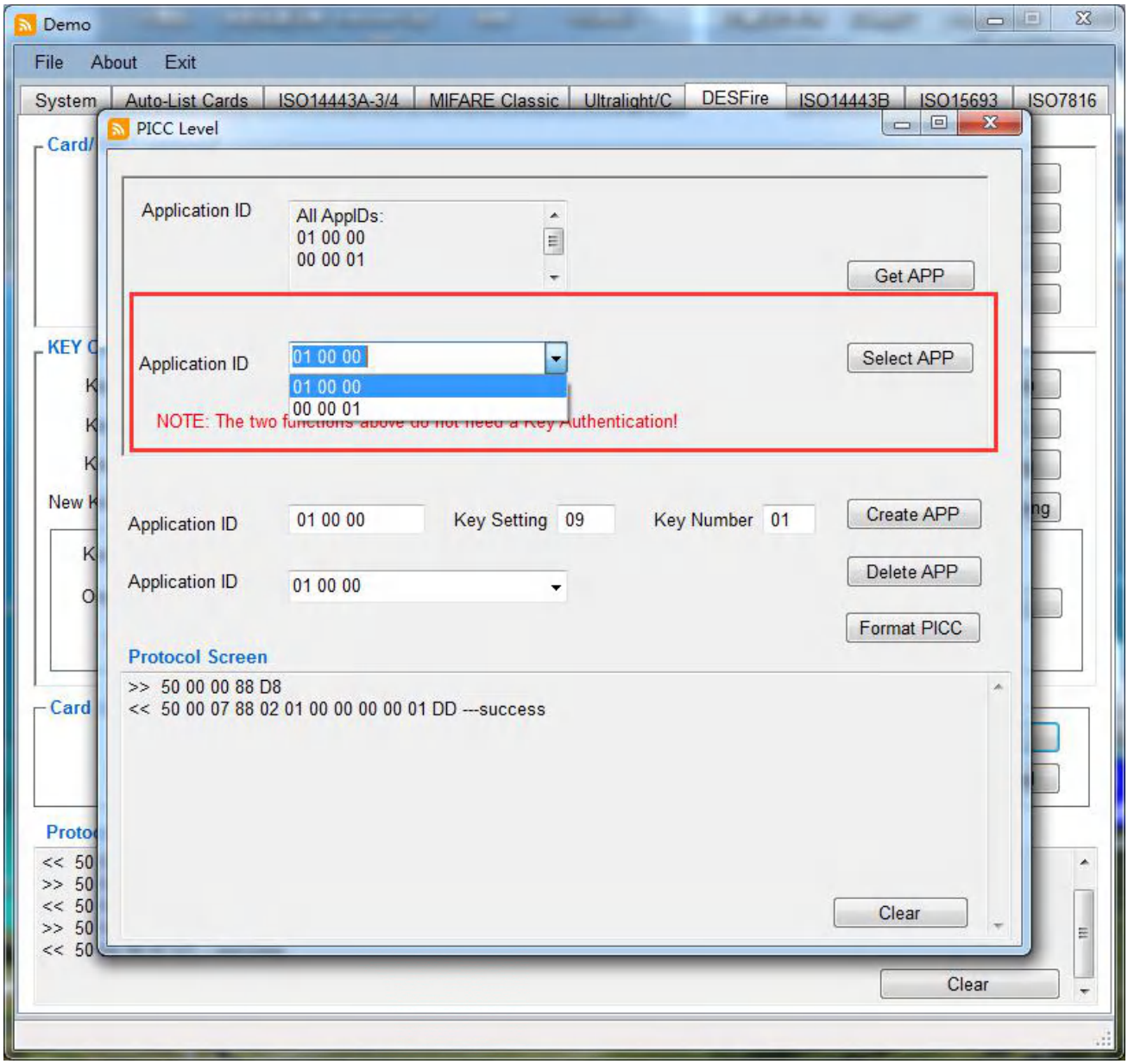
2.8.9.2 PICC Level-Get Application

To Get the Application ID or IDs stored in the card.



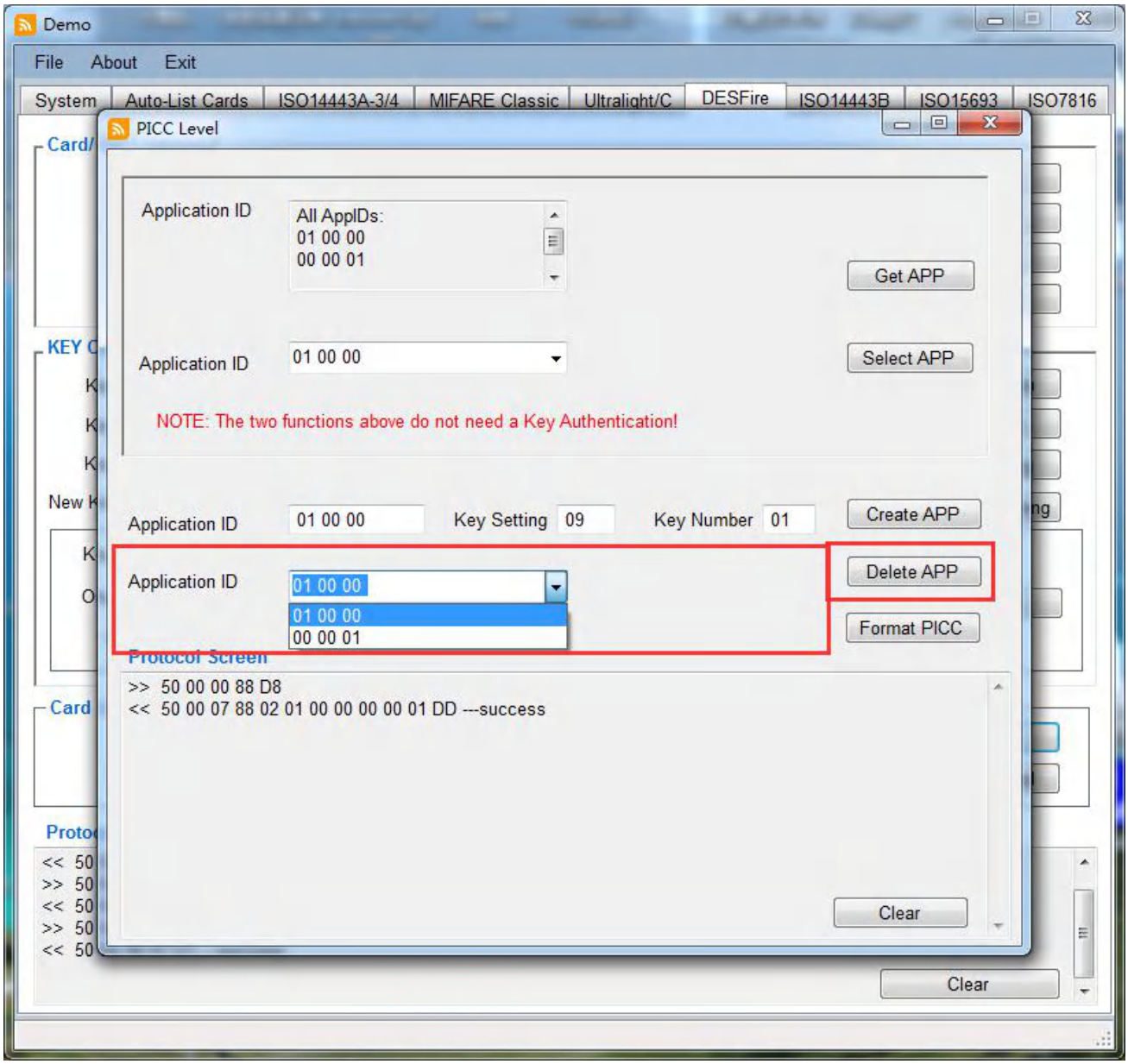
2.8.9.3 PICC Level-Select Application

To select the Application ID going for next further Application Level operations



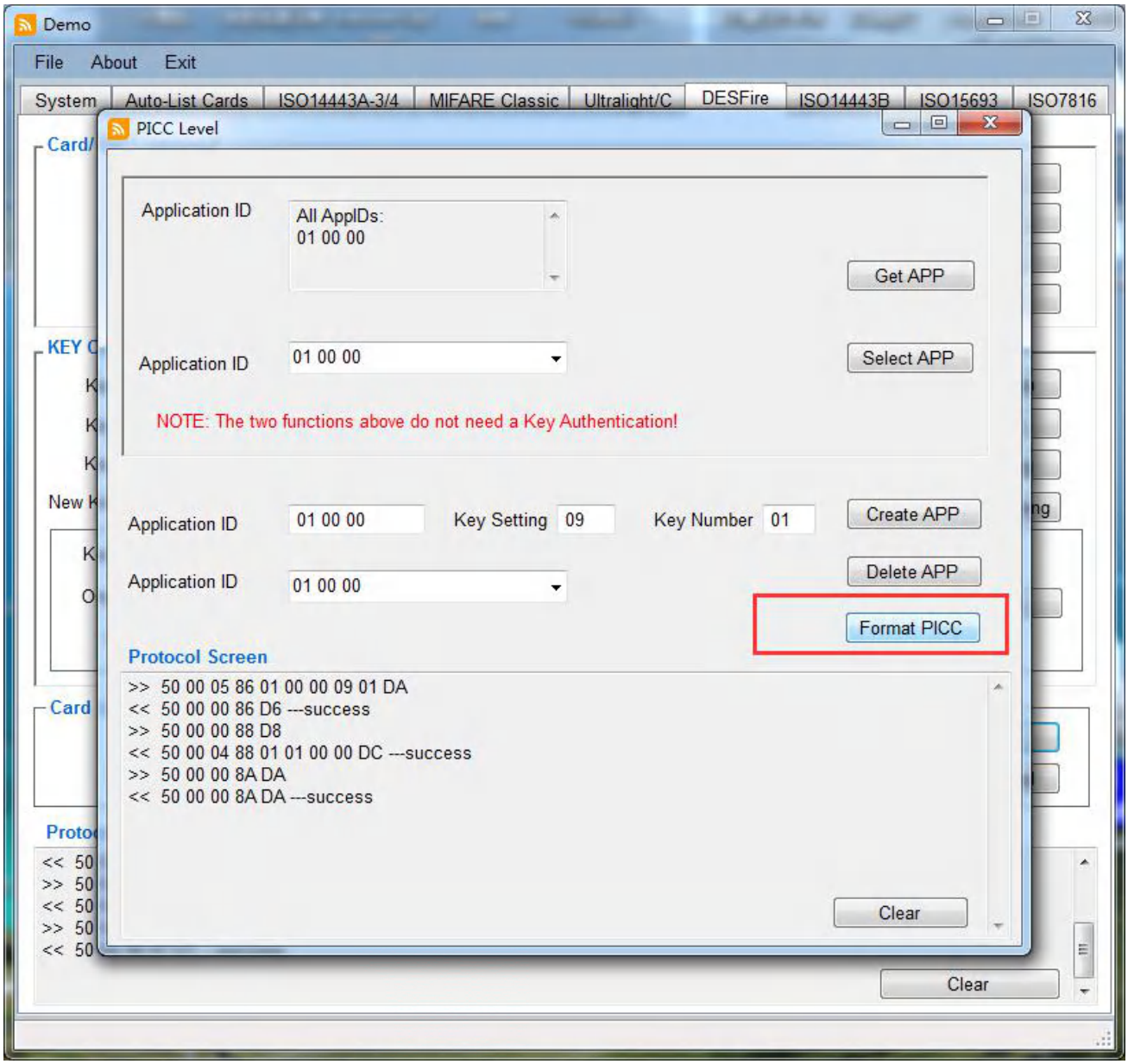
2.8.9.4 PICC Level-Delete Application

This command is to delete the application ID or IDs, the all application IDs will be listing on left side box.



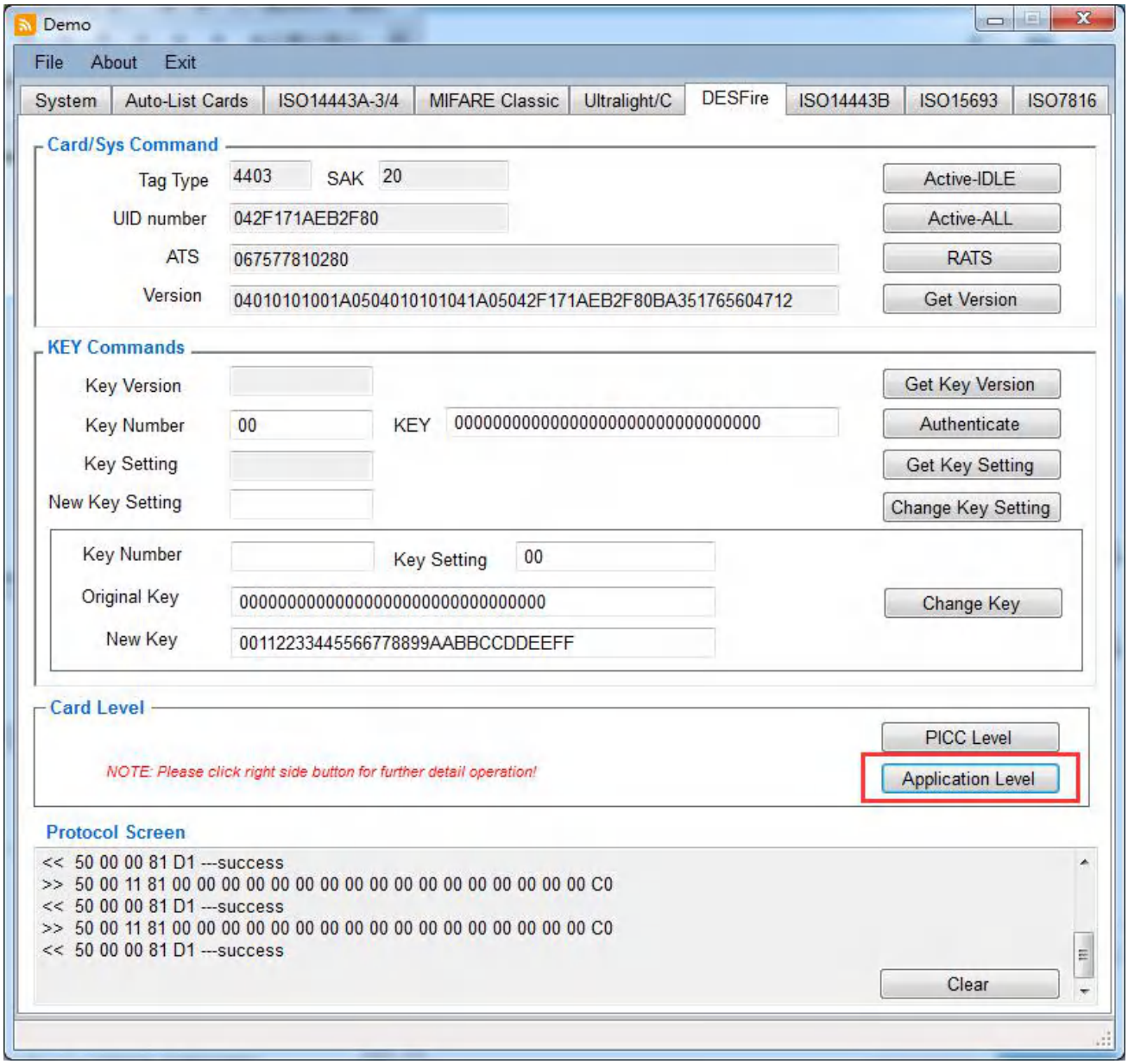
2.8.9.5 PICC Level-Format PICC

This command releases the PICC user memory and no parameter are passed with this command



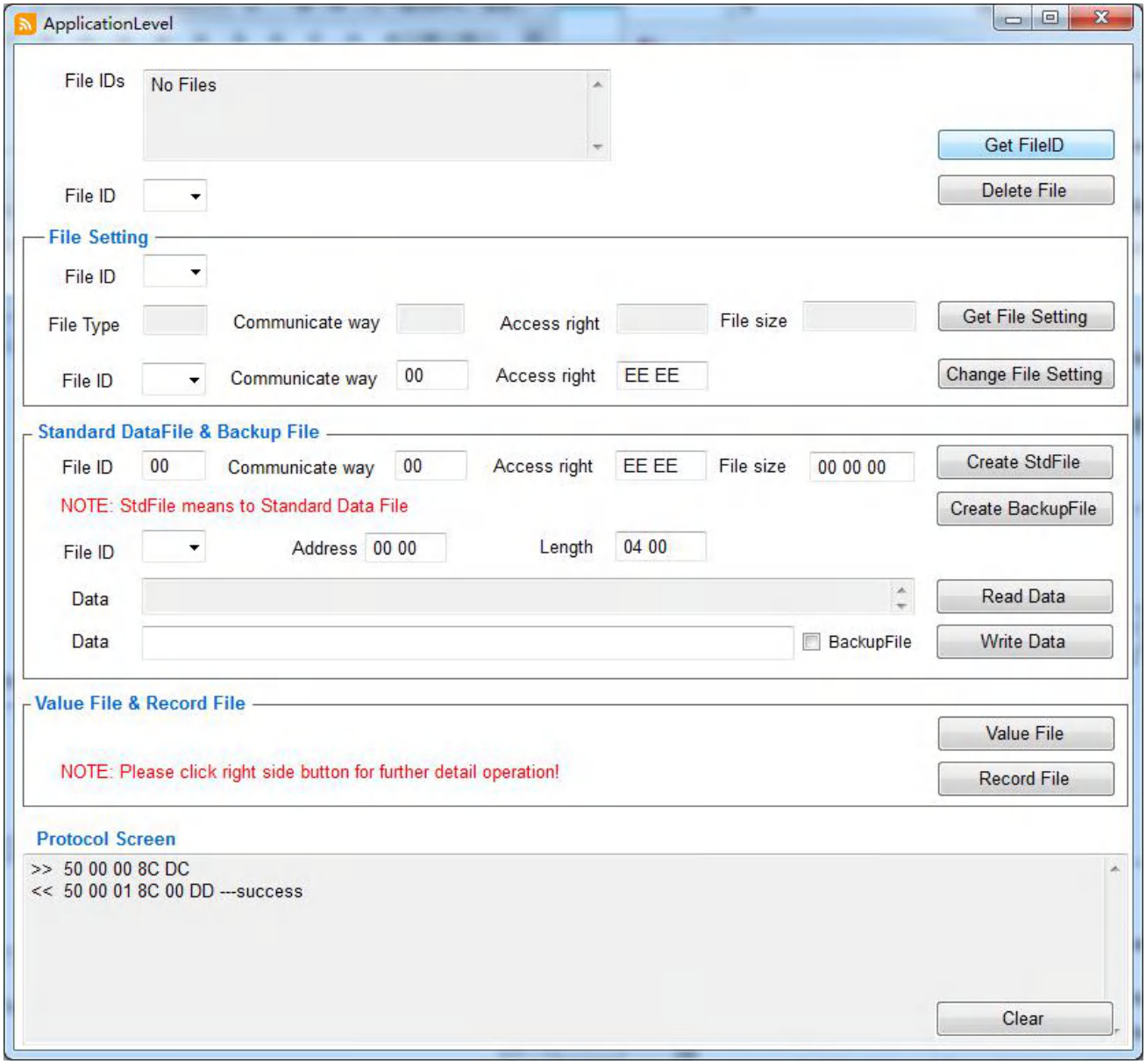
2.8.10 DESFire Card- Application Level

When enter into Application Level, it must do Select APP --> Authenticate Master Key firstly .



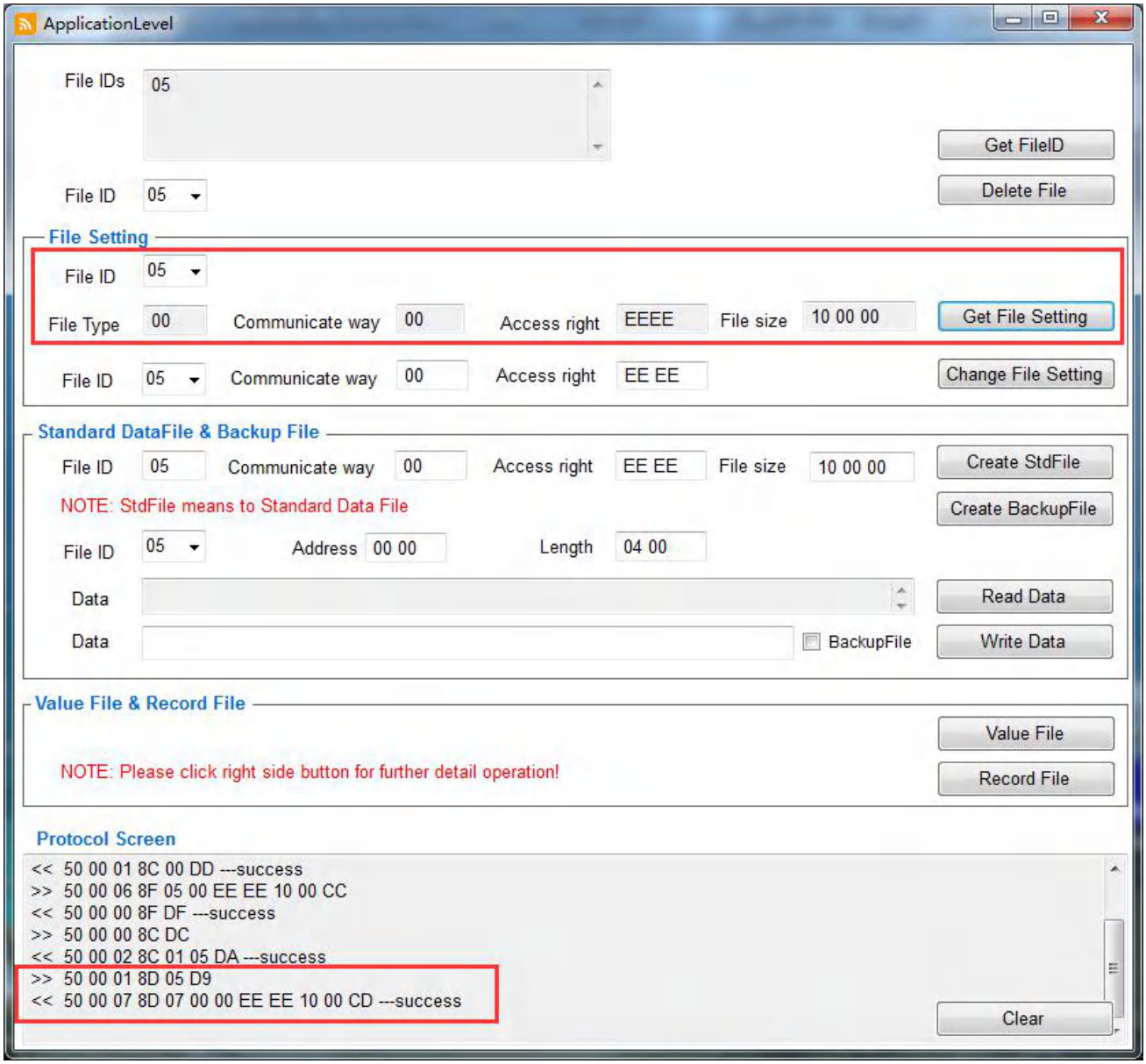
2.8.10.1 Application Level-Get File IDs

This command returns the File IDs of all active files within the currently selected application



2.8.10.2 Application Level-Get File Setting

To Get information on the properties of a specific file, and the File ID need to be selected when proceeding

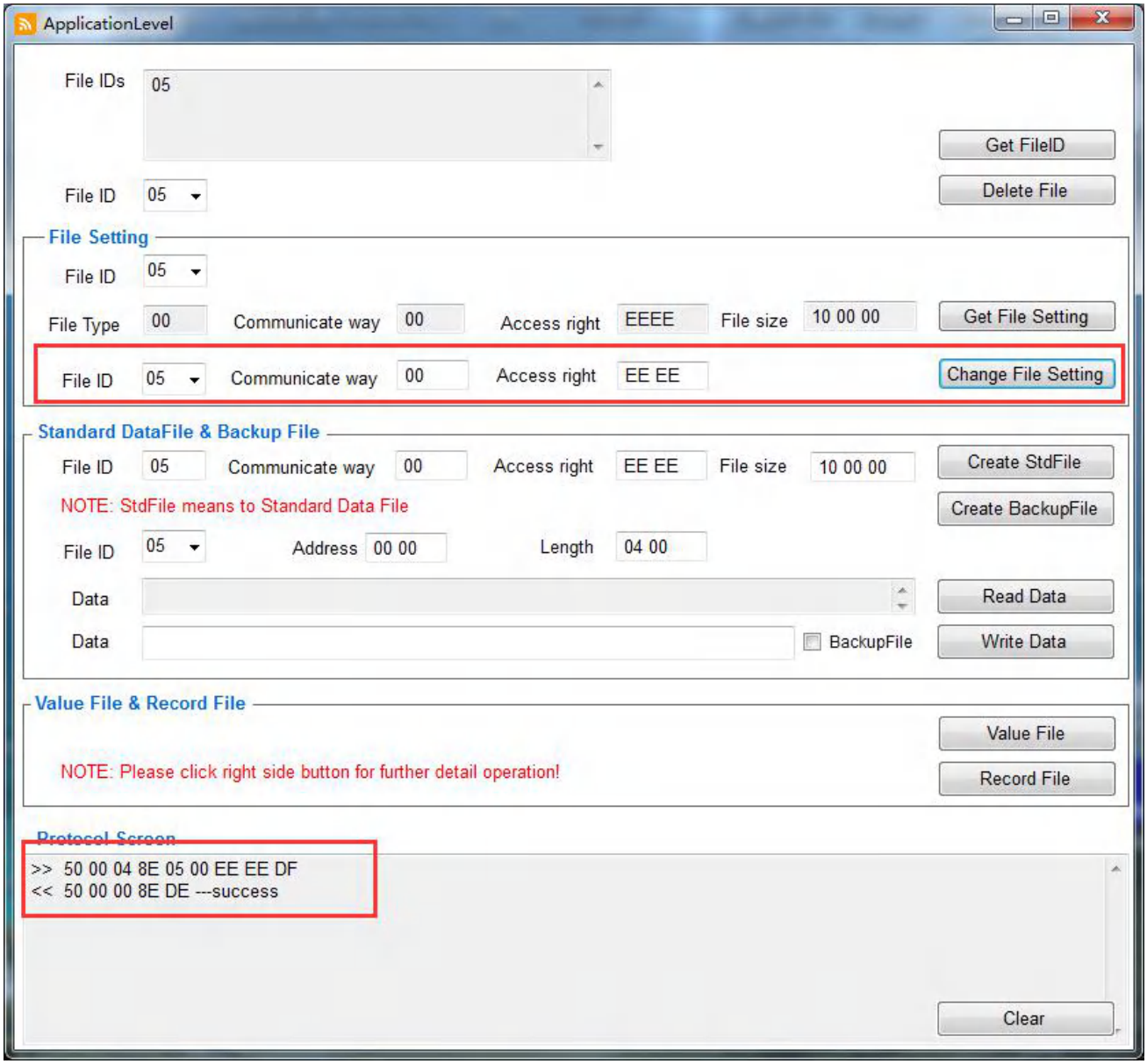


2.8.10.3 Application Level-Change File Settings

This is to change the access parameters of an existing file.

Parameters to be changed:
File ID: file number within currently selected application, One byte
Communication way: new communication settings, One byte
Access right: new access rights, Two byte

More details information, please refer to datasheet of using card accordingly

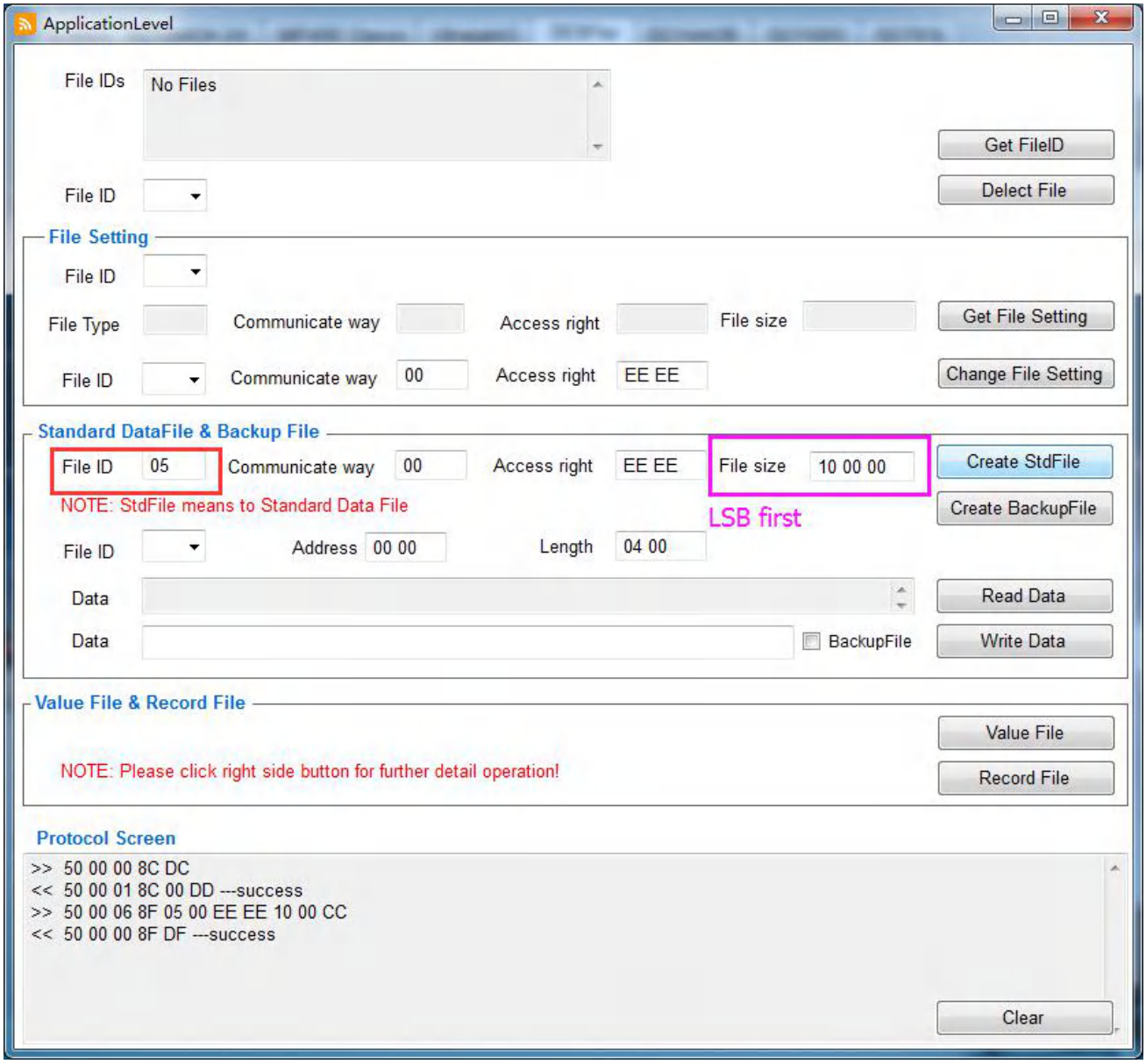


2.8.10.4 Application Level-Create Std Data File/ Create Backup Data file

This is used to create files for the storage of plain unformatted user data within an existing application on the PICC, and Create Backup Data File supporting the feature of an integrated backup mechanism.

Parameters to be created:
File ID: File number of the new file and range from 0x00 to 0x0F, ONE byte
Communicate way: Communication setting, ONE byte
Access right: Access right for the new file, TWO byte
File size: the file of the file in byte, THREE byte

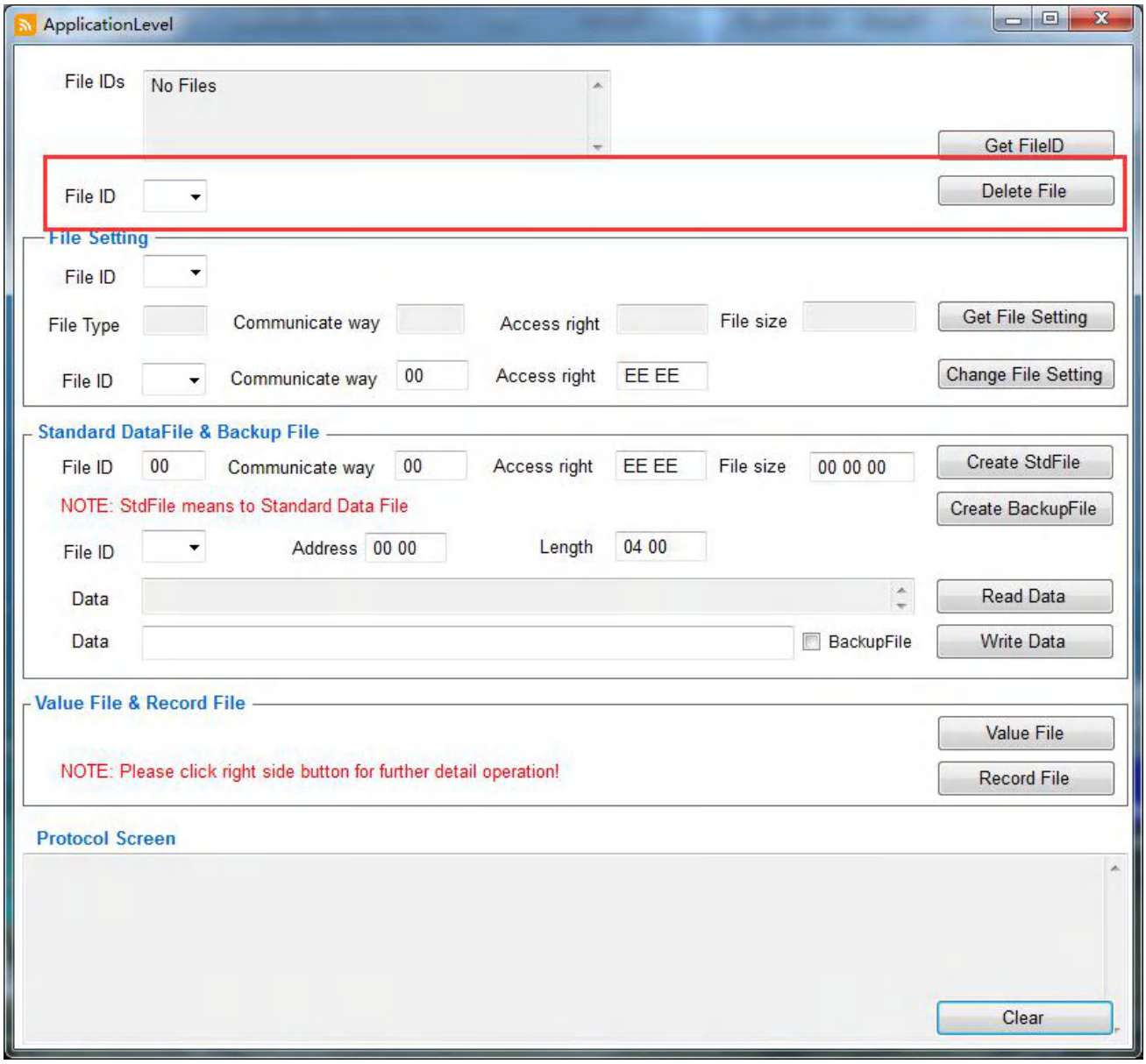
More details information, please refer to datasheet of using card accordingly



2.8.10.5 Application Level-Delete File

This command is to permanently deactivate a file within the file directory of currently selected application

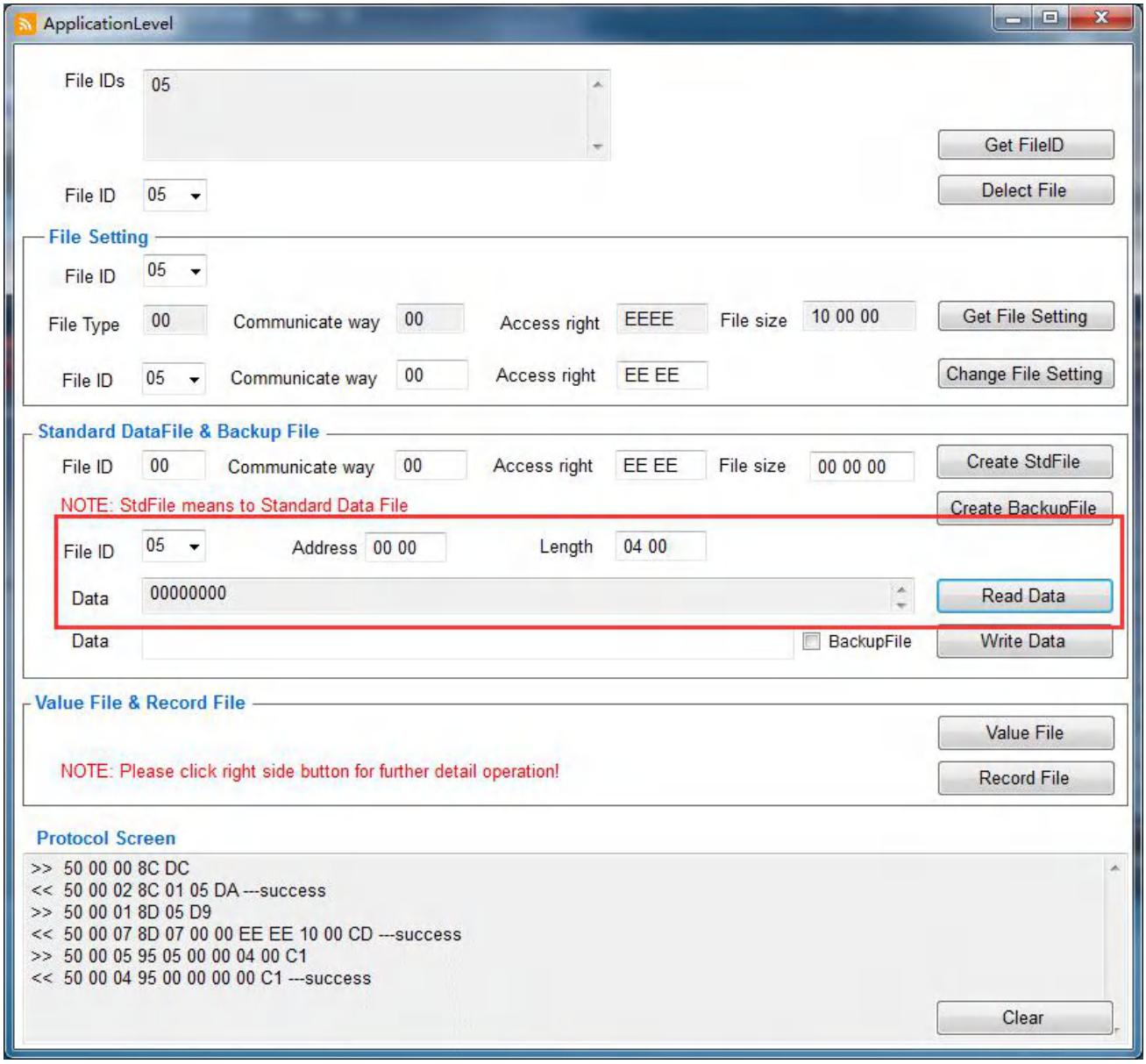
This operation invalidates the file directory entry of the specified file which means that the file can't be accessed anymore.



2.8.10.6 Application Level-Read Data

To read data from Standard Data Files or Backup Data Files

Parameters to be operated:
File ID: the file number to be read from, ONE byte
Address: the starting position for the read operation , THREE byte, range from 0x00 00 00 to 0x FF FF FF
Length: the number of data bytes to be read, THREE byte, and range 0x00 00 00 to 0x FF FF FF

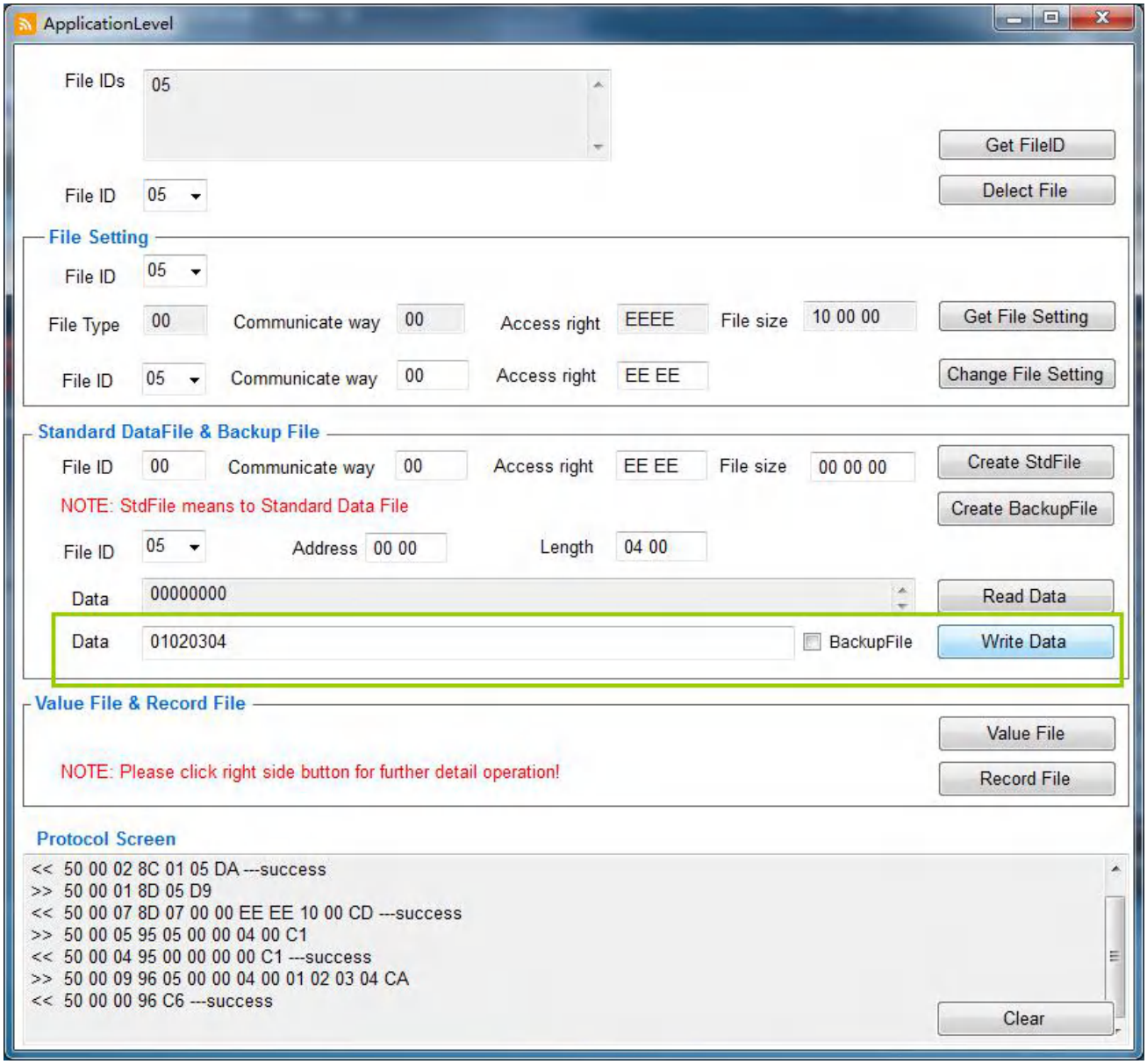


2.8.10.7 Application Level-Write Data

To write data to Standard Data Files and Backup Data Files

Parameters to be operated:
File ID: the file number to be written into, ONE byte
Address: the starting position for the writing operation , THREE byte, range from 0x00 00 00 to 0x FF FF FF
Length: the number of data bytes to be read, THREE byte, and range 0x00 00 00 to 0x FF FF FF
Data:

More details information, please refer to datasheet of using card accordingly

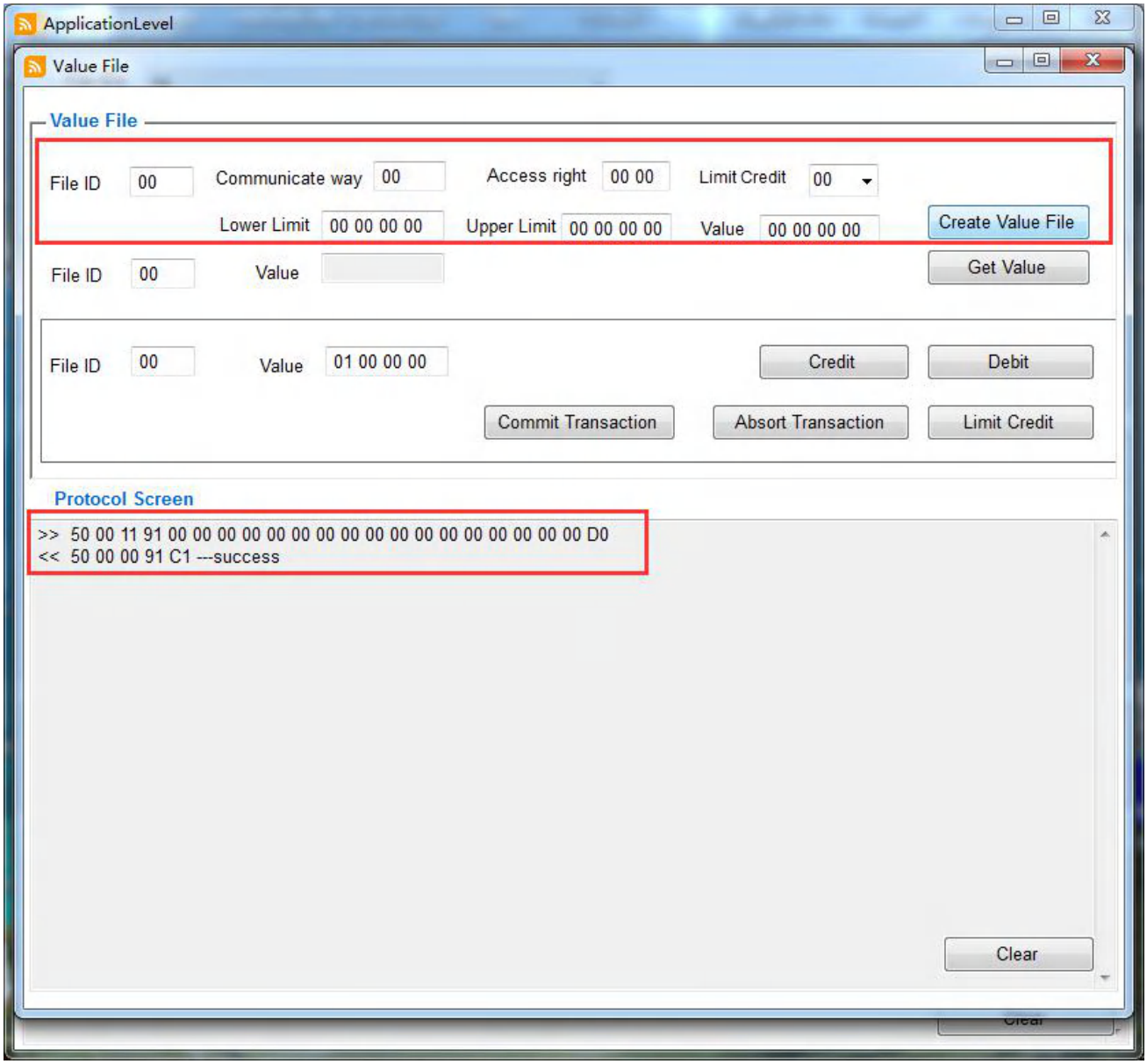


2.8.11 Application Level-Value File

2.8.11.1 Value File -Create Value File

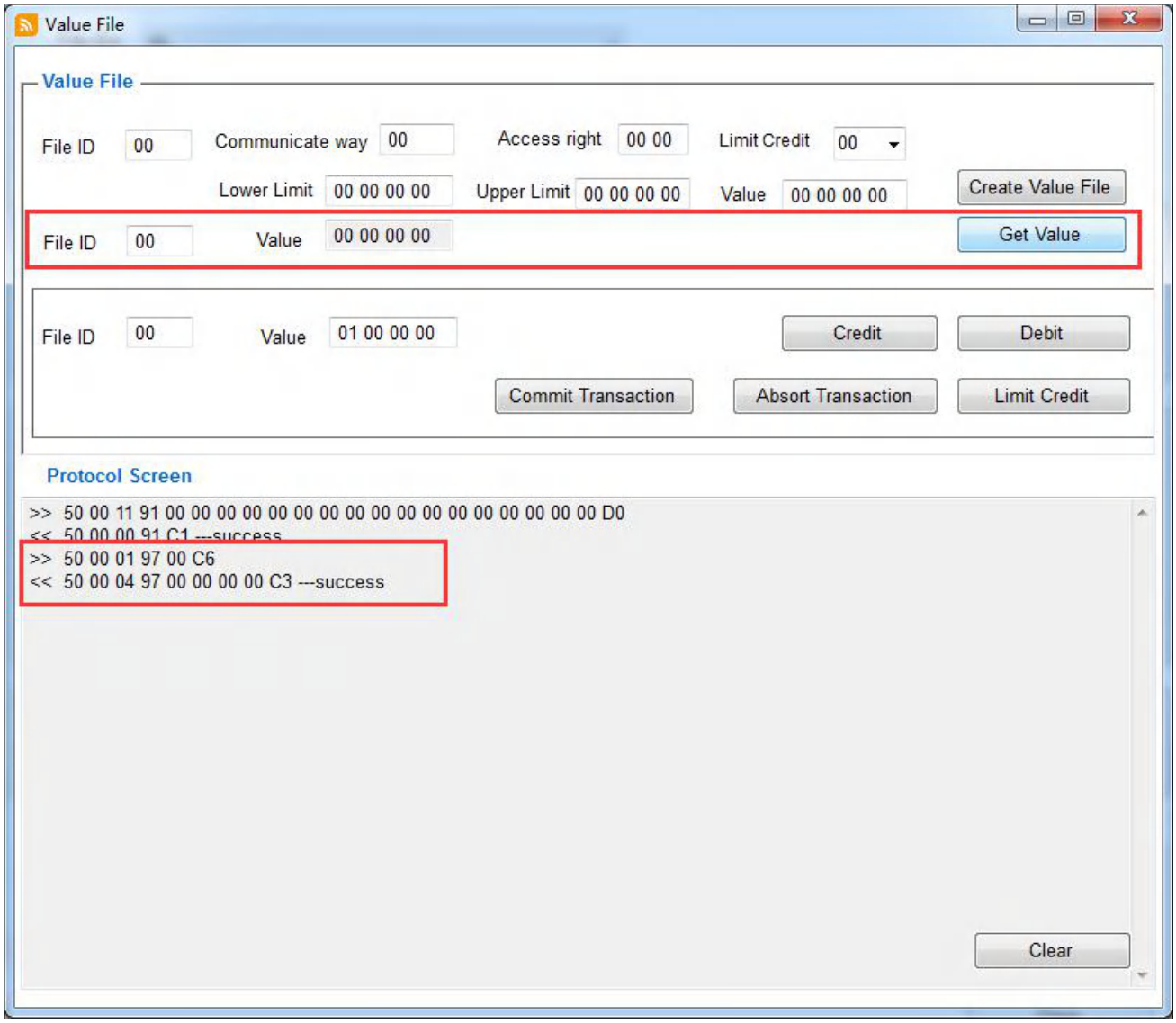
To create files or the storage and manipulation of 32bit signed integer value within an existing application on the PICC

More details information, please refer to datasheet of using card accordingly



2.8.11.2 Value File -Get Value

It allows to read the currently stored value from Value File



2.8.11.3 Value File-Transactions operation

The transactions are including:

Credit: increase a value stored in a Value File

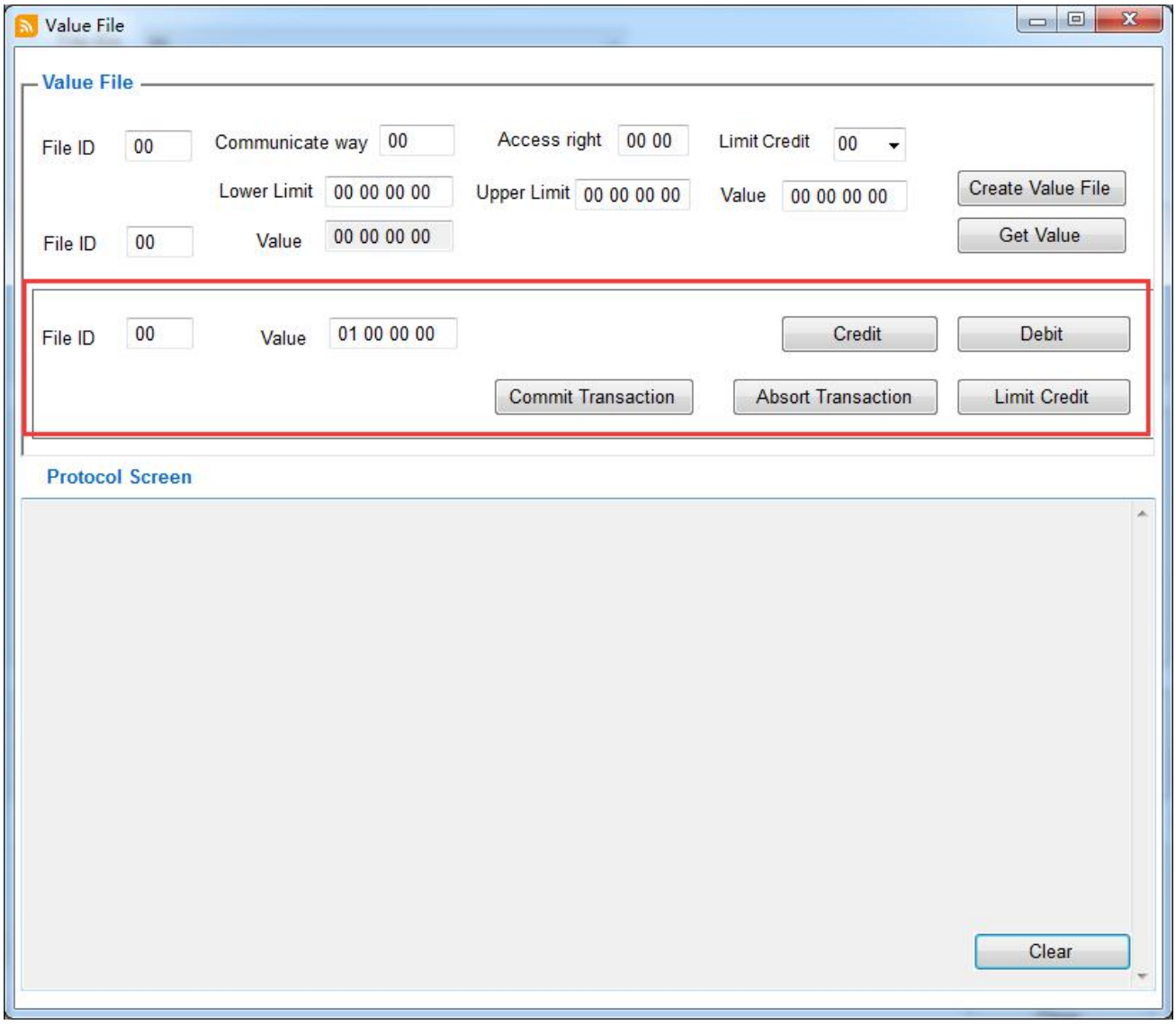
Debit: decrease a value stored in a Value File

Commit Transaction: Validate all previous write access on Backup Data File, Value Files and Record Files within one application

Abort Transaction: invalidate all previous write access on Backup Data File, Value Files and Record Files within one application

Limit Credit: limited increase of a value in a Value File without having full Read&Write permission to the file

More details information, please refer to datasheet of using card accordingly

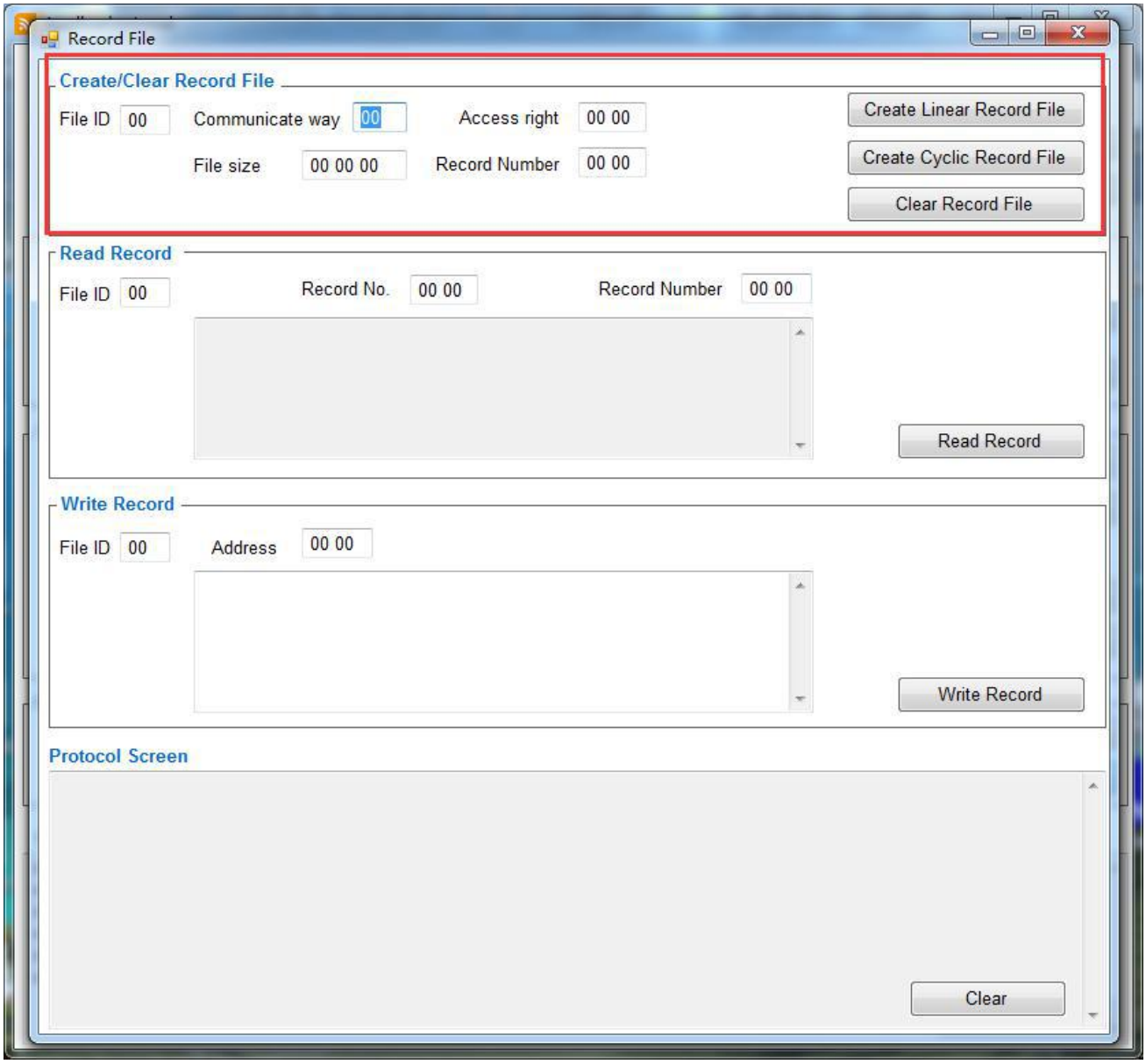


2.8.12 Application Level- Record File

2.8.12.1 Record File-Create Linear/Cyclic Record File

This is used to create files for multiple storage of structural data, for example for logging transactions,

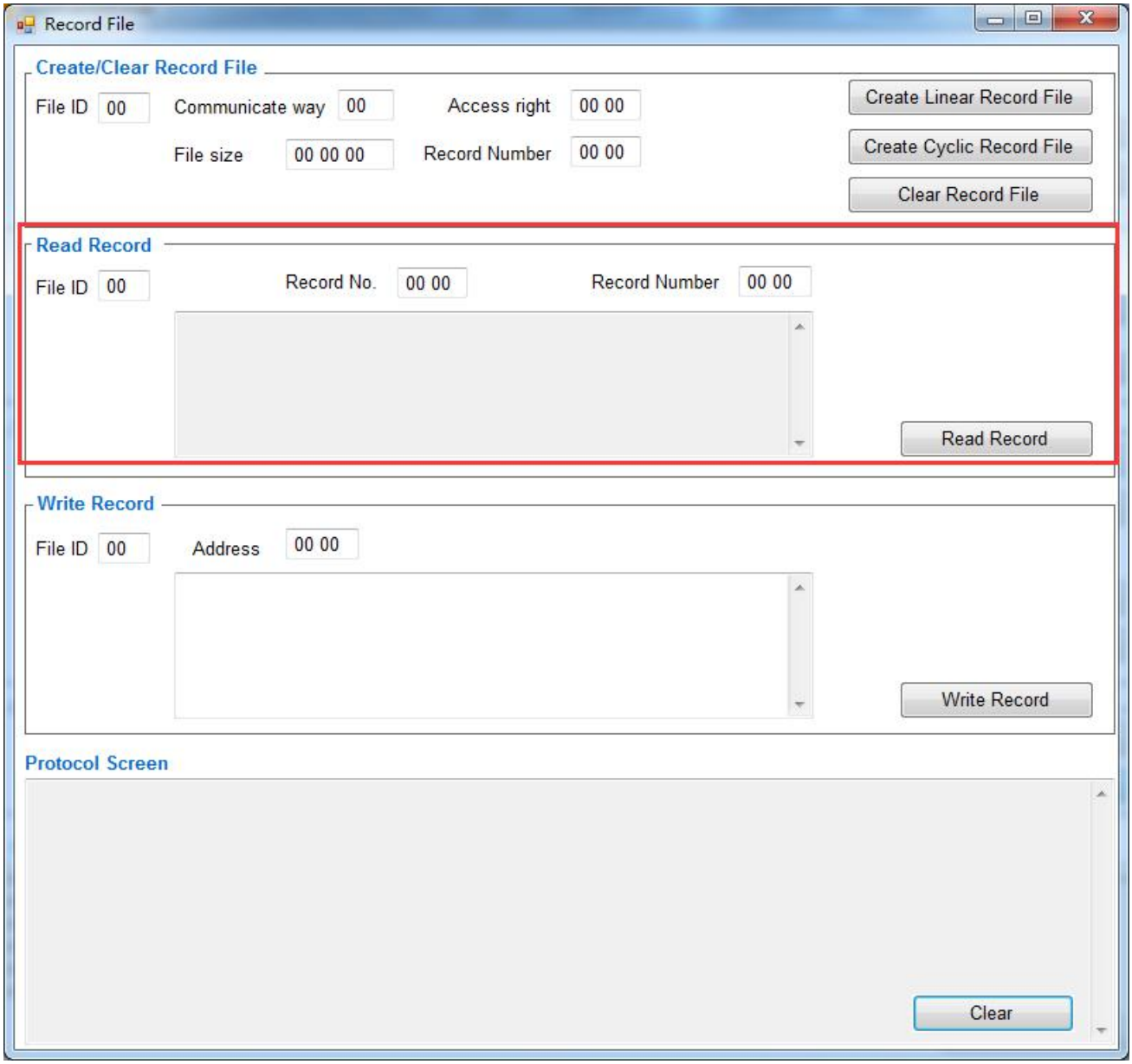
More details information, please refer to datasheet of using card accordingly



2.8.12.2 Record File-Read Record

To read out a set of complete records from a Cyclic or Liner Record File

Parameters to be read:
File ID: the file number to be read from, ONE byte length
Record No: the offset of the newest record which is read out, THREE bytes long
Record Number: the number of records to be read from PICC



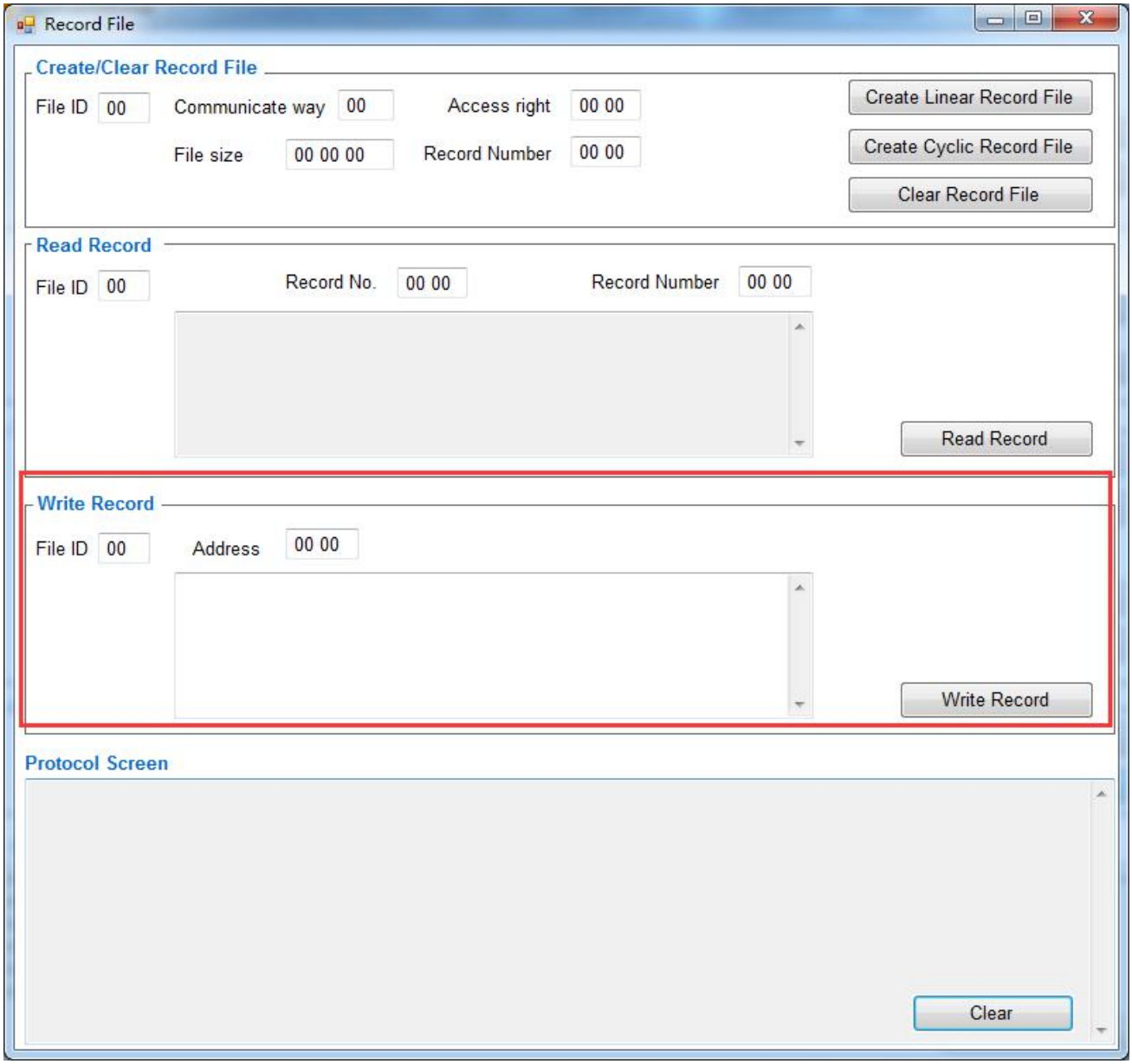
2.8.12.3 Record File-Write Record

To write data to a Cyclic or Liner Record File

Parameters to be written:

File ID: the file number to be written into and has to be range from 0x00 to 0x07, ONE byte length

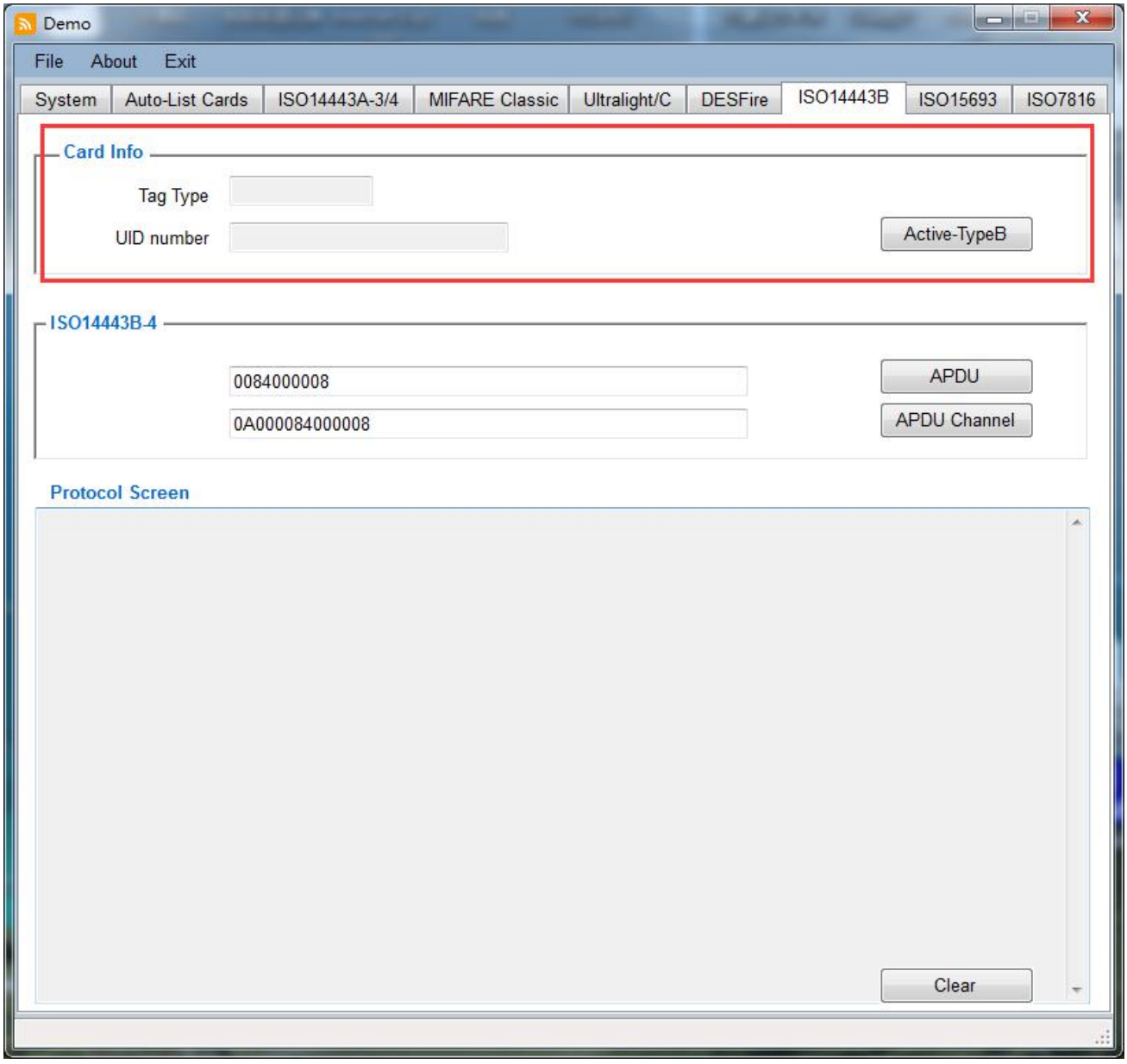
Address: the offset within one single record, and range from 0x00 00 00 00 to record size - 1



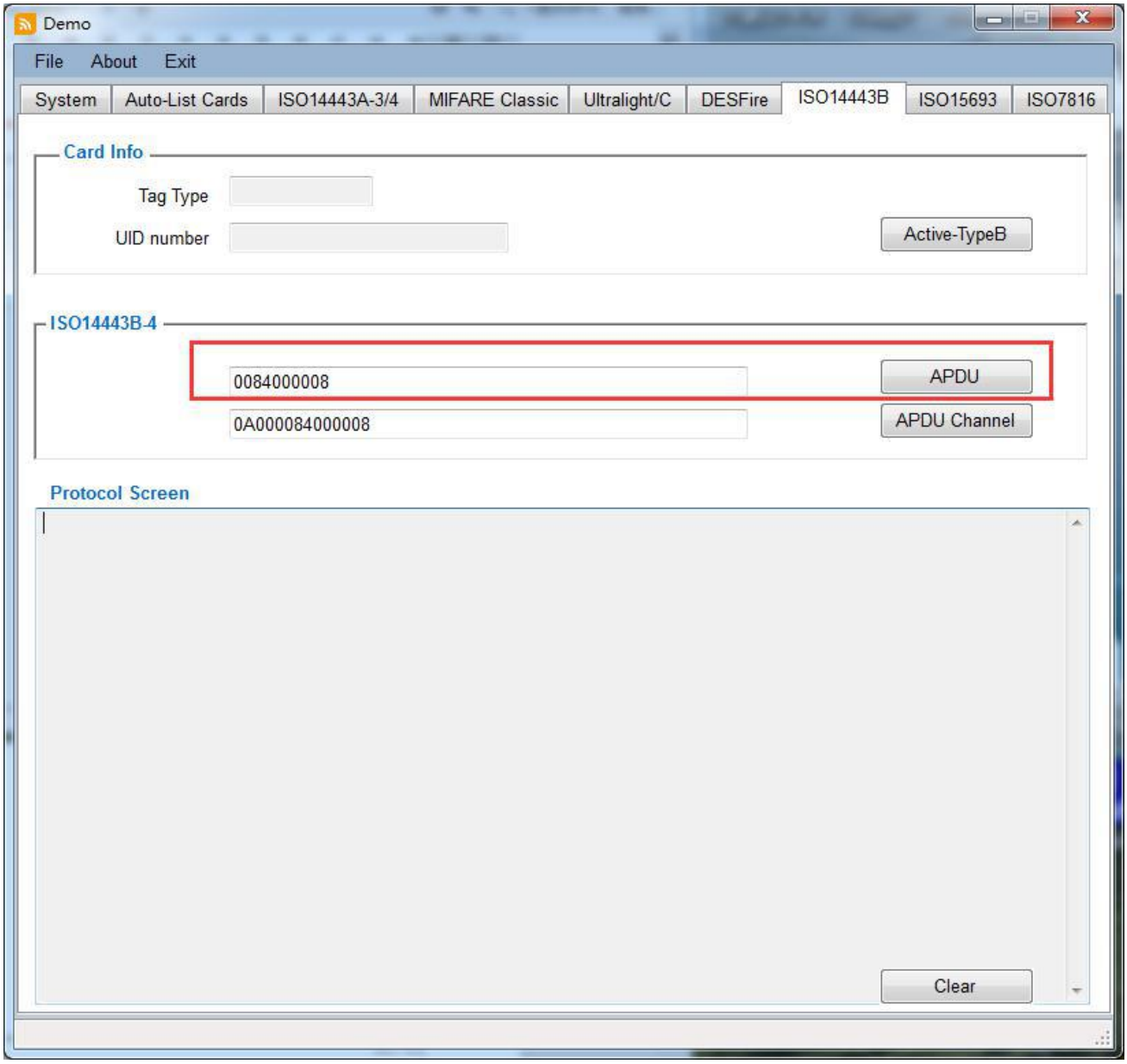
2.9 ISO14443B

2.9.1 ISO14443B- Active-TypeB

To active ISO14443 Type B cards/tag



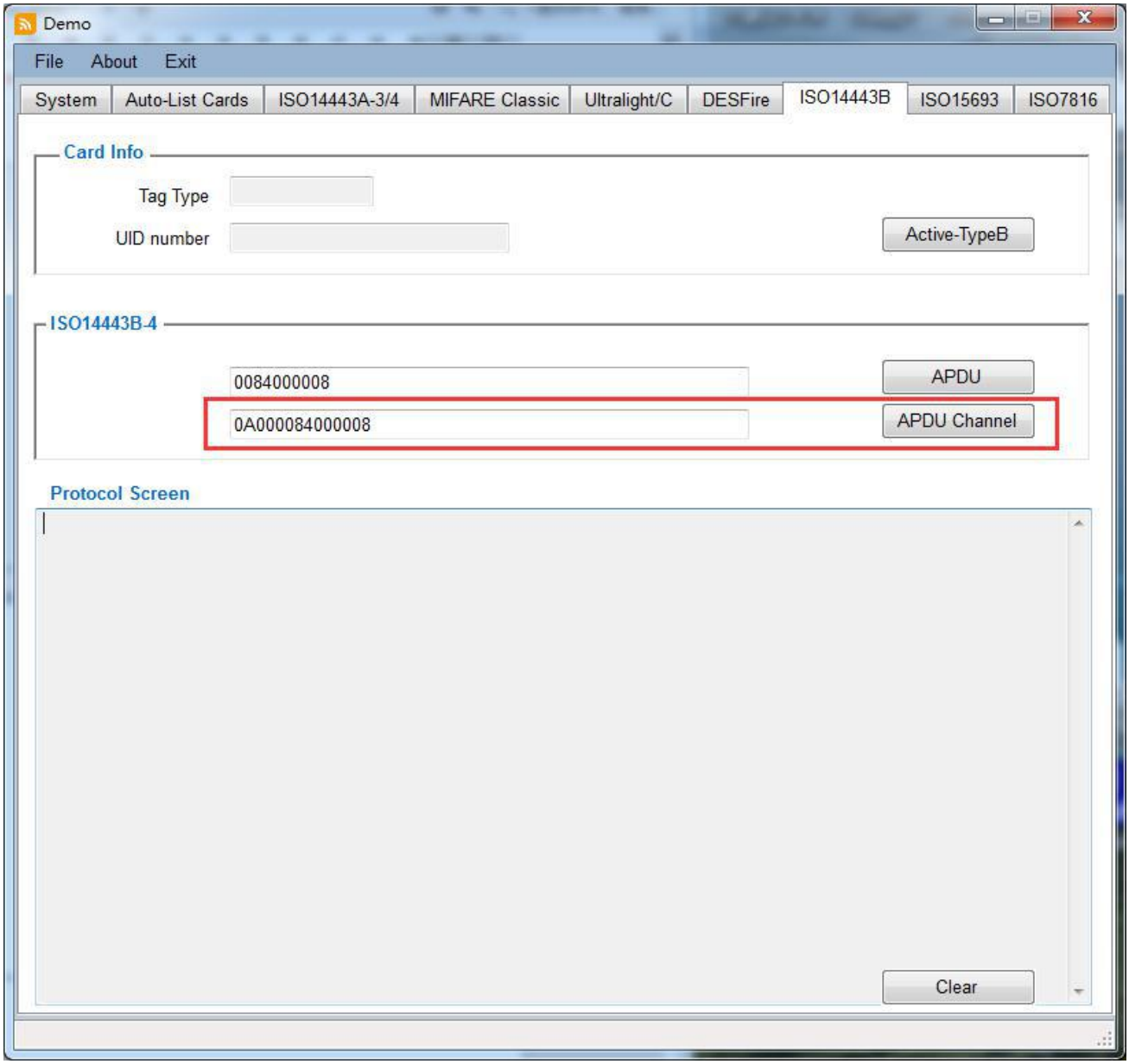
2.9.2 ISO14443B-4 APDU



2.9.3 ISO14443B-4 APDU Channel

This is transfer channel to send any available commands to the card directly through RF chipset.

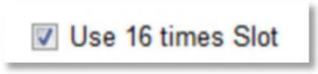
Details commands please refer to ISO14443B-4 Standard .



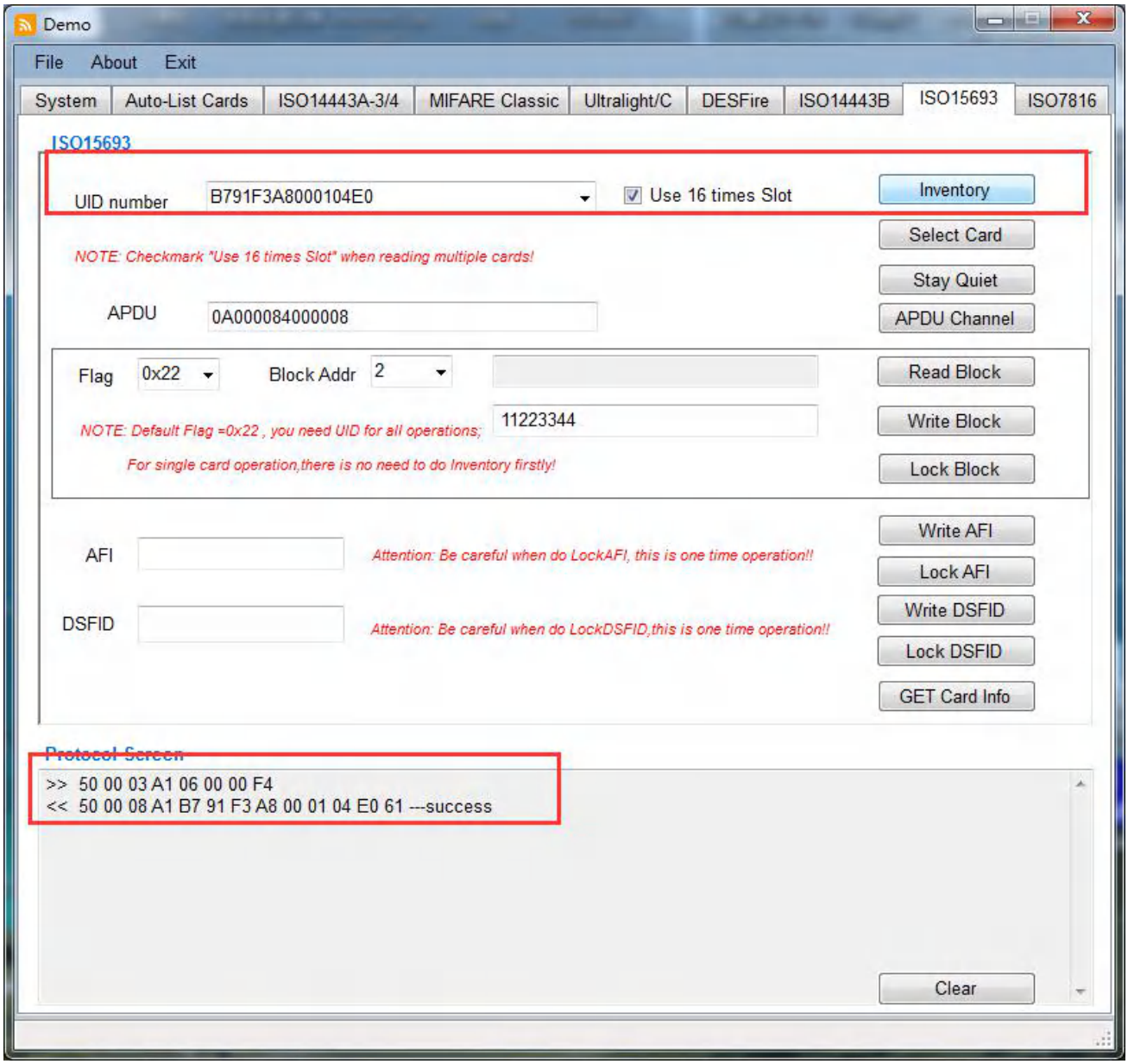
2.10 ISO15693

2.10.1 ISO15693-Inventory

To get the UID of ISO15693 standard cards/tags.

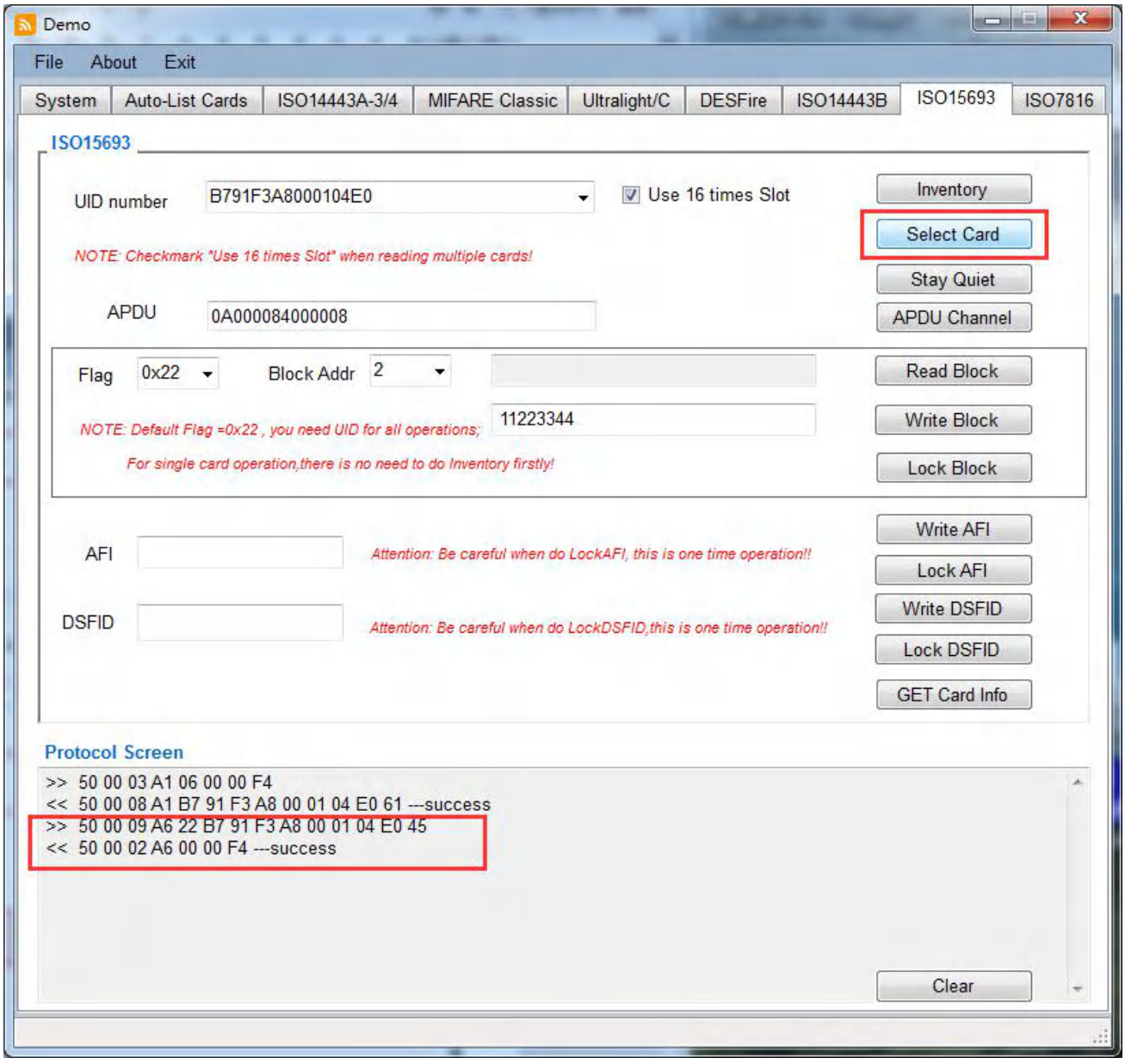
When 

is selected, it can be read multiple cards in one time, and the all UID numbers will be listing on leftside box.



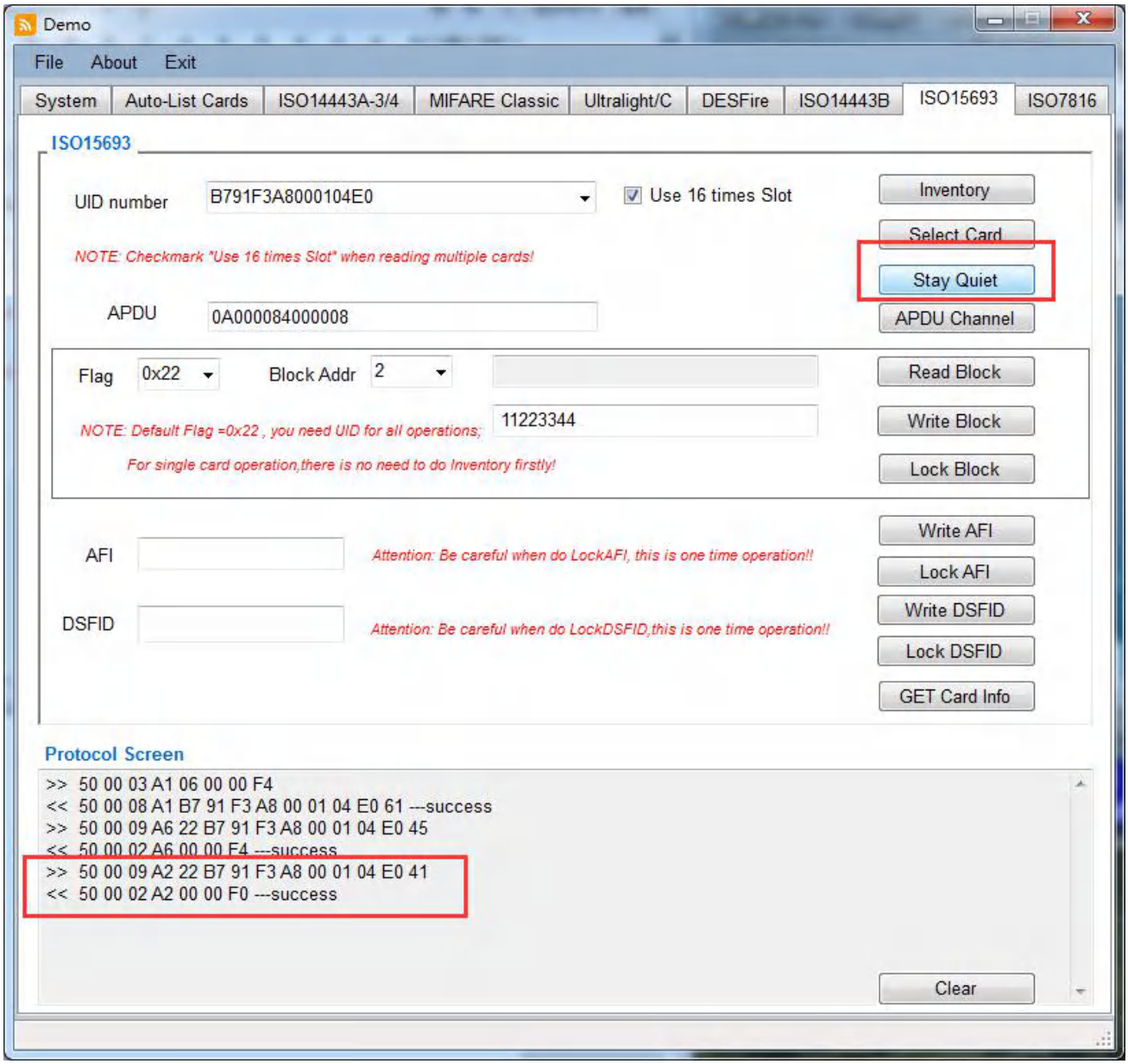
2.10.2 ISO15693-Select card

To select the card for further read/write operations, when there are multiple cards, please select the right one on UID number lists after inventory.



2.10.3 ISO15693-Stay Quiet

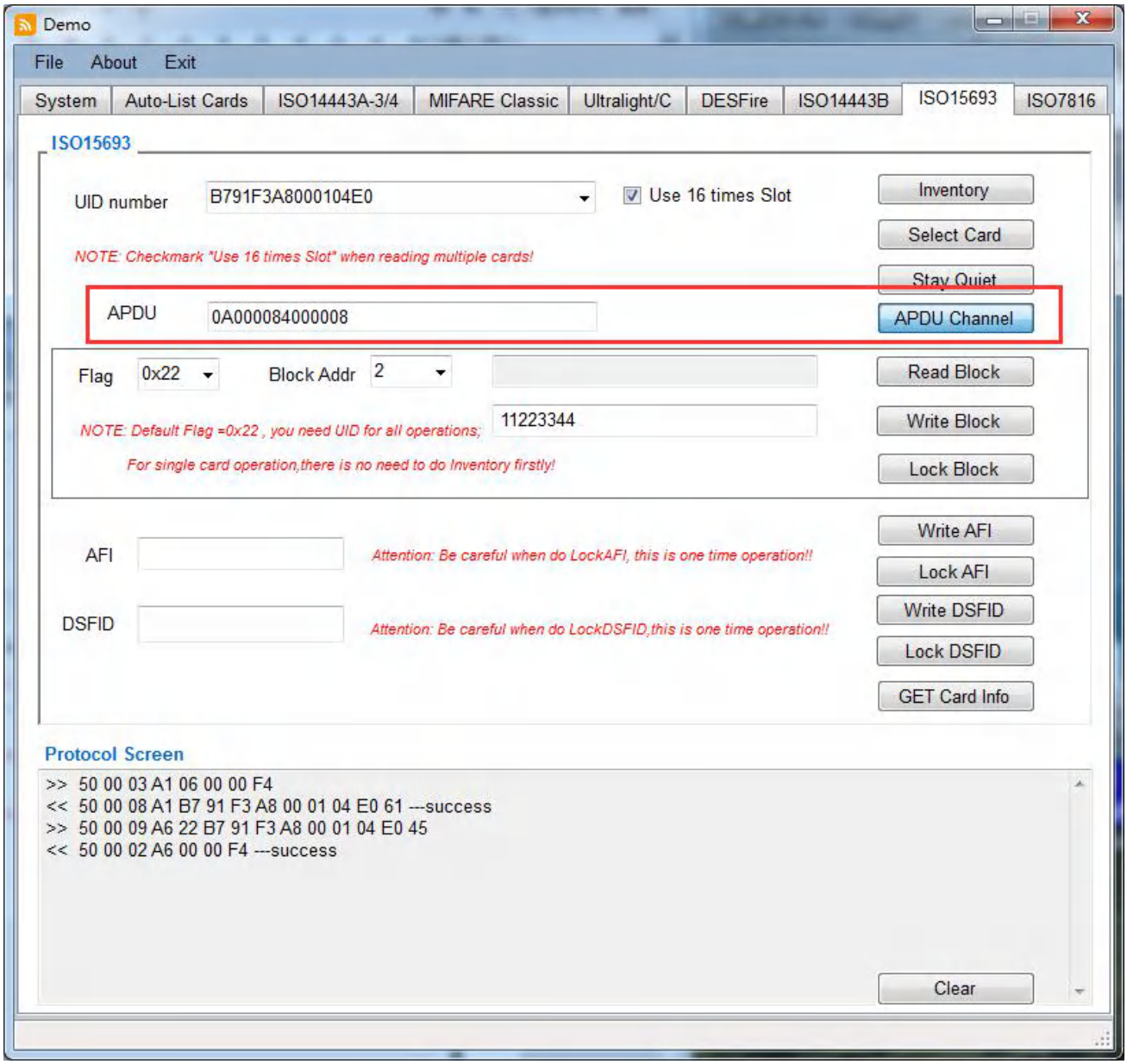
To make the card to be slept



2.10.4 ISO15693-APDU

This is transfer channel to send any available commands to the card directly through RF chipset.

And The first CMD before transfer must be ISO15693_Inventory, this will set the reader (or module) go into ISO15693 mode, Details commands please refer to ISO15693 Standard .



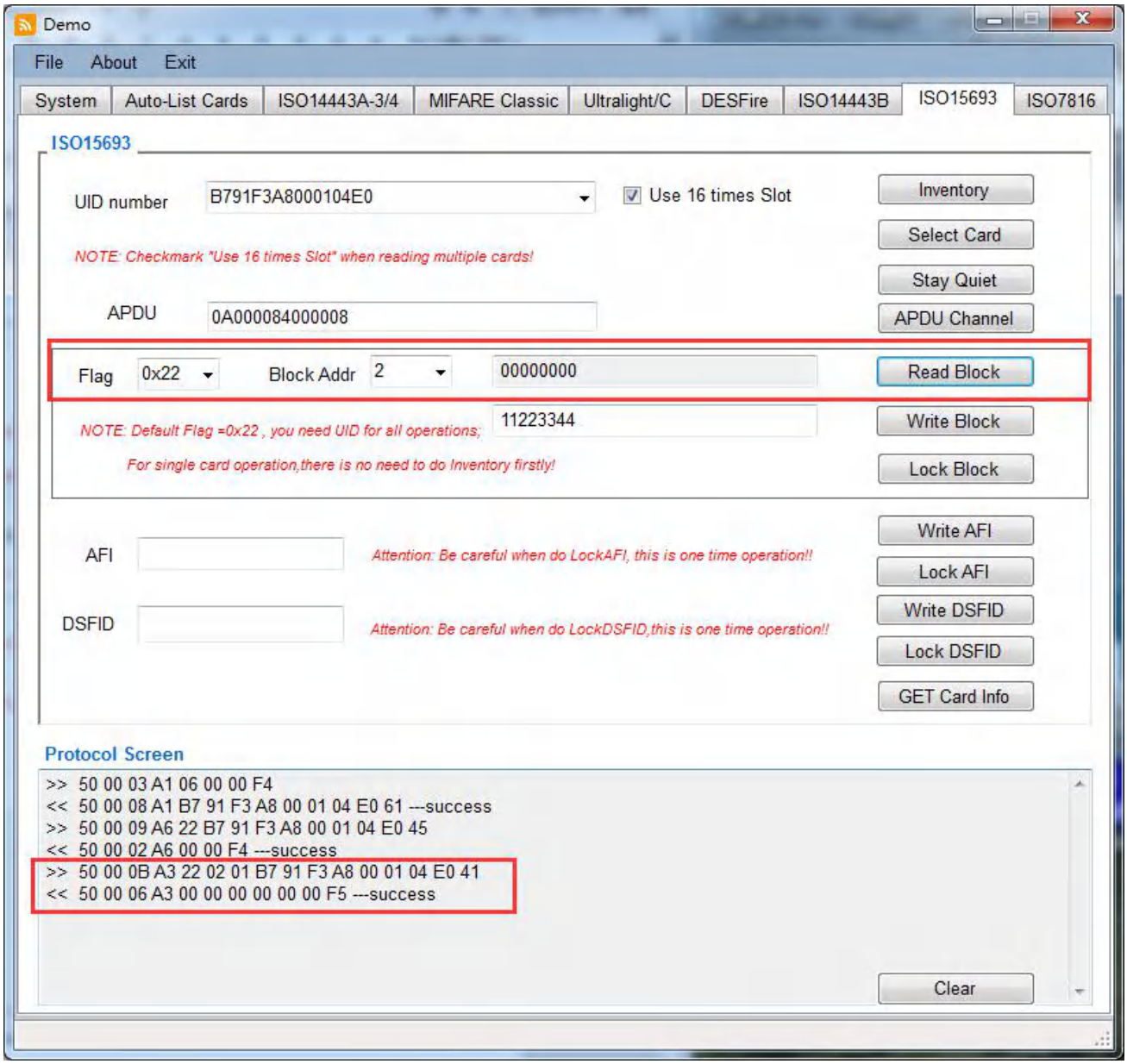
2.10.5 ISO15693-Read Block

To read the data in specific block address

Parameters to be optional:

Flag: 0x22 or 0x02, refer to datasheet of using card

Block Addr: the block address to be read



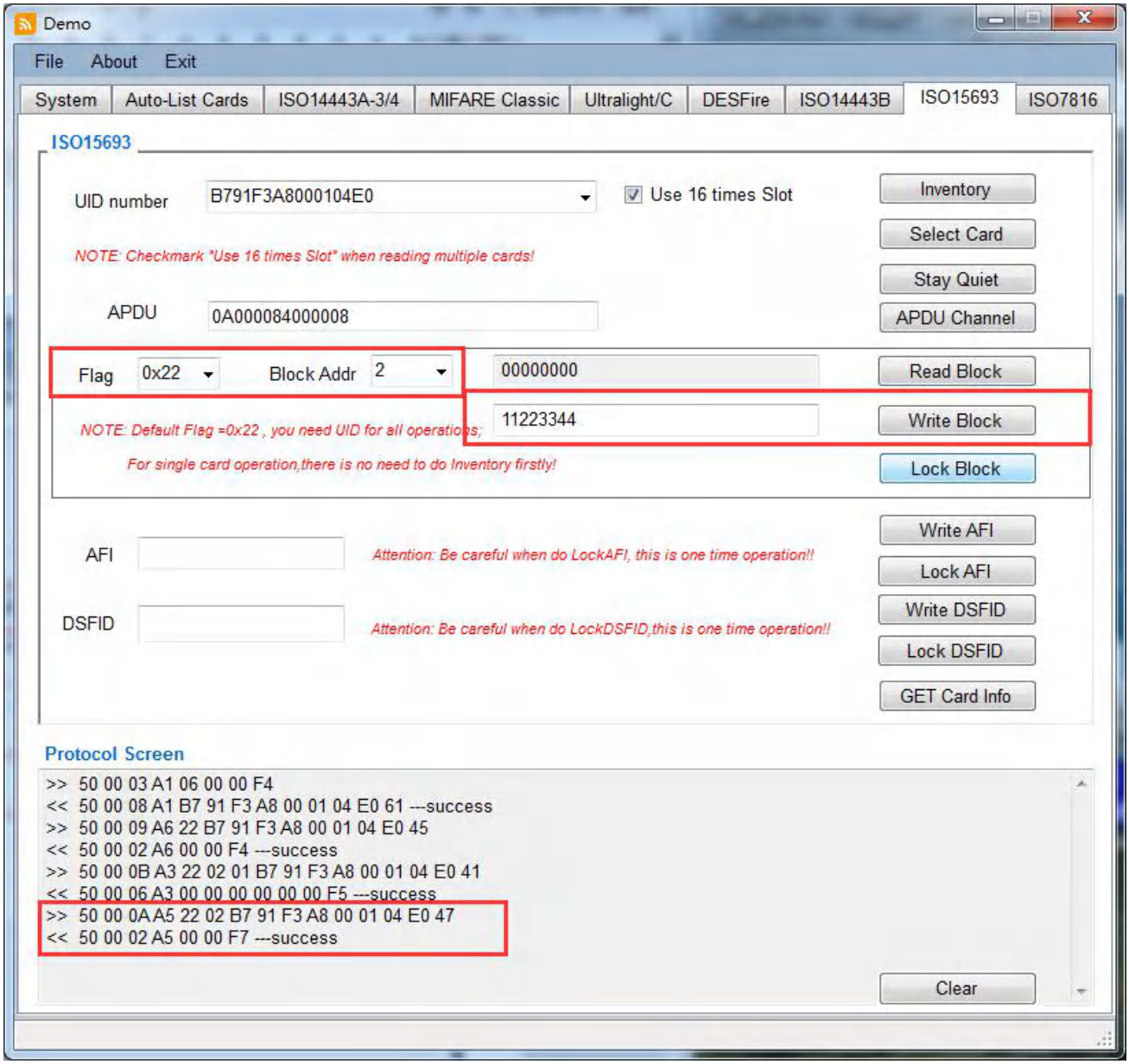
2.10.6 ISO15693-Write Block

To write data into specific block address

Parameters to be optional:

Flag: 0x22 or 0x02, refer to datasheet of using card

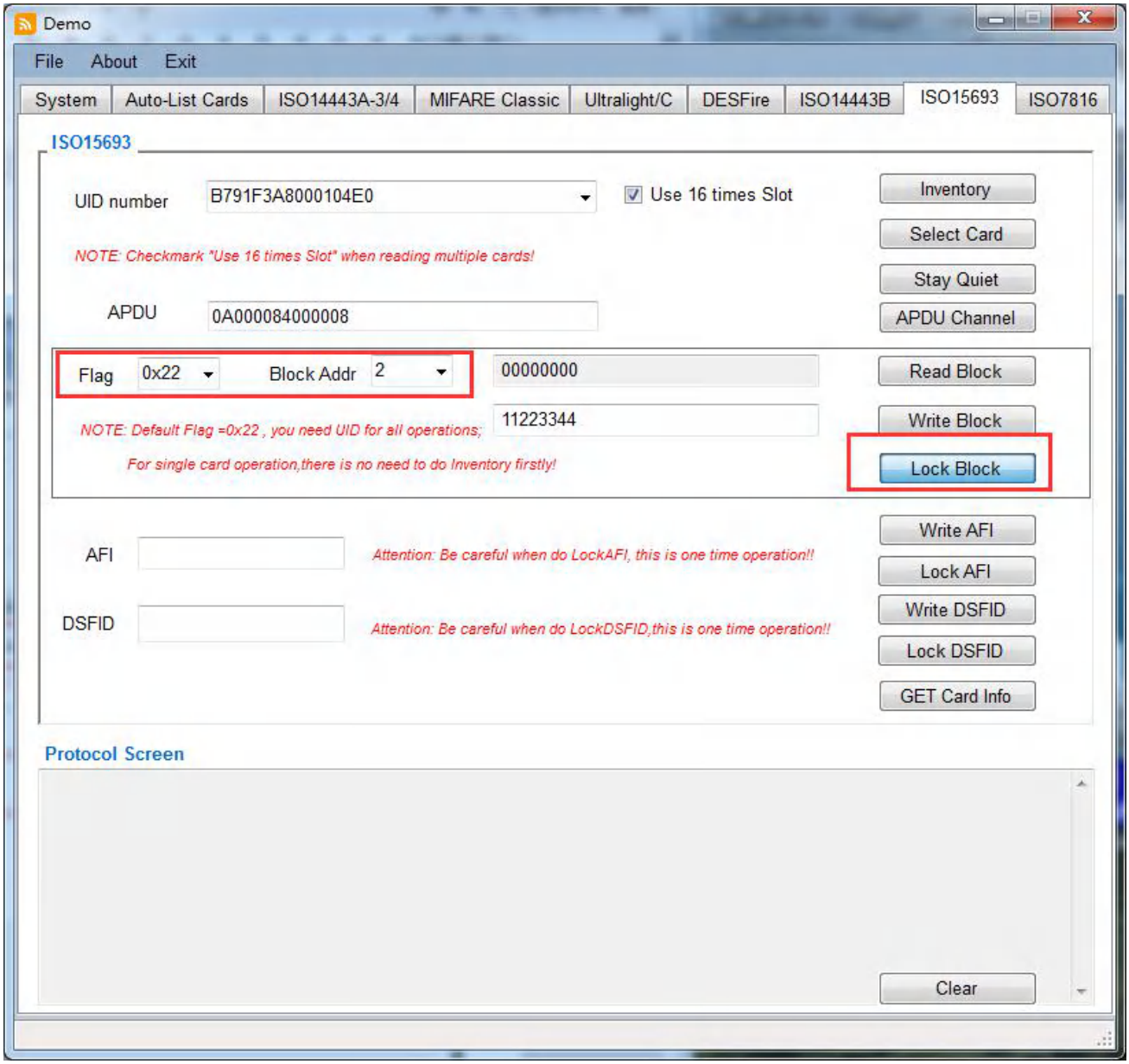
Block Addr: the block address to be written, 4byte length



2.10.7 ISO15693-Lock Block

To lock the specific block address

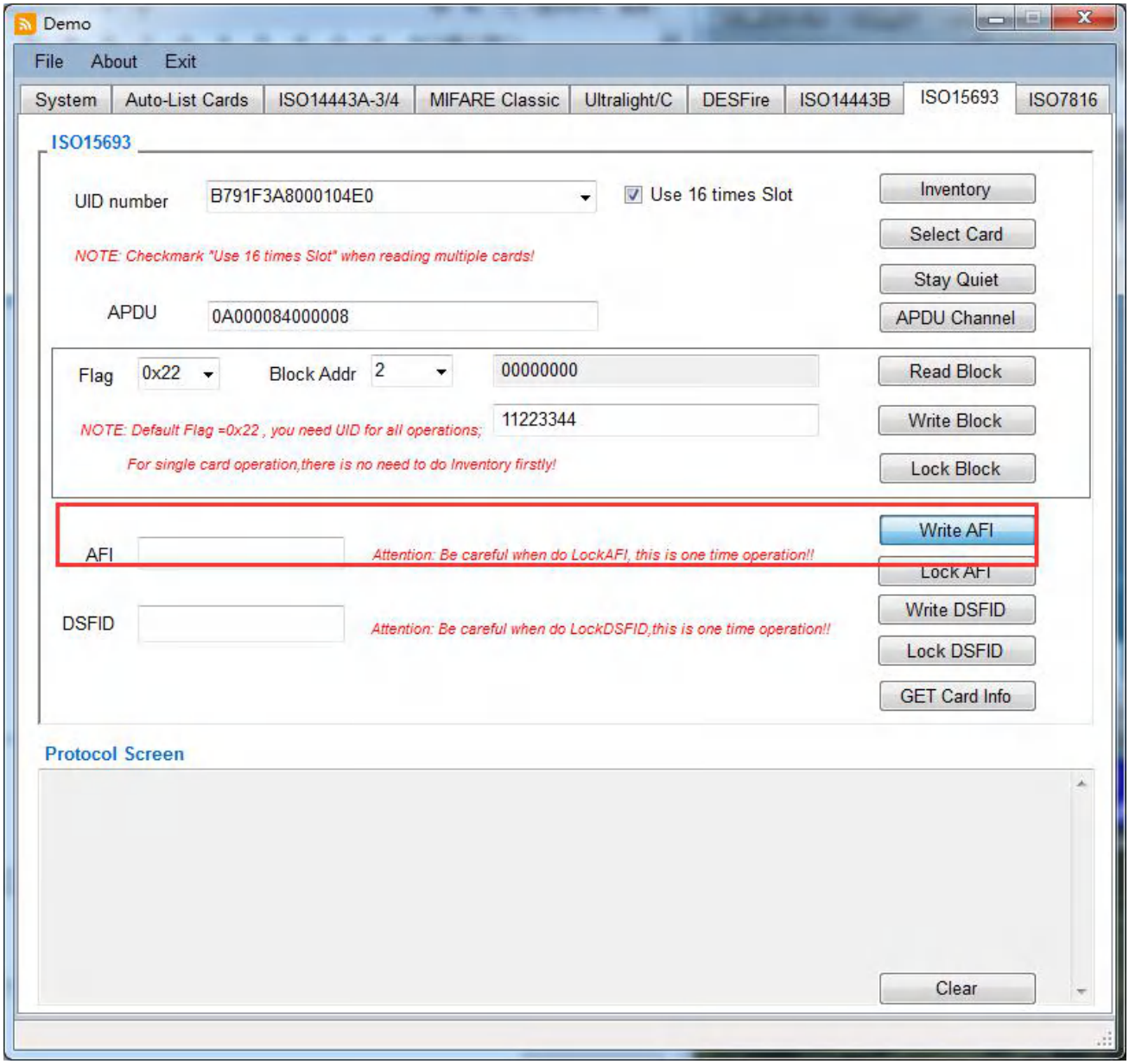
Parameters to be optional:
Flag: 0x22 or 0x02, refer to datasheet of using card
Block Addr: the block address to be locked



2.10.8 ISO15693-Write AFI

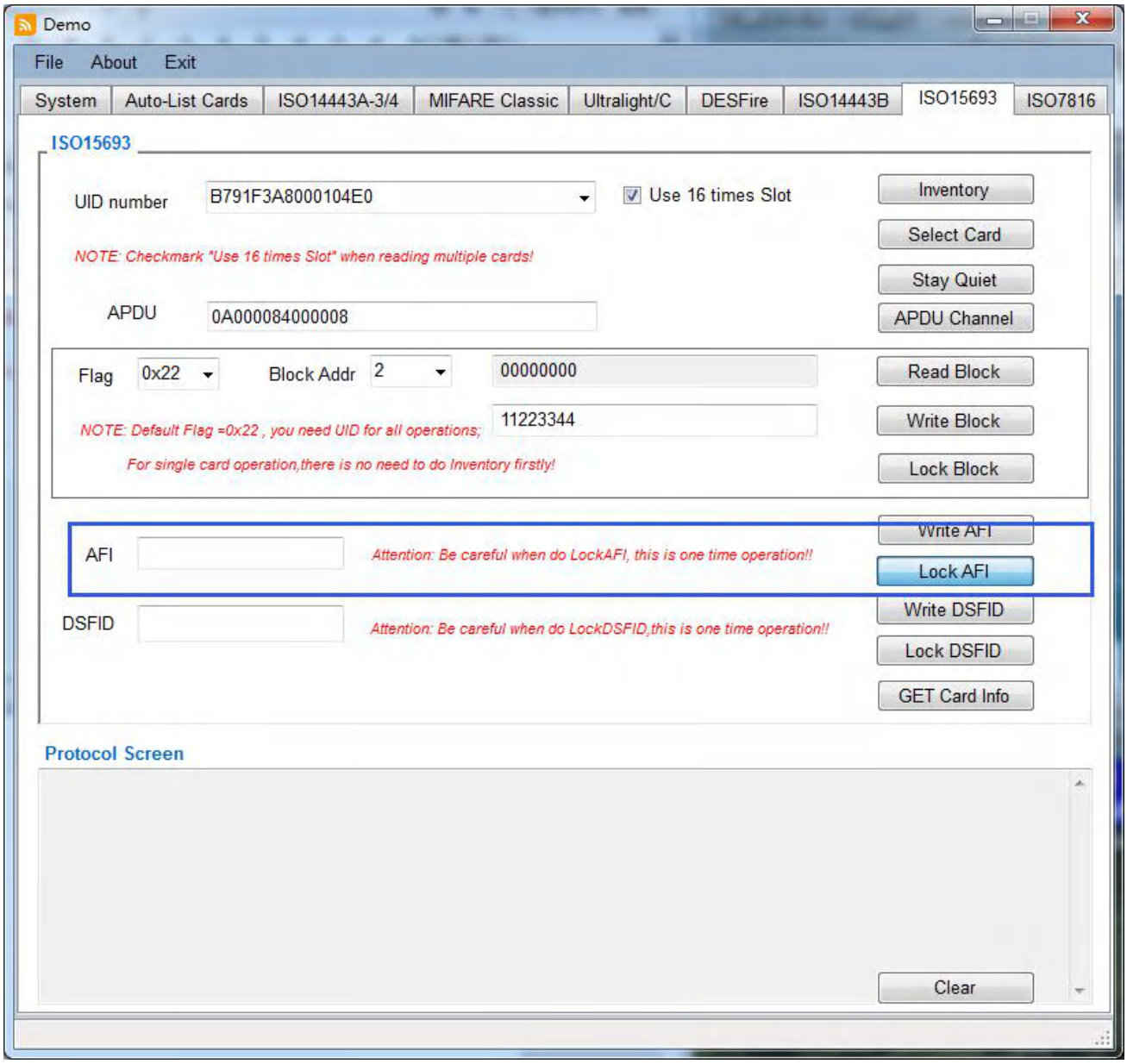
AFI=Application Family Identifier, which it's a 8-bit value and located at Byte 2 in Block -2 ,and it allows for example the creation of label families.

For details please refer to ISO 15693-3.



2.10.9 ISO15693-Lock AFI

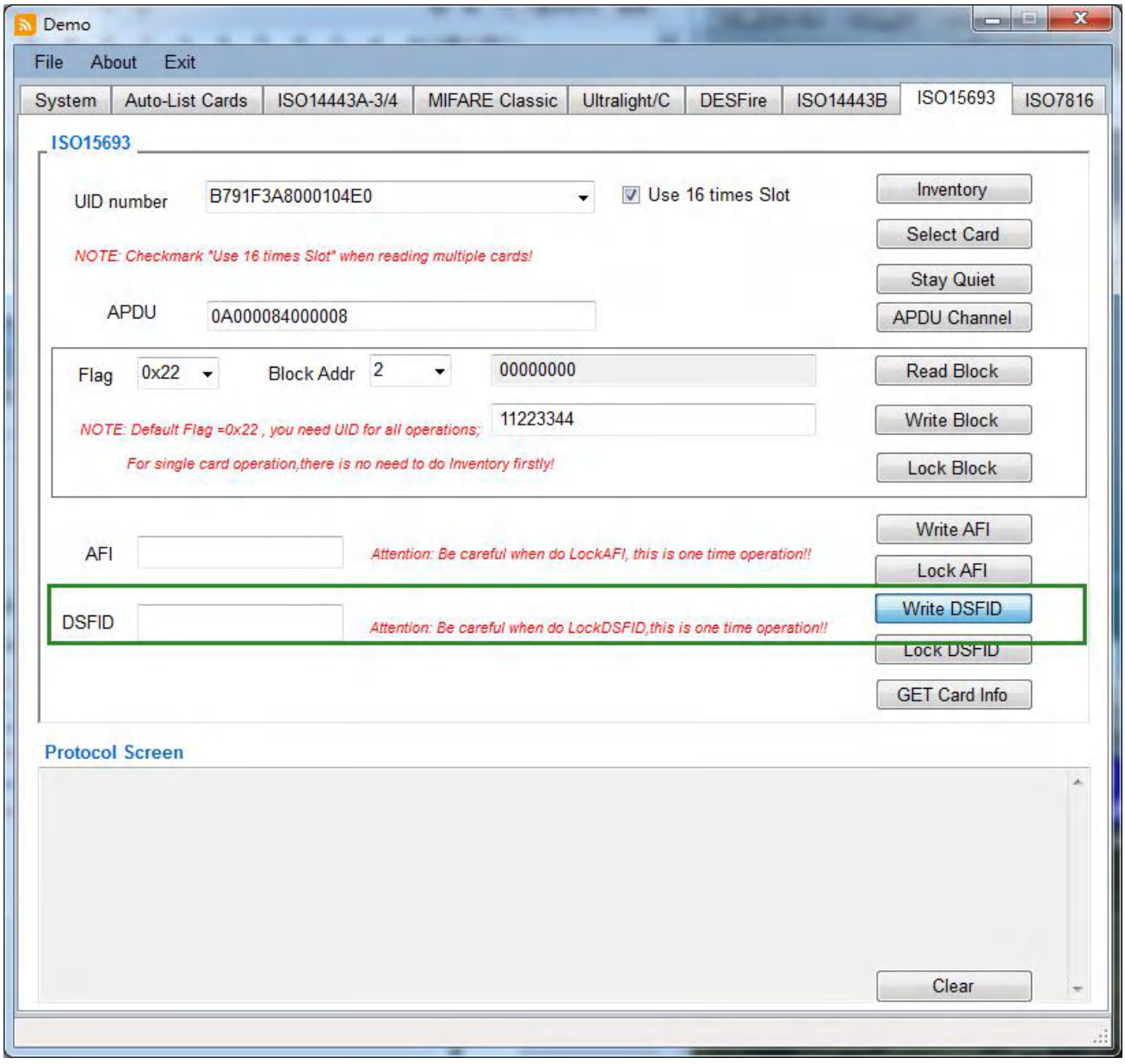
For details please refer to ISO/IEC 15693-3.



2.10.10 ISO15693-Write DSFID

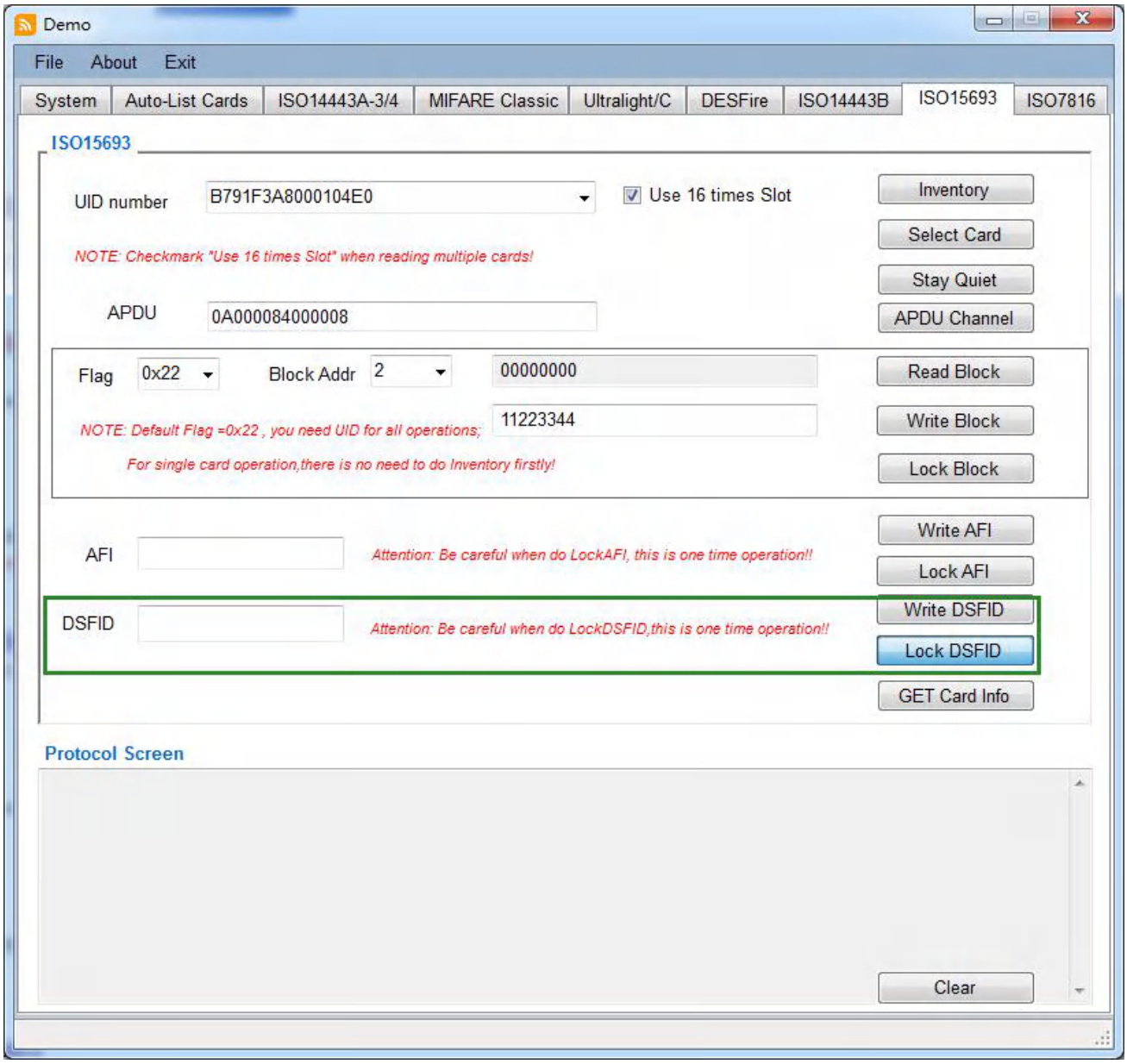
DSFID= Data Storage Format Identifier, whichis located at Byte 3 in Block –2.

For details please refer to ISO/IEC 15693-3.

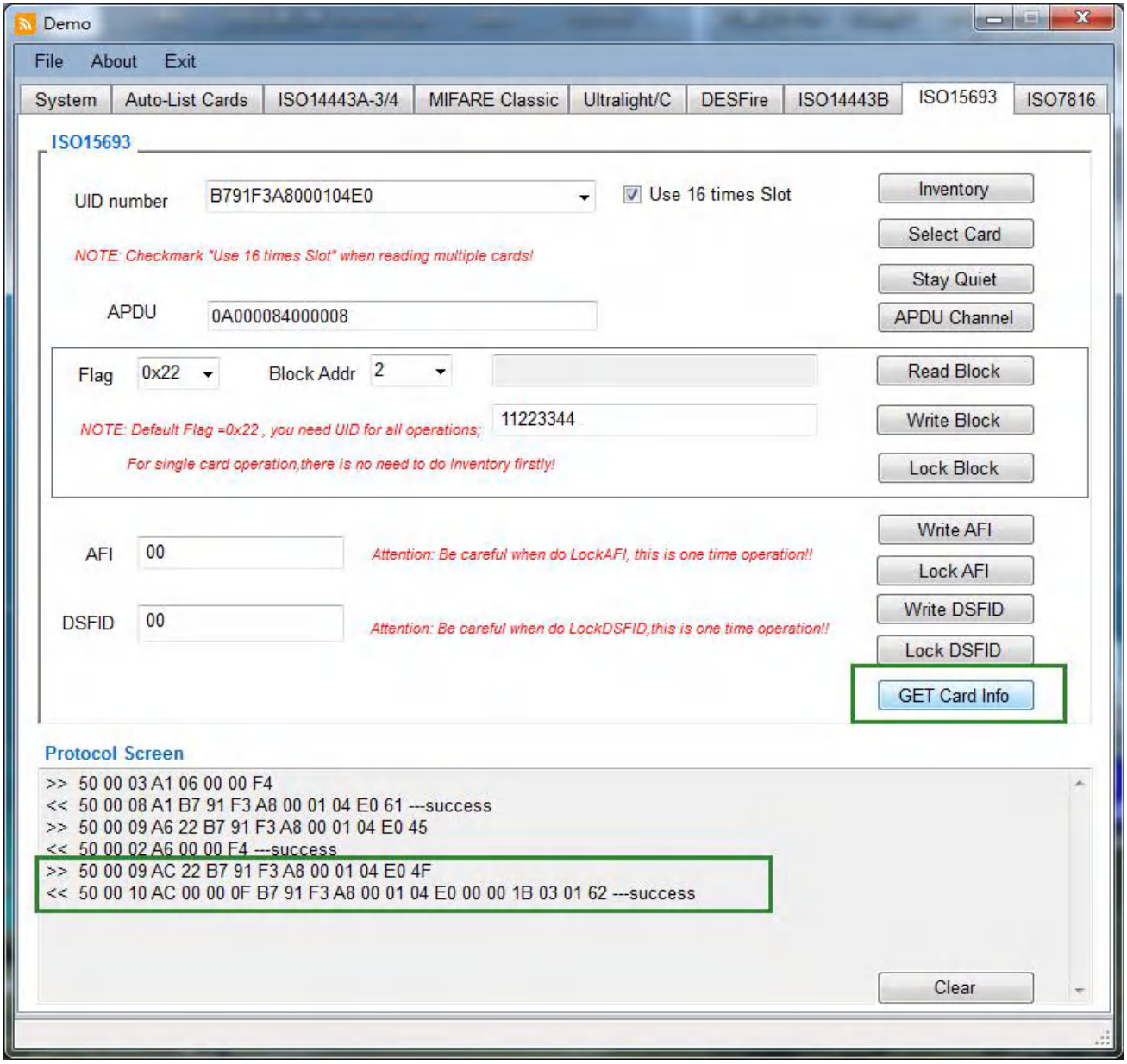


2.10.11 ISO15693-Lock DSFID

For details please refer to ISO/IEC 15693-3.



2.10.12 ISO15693-Get Card Info



Other functions not on above listing or any other specific request about our device, please contact our sales person or technical engineers for support, THANK YOU.

Contact information:

SHENZHEN CHIKEK Intelligent TECH CO.,LTD
Room 210, 2nd Bldg, WanYuan Commercial Building, 71th District, XinAn Street,BaoAn, 518101, SHENZHEN

TEL: 86-755-23766242 -803 FAX: 86-755-23571242
Email: sales@chikek-rfid.com , support@chikek-rfid.com
Website: www.chikek-rfid.com

FCC statement

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:
1) this device may not cause harmful interference, and
2) this device must accept any interference received, including interference that may cause undesired operation.
Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
--Reorient or relocate the receiving antenna.
--Increase the separation between the equipment and receiver.
--Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
--Consult the dealer or an experienced radio/TV technician for help.
Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.
FCC Radiation Exposure Statement
This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.