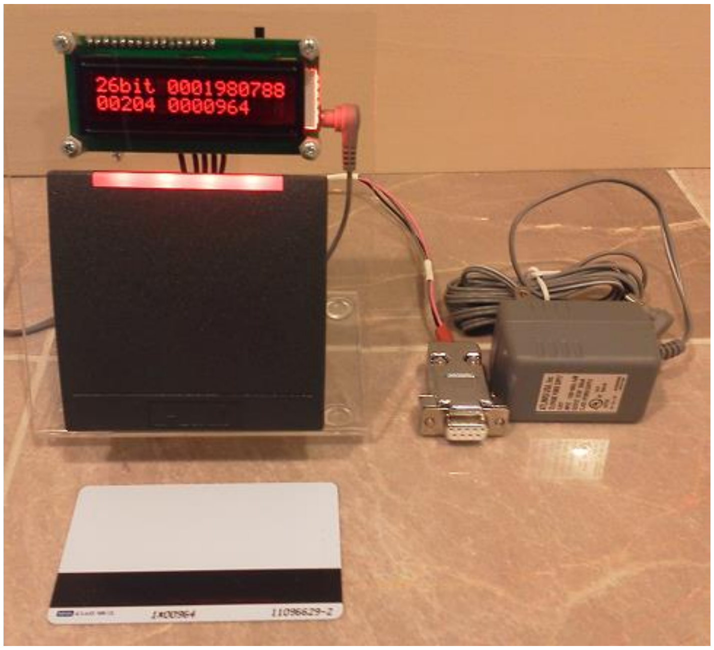


Hardware Setup

The iClass Cloner application operates in conjunction with an off-the-shelf iClass Reader Writer manufactured by HID Corporation. Communication with the reader is via the iClass readers RS-232 serial interface. An optional connection between the readers Wiegand interface and a special microcontroller/LCD display circuit allows card data to be displayed even when the reader is not attached to a PC.

A block diagram of the system is shown in Figure 1 below. The iClass reader requires a connection to both dc power and the PC's RS-232 interface in order to function properly. An off-the-shelf USB to Serial converter is required if the PC does not provide an integrated serial COM port. A switch located above the LCD display is used to apply power to the wiegand decoder/LCD display and RW300 iClass reader/writer.

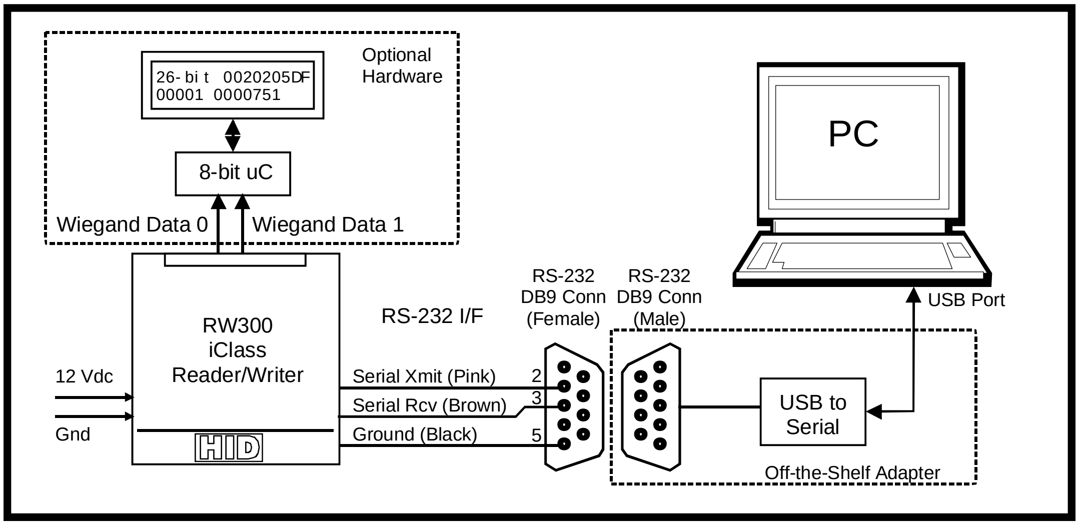


Figure 1. iClass Reader System Configuration

Software installation

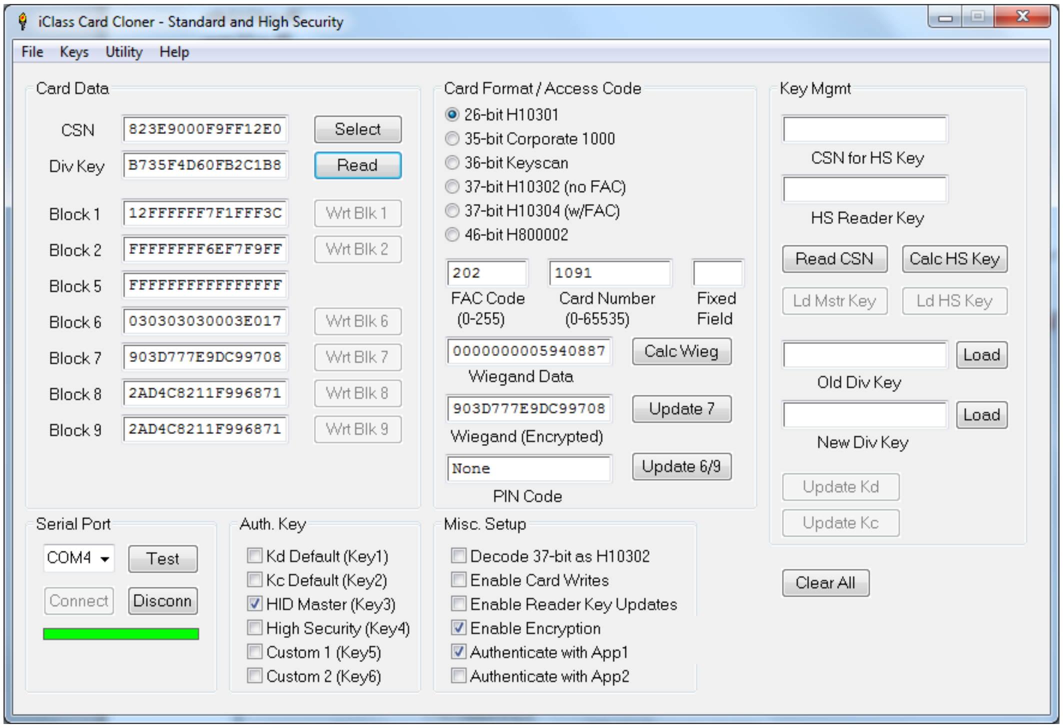
The iClass cloner application is contained in a single compressed file named iclass_cloner.zip. The files must be extracted to any user-selected directory before use. The application consists of the following files:

iClass_Cloner_rev10a.exe – Main Application
iClass_Cloner_rev10a.tkn
iClass_Cloner_Instructions_Rev10a.pdf – This set of installation/operating instructions
vbas31w.sll
vgui31w.sll
voflr31w.sll
vthk31w.dll
vtk1631w.dll
vtk3231w.dll
vvm31w.dll
vvmt31w.dll

One additional High Security key table file has also been included to allow interaction with cards used in Keyscan High Security systems. This file is as follows:

hskeytable_keyscan.key

Execute the iclass_cloner_rev10a.exe file to start the iClass cloner application. The main screen will be similar to the one shown in Figure 2 below.



CSN: 823E9000F9FF12E0
Div Key: B735F4D60FB2C1B8
Block 1: 12FFFFFF7F1FFF3C
Block 2: FFFFFFFF6EF7F9FF
Block 5: FFFFFFFFFFFFFFFF
Block 6: 030303030003E017
Block 7: 903D777E9DC99708
Block 8: 2AD4C8211F996871
Block 9: 2AD4C8211F996871

● 26-bit H10301
○ 35-bit Corporate 1000
○ 36-bit Keyscan
○ 37-bit H10302 (no FAC)
○ 37-bit H10304 (w/FAC)
○ 46-bit H800002

FAC Code (0-255): 202
Card Number (0-65535): 1091
Fixed Field:
Wiegand Data: 0000000005940887
Wiegand (Encrypted): 903D777E9DC99708
PIN Code: None

CSN for HS Key:
HS Reader Key:
Old Div Key:
New Div Key:

COM4

□ Kd Default (Key1)
□ Kc Default (Key2)
☑ HID Master (Key3)
□ High Security (Key4)
□ Custom 1 (Key5)
□ Custom 2 (Key6)

□ Decode 37-bit as H10302
□ Enable Card Writes
□ Enable Reader Key Updates
☑ Enable Encryption
☑ Authenticate with App1
□ Authenticate with App2

Figure 2. iClass Cloner Main Window Layout

Serial Interface Setup

[**IMPORTANT**: If the iClass cloner unit is using an iClass RK keypad reader (instead of an RW300) then the unit has a USB virtual COM port interface already attached to the reader. The serial driver for this interface must be installed prior to attaching the unit to a USB port. The latest "Windows Driver Installer Setup Program" **for the** PL2303TA device can be downloaded from the following location:
http://prolificusa.com/pl-2303hx-drivers/].

The RS-232 serial interface must be setup before the application can communicate with the iclass reader. To setup the serial port a valid COM port must be selected and the "Connect" button pressed to open serial port communications. An open serial port will be signified by a green bar below the connect button. If the serial port is disconnected, the bar will be red. The "Test" button can be pressed to verify communication with the reader. A series of three beeps will be emitted by the reader when the test button is pressed if a proper communication channel has been established.

Reader Key Initialization

[*Note: This step is not required for readers obtained from proxclone.com since the HID Master Authentication key has already been pre-installed.*]
In order to authenticate with a HID iClass credential, a valid authentication key must first be installed into the user key space of the reader. Off-the-shelf readers have the default debit and credit keys pre-installed in user key locations 1 and 2 to support communication with non-configured (blank) credentials. The HID "master" authentication key must be installed in user key location 3 in order to authenticate with standard security credentials that have been configured by HID. The iClass cloner application can install this key into the reader by checking the box labeled "Enable Reader Key Updates" and then pressing the "Ld Mstr Key" button. This operation only has to be done once for each "Factory Default" reader since the key will be saved to the readers EEPROM memory.

Standard Security vs. High Security

The Proxclone iClass cloner unit utilizes a commercial iCLASS reader that has been configured to operate in standard security mode. High Security/Elite credentials cannot be read by the reader's built-in HID application program unless the reader has been placed in high security mode using a special "HS Key" configuration card. That being said, the iclass cloner software is capable of reading either standard security or high security cards via the readers RS-232 serial interface. In other words, card information from a high security card will not be read by the reader and displayed on the LCD but it can still be read by the iclass cloner application and displayed on the screen.

If a user is uncertain whether a particular iClass system is operating in "Standard" mode or "High Security" mode a simple test can be performed as follows: If a known "Standard" security card is presented to an iclass reader and the reader reacts (e.g. beeps and blinks the LED) it can be assumed that the reader is operating in "Standard security mode. If the reader shows no reaction at all, it can be assumed that the reader is operating in a "High Security" mode.

Reading a Standard Security Credential

Once the serial port has been configured and the HID Master key installed, a standard security iclass credential can now be read. The procedure is as follows:

1. Place a standard security credential near the reader.
2. Ensure that the HID Master (Key3) authentication key checkbox has been selected.
3. Ensure that the Authenticate with App1 checkbox has been selected.
4. Press the “Select” button which will begin communication with the credential. The credentials CSN (Card Serial Number) and Diversified key will be shown in the appropriate boxes.
5. Press the “Read” button to authenticate with the card and read the data blocks associated with the HID access application. The retrieved information will be displayed in the appropriate boxes for each data block read. The access ID code will also be decrypted and decoded. The credentials decoded format, facility code, card number and PIN code (if applicable) will be displayed in the center section of the window.

Duplicating/Cloning a Standard Security Credential

Cloning an iClass card requires, at a minimum, that the access data residing in Blocks 6,7,8 and 9 be copied to the new card. This will transfer the card format, facility code, card number, and PIN code (if used) to the new card. The procedure for duplicating a card is as follows: *[Note: an alternate (simpler) method to copy a card using a feature located in the “Utility” menu is also available and is discussed in a later part of this document.]*

1. Ensure that the HID Master (Key3) authentication key checkbox is selected.
2. The card being duplicated should first be read using the procedure outlined in the section above.
3. Remove the original card from the vicinity of the reader and place the card to be used as a clone next to the reader. Press the “Select” button to begin communication with the new card. The credentials CSN (Card Serial Number) and Diversified key will be shown in the appropriate boxes. DO NOT press the “Read” button.
4. Enable card writes by checking the “Enable Card Writes” checkbox.
5. Press the “Wrt Blk6” button to copy the card configuration and encryption information to the credential.
6. Press the “Wrt Blk7” button to write part 1 of the HID access control data to the credential.
7. Press the “Wrt Blk8” button to write part 2 of the HID access control data to the credential.
8. Press the “Wrt Blk9” button to write part 3 of the HID access control data and the embedded PIN to the credential.
9. Disable card writes by un-checking the “Enable Card Writes” checkbox.
10. Remove the card from the vicinity of the reader.

Modifying a Standard Security Credential

Once a standard security credential has been read using the procedure outlined earlier, the access code data can be modified using the following procedure.
[*Note: After reading the card , make sure that it is not removed from the vicinity of the reader until the entire procedure below has been completed*.]

1. If desired, modify the format of the credential by selecting a different format using the “radio” style buttons located on the top center of the main window.
2. If the facility code or card code of the credential is to be modified then the user simply types a new value in the appropriate box.
3. If the 36-bit “Keyscan mode is selected, a value (0-1024) must also be entered into the “Fixed Field” box. A value of 0900 is the most common entry. This field is unused for all other card formats.
4. Press the “Calc Wieg” button to generate a new wiegand code for the modified format or card code information. The wiegand value will also be encrypted using the HID standard TDES encryption/decryption keys.
5. Press the “Update 7” button to copy the new encrypted value over to the box that shows the Block 7 data value.
   [Note: If the “Decrypt Blk 7” checkbox is unchecked, the unencrypted wiegand code will be copied over instead of the encrypted value.]
6. If a new (or modified) PIN code is desired, enter the new PIN code (15 digits max.) and then press the “Update 6/9” button to copy the new PIN information over to Block 6 and Block 9.
7. Enable card writes by checking the “Enable Card Writes” checkbox.
8. Ensure that the HID Master (Key3) authentication key checkbox is selected.
9. Press the “Wrt Blk7” button to write the modified card data back to the credential.
10. If a PIN update has been made then press the “Wrt Blk 6” button followed by the “Wrt Blk 9” button to update the credential with the new PIN code information.

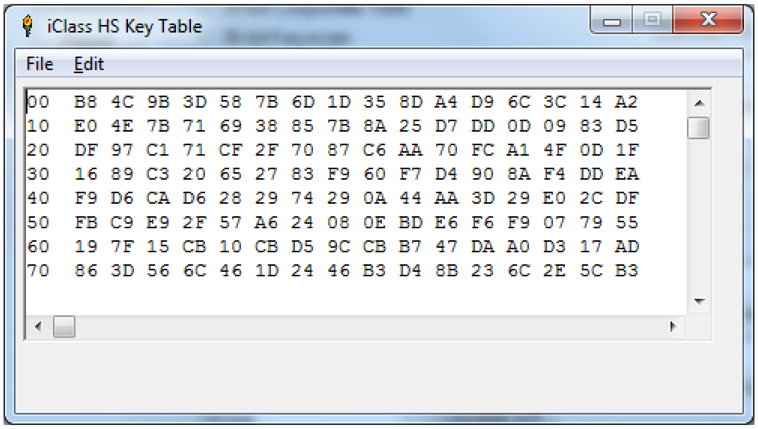
Reading a High Security Credential

Reading a High Security credential uses basically the same procedure as reading a standard security credential. The only difference is that a different authentication key is used (User Key 4). The applicable high security table must first be loaded and the card-specific high security authentication key must be calculated (using the procedures below) before a high security credential can be read or modified.

Loading the High Security Key Table

In order for the iClass cloner application to authenticate with a high security credential, the proper high security key must first be loaded into the User Key4 keyspace. (This MUST be done for “each” High Security card read!). Since each HS credential requires a unique key, the calculation of the HS key uses a 128-byte key table which must first be loaded into the iclass cloner application. The key table can be loaded using the “File Load” option in the HS_Key menu.

By selecting “HS_Keys” from the top menu bar and then the “HSKey Table” selection, a second window will be generated. An example of this new window is shown in Figure 3 below. This HS keys window then allows any previously stored HS Key file to be loaded by selecting the “File” / “Load” menu option. The selected 128-byte key table will be loaded and displayed in the window. The key table is automatically loaded into a variable array and will now allow HS keys to be created for any credential using its CSN. Once the window is displayed, the key table data is automatically loaded and the window may then be closed (if desired).



```
00   B8 4C 9B 3D 58 7B 6D 1D 35 8D A4 D9 6C 3C 14 A2
10   E0 4E 7B 71 69 38 85 7B 8A 25 D7 DD 0D 09 83 D5
20   DF 97 C1 71 CF 2F 70 87 C6 AA 70 FC A1 4F 0D 1F
30   16 89 C3 20 65 27 83 F9 60 F7 D4 90 8A F4 DD EA
40   F9 D6 CA D6 28 29 74 29 0A 44 AA 3D 29 E0 2C DF
50   FB C9 E9 2F 57 A6 24 08 0E BD E6 F6 F9 07 79 55
60   19 7F 15 CB 10 CB D5 9C CB B7 47 DA A0 D3 17 AD
70   86 3D 56 6C 46 1D 24 46 B3 D4 8B 23 6C 2E 5C B3
```

Figure 3. 128-Byte HS Key Table Window

Calculating & Loading HS Keys

Once the HS key table has been loaded, high security credentials that were created using the same HS key table may now be read or modified using the following procedure:

1. Place a HS credential near the reader. On the main window press the “Read CSN” button on the right side of the window. The CSN of the credential will now be displayed in the upper right corner of the display.
2. Press the “Calc HS Key” button to calculate a key (using the key table) that is unique for that credential. The new HS key value will be shown in the box below the CSN value. [*This is the key value that the reader must use to authenticate with that one card.*]
3. Ensure that the “Enable Reader Key Updates” checkbox is checked.
4. Press the “Ld HS Key” button to load the calculated key into the User Key 4 location of the reader.

The reader is now able to read the HS credential by following the “Read Standard Security Credential” procedure described earlier but with the “HS Key4” authentication key checkbox selected instead.

Modifying the Diversified Key of a Credential

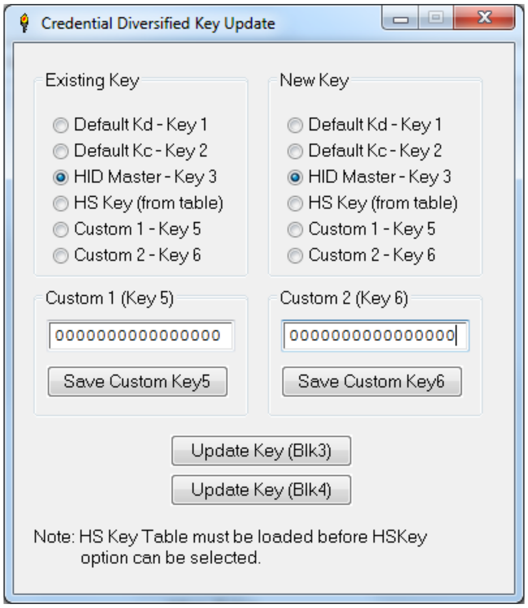
Each iclass credential stores a unique 64-bit authentication key that has been “Diversified” from the 64-bit authentication key that is stored in the reader. This key may occasionally need to be modified for various reasons including:

- An uninitialized credential using the factory default authentication key may need to be updated to work with standard security iClass readers that use the HID Master Key.
- A standard security credential may need to be upgraded to work in a high security/Elite iClass system.
- A standard security credential may need to be updated to operate in an iClass system that uses a “Custom” standard security authentication key that replaces the recently compromised “HID Master” authentication key.

Modifying the credential's Diversified Key is done within a separate window in the iClass Cloner Application. **To modify the diversified key of an iClass credential the following procedure should be used:**

Note: See next page for important information related to the procedure below.

1. Select the <Card Key Update> option from the <Keys> menu. This will bring up a separate window as shown below:



Existing Key
○ Default Kd - Key 1
○ Default Kc - Key 2
● HID Master - Key 3
○ HS Key (from table)
○ Custom 1 - Key 5
○ Custom 2 - Key 6

New Key
○ Default Kd - Key 1
○ Default Kc - Key 2
● HID Master - Key 3
○ HS Key (from table)
○ Custom 1 - Key 5
○ Custom 2 - Key 6

Custom 1 (Key 5): 0000000000000000

Custom 2 (Key 6): 0000000000000000

Note: HS Key Table must be loaded before HSKey option can be selected.

2. Select a key option from the "Existing Key" list. This selection should identify which key is currently being used in the credential being modified.
3. Select a key option from the "New Key" list. This selection should reflect which key will be used to create the "new" diversified key of the credential being modified.
4. Place the card near the reader. Press the "Update Key Blk 3" button to write the new key to the credential. The reader will beep when the key update operation is complete.
   If the diversified key for Application area 2 is being updated then the "Update Key Blk 4" button should be pressed instead. An update to the App2 diversified key should only be attempted by experienced users who have already loaded the necessary App2 authentication key.

   [Note: After the key update is complete, the values of the old/existing key and the new key will be displayed in the "Old Div Key" and "New Div Key" text boxes in the main application window.]

Other Important Notes:

[Note 1] If the credential being modified currently uses (or will be modified to use) a high security key, then the High Security Key table must be loaded before the HS Key menu option can be selected. The unique diversified key for each credential will automatically be calculated by the software using the pre-loaded HS Key table.

[Note 2] If a Custom authentication key is desired, then that key (Key 5 or Key 6) must first be loaded into the reader EEPROM using the “Save Custom Key” function. Once loaded, this key will remain in reader EEPROM until it is either modified by the user or deleted through the use of a “RESET” configuration card.

Utility/Debug Options

Software revisions 7 and higher include some additional utility/debug capabilities. Invoking the “Utility – Misc” menu option will open a special utility/debug window. Use of these functions requires a special (non-factory) version of RW300 firmware that has been pre-loaded by Proxclone.com. A description of these special functions is included below.

Read EEPROM

Pressing the “Read EE” will cause the current contents of the RW300 EEPROM to be displayed. This can be used to verify that certain key values have been correctly stored by the reader. A breakdown of the EEPROM addresses and their use is included below:

0x00-0x07	Reader Product ID and Version Information
0x08-0x0F	HID Exchange Key (Required to load new keys)
0x10-0x17	User Key 1 - Default HID Key (Kdebit)
0x18-0x1F	User Key 2 - Default HID Key (Kcredit)
0x20-0x27	User Key 3 – Master Authentication Key
0x28-0x2F	User Key 4
0x30-0x37	User Key 5
0x38-0x3F	User Key 6
0x40-0x47	User Key 7
0x48-0x67	Unused ?
0x68-0x6F	HS Key 1
0x70-0x77	HS Key 2
0x78-0x7F	HID Encryption Key 1
0x80-0x87	HID Encryption Key 2
0x88-0x8F	HID Master Auth Key
0x90-0x97	HS Key Config Parameters
0x98-0x9F	Unused ?
0xA0-0xBF	Reader Config Parameters (e.g. LED , wiegand output)
0xB0-0xDF	Unknown ???
0xE0-0xFF	Unused ?

Dump RAM

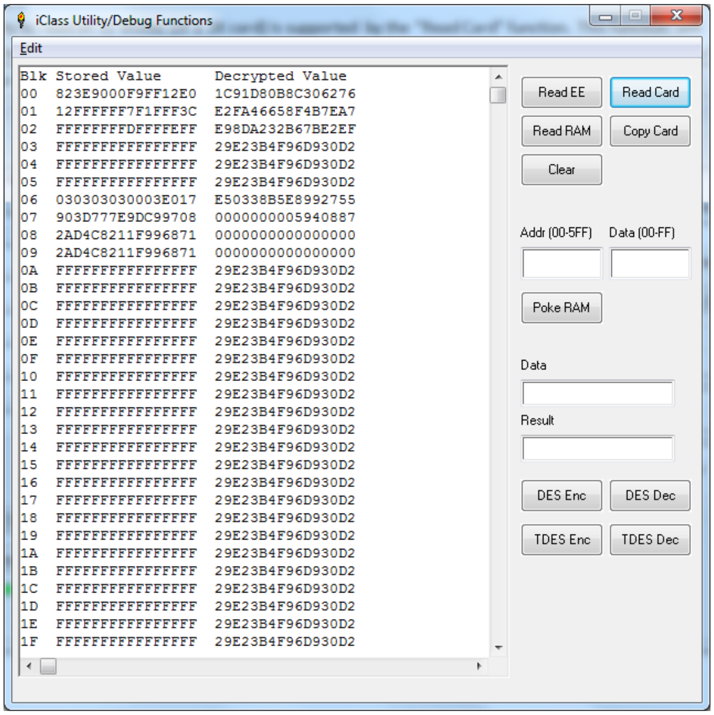
Pressing the “Read RAM will cause the current contents of the RW300 File RAM to be displayed. The 1536 byte (0x000-0x5FF) RAM is used to store all of the global and static variables used within the HID access application. A list and description of the known variable storage locations has not yet been assembled and is therefore not included herein.

Poke RAM

The user has the option to poke any address of RAM using any 8-bit (byte) value. Poking RAM allows unique “debug” test scenarios and specialized experiments to be explored. To utilize this feature, a valid address and data value should be entered into the appropriate boxes followed by pressing the “Poke RAM” button. The “Dump RAM” feature can then be used to verify that the new value has been placed into RAM. *[Note: Certain locations of RAM cannot be visibly modified using this procedure due to the nature of their use. e.g. RS-232 serial parameter storage being used for the iClass Serial Protocol communication]*

Read Card

The ability to read all 32 blocks (of a 2K card) is supported by the “Read Card” function. This function will attempt to display (and decrypt if enabled) all data blocks read from a card assuming the correct authentication key has been selected beforehand. It should be noted however that not all blocks may be readable since cards configured by HID usually have the applications limit field (in Block 1) set to 0x12. A value of 0x12 means that only the first eighteen blocks are part of Application area 1 and are therefore the only blocks that can be read using the currently selected authentication key. All unreadable blocks will return a value of all 1’s (0xFFFFFFFFFFFFFFFF) as the stored value. A typical example of the “Read Card” output is shown in Figure 4 below.



```
Blk Stored Value       Decrypted Value
00  823E9000F9FF12E0  1C91D80B8C306276
01  12FFFFFF7F1FFF3C  E2FA46658F4B7EA7
02  FFFFFFFFDFFFFEFF  E98DA232B67BE2EF
03  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
04  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
05  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
06  030303030003E017  E50338B5E8992755
07  903D777E9DC99708  0000000005940887
08  2AD4C8211F996871  0000000000000000
09  2AD4C8211F996871  0000000000000000
0A  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
0B  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
0C  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
0D  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
0E  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
0F  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
10  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
11  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
12  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
13  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
14  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
15  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
16  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
17  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
18  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
19  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
1A  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
1B  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
1C  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
1D  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
1E  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
1F  FFFFFFFFFFFFFFFF  29E23B4F96D930D2
```

Figure 4. “Read Card” Sample Output

Copy Card

The data obtained from reading a card can also be used to write a card, in effect copying the originally read card. When the “Copy Card” button is pressed the data (Blocks 06-1F) being displayed in the window (from the previous card read) is written to a second card provided the card has been properly “Selected” using the correct authentication key before the "Copy" button is pressed. The user also has the option of editing the displayed data before it is written to the card if desired.

[Note: Changes to the data block values should only be made to the stored value data and not to the decrypted data since the decrypted data is not used as part of the card write sequence.]

The copy function takes approximately five seconds to complete and the reader will beep upon completion of the card write. **DO NOT remove the card from the vicinity of the reader until the copy function has been completed**.

Encrypt/Decrypt

The Utility menu provides the ability to encrypt or decrypt any user entered 64-bit data value using either DES or TDES encryption/decryption. The data value entered into the "Data" field textbox will be used in conjunction with the HID Master Encryption Key1 and Key2 values to perform either an encrypt or decrypt function depending on which button has been pressed. The calculated encrypted or decrypted data will be displayed in the "Result" textbox. Data values can be copied/pasted from other data fields within the iClass Cloner application by right clicking the mouse and selecting the appropriate copy/paste option.

Any problems or questions related to the operation of the iClass Cloner software or this set of instructions should be sent to info@proxclone.com .