Overview

The portable iClass cloner/programmer circuit is comprised of a commercial HID RW100 iClass Reader/Writer unit operating in conjunction with a customized embedded microcontroller/display unit. The design provides the ability to read, duplicate (clone), and program standard iClass credentials (cards and fobs).

Some of the main features of the unit are as shown below.

- Supports two “switch-selectable” modes of operation (Read/Clone and Program).
- Reads and Copies all data blocks used with the HID Access Control Application
- Displays card content information including format, facility code, card number & PIN.
- Program mode supports programming credentials with a user specified format, facility code, card number and PIN.
- Operates with all “standard security” Legacy iClass credentials
- PIC32 Microcontroller used to manage reader communication and OLED display interface.
- Pre-loaded HID Master Authentication and Encryption Keys
- Fully Portable (Standalone) Handheld Operation

- Simple two-button Operation ("Arm" and "Write") used in Read/Clone mode.
- Fast user data entry in Programmer mode using numerical keypad interface.
- Supports single button card number increment feature.
- Three multi-color Status LED's
- Powered by a 4 standard AA batteries.

The iclass cloner/programmer unit uses a PIC32 microcontroller to interact with the RW100 reader/writer over an RS232 interface using the HID iClass Serial Protocol.
The device is capable of operating in two different modes depending on the setting of the "Mode Select" switch at the time power is applied. Due to limited processing resources, the unit does NOT allow both modes to operate at the same time.

Read/Clone Mode

The Read/Clone mode provides the ability to read a credential and have its stored data automatically decoded and displayed. If the user desires to make a copy of the credential read then a new card can be presented and the previously captured data can be copied over to the second card using a simple one button operation.
When operating in Read/Clone mode, the microcontroller commands the RW100 to continuously poll for the presence of an iClass credential. When an iClass credential is encountered, the microcontroller will command the RW100 to read all data blocks and store all information obtained. The relevant card information will then be decoded, decrypted and displayed on the small OLED display.
After the credential data has been obtained, the user then has the option to write the captured data to another iclass credential, in effect cloning the original card.

Program Mode

The Program mode allows the user to enter a set of data that will be used to program a custom credential. The user has the option to select one of four widely used HID credential formats (26-bit, 34-bit, 35-bit Corp 1000, or 37-bit. After selecting a format the user can then enter a custom facility code, card number and optional PIN using the keypad interface. After the data has been entered the microcontroller will perform a validity check of the data before allowing the credential to be programmed. If the data is valid then the user can initiate a write operation to a credential using a simple one button operation. If the data entered is invalid or out-of-range for the format chosen then the operator will be notified and corrections can be easily made before writing the credential.
To support sequential card programming, the card number can be easily incremented by one without having to manually enter new data each time.

User Interface

The iCLASS cloner/programmer unit utilizes a set of sixteen pushbutton switches, one mode select slide switch and three status LED's to interact with the user. A separate small blue pushbutton switch is used to power the unit on and off. A description of each of the switch and status LED functions is included below. The layout of the printed circuit board showing all switch locations is shown in Figure 1 below.

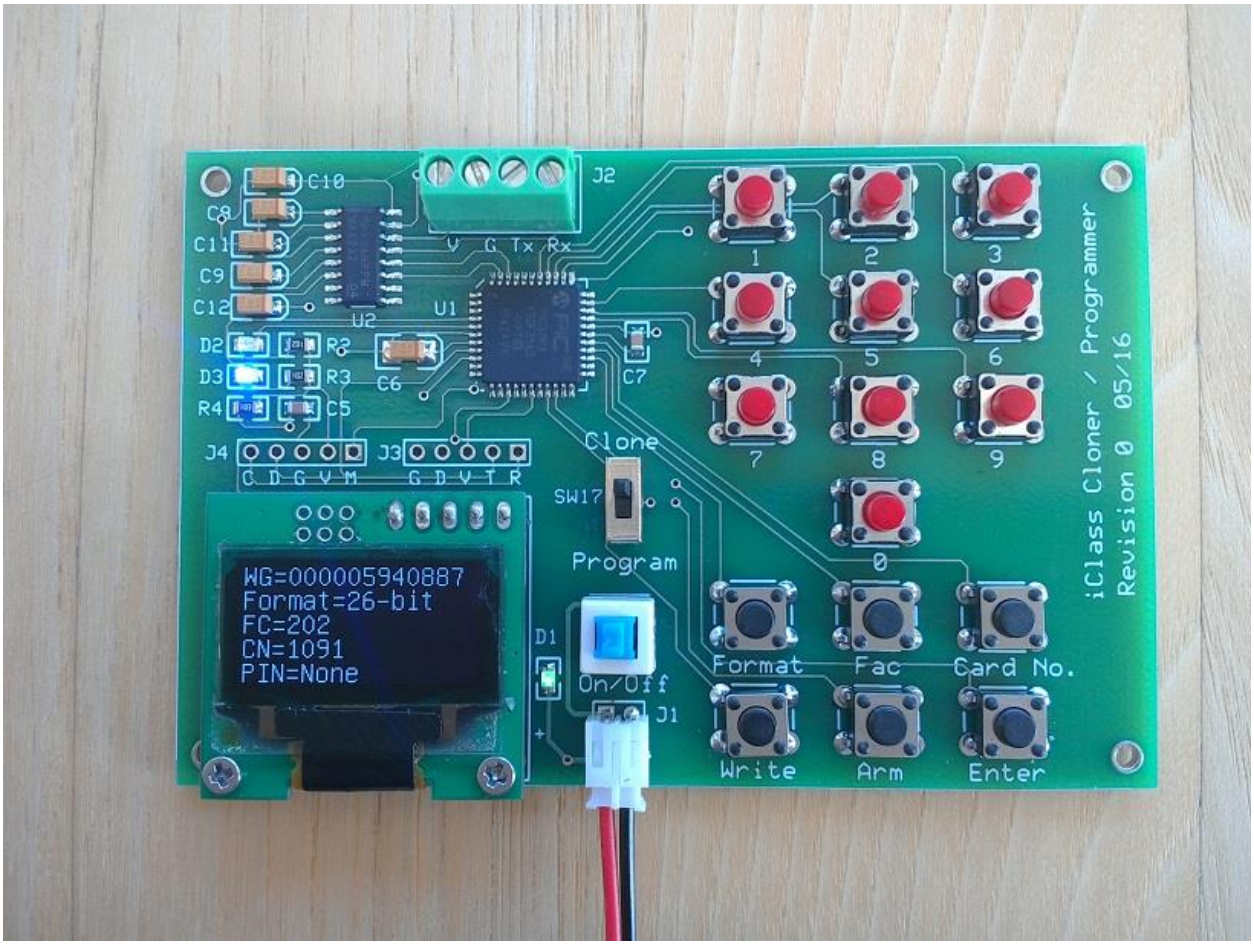

Figure 1. iClass Cloner/Programmer Circuit Board and OLED Display

Switch Functions

[On/Off]

Power to the iCLASS Cloner unit is handled by the small blue pushbutton switch located near the right side of the OLED display. Push the switch once to turn the unit on, push it again to turn the unit off.

[Mode]

The "Mode" switch is located directly above the power On/Off switch. Depending on the state of this switch when the unit is powered on, the unit will either enter "Read/Clone" mode or "Program" mode. Put it in the up position to select "Clone" mode and the down position to select "Program" mode.

[Numeric Data Entry 0-9]

The ten red pushbuttons are used to enter numeric data when operating in "Program" mode. These push buttons are used when entering the facility code, card number and PIN data fields. These switches are NOT used in the "Read/Clone" mode.

[Format]

When operating in Program Mode, the "Format" button is used to select one of four supported

credential formats. Each time the button is pressed the selected format will cycle between 26-bit, 34-bit, 35-bit and 37-bit. This switch is NOT used in the "Read/Clone" mode.

[Facility]
When operating in Program Mode, the "Facility" button is used to inform the microcontroller that subsequent data entry should be directed to the Facility Code field. Any numeric data entered after pressing this button will be used to specify a Facility Code that will be used when programming the credential. This switch is NOT used in the "Read/Clone" mode.

[Card No.]
When operating in Program Mode, the "Card No." button is used to inform the microcontroller that subsequent data entry should be directed to the Card Number field. Any numeric data entered after pressing this button will be used to specify a Card Number that will be used when programming the credential. This switch is NOT used in the "Read/Clone" mode.

[Enter]
When operating in "Program" mode, pressing this button will cause the microcontroller to perform a validity check on the credential data that has already been entered. This button should only be pressed after all desired credential data (Format, Fac Code, Card No., and PIN) has been entered. No write to a credential will occur unless a validity check has been performed and the blue LED has been lit. This switch is NOT used in the "Read/Clone" mode.
After the data has been checked and verified, subsequent presses of the "Enter" key will cause the card number to increment by one. This feature allows sequential card numbers to be programmed in rapid succession without having to enter a new card number between back-to-back "Write" operations.

[Arm/PIN]
The "Arm/PIN" pushbutton has two different functions depending on the current operating mode.

In "Read/Clone" mode the button is used to instruct the iclass reader to Re-Arm and begin polling again for another iclass credential. Pushing this button will erase all previously captured credential data which will then be replaced with new credential data when it becomes available.

When operating in "Program" mode, this button is used to inform the microcontroller that subsequent data should be directed to the PIN code field. Any numeric data entered after pressing this button will be used to specify an optional PIN Code that will be used when programming the credential.

[Write]
The "Write" pushbutton is used when operating in either "Read/Clone" mode or "Program" mode. Pressing this button will initiate a write operation to a credential that has been placed near the RW100 reader/writer unit. Data can only be written if the "Blue" LED is on.
In "Read/Clone" mode, this operation will write data that was captured from a previous credential read.
In "Program" mode, this operation will write all user specified data that has been entered from the keypad. The card data written is always what is currently being shown on the display.

Status LED's

[Green LED]

The green LED is located next to the On/Off switch on the printed circuit board. This LED is on whenever power has been applied to the unit.

[Blue LED]

The blue LED (labeled "D3") is located above the OLED display on the cloner circuit board. This LED is activated whenever valid data is available to be written to a credential.
In "Read/Clone" mode, this LED will be lit whenever a successful read of a credential has been completed.
In "Program" mode this LED will be lit once all user data has been entered and a data validity check has been performed.
[Note: Attempting to write data to a card/fob when the blue LED is off could potentially result in unknown/invalid data being written to the credential.]

[Red LED]

The red LED (labeled "D2") is located above the OLED display on the printed circuit board. This LED is activated whenever an error condition is encountered. Some of the more common reasons this LED may be activated is due to the following:

- The credential is NOT within range of the RW100 Reader/Writer.
- The card/fob being read or written is NOT a valid iClass credential.
- The card/fob is a "High Security" credential.
- The card/fob is an iClass SE credential.
- The card or fob was removed before the "Read" or "Write" operation was complete.
- The user specified data has NOT been verified (e.g. blue LED not lit).

"Read/Clone" Mode Operation

To Read a Credential:

1. Position the "Mode" switch in the up position to select "Read/Clone" mode.
2. Apply power to the unit. The green LED will be on.
   The RW100 will take approximately 4 seconds to power up. The RW100 LED bar will flash red when the reader/writer has completed its power-up initialization. The RW100 LED bar is then turned off and the OLED display will now show the message "Awaiting Data …"
   The unit is now armed and polling for a valid iClass credential.
3. Place a credential near the RW100 Reader/Writer (within 2-3 inches).
   The reader will automatically read the credential data and display the results on the OLED display. The blue LED will be activated indicating that valid data has been captured. The unit will disable further credential polling until the "Arm" pushbutton is activated or power has been cycled.

NOTE: Reading all data blocks of the credential takes approximately 1.5 second. The credential being read must remain within the vicinity of the reader for the full time or else a read error will occur and the red LED will flash. This is a longer time than a normal read by the HID Access Control Application since "ALL" data blocks must be read by the cloner application, not just blocks 6-9.

To Write a Credential:

1. Ensure that the Blue LED is ON. If not, follow the read procedure above.
2. Place the credential to be written near the RW100 Reader/Writer (approx 1" above reader).
3. Press and release the red "Write" pushbutton.
4. Wait for the RW100 LED bar to flash green (~ 2 seconds).
5. If another credential is to be written with the same data then repeat steps 2,3,and 4 above.
6. If the red LED is activated, correct the problem and repeat steps 1-4 above.
7. Remove the credential from the vicinity of the RW100.

"Program" Mode Operation

To Program a credential with user specified data:

1. Position the "Mode" switch in the down position to select "Program" mode.
2. Apply power to the unit. The green LED will be on.
   The RW100 will take approximately 4 seconds to power up. The RW100 LED bar will flash red when the reader/writer has completed its power-up initialization. The RW100 LED bar is then turned off and the OLED display will now show the following:

```
Program Mode
Fmt:
FC : 0
CN : 0
PIN: None
```

3. Press the "Format" button one or more times to roll through the available format options.
4. Press the "Fac" button followed by the desired Facility Code value.
5. Press the "Card No" button followed by the desired Card Number value.
6. If desired, press the "Arm/PIN" button followed by the desired PIN value. PIN codes are optional and are restricted to ten digits or less (e.g. 1-9999999999).
7. Press the "Enter" button to perform a validity check of the data that was entered above. If the data entered is valid then the Blue LED will be lit. If an error is detected, the Red LED will be momentarily lit, indicating to the user that a portion of the data needs to be re-entered .
8. Place a credential approximately 1-2 inches above the reader and press the "Write" button.

9. If another “sequential” card is to be written, press the “Enter” button to increment the card number . The OLED display will reflect the new card number. Place a credential approximately 1-2 inches above the reader and press the “Write” button.
10. Repeat step 9 for each sequential card that is to be programmed.

Program Example:

To program a credential with the following parameters, the keypad sequence should be as shown below.

Sample Card Parameters:

```
Format: 35-bit Corporate 1000
Facility Code:  150
Card Number:  300525
PIN Code:  321
```

The key sequence for the above parameters would be:
[Fmt] [Fmt] [Fmt] [Fac] [1] [5] [0] [CN] [3] [0] [0] [5] [2] [5] [Arm/PIN] [3] [2] [1] [Enter] [Write]

If data is accidently entered incorrectly simply press the appropriate field selection key again followed by the correct numerical data (e.g. [Fac] [1] [5] [2] ...)

Other Important Information

[Keypad Markings]
The Revision 0 printed circuit board has one pushbutton incorrectly marked. The pushbutton labeled “Arm” should be marked as “Arm/PIN . The switch performs different functions depending on the operating mode selected.

[Valid Data Ranges]
The following data ranges are applicable to the specified credential formats. Any value entered outside of this range will cause the “Red” LED to flash when the “Enter” key is pressed.

Format	Facility Code Range	Card Number Range	PIN Code Range
26-bit H10301	0-255	0-65535	1-9999999999
34-bit N1002	0-65535	0-65535	1-9999999999
35-bit Corp 1000	0-4095	0-1048575	1-9999999999
37-bit H10304	0-65535	0-524287	1-9999999999

[Battery Life]
The iClass Cloner unit is powered by 4 “AA” batteries. The unit draws approximately 100 ma of current from the batteries which should allow for approximately 10 hours of use from a standard set of alkaline batteries. To preserve battery life the unit should be switched off when not being used.

If there are any questions regarding these instructions please contact Carl at info@proxclone.com