Overview

The iClass spoofer circuit was designed to electronically emulate iClass RFID smart card credentials. Some of the main features of the unit are as shown below.

- Fully Portable (Standalone) Handheld Operation
- User Programmable to Support Multiple Card Identities.
- 16x2 Backlit LCD Display.
- Supports Common 26-bit H10301 Card Format.
- Multiple Operating Modes (Static ID, Auto-Increment FAC Code, Auto-Increment Card Number).
- Allows Manual Entry of up to 16,777,216 different credential identities.
- EEPROM Memory Allows Store/Recall of up to 16 Pre-stored Identities.
- Operates with both “Legacy iCLASS” and the latest “iCLASS SE” Readers.
- Powered by three “AA” Batteries.

The iCLASS Spoofer communicates with iCLASS readers using the ISO15693 protocol. The design utilizes a fixed CSN and Diversified Key value while emulating more than 16 million possible card identities. An 8-bit microcontroller/CPLD combination is responsible for handling the low level communication sequences and the generation of all required cryptographic signatures.

The design is compatible with all Legacy iCLASS readers as well as the new iCLASS SE readers that support the Legacy iCLASS Interpreter option (Denoted by a “T” in the fifth digit of the reader Part Number – e.g. 920NTNNEK0000). In addition, the spoofer is currently limited to only emulating

Standard Security credentials. The ability to spoof “High Security/Elite” credentials is supported by the hardware design but would require a minor firmware modification to change the spoofers fixed Diversified Key value.

User Interface

The iCLASS spoofer utilizes a set of five pushbutton switches to interact with the user. A separate push-on/push-off switch is also provided in order to power the unit on and off. A backlit LCD display provides a visual indication of the current operating mode and selected credential parameters. The layout of the various switches and display can be seen in Figure 1.
A description of each of the switch functions is included below.

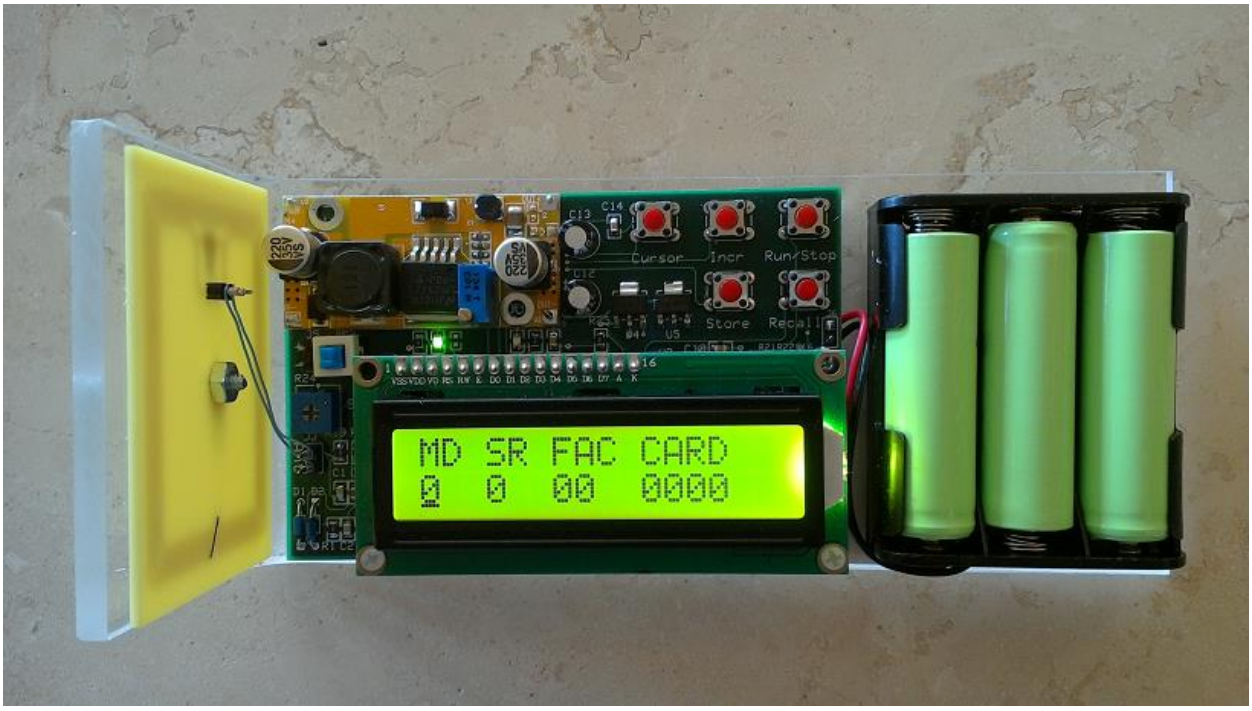


Figure 1. Spoofer User Interface Layout

Switch Functions

[On/Off]

Power to the iCLASS Spoofer is handled by the small square blue/white pushbutton switch located near the top left corner of the LCD display. Push once to turn the unit on, push again to turn the unit off.

[Cursor]

The <cursor> button is top leftmost small red pushbutton in the layout shown above. Each press of this button moves the LCD Display cursor one position to the right. The cursor is used to select a particular digit of the display to be modified. The cursor is only visible while operating in Setup mode (MD=0)

[Incr]

The <Increment> button is the top middle red pushbutton in the layout shown above. Each press of this button will increment (by one) the digit where the cursor is currently located.

[Run/Stop]

The <Run/Stop> button is the top rightmost red pushbutton in the layout shown above. Depending on the current mode selected, a press of this button will either transition the unit from "Setup" mode to "Run" mode or from "Run" mode back to "Setup" mode. The unit MUST be operating in Run mode before any "spoofer" interaction with the reader will occur.

[Important: In order to transition from "Setup" mode to "Run" mode the "MD" field must first be set to either 1,2,or 3 (as defined below). The spoofer will not be allowed to transition to Run mode if the Mode field is "0".]

[Store]

The <Store> button is the small red pushbutton that is located directly beneath the <Increment> button. Pressing this button will initiate a memory operation that will store the currently displayed credential data to one of sixteen possible memory locations as determined by the Store/Recall (S/R) address value.

[Recall]

The <Recall> button is the small red pushbutton that is located directly beneath the <Run/Stop> button. Pressing this button will initiate a memory operation that will recall saved credential data from one of sixteen possible memory locations as determined by the Store/Recall (S/R) address value.

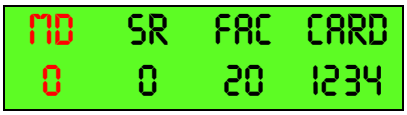
[Note: Holding down the <Recall> button while turning power on will force the credential storage memory area to be cleared and the first five locations to be loaded with pre-defined default data values.]

The spoofer contains sixteen pre-loaded card identities which can be modified by the user as desired. The default data values can be restored at any time by following the procedure in the previous paragraph. The default stored credential identities are as shown below.

Pre-Stored Card Identities				
SR Address	Fac Code (Decimal)	Card No. (Decimal	Fac Code (Hex)	Card No. (Hex)
0	255	1234	FF	04D2
1	01	1000	01	03E8
2	02	2000	02	07D0
3	03	3000	03	0BB8
4	04	4000	04	0FA0
5 - F	00	0000	00	0000

LCD Display Fields

Operating Mode (MD)



The iCLASS Spoofer supports four different operating modes (0-3) which are defined as follows.

Mode 0 – Setup Mode

This mode is the default power-up mode. The unit must be in Setup mode in order to modify any of the LCD display fields or credential data. Setup mode 0 is manifested by the presence of the display cursor. The cursor will NOT be visible while operating in any other mode.

Mode 1 – Fixed Credential Mode

Placing the unit in Mode 1 will cause the credential data that currently displayed to be sent to the iCLASS reader whenever the credential data is requested. The card identity being sent will be "fixed" and will not change regardless of how many times the data is requested by the reader.

Mode 2 – Incrementing Facility Code

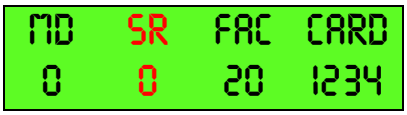
Selecting Mode 2 will cause the spoofer to respond with a Facility Code value that is one greater than the last Facility Code sent. This auto-incrementing feature allows the spoofer to walk through a series of facility codes in an attempt to discover which Facility Code value(s) will be accepted by the reader.

Mode 3 – Incrementing Card Number

Selecting Mode 3 will cause the spoofer to increment the card number value each time the credential data is read by the reader. This auto-incrementing feature allows the spoofer to walk through a series of card numbers in an attempt to discover which card number (or range of card numbers) will be accepted by the reader.

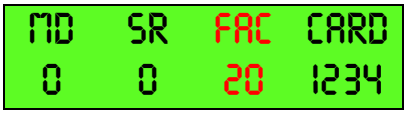
[Note: The card number value displayed on the LCD always reflects the "next" value that will be sent to the reader , not the last value that the reader received.]

Store / Recall (SR)



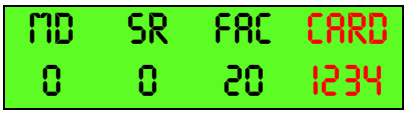
The iCLASS Spoofer supports the ability to store and recall up to sixteen different card identities. The value of the SR field determines which one of sixteen memory locations will be addressed when performing either a <Store> or a <Recall> function. The SR field uses hexadecimal notation for the 16 different memory pointer values (0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F).

Facility Code (FAC)



The 2-digit Facility Code field allows the user to define a hexadecimal Facility code value in the range of 0x00-0xFF (0-255 decimal) that will be sent to the reader when the credential data is requested.
[Note: The Facility code value displayed on the LCD always reflects the "next" value that will be sent to the reader , not the last value that the reader received.]

Card Number (CARD)



The 4-digit card number field allows the user to define a hexadecimal card number value in the range of 0x0000-0xFFFF (0-65535 decimal) that will be sent to the reader when the credential data is requested.
[Note: The Card Number value displayed on the LCD always reflects the "next" value that will be sent to the reader , not the last value that the reader received.]

Spoofer Operation

To Emulate(Spoof) a Card

1. Power the Spoofer unit on by pressing the blue Power-On/Power-Off pushbutton.

2. The cursor is initially positioned beneath the "MD" field. Press the <Incr> button to select the desired mode of operation (1,2 or 3 as defined in the Operating Mode section above).

3. If the user desires to load a stored card identity then …
   a. Move the cursor to the SR field.
   b. Press <Incr> until the desired pre-stored card identity location is shown.
   c. Press <Recall> to load the selected card identity.
   d. Press <Run/Stop> to exit setup mode and enter Run mode.
   e. Place the spoofer antenna approximately 1" from the reader to begin card emulation.

4. Alternatively, if the user desires to enter a new credential identity then …
   a. Move the cursor to either of the two Facility Code fields.
   b. Press <Incr> to increment the selected field until the desired value is obtained.
   c. Move the cursor to either one of the four Card Number fields.
   d. Press <Incr> to increment the selected field until the desired value is obtained.
   e. Repeat steps c & d above until the complete card number has been entered.

f. Press <Run/Stop> to exit setup mode and enter Run mode.
g. Place the spoofer antenna approximately 1" from the reader to begin card emulation.

5. If a new card identity is desired then press the <Run/Stop> button to exit Run mode and return to Setup mode.

To Store a Card Identity

1. While in Setup Mode (MD=0), move the cursor to the SR field.
2. Press <Incr> until the desired pre-stored card identity location is shown.
3. Perform Steps 4a-4e above.
4. Press the <Store> button to store the displayed card identity into the memory location specified by the SR field.

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