80141506-001

ID TECH Spectrum Pro and SmartPIN L100 Pairing

Rev. B
Revised: May 2, 2017

ID TECH

10721 Walker Street, Cypress, CA90630 Voice: (714) 761-6368 Fax: (714) 761-8880

The information contained herein is provided to the user as a convenience. While every effort has been made to ensure accuracy, ID TECH is not responsible for damages that might occur because of errors or omissions, including any loss of profit or other commercial damage, nor for any infringements or patents or other rights of third parties that may result from this information's use. The specifications described herein were current at the time of publication, but are subject to change at any time without prior notice.

LIMITED WARRANTY

ID TECH warrants to the original purchaser for a period of 12 months from the date of invoice that this product is in good working order and free from defects in material and workmanship under normal use and service. ID TECH's obligation under this warranty is limited to, at its option, replacing, repairing, or giving credit for any product that returned to the factory of origin with the warranty period and with transportation charges and insurance prepaid, and which is, after examination, disclosed to ID TECH's satisfaction to be defective. The expense of removal and reinstallation of any item or items of equipment is not included in this warranty. No person, firm, or corporation is authorized to assume for ID TECH any other liabilities in connection with the sales of any product. In no event shall ID TECH be liable for any special, incidental or consequential damages to purchaser or any third party caused by any defective item of equipment, whether that defect is warranted against or not. Purchaser's sole and exclusive remedy for defective equipment, which does not conform to the requirements of sales, is to have such equipment replaced or repaired by ID TECH. For limited warranty service during the warranty period, please contact ID TECH to obtain a Return Material Authorization (RMA) number & instructions for returning the product.

THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE. THERE ARE NO OTHER WARRANTIES OR GUARANTEES, EXPRESS OR IMPLIED, OTHER THAN THOSE HEREIN STATED. THIS PRODUCT IS SOLD AS IS. IN NO EVENT SHALL ID TECH BE LIABLE FOR CLAIMS BASED UPON BREACH OF EXPRESS OR IMPLIED WARRANTY OF NEGLIGENCE OF ANY OTHER DAMAGES WHETHER DIRECT, IMMEDIATE, FORESEEABLE, CONSEQUENTIAL OR SPECIAL OR FOR ANY EXPENSE INCURRED BY REASON OF THE USE OR MISUSE, SALE OR FABRICATIONS OF PRODUCTS WHICH DO NOT CONFORM TO THE TERMS AND CONDITIONS OF THE CONTRACT.

Table of Contents

Introduction

ID TECH's SmartPIN L100 encrypting PIN pad provides a compact, rugged, secure keypad interface for POS systems in which PIN and/or manual data-entry capability are required. As such, the L100 is a natural complement to ID TECH's Spectrum Pro insert reader. Together, the Spectrum Pro and L100 provide an EMV Level 2 chip-and-PIN solution (suitable for use in kiosks and other unattended applications), meeting ADA, ANSI, PCI, and ISO standards for PIN Entry.

This document describes the steps that must be undertaken in order to pair a SmartPIN L100 keypad with a Spectrum Pro card reader.

1 Theory of Operation

The SmartPIN L100 is intended to offer a PCI-compliant solution for systems that require encryption of PIN data. To achieve this goal, the SmartPIN L100 must be *paired* with a compatible card reader. Once paired, the L100 encrypts keypad data at the point of entry, and no clear-text data is ever exchanged between the L100 and the connected reader.

In order for pairing to occur, each device (PIN pad and reader) must be injected, ahead of time, with a so-called Pairing Key, representing a shared secret. This key is ultimately used to enable secure sharing of data between reader and PIN pad. The data shared includes both PAN (primary account number) data *and* PIN data. Cryptographic keys (and TDES encryption) are used to protect the PAN and PIN data at all times. Each unit (reader, and PIN pad) must be injected with the Pairing Key. This key represents a shared secret which unites the two devices such that they can communicate with each other using encrypted data (hence, the units are "paired").

Once the reader and the PIN pad are in the proper state (see discussion to follow), the pairing process itself is mostly automatic and out of the operator's control. From a high level, it involves the following steps:

1. Both units (Spectrum Pro and L100) need to have been injected with Pairing Keys. This step is not covered in this document. You should start by getting units key-injected, if they are not already injected. (Contact your ID TECH representative for details. ID TECH is a certified Key Injection Facility.)
2. The SmartPIN L100 needs to be in Removal Detection Mode in order to undergo the pairing process. This document describes (in detail) the steps needed to put the PIN pad into this state. (See Setting Up Removal Detection.)
3. With the units connected to each other, a pairing command (76 46 38 00 00) needs to be sent to the Spectrum Pro. The Spectrum Pro will then automatically carry out all

necessary communications with the PIN pad, and pairing will be complete. You will be able to verify this by (for example) conducting an MSR read (Start MSR command) followed by a Get PIN from MSR, using the Universal Demo program; the latter will result in a PIN prompt from the L100, and then (after a PIN is entered manually) the command will allow the L100 to return an encrypted PIN block.

This document tells how to perform all of these steps (except for key injection). Since the process is somewhat involved, it's recommended that you read this document over, from start to finish, to familiarize yourself with the overall process, first, before you begin.

2 Prerequisites

To complete the pairing process, you will need the following items (see also the photograph further below):

- A SmartPIN L100, injected with Pairing Key
- A Spectrum Pro, injected with Pairing Key
- RJ-11 to Serial cable, to connect Spectrum Pro's RJ-jack to the L100 serial port
- A 5-volt DC power source for the L100
- USB cable to connect Spectrum Pro to host
- Two large steel binder clips, C-clamps, or other fixture(s) to hold the L100's tamper buttons down
- One large steel clip or C-clamp to depress the Spectrum Pro's removal-detection buttons
- Host software that can open a connection with Spectrum Pro and send firmware commands (e.g., ID TECH Universal SDK Demo app)

3 Setting Up Removal Detection

Before the SmartPIN L100 can be paired, it must be placed in Removal Detection Mode. Please follow the steps below carefully to activate the Removal Detection feature on the PIN pad. It is highly recommended that you read through the entire procedure, and become thoroughly familiar with it, before attempting to carry it out.

> **Note:** Removal Detection is a security mechanism to protect the sensitive data in the PIN pad, such as encryption keys, transaction data, etc. Removal Detection mode requires that the small buttons on the top and bottom of the frame be depressed. Once the L100 has been placed into Removal Detection mode, the anti-tamper buttons must not be released without first *deactivating* Removal Detection. (See How to Deactivate Removal Detection.) If you release the removal detection buttons prematurely, any passwords stored in the L100 will be reset to the factory defaults.

Setting up Removal Detection mode is a 3-step process in which you need to secure the removal-detection buttons; then set the device's removal-detection passwords; then (finally) put the device in Removal Detection mode, using the passwords you set in the second step. We'll now talk about those three steps, one by one.

3.1 Step One: Secure the PIN Pad's Removal Detection Buttons

Removal Detection Mode requires depressing the tamper buttons located at the top and bottom of the unit's frame, on the front (as shown by the red arrows in the illustration further below). You can keep these buttons depressed by installing metal strips (screwed in place) along the top and bottom of the L100's housing; or you may install the unit in a kiosk; or you can temporarily use

stout spring-clips (or C-clamps, etc.) to hold the buttons down. If you use spring clips, take care that they don't slip off prematurely.

After the buttons are secured, you will need to activate Removal Detection Mode. (You can later *deactivate* this mode, then move the unit to a kiosk or other fixture, then *reactivate* it.) But first, you need to set the removal detection passwords.

Tamper-detection buttons are at the top and bottom of the front face.

3.2 Step Two: Set the Removal Detection Passwords

The SmartPIN L100 comes with two *default* Removal Detection passwords that need to be reset with *user-supplied* passwords before the Removal Detection feature can be activated. The following steps will let you set the passwords.

1. Power on the SmartPIN L100 by connecting the device to the computer with the appropriate cables, using a 5V/1.2-amp power supply. (Do not use more than 5 volts.) The device will beep once to signify that the device is powered on, and the LCD screen will illuminate.

2. Immediately press the following sequence of keys: **Cancel, Clear, Enter, Blank, Clear, Enter**. (The sequence must be initiated within 5 seconds of the unit beeping after

powering on.) After this, the device will start beeping continuously to signify that the passwords have not yet been set. Also, the LCD screen will prompt you to enter a password.

Note: If the device does *not* beep continuously after the **Cancel, Clear, Enter, Blank, Clear, Enter** sequence was entered, it means the passwords have already been set and you can skip to the next section: Activate Removal Detection.

3. Enter default **Password A**: 12345678. (Make sure the device beeps after each button is pressed to ensure that the input was registered.) After the default **Password A** is entered correctly, the device will beep twice.

4. Enter a new *user*-generated **Password 1** to replace **Password A**. (The new **Password 1** must be 8 digits. For example: 11111111.) After the new **Password 1** is entered, the device will beep twice to confirm the input of the new password. Keep the new **Password 1** in your records.

5. The device will prompt you to reenter the password. Enter the new **Password 1** again to confirm the setting of the new password. After the new **Password 1** is entered for a second time, the device will beep twice to confirm the successful input of the new password. If the new **Password 1** was entered correctly, the device will beep twice again to confirm that **Password 1** is set.

6. Next enter default **Password B**: 87654321. Make sure the device beeps after each button is pressed to ensure that the input was registered. After the default **Password B** is entered correctly, the device will beep twice.

7. Enter a new *user*-generated **Password 2** to replace **Password B**. The new **Password 2** must be 8 digits and must be different from **Password 1**. For example: 22222222. After

the new **Password 2** is entered, the device will beep twice to confirm the input of the new password. Keep the new **Password 2** in your records.

8. The device will prompt you to reenter the password. Enter the new **Password 2** again to confirm the setting of the new password. After the new **Password 2** is entered for a second time, the device will beep twice to confirm the input of the new password. If the new **Password 2** is entered correctly, the device will beep twice again to confirm that **Password 2** is set. The SmartPIN L100 Removal Detection passwords are now set. (The L100 can safely be powered down now. When it is powered back up, it will remember the passwords. Do not release the removal detection buttons, however. The buttons must stay down until the unit has been taken out of Removal Detection mode. See How to Deactivate Removal Detection, further below.)

3.3 Step Three: Activate Removal Detection

Note: The SmartPIN L100 must be installed with the two Removal Detection Pressure Points (anti-tamper buttons) fully depressed before Removal Detection can be activated. Once Removal Detection has been activated, unauthorized removal (that is to say: premature release of the anti-tamper buttons) will result in the PIN pad losing any passwords that were set.

The following steps describe how to activate Removal Detection. *This section assumes that you have already completed the previous section, which sets up User Passwords.*

1. At all times throughout this process, ensure that the Removal Detection Pressure Points are depressed and held securely in the depressed position. (The buttons must stay down until the unit has been taken out of Removal Detection mode. See How to Deactivate Removal Detection, further below.)

2. Unplug and replug (that is, power-cycle) the L100. The device will beep once to signify that the power is on.

3. Immediately press **Cancel**, **Clear**, **Enter**, **Blank**, **Clear**, and **Enter** (6 keys) to enter Removal Detection Mode. The unit will prompt you to enter the first User Password (which was 11111111, in the examples shown earlier). If the password is accepted, you'll be prompted to enter the second User Password (which was 22222222, in the examples shown earlier). Make sure the device beeps after each button is pressed to ensure that the input was properly registered.

4. If the passwords are accepted, you will see a prompt as follows:

5. Use ***** or **#** buttons to scroll up or down.

6. Accept the **Enable PINPAD** option by pressing the Enter (ENT) button.

7. The SmartPIN L100 will beep twice more to signify that the device has been activated with Removal Detection.

In order to *remove* the SmartPIN L100 from its installation (that is, before pressure is released from the Removal Detection Pressure Points), Removal Detection must first be *deactivated*, or else the unit will become disabled and any passwords will be lost. The section called How to Deactivate Removal Detection describes the steps that must be taken to make the unit safe for removal.

4 Pairing (High Level Overview)

As long as the Spectrum Pro and L100 have each been injected with a Pairing Key, pairing the units is straightforward, as it merely requires sending Spectrum Pro a specific firmware command (76 46 38 00 00), which you can easily do with the Universal Demo's "Send Data Command" facility. (Be sure to check the "Wrap as NGA" checkbox when sending a raw command.)

When it receives the pairing command, Spectrum Pro will communicate directly with the L100 to carry out the sequence of steps that will culminate in pairing. The steps are automatic and will happen outside of the user's control.

To pair units, follow the detailed procedure given below. You will first verify Spectrum Pro's key status; then verify L100's key status; then put Spectrum Pro in pass-through mode; and issue the pairing command. Afterwards, you can take steps to verify that pairing occurred.

4.1 Verify Spectrum Pro Key Status

Before issuing the Pairing command, you should verify that your Spectrum Pro contains the proper keys. You can do this as follows.

1. Connect L100 to Spectrum Pro via the Spectrum Pro's RJ-11 port.
2. Connect Spectrum Pro to the host computer.
3. Run host software that can communicate with Spectrum Pro (e.g., Universal SDK Demo app). Verify that a connection has been established.

Send the Poll Reader command to Spectrum Pro. (The complete NGA-format command string is `02050076462500001 5E103`.) This produces 6 bytes of flag data in return. (See discussion below. For a full discussion of the Poll Reader command, see the *Spectrum Pro Low Level API Command Guide*, available from https://atlassian.idtechproducts.com/confluence/display/KB/Downloads+-+Home.)

4. Confirm that the command was successful (i.e., it returns a response containing ACK, or 0x06).
5. Examine the data bytes that come back.

The response to Poll Reader should contain 6 data bytes, with flags that signal the status of various device configuration settings and capabilities. The info you're looking for can be found in the second data byte (see below). A typical response looks as follows:

Poll Reader Results (Before Pairing)

Note: The Poll Reader command returns six bytes of data. We refer to the first byte as Byte Zero, the second byte as Byte 1, etc. Refer to the *Spectrum Pro Low Level Command API Guide* (P/N 8014505-001) for further details.

Byte 1 of the Poll Reader response will change after pairing is complete. Prior to pairing, the response (in Byte 1) will look something like this:

```
Byte 1 (before Pairing):
1-------  HSM_DUKPT_KEY valid if set to 1
-1------  CR_PINPAD_RKL_DUKPT_KEY valid if set to 1
--0-----  PIN Pairing DUKPT Key valid if set to to 1
---0----  DATA Pairing DUKPT Key valid if set to 1
----0---  CR_PINPAD_MAC Keys valid (Authenticated) if 1
-----0--  CR_PINPAD_MASTER_DUKPT_KEY valid if set to 1
------0-  Authenticated with Pinpad if set to 1
-------0  Firmware Key valid  if set to 1
```

Note that Byte 5, bit 5, of the response will confirm that the PIN pad is connected:

```
Byte 5:
1-------  0-Maxq Manufacture FW; 1-Maxq Production
-1------  0-K21 Manufacture FW; 1-K21 Production FW
--1-----  MSR Header connected if set to 1
```

```
---1----  PINPAD connected if set to 1
----0---  Contactless  available if set to 1
-----1--  Host connected if set to 1
------1-  Chip card reader available if set to 1
-------1  SAM available  if set to 1
```

Summary: In Byte 1, the CR_PINPAD_RKL_DUKPT_KEY valid bit should have a value of 1, as shown above. In Byte 5, the PINPAD CONNECTED bit should have a value of 1 (if L100 is connected to Spectrum Pro).

4.2 Verify L100 Key Status

Connect L100 to Spectrum Pro and place the Spectrum Pro in pass-through mode using the 72 46 20 command. Essentially, pass-through mode enables commands to be sent to the L100 while it is connected to Spectrum Pro (with Spectrum Pro connected to a host computer). Instead of commands going to Spectrum Pro, they are "passed through" to the L100.

The full command string (with protocol wrapper) for entering pass-through mode should look like 0206007246200100011 4DA03. The final 01, before the last three bytes (14 DA 03), means to turn pass-through mode ON. (See the *Spectrum Pro Low Level API Command Guide*, available from https://atlassian.idtechproducts.com/confluence/display/KB/Downloads+-+Home, for details.)

Using the Universal SDK Demo app, send the Get Status for Key command string, 0203007846251be303, to the L100. The response will look something like

```
02630006180000000000010000010300000104000001060000010700000108000
00000800010008000200080003000800040008000500080006000800070008000
08000800090008000a0008000b000a0000000a03e8010c0000000d0000001400000
0128000000ce3003.
```

After STX (02), length (63 00), and ACK (06) is the number of key status blocks (in this case, 18 00, which is little-endian, hence there are 24 actual key blocks). Each key status block is four bytes long. The blocks are formatted as

Key Index: 1 byte
Key Slot: 2 bytes
Key Status: 1 byte

The above data can be parsed into key status blocks that look like this:

["00000000", "01000001", "03000001", "04000001", "06000001", "07000001",
"08000000", "08000100", "08000200", "08000300", "08000400", "08000500",
"08000600", "08000700", "08000800", "08000900", "08000A00", "08000B00",
"0A000000", "0A03E801", "0C000000", "0D000000", "14000001", "28000000"]

The Pairing Key has a key index of 03 and can be recognized as the third block (03000001) in the array above. Because the final byte of that block has the first bit set, the Pairing Key is known to exist (in this example); the unit has been injected. If the Pairing Key did *not* exist, the block would look like 03000000 and you would need to have the unit injected with a Pairing Key that corresponds to the Pairing Key injected into the Spectrum Pro. (Contact your ID TECH representative for information on how to get your devices injected.)

4.3 Pair the Units

To pair L100 with Spectrum Pro, it is recommended that you do the following:

1. Ensure that the L100 is in the Removal Detection activated state (see previous sections of this guide).
2. Plug the L100 into Spectrum Pro's RJ-11 port. Power the unit with 5 volts DC.
3. Connect the Spectrum Pro to the host system.
4. Run the Universal SDK Demo app (or other software that can send firmware commands to the Spectrum Pro). Ensure that connectivity has been established.
5. Send the pairing command to Spectrum Pro. (The complete NGA-format command string is 020500764638000008F403.)
6. Verify that the units are paired. (See below.)

4.4 Verify the Pairing

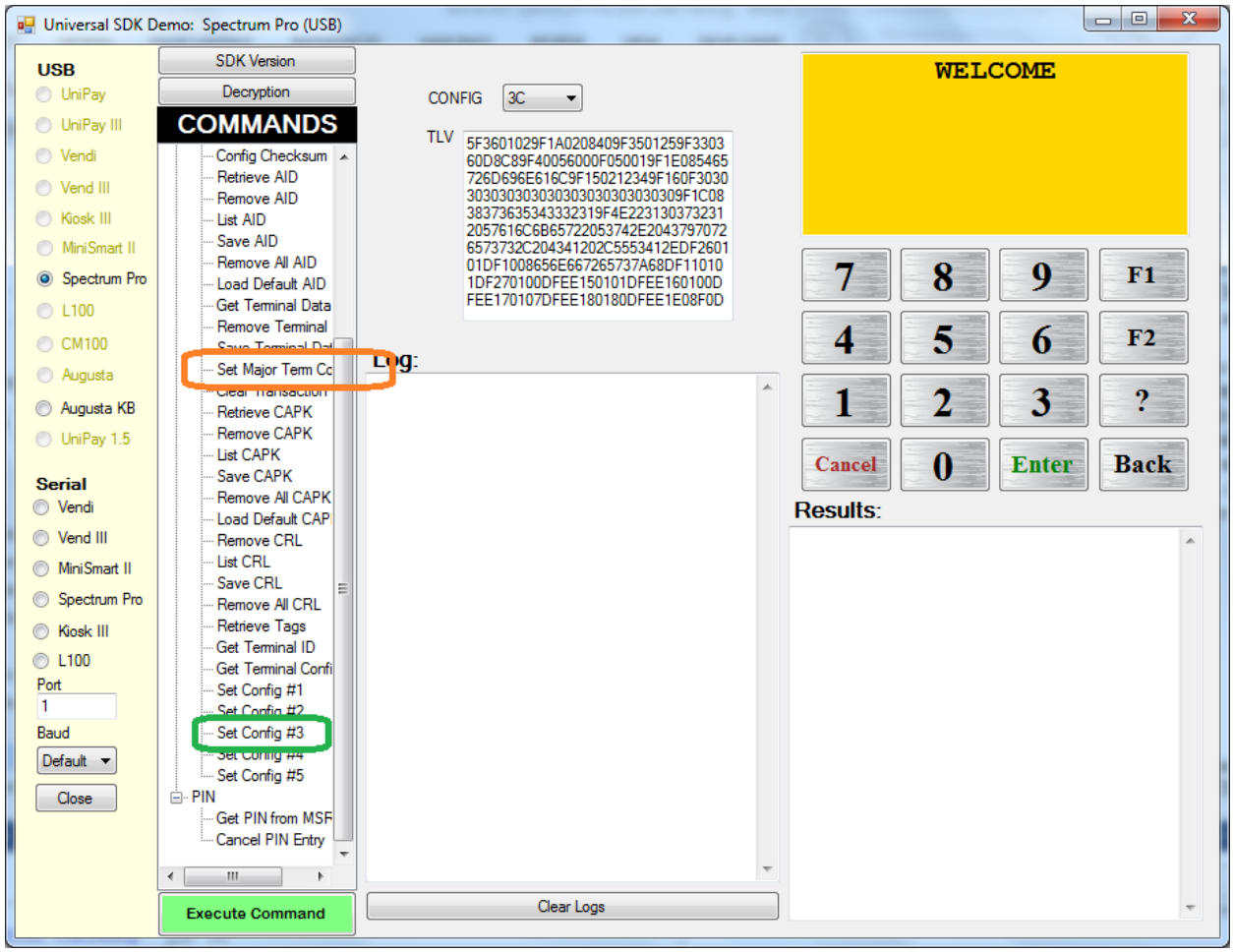
You can and should verify that the Spectrum Pro has recognized the L100 and is correctly paired with it. The recommended procedure is as follows.

1. With the L100 connected to the Spectrum Pro and the Spectrum Pro connected to a host, send the Spectrum Pro the Poll Reader command. The complete NGA-format command string is `020500764625000015E103`.
2. Examine the data that comes back and compare it to the Poll Reader results you obtained earlier, in Verify Spectrum Pro Key Status. The results this time should show that several bits have changed in Byte 1 of the data (see boldface items below):

   Poll Reader Results (After Pairing)

```
Byte 1:
1-------  HSM_DUKPT_KEY valid if set to 1
-1------  CR_PINPAD_RKL_DUKPT_KEY valid if set to 1
--1-----  PIN Pairing DUKPT Key valid if set to to 1
---1----  DATA Pairing DUKPT Key valid if set to 1
----1---  CR_PINPAD_MAC Keys valid (Authenticated) if 1
-----1--  CR_PINPAD_MASTER_DUKPT_KEY valid if set to 1
------0-  Authenticated with Pinpad if set to 1
-------0  Firmware Key valid  if set to 1
```

3. Attempt to use the paired devices to conduct a Chip-and-PIN EMV transaction (or other transaction that requires the use of a PIN). To do this, you will need a test card (or live credit card) that specifies Chip-and-PIN in its CVM list, and you will need to ensure that your Spectrum Pro is configured (via its terminal settings) to participate in Chip-and-PIN sessions. The Windows version of the ID TECH Universal SDK Demo app offers a convenient GUI for selecting the necessary terminal settings.
    a. First, select the command **Set Config #3** in the EMV command tree; then run it. (This enables the Spectrum Pro L2 EMV kernel to use a predetermined terminal configuration, but it does not actually set the config values; that's the next step.)
    b. Next, select the command **Set Major Term Config** in the EMV command tree; a configuration panel will appear, with a dropdown menu, at the top of the middle pane. Choose **3C** from the dropdown menu. Then Execute the command; see screenshot below. (Executing this command loads a terminal configuration that has appropriate bits of tag 9F33 set to enable PIN-related CVMs.)



Insert a Chip-and-PIN ICC payment card in the Spectrum Pro and run the Start EMV Transaction command. Monitor the L100 LCD screen. If the card requires PIN entry, you

will be prompted by the L100 to enter a PIN at the appropriate moment. Enter the PIN (followed by the ENT button). The transaction should finish normally.

4.5 Checking for Encrypted PIN Block

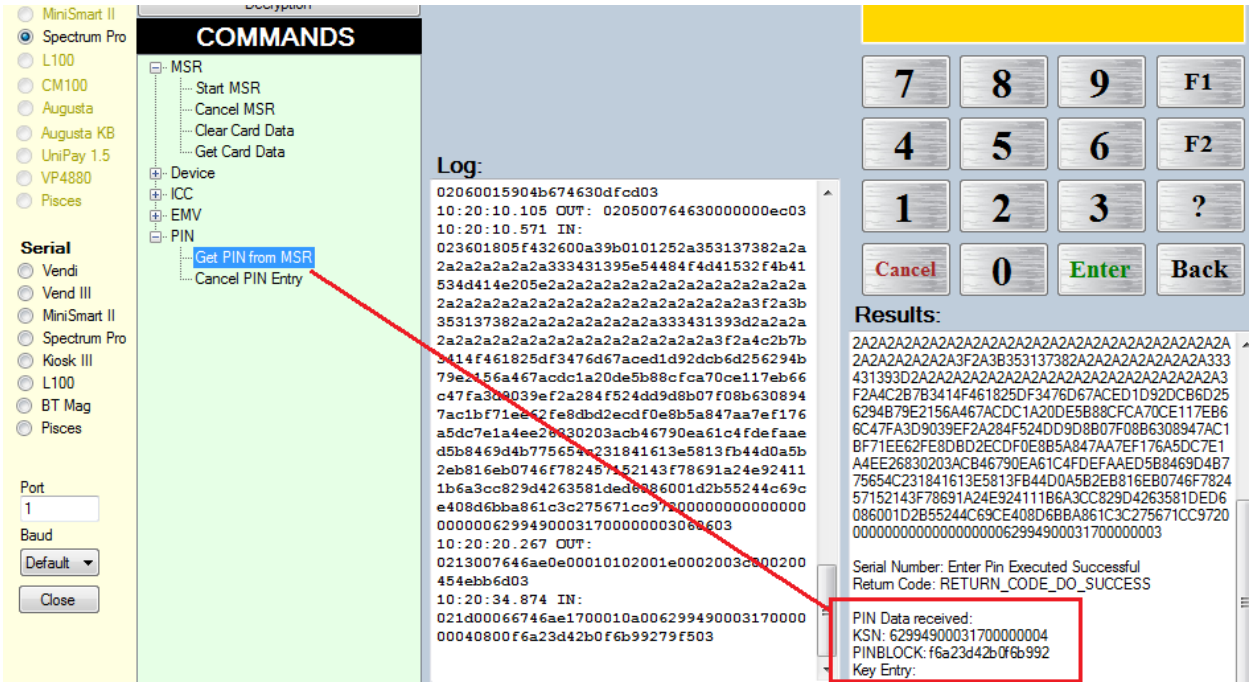
You can also verify the pairing status by seeing if the Spectrum Pro/L100 combo will prompt you for a PIN, and returned an encrypted PIN block, when you use the Get PIN from MSR command in the Universal Demo app. The procedure is:

1. Connect the L100 to the Spectrum Pro using the serial-to-RJ cable.
2. Connect Spectrum Pro to a host computer that's running the Universal Demo app.
3. Ensure that the Spectrum Pro has been recognized by the app.
4. Place the Spectrum Pro in Removal Detection mode.
    a. Depress the removal-detection buttons on the edge of the bezel. (NOTE: You need to depress only the set of buttons on the side of the bezel opposite the green light on the face. See arrow, below.) Hold the buttons down with a steel clip or clamp of some kind, or mount the unit in a kiosk or other enclosure that will fully depress the removal buttons when he unit is in final position.

    b. Power-cycle the Spectrum Pro and inspect the status lights near the rear of the unit (on the underside) to see that a green light is illuminated. If the green light is not illuminated, it's likely you have not fully depressed the removal-detection buttons on the front face of the bezel flange. Adjust your mountings as necessary and repower the unit, until you see the green light at the back.
    c. Power up the L100, and when it beeps, quickly press CANC CLR ENT BLANK CLR ENT; then at the prompts, enter the user passwords. If the passwords are accepted, a menu will appear on the screen.

d. Select **Enable CR** from the menu. (Use * and # keys to move up and down on the menu.)

5. Use the demo app's **Start MSR** command, and insert/remove a magstripe card into/out of the reader.
6. Use the demo app's **Get PIN from MSR** command (see screen shot below). The L100, if it is paired properly, will prompt you for PIN entry. Enter a PIN. The resulting PIN block will appear in the Results pane of the demo app. (See below.)



5 How to Deactivate Removal Detection

In order to safely remove the SmartPIN L100 from its installation, Removal Detection mode must first be deactivated or else the unit will become disabled and passwords will be reset. The steps in this section describe how to *deactivate* Removal Detection.

Note: SmartPIN L100 Removal Detection deactivation uses the same **Password 1** and **Password 2** that were set before. Refer to Section 2 as necessary.

1. Power on the SmartPIN L00 by connecting the device to the computer with the USB or RS-232 cable. The device will beep once to signify that the device is powered on.

2. Immediately press the following sequence of keys: **Cancel, Clear, Enter, Blank, Cancel, Blank**. The sequence must be initiated within 5 seconds of the unit beeping after

powering on. The device will beep once to signify that the passwords have already been set.

3. Enter the user-generated **Password 1** that was set earlier. Make sure the device beeps after each button is pressed to ensure that the input was properly registered. After **Password 1** is entered correctly, the device will beep twice.

4. Next, enter the user-generated **Password 2** that was put in earlier. Make sure the device beeps after each button is pressed to ensure that the input was properly registered. After **Password 2** is entered correctly, the device will beep twice.

5. The SmartPIN L100 will beep one final time to signify that the Removal Detection has been deactivated.

5.1 Troubleshooting Tips

Spectrum Pro is designed to interoperate with L100 when both units are in a "final-installation" state, such that each unit has its removal detection features enabled. If units that were working properly in the lab suddenly fail to produce a PIN block after installation in the field, the most likely reason is that one or the other unit is not in the removal-detection state.

If the L100 has exited removal-detection mode, passwords will have been lost (reset), and you'll need to enter new passwords. (See Set the Removal Detection Passwords.) Reinstall the unit, making sure the removal-detection buttons on the frame are securely depressed. *After* you're sure the removal-detection buttons are depressed, power up the L100 and put the unit in Removal Detection mode (follow the steps at Activate Removal Detection).

If PIN blocks are not being received and you are sure the L100 is securely mounted and working properly, check that the green operating status light on the *back* of the unit (not the front bezel), near the power wiring, is illuminated. If it is not (if just the amber light is showing), readjust clamps or mountings on the front bezel to be sure the removal-detection buttons are depressed, and recheck the light. (These buttons can be tricky. Use thin shims or metal strips if necessary to make sure the buttons are down when the unit is in final position.) When the green light is showing, you can put the reader in Removal Detection Mode: Re-power the L100, and when the unit beeps, quickly enter the logon sequence (Cancel Clear Enter Blank Clear Enter), then at the prompts, enter the user passwords; then select Enable CR from the menu. You should see an Activation Success message.