USER MANUAL

Spectrum Air

Outdoor Dual Headed Magnetic-Only Insert Reader

USB and RS232 Interfaces

80116501-001-N
10 September 2020

ID TECH
10721 Walker Street
Cypress, CA 90630 USA

Agency Approved
Specifications for subpart B of part 15 of FCC rule for a Class A computing device.

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 which has, within the warranty period, been returned to the factory of origin, transportation charges and insurance prepaid, and which is, after examination, disclosed to ID TECH's satisfaction to be thus 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.

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. The specifications described herein were current at the time of publication but are subject to change at any time without prior notice.
ID TECH and Value through Innovation are registered trademarks of International Technologies & Systems Corporation.

Revision History

Revision	Date	Description of Changes	By
50	05/07/2012	Initial draft	JW
A	08/06/2012	Initial release	JW
	12/30/2012	Updated Appendix A	BK
B	05/05/2013	• Remove the TTL part Remove conformal coated PCA from features	CH
C	05/08/2013- 03/14/2014	• Enumeration SN and special terminator CRLF Clarify configuration 1C setting bits • Correct Original and Enhanced Encryption Format Added Encryption Field 8 and 9 definitions Updated HID block Size • NGA flag added to Status report 2 byte Added Raw track prefix or sync char if KB mode Corrected PID for standard and secure HID/HIDKB	BK
D	10/13/2015	• Correct 72, 73 & 84 descriptions; add loop and Service Code support; clarify field 8;	
E	12/16/2015	• Added Minor version support; Added review Encryption settings	BK
F	05/27/2016	Documented features added with Version V2.89.	BK
G	07/21/2016	Document feature (card present and different error response codes) added with Version 2.90	BK
H	08/21/2017	Added section 5.1 for physical mounting	JH
J	05/10/2019	Reformatted and repaginated document Added Table of Contents Installation 4.2: Added a section about installing a drain wire in cases of ESD	CB
K	02/17/2020	Font update. Added info about compatible Molex parts in Pin Out info. Removed Command documentation.	CB
L	07/7/2020	Added mounting info.	CB
M	08/18/2020	Added horizontal mounting disclaimer.	CB
N	09/10/2020	Added exploded mounting drawing to Appendix B.	CB

Table of Contents

1. Introduction

The Spectrum Air outdoor insert reader is designed for installations that might be subjected to harsh environments such as fuel pumps and outdoor kiosks. This insert reader meets IP 65 rating with dual head configurations supporting up to 3 tracks of information from ISO and AAMVA encoded cards. A card is read by inserting it into and/or removing it out of the card slot. The Spectrum Air uses TriMag III and offers encryption feature for USB and RS232 interface.

2. Features

- Dual Head Magnetic only insert reader (MIR)
- Low Insertion Force
- Interface: USB/KB, USB/HID, USB/CDC, RS232
- IP 65 rating
- Reads up to 3 tracks of card data
- Sealed bezel and chassis – meaning that unit can allow water ingress but not allow water to seep into the host unit
- Optional gasket for sealing around bezel cutout
- Ideal for gas pumps and outdoor kiosk applications
- TDES / AES encryption
- DUKPT key management
- Card seated switch
- Optional card present switch
- OPOS & JPOS support
- Support all software features current SPT MIR supports
- One-year Warranty
- Gas pump mounting – compatible with UIC/Panasonic mounting
- Mounting: Compatible with Panasonic ZU-1870MA8T2
- Supports several protocols for compatibility

3. Abbreviations

AAMVA	American Association of Motor Vehicle Administration
ABA	American Banking Association
ACK	Acknowledge
AES	Advanced Encryption Standard
ASIC	Application Specific Integrated Circuit
BPI	Bits per Inch
CADL	California Driver's License Format (obsolete)
CE	European Safety and Emission approval authority
COM	RS232 serial communication port
CTS	Clear-To-Send
CBC	Cipher-block chaining
CDC	USB to serial driver (Communication Device Class)
DC	Direct Current
DES	Data Encryption Standard
DUKPT	Derived Unique Key per Transaction
DMV	Department of Motor Vehicle
ESD	Electro-Static Discharge
ETX	End of Transmission
FPC	Flexible Printed Circuit
FCC	Federal Communications Commission
GND	Signal Ground
Hex	Hexadecimal
HID	Human Interface Device
IPS	Inches per Second
ISO	International Organization for Standardization
ITP	ID TECH Transport Protocol
JIS	Japanese Industrial Standard
JPOS	Java for Retail Point of Sale
KB	Keyboard
KSN	Key Serial Number
LED	Light Emitting Diode
LRC	Longitudinal Redundancy Check Character.
LSB	Least significant Bit
mA	Milliamperes
MAC	Message Authentication Code
MIR	Magstripe Insert Reader (previously MOIR)
MSB	Most significant Bit
msec	Milliseconds
MSR	Magnetic Stripe Reader
mV	Millivolts

NACK	Non-acknowledge
NGA	Next Generation Architecture
OLE	Object Linking and Embedding
OPOS	OLE for Retail Point of Sale
OTP	One Time Programmable
PAN	Primary account number
PCA	Printed Circuit Board (Assembled)
PCB	Printed circuit board bare.
PCI	Payment Card Industry
POH	Powered On Hours
POS	Point of Sale
PPMSR	Serial Port Power Magstripe Reader
P/N	Part Number
PS/2	IBM Personal System/2 Keyboard Interface
RoHS	Restriction of Hazardous Substances
RTS	Request To Send
SHA-1	Enhance Cryptographic Hash Function
SPI	Serial Peripheral Interface
T1, T2, T3	Track 1 data, Track 2 data, Track 3 data
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus
UV	Ultraviolet – spectrum of light rays

Note: many unusual words used in this document are defined in the Function ID table on page.

3.1. Formatting to designate certain data types

'A'	A single character in ASCII
41h	A single character in hexadecimal
41	A single character in a group of hexadecimal digits
"String"	ASCII character group if in communication group, not NULL terminated.
Default	A default value will be bolded
<ETX>	A communication member, one byte in size, except the message length.
6913	four-digit hex numbers are error status indications
[xxx … xxx]	Square brackets designate optional or repeated data groupings
[52 4E]	Bold square brackets in headings are the key communication bytes for a particular command
B0	bit positions are all from position 0 to position 7 so if only B1 is set the value of a byte is 02h.

3.2. Related Documents

ISO 7810	Identification Cards - Physical Characteristics (1995)
ISO 7811	Identification Cards -Recording Technique (1995)
AAMVA	Best Practices Guidelines for the Use of Magnetic Stripe
ISO 4909	Magnetic stripe content for track 3
ISO 7812	Identification Cards – Identification for issuers Part 1 & 2
ISO 7813	Identification Cards – Financial Transaction Cards
ANSI X9.24-2002	Retail Financial Services Symmetric Key Management
USB ORG	USB Specification Rev. 2.0

3.3. Supported Programs

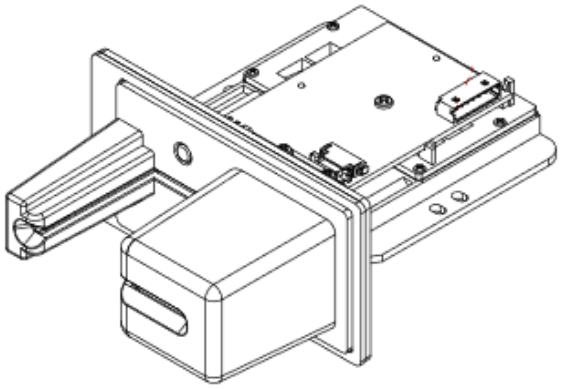
- Secure MOIR RS232 Demo Program
- Secure MOIR USB Demo Program
- Secure MOIR Configuration Program

4. Installation

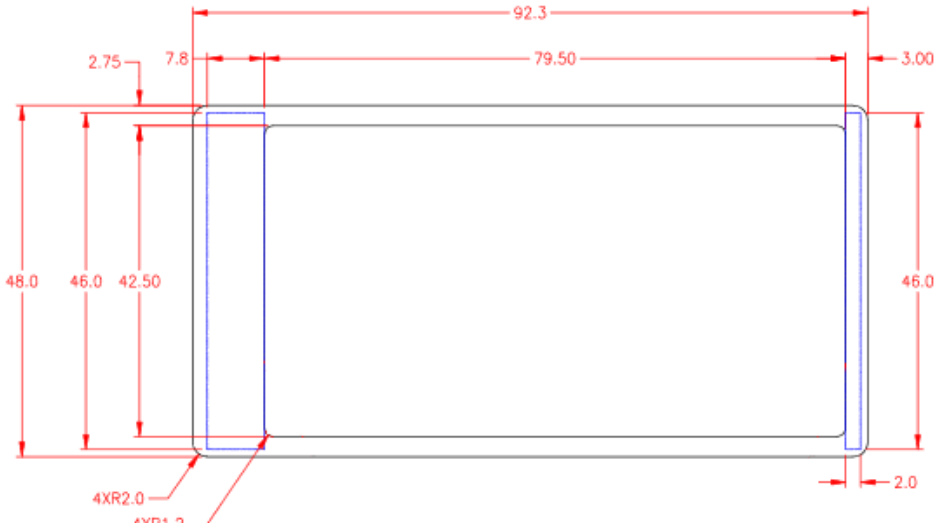
4.1. Physical Installation

The Spectrum Air requires a cutout to be made for the bezel to protrude. The bezel is available in both a flush mount and standard extended bezel option. To protect against moisture entering from the bezel cutout, it is advised to order a unit that has a gasket installed or use protective sealant preventing intrusion of moisture into the internal kiosk area.

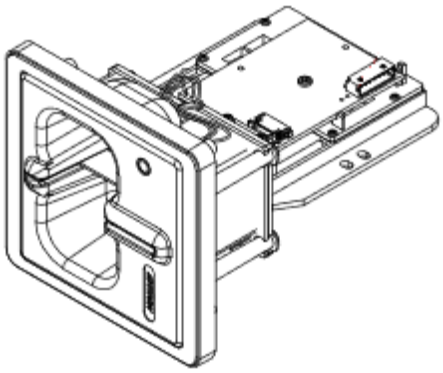
Standard Bezel



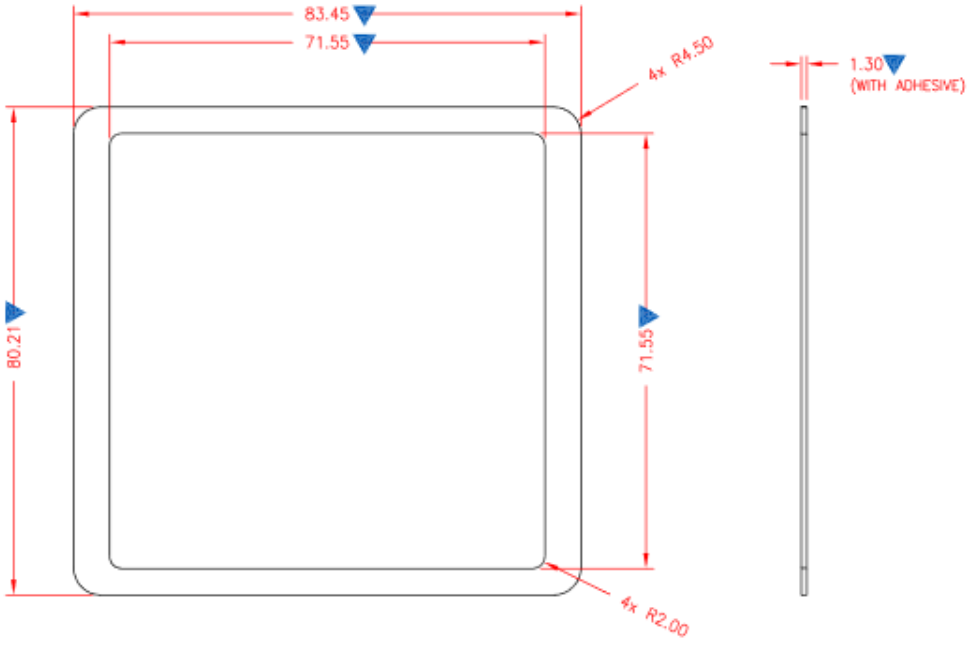
Cutout/Gasket



Flush Bezel

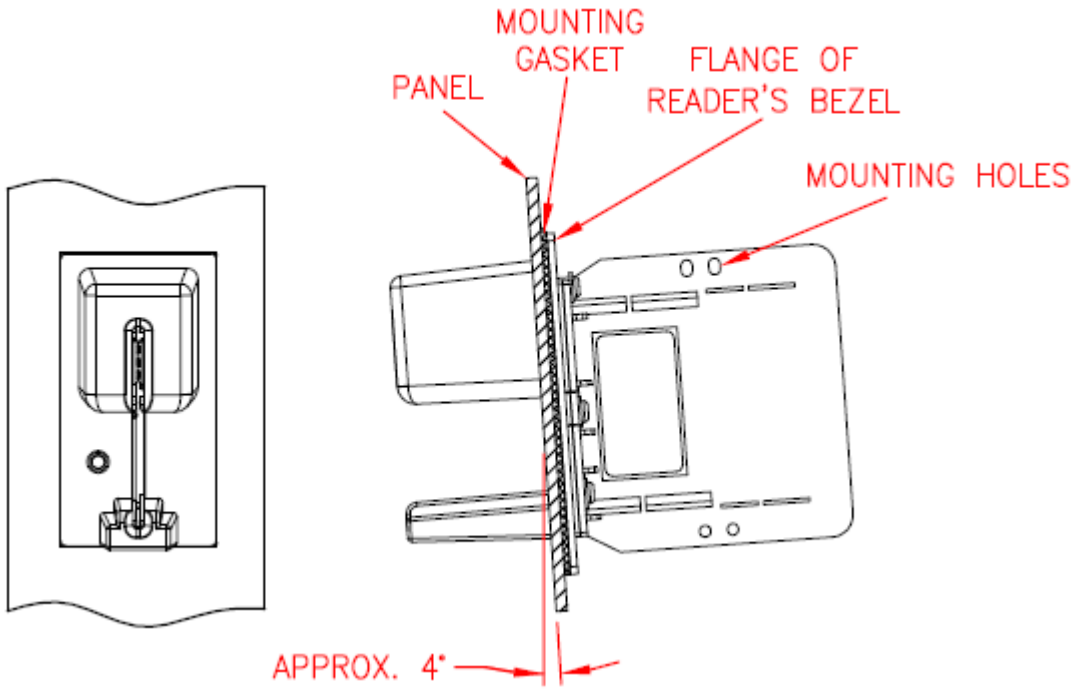


Cutout/Gasket



4.2. Mounting Guidelines

Follow the guidelines below when mounting a Spectrum Air reader.



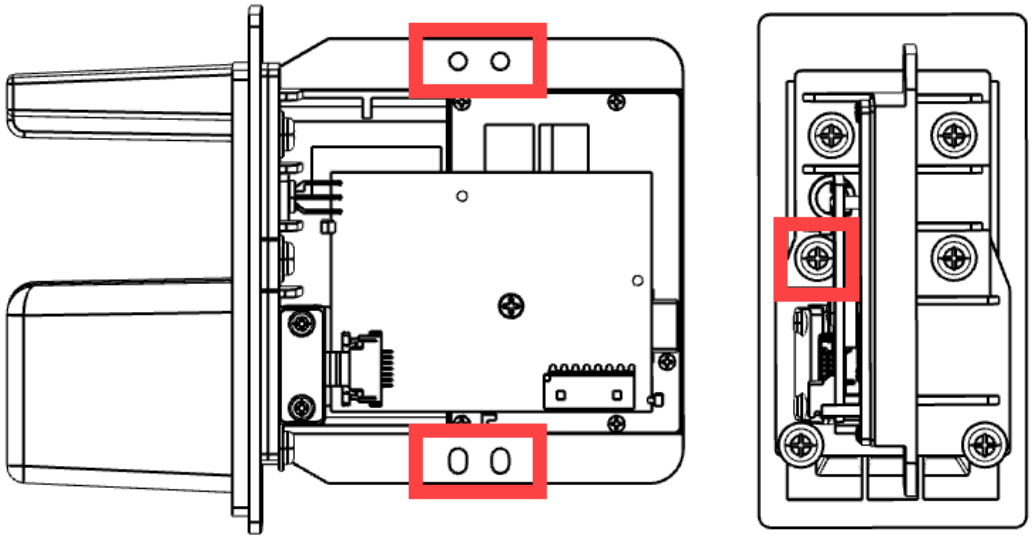
- Mount the reader vertically with the heads up so fluids do not collect in the bezel.
- Mount the reader at a slight angle (with the slot angled downward) to allow for drainage.
- Place a gasket between the reader and mounting surface; tighten the reader firmly to prevent water from leaking through the mounting surface.
- See recommended panel cutout and mounting gasket pattern above.
- Use the four mounting holes or other customized mounting hardware to mount the reader.

Note: ID TECH does not recommend mounting Spectrum Air readers horizontally; doing so prevents effective water drainage. However, if you do require horizontal mounting, make sure to follow the mounting guidelines above.

4.3. Installing a Drain Wire

If you're experiencing a loss of communication with the Spectrum Air and suspect it could be related to ESD, grounding the chassis to earth ground will provide additional protection.

To ground the Spectrum Air, attach a drain wire to the Spectrum Air's frame at one of the points highlighted below using a M3.0x8mm screw and corresponding nut with M3x0.5mm thread, or to the screw securing the chassis to the bezel:



4.4. Interface

4.4.1. RS232 Interface

The reader is plugged into a DB9 connector on the host computer and the 5-volt power supply connected to the DC connector on the backside of the DB9 connector.

As a standard serial interface, the host must be configured to accept the data and perform the appropriate processing. For the RS232 interface device, the host application's RS-232 parameters (baud rate, Start/Stop characters, parity, and handshaking method) need to match those expected by the reader. The reader by default communicates at 38.4K BAUD, 8-bit, no parity, and 1-stop bit. The magnetic reader's output can be formatted with terminating characters and special preamble and/or postamble character strings to match the data format expected by the host.

4.4.2. USB CDC Interface

Plug the reader into a standard USB connector on the host computer. The "found new hardware" screen would pop up. Follow the prompts and install the USB CDC driver 80066803-004 Sftw; USBCDC inf;MM2;SM;MOIR;HIR;Win7. After the USB CDC driver is installed, the reader would be a virtual COM device.

4.4.3. USB HID Interface

Plug the reader into a standard USB connector on the host computer. The reader gets all needed power through the USB connector. The host will receive data from the reader as if it is coming from a USB HID device. The host must be configured and be running an application ready to accept and process the data from the reader.

4.4.4. USB HID Keyboard Interface

Plug the reader into a standard USB connector on the host computer and it should be ready to operate. The reader gets all needed power through the USB connector. The host will receive data from the reader as if it is coming from a USB keyboard.

5. Operation

5.1. Operating Procedure

The Spectrum Air is easy to operate. Make sure the reader is properly connected and receiving sufficient power. The green LED will indicate that it is ready to read. After a card is read, the green LED will light if the read was good; after a bad card read, the red LED will light for half a second. Note the LED changes immediately after the MSR is read in auto mode, but not until the host requests MSR in buffered mode (in normal operation these should be similar). The LED will be dark (that is off) when the MSR is being processed.

LED INDICATION	MEANING (LED controlled by reader)
Solid amber	Reader has not connected properly to the host.
Solid green	Reader is ready to read a magnetic stripe or is idle.
Slow flash green	Reader is in buffered mode but has not been armed to read.
Red for half second	Bad magnetic stripe read.
Off	Reader is decoding magnetic stripe data.

By default, the LED is under the control of the reader. The LED can also be under the control of the host application. If the LED is under the control of the host, the following settings are available:

- Turn the LED off (dark)
- Turn on the LED green, red or amber
- Set the LED flashing green, red or amber
- Set the LED slow flashing green, red or amber

5.2. Standard Mode (Automatic Transmit)

To read a Magnetic Stripe Card, follow these steps:

1. Insert the card into the reader until it hits a hard stop.
2. Withdraw the card in one continuous motion. The green LED will go off briefly. (The reader by default reads the card on insert and on withdrawal and combines these reads, but only sends the track data after withdrawal.)
3. When the card has been fully withdrawn, the LED will turn red (to indicate a bad read) or to green (to indicate a good read). The track data is automatically sent to the host.

5.3. Buffered Mode

Buffered mode is more complicated than standard mode; see the suggested steps below for buffered mode application.

When the unit is armed to read in buffer mode, decoded data is retained in reader memory and an optional notice is sent to the host to indicate its presence. Data is held in memory until the reader receives the next ARM TO READ or MSR RESET command, at which point all data in memory will be

erased. Refer to the specific in Buffered Mode Arm to Read [50 01 30], Buffered Mode MSR Reset Command, and Read MSR Data in Buffered Mode [51 01 xx] commands for more details.

In buffered mode, the LED is set to slowly flash green until the reader is armed to read, at which point it turns solid green. It remains green when the card track data is captured. When the host requests the buffered data, the LED will briefly go dark during track decode then return to slow flashing green if the read was successful; if the read was unsuccessful the LED turns red for .5 second and remain at slow flashing green until it is rearmed. In normal operation the host will arm to read before the patron tries to use the reader and will request the card track data immediately after the card is read so the LED will be green for a successful read or red for an unsuccessful read. It will then revert to solid green because the host immediately arms the reader to read the next card.

5.3.1. Suggested steps for buffered mode application

1. Run **53 1A 01 32** to set the reader to buffered mode (it only needs to be set one time; use Configurator software, not in regular application; the result will be stored in EEPROM).
    a. The LED will slowly fash green.
2. Run **50 01 30** to arm the reader to read.
    a. The LED turns solid green, indicating that it's ready to read a card.
3. Prompt the user to insert and remove a card.
    a. The LED stays a solid green and the card track data was captured.
    b. By default, the reader sends out the statuses for card inserted, card removed, and mag data present.
    c. The host can discover the state of the reader by one of two methods:
        i. The host can wait for the reader to report that it has mag data buffered (from the mag data present status) then request that data
        ii. The host can poll the reader for the track data.
4. Poll for Read Buffered Data.
    a. Run **51 01 30** to read any track data (Or **51 01 3X** if for a specific track).
    b. The LED turns off while the card track data is processed.
    c. The LED turns RED for .5 seconds if any of the required tracks are bad or there is data on an optional track that did not decode properly.
    d. The LED slowly flashes green otherwise and holds this setting until the reader is rearmed or put into auto mode.
5. Process the data.
6. Display proper notification to user.
7. Go back to step 2 for next the read.

6. Specification

Physical dimensions	120mm x 92mm x 48mm (LxWxH with bezel)	
Environments	Operating Temperature	-20 °C to 70 °C (-4 °F to 158 °F)
	Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
	Operating humidity	10% to 90% (no condensation allowed)
	Storage humidity	10% to 90% (no condensation allowed)
Magnetic Reading	Reading direction	Insertion/Withdrawal
	Life of magnetic heads	1,000,000 operations minimum
	Media Thickness	0.76mm (tolerance +- 0.08mm)
	Swipe Speed	3 to 60 ips
	ESD	+- 8kV air discharge, contact +- 4kV
Cable	CAB1041-1 (drawing PN 80028211) for RS232 interface 80035212-002 for USB interface	
Agency Approval	FCC Class A, CE, RoHS	
Power	Input Voltage (Vin)	DC +4.5V~ +5.5V Maximum Input
	DC +6V	
	Power Consumption	< 20mA @ Vin = +5V

6.1. Interfaces, signals and main components

6.1.1. USB

P1	Signal	Description
1	Chassis GND	Chassis Ground
2	--	--
3	D+	USB Data +
4	--	--
5	Vin	Power Input: 5V
6	D-	USB Data -
7	GND	Power Ground

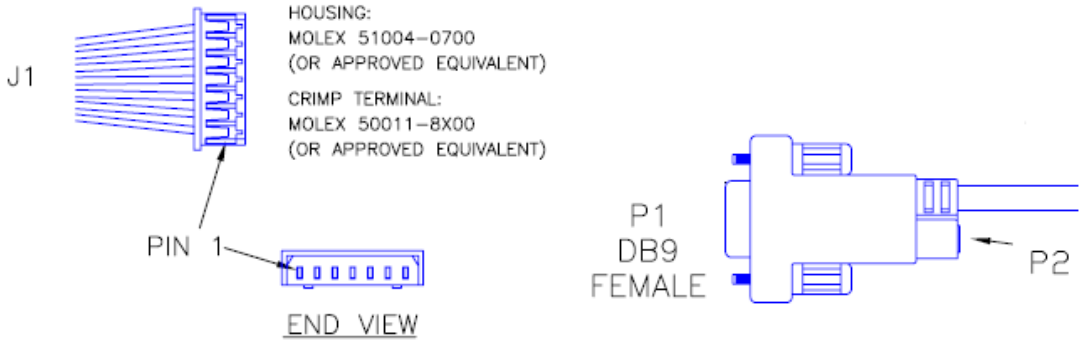
6.1.2. RS232

P1	Signal	Direction	Description
1	Chassis GND	--	Chassis Ground
2	TXD	OUT	Transmit Data: RS232 Signal
3	RXD	IN	Receive Data: RS232 Signal
4	Vin	--	Power Input: 5V
5	--	--	--
6	--	--	--
7	GND	--	Power Ground

7. Connector Pinout

7.1. RS232 Interface

Cable part number: CAB1041-1 (drawing PN 80028211)



7.1.1. Wire Connection

J1	Signal	P1	P2
1	Chassis GND	SHELL	-
2	TXD	2	
3	RXD	3	
4	Vin	-	PIN
5	RTS	8	
6	CTS	7	
7	GND	5	SLEEVE

7.1.2. PCA PIN Assignment

P1	Signal
1	CHASSIS GND
2	TXD
3	RXD
4	Vin
5	--
6	--
7	GND

7.1.3. FPC Interface

P2	Magnetic Head Signal	Description
1	T1A	Magnetic head input A (+) track 1
2	T1B	Magnetic head input B (-) track 1
3	T2A	Magnetic head input A (+) track 2
4	T2B	Magnetic head input B (-) track 2
5	T3A	Magnetic head input A (+) track 3
6	T3B	Magnetic head input B (-) track 3
7	Chassis GND	Power Ground

7.1.4. LED Interface

LED1	Signal
1	Red
2	GND
3	Green

7.1.5. Molex-Compatible Parts

The following parts are compatible with the Molex housing and crimp terminal listed above.

Molex 51004-0700-compatible housings:

- Ever connector/ECI 2040H-07
- Joint Tech/HR A2002H-07P
- Tarng Yu/TYU TU2002HNO-07
- Zhiji A2002H-7P

Molex 50011-8X00-compatible crimp terminals:

- Ever connector/ECI 2040-P
- Joint Tech/HR A2002-TPE
- Tarng Yu/TYU TU2002TPO-A
- Zhiji A2002-TPE

8. Security Features

The Secure MIR Reader features configurable security settings. Before encryption feature can be enabled, Key Serial Number (KSN) and Base Derivation Key (BDK) must be loaded before encrypted transactions can take place. The keys are to be injected by certified key injection facility.

There are five security levels available on the reader:

- **Security Level 0:** Security Level 0 is a special case where all DUKPT keys have been used (exhausted) and is set automatically when it runs out of DUKPT keys. The lifetime of DUKPT keys is 1 million. After the key's end of lifetime is reached, user should inject DUKPT keys again.
- **Security Level 1:** By default, non-secure readers from the factory are configured to have this security level. There is no encryption process, no key serial number transmitted with decoded data. The reader functions as a non-encrypting reader.
- **Security Level 2:** Key Serial Number and Base Derivation Key have been injected but the encryption process is not yet activated. The reader would send out decoded track data in default format, the same as security level 1.
- **Security Level 3:** By default, secure readers from the factory have this security level. Both Key Serial Number and Base Derivation Keys are injected and encryption mode is turned on. For payment cards, both encrypted data and masked clear text data are sent out. Users can select the data masking area; and the encrypted data format.
- **Security Level 4:** When the reader is at Security Level 4, a correctly executed Authentication Sequence is required before the reader sends out data for a card. Commands that require security must be sent with a four-byte Message Authentication Code (MAC) at the end. Note that data supplied to MAC algorithm should NOT be converted to ASCII-Hex, rather it should be supplied in its raw binary form. Calculating MAC requires knowledge of current DUKPT KSN, this could be retrieved using Get DUKPT KSN and Counter command.

Default reader properties are configured to have security level 1 (no encryption). In order to output encrypted data, the reader has to be key injected with encryption feature enabled. After the reader has been configured to security level 2, 3 or 4, it cannot be reverted to a lower security level.

8.1. Encryption Management

The Encrypted read supports TDES and AES encryption standards for data encryption. Encryption can be turned on via a command. TDES is the default.

If the reader is in security level 3, for the encrypted fields, the original data is encrypted using the TDES/AES CBC mode with an Initialization Vector starting at all binary zeroes and the Encryption Key associated with the current DUKPT KSN.

8.1.1. Security Management

This reader is intended to be a secure reader. Security features include:

- Can include Device Serial Number
- Can encrypt track 1, track 2, and track 3 data for bank cards and other cards
- Provides clear text confirmation data including card holder's name and a portion of the PAN as part of the Masked Track Data for bank cards
- Optional display expiration date
- Security Level is settable
- By default setting (See AF) will allow and encrypt Samsung Pay Reader transaction (added with Version V2.89).

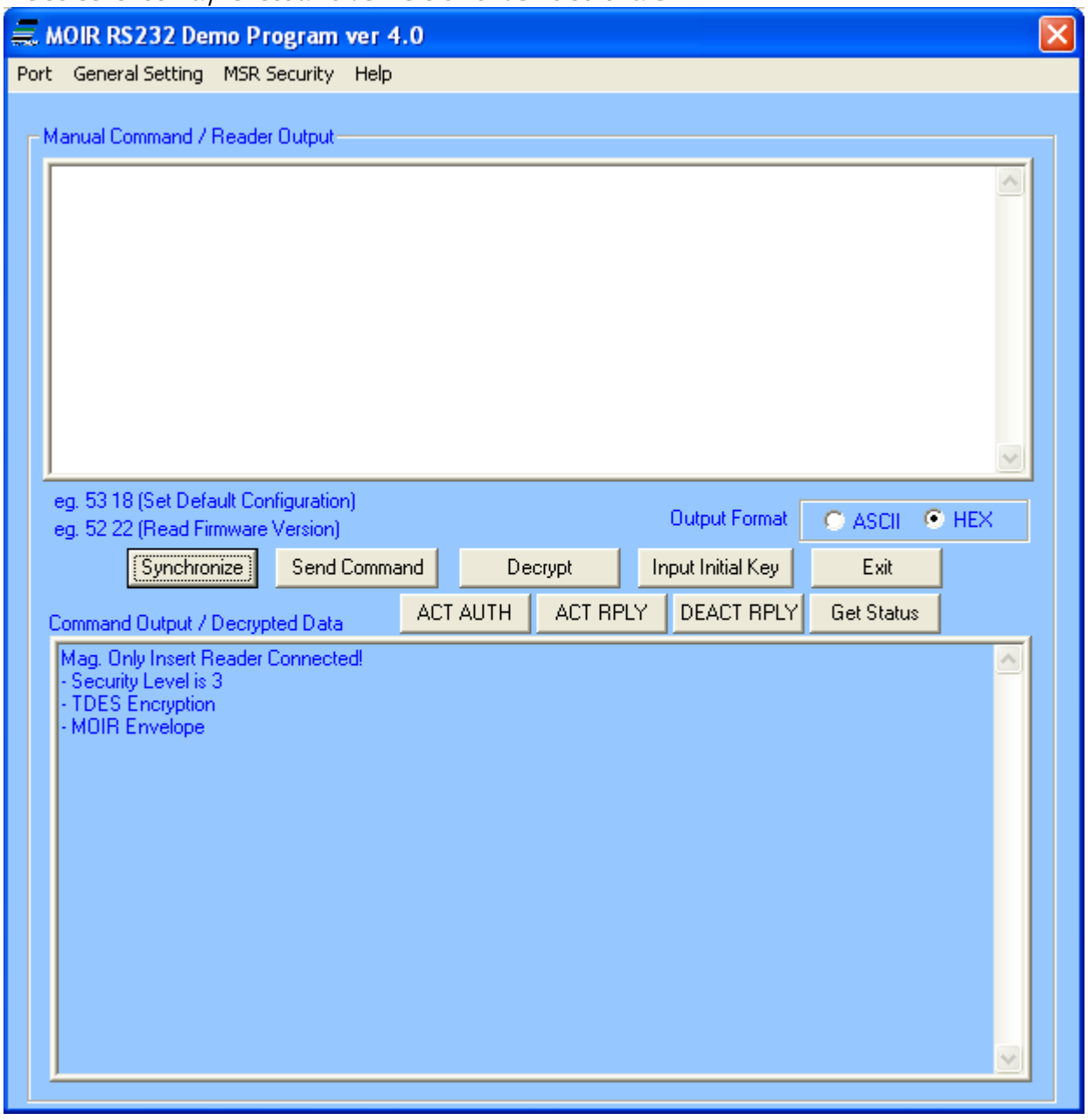
The reader features configurable security settings. Before encryption can be enabled, Key Serial Number (KSN) and Base Derivation Key (BDK) must be loaded before encrypted transactions can take place. The keys are to be injected by certified key injection facility.

9. Using the Demo Program

The Spectrum Air reader uses the same demo software as the SecureMIR reader. The demo software is provided to demonstrate features of the Encrypted MSR. It supports decrypting the encrypted data and sending command to MSR.

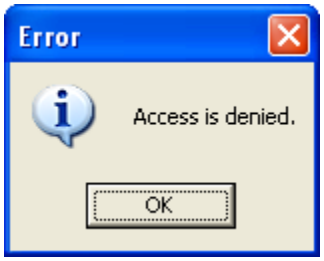
9.1. Secure MIR Demo Overview

The screenshot may reflect an older version of demo software.



The "Synchronize" button allows the demo program to query the reader determine its security/communication setting and "synchronize" to the readers setting. This button does not determine every possible reader feature such as baud rate, it assumes the reader is able to communicate with the demo program.

When the RS232 demo starts up, it attempts to open COM 1 and connect to the reader.



If this dialog box displays, COM 1 was either not installed or already in use. Just select the correct port under the port tab and you should be connected to the reader. A check mark next to the port and to open indicates that the port is connected.

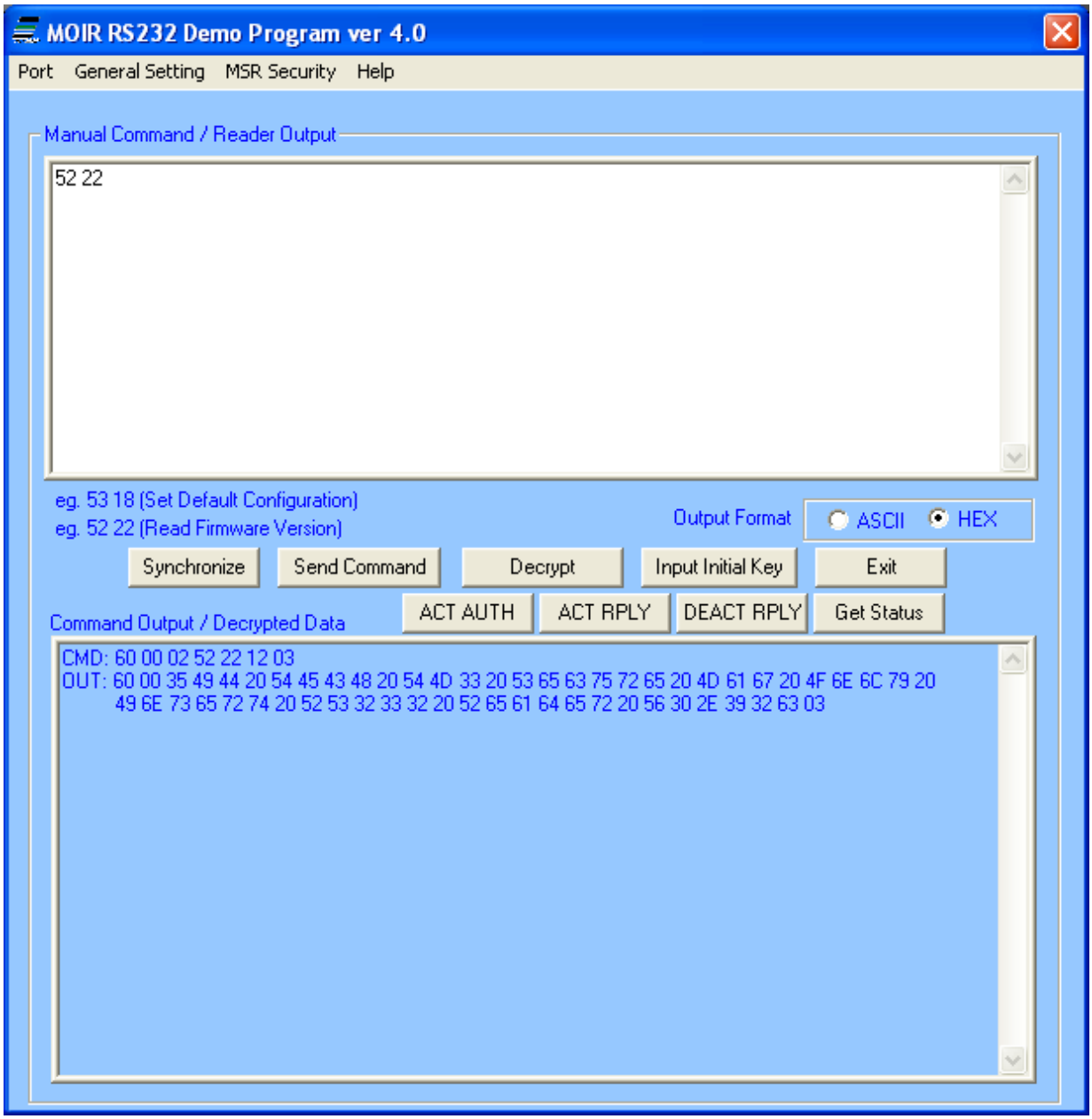
9.2. Manual Command

The demo software allows users to manually input and send commands to the device. Type the <Command Data> in the field, and the command will be sent

Commands are sent out in the following structure:
60 00 <LenL><Command_Data><LRC> 03

- <Command_Data>: Please refer to Appendix A for a complete list of commands
- <LRC> is a one-byte Xor value calculated for the above data block from <STX> to <ETX>
- e.g. 60 00 02 53 18 4A 03 (Set Default Configuration)
- e.g. 60 00 02 52 22 71 03 (Read Firmware Version)

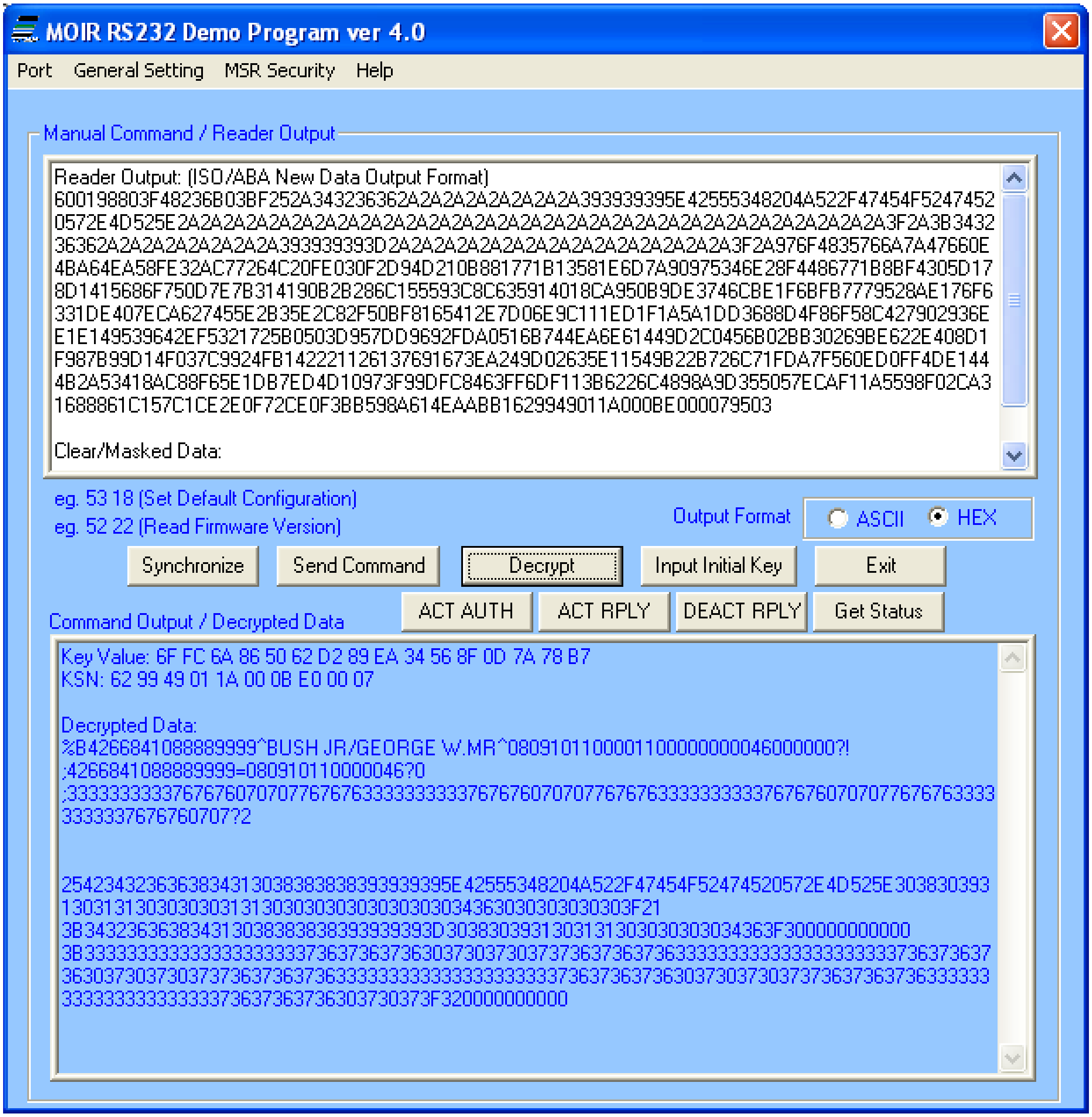
Press **Send Command** and the input and output are shown in the lower text box.



9.3. Security Level 3 Decryption

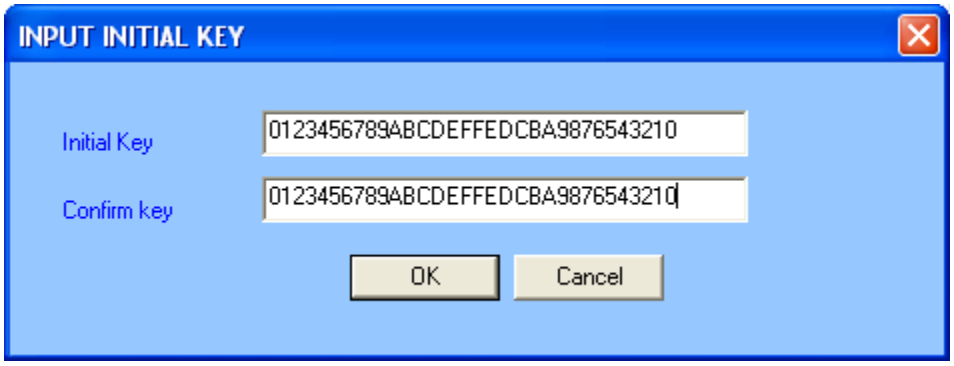
The encrypted data will show in the Manual Command / Encrypted Data textbox after a card is inserted and/or removed. By default, the cursor is in Manual Command / Encrypted Data textbox

NOTE: In order to allow the demo to know that the reader is in secure mode, select the **Synchronize** button. The decrypt button will not work until this is done unless the demo is configured to match the reader.

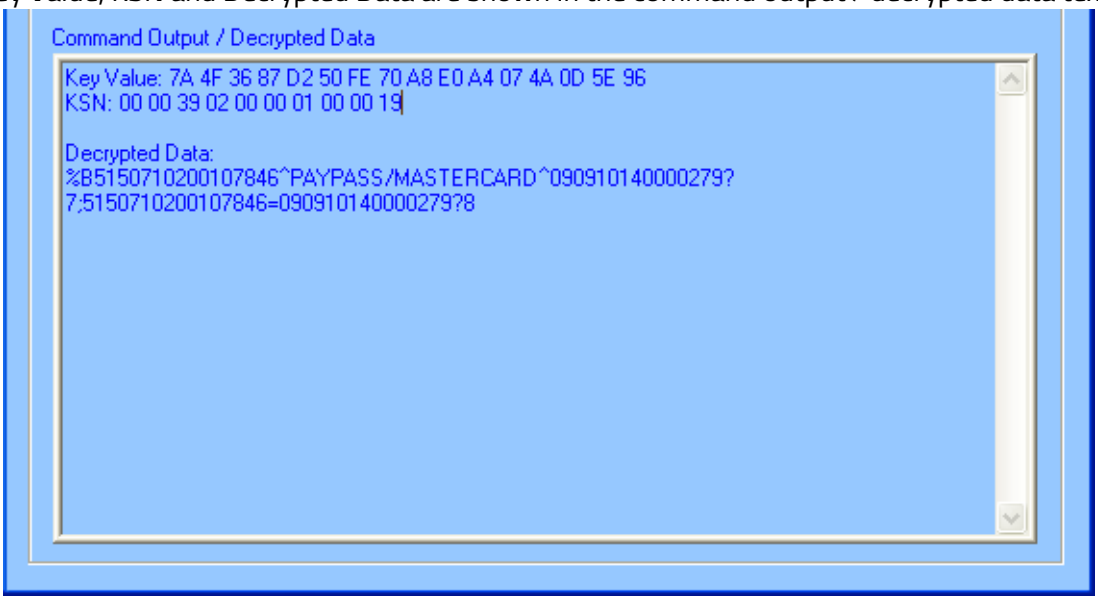


To get the decrypted data, press the **Decrypt** button and the decrypted card data will be displayed in the lower box.

The default initial key is 0123456789ABCDEFFEDCBA9876543210. If the reader is programmed with a user-defined key, load the same key to the demo software by pressing the **Input Initial Key** button. Type the initial key in the box and press **OK** when finished.



The Key Value, KSN and Decrypted Data are shown in the command output / decrypted data textbox.



9.4. Security Level 4 Features and Decryption

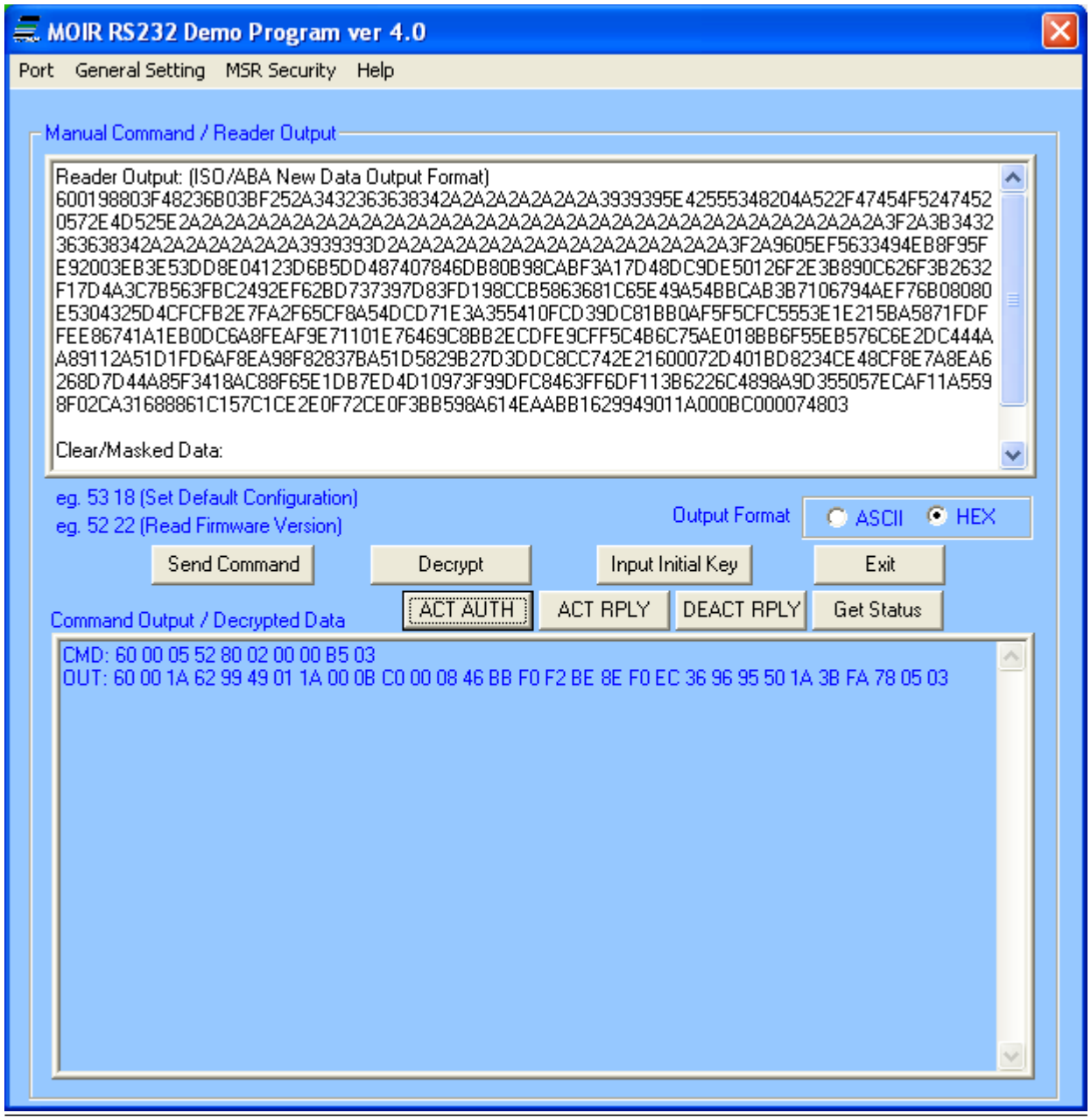
When the reader is set to security level 4, an authentication process is required to capture and decode the data from a card insertion or removal.

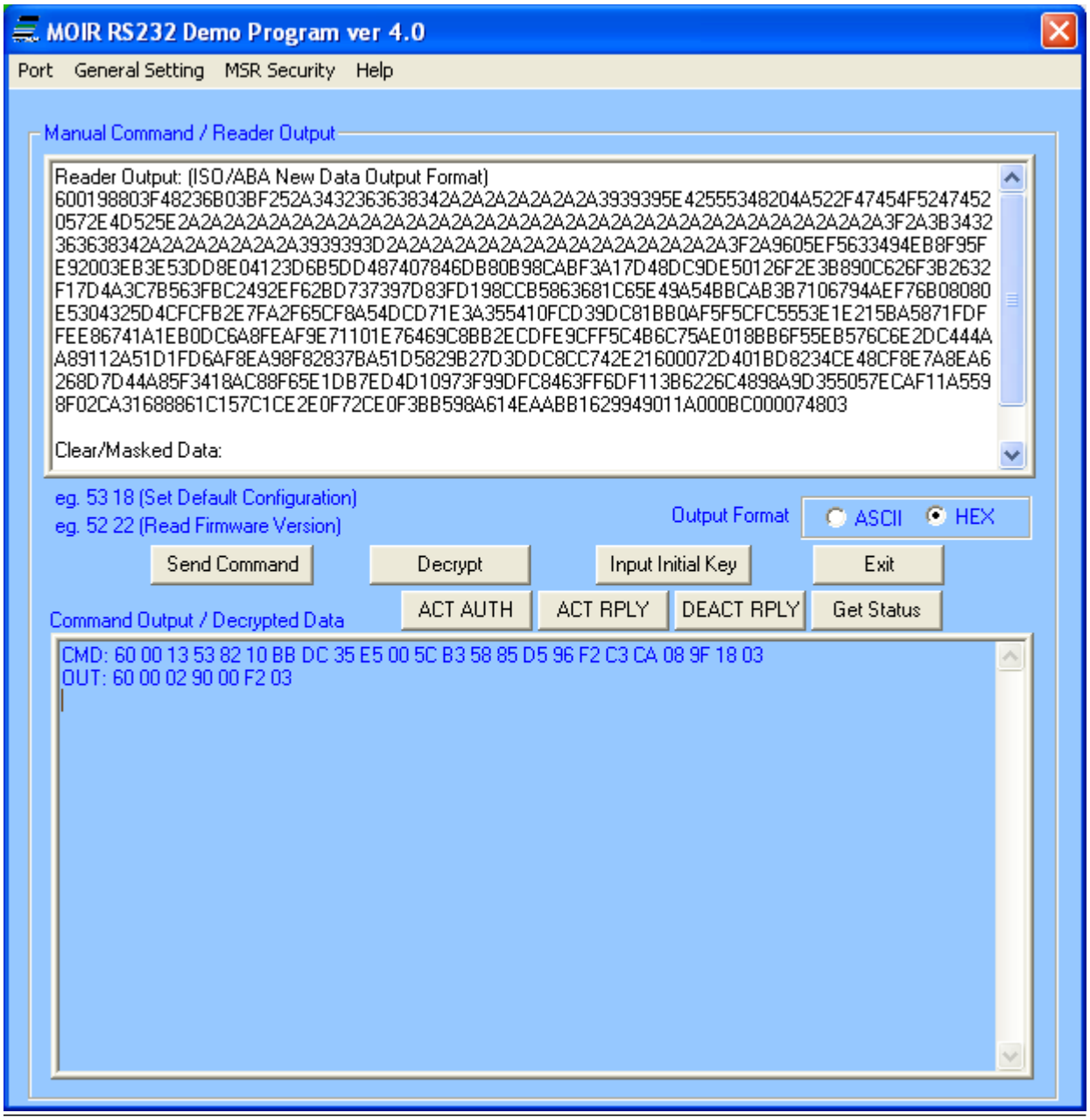
9.4.1. Activate Authentication Command

The **ACT AUTH** button sends the Activate Authentication Command. To enable card track data capture in security level 4, first click the **ACT AUTH** button. Then go to the Activation Challenge Reply Command.

9.4.2. Activation Challenge Reply Command

Click the **ACT REPLY** button after an Activate Authentication Command is sent. After receiving an <ACK> (06h), the reader is ready to receive a card insertion and/or removal.





9.4.3. Deactivate Authentication Mode Command

Clicking the **DEACT RPLY** button exits or cancels the authenticated mode.

9.4.4. Get Status

The **Get Status** button gives the reader activation status and precondition in this format:
<83h><02h><Current Reader Status><Pre-condition>

For example, 60 00 02 83 02 02 LRC 03 represents:

- Reader Status: the reader is waiting for a card insertion and/or removal
- Pre-condition: authentication mode was activated successfully. The reader processed a valid Activation Challenge Reply command.

For more details on the authentication process, please refer to Section 10.5 of the manual.

9.5. Reader Operations

The demo software can be used to display the card data and send reader commands. To view the card data on screen, place the cursor in the "manual command/ reader output" text box and insert and/or remove the card. To send a reader command, type the appropriate command in the text box and press the **Send Command** button.

9.5.1. General Setting

Provide options such as reader default settings, firmware version, and buffered mode options.

9.5.2. MSR Security

The security is enabled by selecting TDES or AES. After the encryption is enabled, the reader cannot be changed back to non-encrypted mode.

9.5.3. Port

Select Com port and open/ close port.

9.5.4. Help

Provides version information of the demo software.

10. Appendix A: Key Code Table in USB Keyboard Interface

For most characters, "Shift On" and "Without Shift" will be reverse if Caps Lock is on. Firmware needs to check current Caps Lock status before sending out data.

For Function code B1 to BA, if "Num Lock" is not set, then set it and clear it after finishing sending out code.

For Function code BB to C2, C9 to CC, if "Num Lock" is set then clear it and set it after finishing sending out code.

Keystroke	Hex Value	Functional Code	USB KB Code
Ctrl+2	00		1F Ctrl On
Ctrl+A	01		04 Ctrl On
Ctrl+B	02		05 Ctrl On
Ctrl+C	03		06 Ctrl On
Ctrl+D	04		07 Ctrl On
Ctrl+E	05		08 Ctrl On
Ctrl+F	06		09 Ctrl On
Ctrl+G	07		0A Ctrl On
BS	08	\bs	2A
Tab	09	\tab	2B
Ctrl+J	0A		0D Ctrl On
Ctrl+K	0B		0E Ctrl On
Ctrl+L	0C		0F Ctrl On
Enter	0D	\enter	28
Ctrl+N	0E		11 Ctrl On
Ctrl+O	0F		12 Ctrl On
Ctrl+P	10		13 Ctrl On
Ctrl+Q	11		14 Ctrl On
Ctrl+R	12		15 Ctrl On
Ctrl+S	13		16 Ctrl On
Ctrl+T	14		17 Ctrl On
Ctrl+U	15		18 Ctrl On
Ctrl+V	16		19 Ctrl On
Ctrl+W	17		1A Ctrl On
Ctrl+X	18		1B Ctrl On
Ctrl+Y	19		1C Ctrl On
Ctrl+Z	1A		1D Ctrl On
ESC	1B	\esc	29
Ctrl+\	1C		31 Ctrl On

Ctrl+]	1D		30 Ctrl On
Ctrl+6	1E		23 Ctrl On
Ctrl+-	1F		2D Ctrl On
SPACE	20		2C
!	21		1E Shift On
"	22		34 Shift On
#	23		20 Shift On
$	24		21 Shift On
%	25		22 Shift On
&	26		24 Shift On
'	27		34
(	28		26 Shift On
)	29		27 Shift On
*	2A		25 Shift On
+	2B		2E Shift On
,	2C		36
-	2D		2D
.	2E		37
/	2F		38
0	30		27 Shift On
1	31		1E Shift On
2	32		1F Shift On
3	33		20 Shift On
4	34		21 Shift On
5	35		22 Shift On
6	36		23 Shift On
7	37		24 Shift On
8	38		25 Shift On
9	39		26 Shift On
:	3A		33 Shift On
;	3B		33
<	3C		36 Shift On
=	3D		2E
>	3E		37 Shift On
?	3F		38 Shift On
@	40		1F
A	41		04 Shift On
B	42		05 Shift On
C	43		06 Shift On
D	44		07 Shift On
E	45		08 Shift On

F	46		09 Shift On
G	47		0A Shift On
H	48		0B Shift On
I	49		0C Shift On
J	4A		0D Shift On
K	4B		0E Shift On
L	4C		0F Shift On
M	4D		10 Shift On
N	4E		11 Shift On
O	4F		12 Shift On
P	50		13 Shift On
Q	51		14 Shift On
R	52		15 Shift On
S	53		16 Shift On
T	54		17 Shift On
U	55		18 Shift On
V	56		19 Shift On
W	57		1A Shift On
X	58		1B Shift On
Y	59		1C Shift On
Z	5A		1D Shift On
[	5B		2F
\	5C		31
]	5D		30
^	5E		23 Shift On
_	5F		2D Shift On
`	60		35
a	61		04
b	62		05
c	63		06
d	64		07
e	65		08
f	66		09
g	67		0A
h	68		0B
i	69		0C
j	6A		0D
k	6B		0E
l	6C		0F
m	6D		10
n	6E		11

o	6F		12
p	70		13
q	71		14
r	72		15
s	73		16
t	74		17
u	75		18
v	76		19
w	77		1A
x	78		1B
y	79		1C
z	7A		1D
{	7B		2F Shift On
|	7C		31 Shift On
}	7D		30 Shift On
~	7E		35 Shift On
DEL	7F		2A
F1	81	\f1	3A
F2	82	\f2	3B
F3	83	\f3	3C
F4	84	\f4	3D
F5	85	\f5	3E
F6	86	\f6	3F
F7	87	\f7	40
F8	88	\f8	41
F9	89	\f9	42
F10	8A	\fa	43
F11	8B	\fb	44
F12	8C	\fc	45
Home	8D	\home	4A
End	8E	\end	4D
→	8F	\right	4F
←	90	\left	50
↑	91	\up	52
↓	92	\down	51
PgUp	93	\pgup	4B
PgDn	94	\pgdn	4E
Tab	95	\tab	2B
bTab	96	\btab	2B Shift On
Esc	97	\esc	29
Enter	98	\enter	28

Num_Enter	99	\num_enter	58
Delete	9A	\del	4C
Insert	9B	\ins	49
Backspace	9C	\bs	2A
SPACE	9D	\sp	2C
Pause	9C	\ps	48
Ctrl+[	9F	\ctr1	2F Ctrl On
Ctrl+]	A0	\ctr2	30 Ctrl On
Ctrl+\	A1	\ctr3	31 Ctrl On
Left_Ctrl_Break	A2	\l_ctrl_bk	Clear Ctrl Flag
Left_Ctrl_Make	A3	\l_ctrl_mk	Set Ctrl Flag for following char(s)
Left_Shift_Break	A4	\l_shift_bk	Clear Shift Flag
Left_Shift_Make	A5	\l_shift_mk	Set Shift Flag for following
char(s)			
Left_Windows	A6	\l_windows	E3 (left GUI)
Left_Alt_Break	A7	\l_alt_bk	Clear Alt Flag
Left_Alt_Make	A8	\l_alt_mk	Set Alt Flag for following char(s)
Right_Ctrl_Break	A9	\r_ctrl_bk	Clear Ctrl Flag
Right_Ctrl_Make	AA	\r_ctrl_mk	Set Ctrl Flag for following char(s)
Right_Shift_Break	AB	\r_shift_bk	Clear Shift Flag
Right_Shift_Make	AC	\r_shift_mk	Set Shift Flag for following char(s)
Right_Windows	AD	\r_windows	E7 (right GUI)
Right_Alt_Break	AE	\r_alt_bk	Clear Alt Flag
Right_Alt_Make	AF	\r_alt_mk	Set Alt Flag for following char(s)
Num_Lock	B0	\num_lock	53
Num_0	B1	\num0	62 Num Lock On
Num_1	B2	\num1	59 Num Lock On
Num_2	B3	\num2	5A Num Lock On
Num_3	B4	\num3	5B Num Lock On
Num_4	B5	\num4	5C Num Lock On
Num_5	B6	\num5	5D Num Lock On
Num_6	B7	\num6	5E Num Lock On
Num_7	B8	\num7	5F Num Lock On
Num_8	B9	\num8	60 Num Lock On
Num_9	BA	\num9	61 Num Lock On
Num_Home	BB	\num_home	5F
Num_PageUp	BC	\num_pgup	61
Num_PageDown	BD	\num_pgdn	5B
Num_End	BE	\num_end	59
Num_ ↑	BF	\num_up	60

Num_→	C0	\num_right	5E
Num_ ↓	C1	\num_down	5A
Num_←	C2	\num_left	5C
Print_Scrn	C3	\prt_sc	46
System_Request	C4	\sysrq	9A
Scroll_Lock	C5	\scroll	47
Pause	C6	\menu	76
Break	C7	\break	
Caps_Lock	C8	\caps_lock	39
Num_/	C9	\num_/	54
Num_*	CA	\num_*	55
Num_-	CB	\num_-	56
Num_+	CC	\num_+	57
Num_.	CD	\num_.	63 Num Lock On
Num_DEL	CE	\num_del	63
Num_INS	CF	\num_ins	62
Delay_100ms	D0	\delay	Delay 100 ms

10.1. Table of Ctrl or Alt output for non-printable characters

ASCII Code	Control Code	Alt Code
SendOptionID	Bit 3: 0	Bit 3: 1
00:	Ctrl-2	Alt-000
01:	Ctrl-A	Alt-001
02:	Ctrl-B	Alt-002
03:	Ctrl-C	Alt-003
04:	Ctrl-D	Alt-004
05:	Ctrl-E	Alt-005
06:	Ctrl-F	Alt-006
07:	Ctrl-G	Alt-007
08:	BS	Alt-008
09:	Tab	Alt-009
0A:	Ctrl-J	Alt-010
0B:	Ctrl-K	Alt-011
0C:	Ctrl-L	Alt-012
0D:	Enter	Alt-013
0E:	Ctrl-N	Alt-014
0F:	Ctrl-O	Alt-015
10:	Ctrl-P	Alt-016
11:	Ctrl-Q	Alt-017
12:	Ctrl-R	Alt-018

13:	Ctrl-S	Alt-019
14:	Ctrl-T	Alt-020
15:	Ctrl-U	Alt-021
16:	Ctrl-V	Alt-022
17:	Ctrl-W	Alt-023
18:	Ctrl-X	Alt-024
19:	Ctrl-Y	Alt-025
1A:	Ctrl-Z	Alt-026
1B:	ESC	Alt-027
1C:	Ctrl-\	Alt-028
1D:	Ctrl-]	Alt-029
1E:	Ctrl-6	Alt-030
1F:	Ctrl--	Alt-031

11. Appendix B: Envelope Drawings

unit: mm, general tolerance: ±0.2mm