USER MANUAL

SecureMOIR

Encrypted Magnetic-Only Insert Reader

RS232, USB HID, USB CDC, And USB HID Keyboard, Interface

80117501-001-D
4/1/2021

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.

Revision History

Revision	Date	Description of Changes	By
50	05/24/2010	Initial Draft	Jenny W
	11/01/2010	Many updates throughout whole document	Bruce K
	11/02/2010	Removed reference to NGA protocol	Bruce K
	11/04/2010	Added Limitations no USB HID, MagTek support.	Bruce K
	11/05/2010	Added note on buffered mode with security level 4	Bruce K
	11/19/2010- 11/30/2010	Made corrections found during DVT	Bruce K
	12/01/2010- 12/09/2010	Made corrections found during DVT	Bruce K
	12/16/2010- 12/17/2010	Enhanced LED handling description and buffered mode support	Bruce K
	12/20/2010- 12/21/2010	Corrections and enhancements throughout document	Bruce K
	01/07/2011	Added OPOS Error byte definition	Bruce K
A	06/07/2011	Initial Release	Jenny W
B	10/24/2013- 3/14/2014	Add optional serial number in output Add field 8 and field 9 explanation enumeration SN and special terminator CRLF Clarify config 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	Candy H
C	2/4/2015	Re-organized the user manual structure and contents Add 30 and 31 commandID Add 32 command ID Change MOIR protocol to TLP Change NGA protocol to ITP	Candy H
D	4/1/2021	Added definition for Custom Equipment Settings Byte 1C bit 4	CB

Table of Contents

1 INTRODUCTION

The ID TECH SecureMOIR is an insert magnetic stripe reader with encryption capability. It can be configured to read 1, 2, or 3 tracks of magnetic stripe data from cards conforming to ISO 7810 and 7811 standards. The reader is offered in different communication interfaces including RS232, USB HID, USB HID KB, and USB CDC interface. All versions are described in this User's Manual. The reader can be configured via different interfaces.

Please note there are a couple of features which are not supported on this reader as listed below:

- This reader does not support report on withdrawal in buffered mode or when reading raw track data, in these cases it reverts to read on withdrawal.
- Doesn't support obsolete California Driver License format.

2 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 Drivers 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
FC	Flexible Circuit
FCC	Federal Communications Commission
GND	Signal Ground
Hex	Hexadecimal
HID	Human Interface Device
IPS	Inches per Second
ITP	ID TECH Transport Protocol
ISO	International Organization for Standardization
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
MSB	Most significant Bit
msec	Milliseconds
MSR	Magnetic Stripe Reader
mV	Millivolts
NACK	Non-acknowledge
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
TLP	Turbo Transport Layer Protocol-224
USB	Universal Serial Bus
UV	Ultra Violet – spectrum of light rays

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 RELATED DOCUMENTS

ISO 7810 Identification Cards - Physical Characteristics (1995)
ISO 7811 Identification Cards -Recording Technique (1995)
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

Supported Programs

SecureMOIR RS232 Demo Program
SecureMOIR USB Demo Program
SecureMOIR Configuration Program

4 INSTALLATION

4.1 RS232 Interface

The reader is plugged into a DB9 COM port on the host computer and the 5-volt power supply connected to the DC connector on the backside of the DB9 connector if using the cable provided by ID TECH.

As a standard serial interface, the host must be configured to accept data and perform the appropriate processing. For the RS232 interface device, the host application's RS232 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.

4.2 USB HID Interface

Plug the reader into a standard USB connector on the host computer. The reader is powered 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. No additional driver needs to be installed on Windows systems as the host will install the driver automatically and recognize the device.

4.3 USB Keyboard Interface

Plug the reader into a standard USB connector on the host computer and it will be ready to operate. The reader is powered through the USB connector. The host will receive data from the reader as if it is coming from a USB keyboard. No driver needs to be installed on the host as the host will install the driver and recognize the driver by itself. The USB Keyboard interface will emulate the keyboard and output the data automatically to any text field.

4.4 USB CDC Serial Interface

Plug the reader into a standard USB connector on the host computer. The reader is powered through the USB connector. The host must be configured and be running an application ready to accept and process data from the reader. Note the CDC reader functions identically to the serial reader as far as host application software is concerned. Driver needs to be installed to recognize the device. The CDC driver download link is: http://www.idtechproducts.com/download/insert-readers/cat_view/95-insert-readers/457-securemoir/515-usbcdc/516-driver.html

5 OPERATION

5.1 Operating Procedure

The SecureMOIR 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 and 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 is not connected properly to the host
Solid Green	Reader is ready to read a magnetic stripe, or is idle. The LED will turn green after reading a magstripe card to indicate a good read
Red for half second	Bad magnetic stripe read
Flashing Amber	The LED will flash amber on start-up if the configuration of EEPROM has a problem
Flashing Red	DUKPT key is exhausted (a million secure card transactions)
Slow Flashing Green	Reader in buffered mode, but not to armed to read
Off	Reader is decoding magnetic stripe data or powered off

LED handling can be under the control of the reader or under the control of the host computer. The default operation is to have the LED under the control of the reader. To switch to LED controlled by host, please see 7.3.3 command for detailed information

If the LED is under the command of the host, the following settings are available.

- Turn the LED off
- Turn the LED on Green
- Turn the LED on Red
- Turn the LED on Amber
- Set the LED to Green flashing
- Set the LED to Red flashing
- Set the LED to Amber Flashing
- Set the LED to flashing Red and Amber alternatively
- Set the LED to slow flashing Green
- Set the LED to slow flashing Red
- Set the LED to slow flashing Amber

Flashing rate is approximately .25 seconds on and .25 seconds off. Regardless of whether the LED is under the command of the host it will still signal certain errors and start up conditions. If there is a problem on first start up with configuring the EEPROM, the LED will hang flashing amber. In the slow flash mode, the reader lights the LED for .12 seconds every 3 seconds.

5.2 Standard Mode (Automatic Transmit)

To read a Magnetic Stripe Card, follow these simple steps:

1. Insert the card with magnetic stripe facing down into the reader until it hits a hard stop (reader is mounted as mounting instruction in Appendix D).
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

When the unit is armed to read in buffer mode, decoded data is retained in reader memory and a magnetic data present notification 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. Please refer to the Buffer Mode Arm to Read Command (section 7.4.6), MSR RESET IN BUFFER MODE (section7.4.7), and READ MSR DATA IN BUFFER MODE (section 7.4.8) commands. In buffered mode, the LED is set to slow flashing green until the reader is armed to read, then 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, or turn red for .5 second if the read was unsuccessful. It will 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.

This mode requires more steps to read card data, please refer to the steps listed below:

1. Set reader to buffered mode (It only needs to be set once; use Configuration software, not in regular application; the result will be stored in EEPROM).
   53 1A 01 32
   The LED will turn to a slow green flash.
2. Arm to read
   50 01 30
   The LED will turn green indicating okay to read a card.
3. Prompt the user to insert and remove a card
   The LED will stay green but card track data was captured.
   The reader by default will send out the card inserted, card removed and mag data present statuses.
   The host can discover the state of the reader by one of two methods, 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 or the host can poll the reader for the track data.
4. Poll for Read Buffered Data
   51 01 30 for any track data (Or 51 01 3X if one requires specific track data)
   The LED will turn off while the card track data is processed.
   The LED will turn RED for .5 seconds if any of the required tracks were bad or there was data on an optional track that did not decode properly. The LED will turn slow flashing

green otherwise. The LED will hold 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 read.

5.4 Auto Buffered Mode

The auto buffered mode is similar to buffered mode. The difference is that in auto buffered mode, when you request the buffered track data, the reader sends the data to the host, then it immediately clears the buffer and rearms the reader to capture the next card read.

6 SPECIFICATION

Power Consumption

- 5VDC +/- 10%
- Operating Current: 45 mA maximum for three tracks of magnetic data
- RS232 interface – 5V external power adaptor supplies power
- USB interface – from host interface. No external power adaptor needed.

Card Insertion / Removal Speed

- 3 to 65 inches per second
- Bi-directional

Indicators

- Tri-color LED
  - Red indicates bad read
  - LED off while decoding MSR or no power
  - Green indicates good read, and ready to read
  - Amber indicates communication not established (PC/SC or USB)

Communication Interfaces

- RS232
  - Baud Rate – 1200, 2400, 4800, 9600, 19200, **38400**, 56700, 115200
  - Data bits – **8**
  - Stop bits – **1** or 2
  - Parity – **none**, odd, even, mark or space
  - Supports RTS/CTS hardware and Xon-Xoff software handshaking but off by default.
- USB
  - Complies with USB 2.0 specification
  - USB HID
  - USB HID Keyboard
  - USB CDC

Card Size

- Supports cards that meets the ISO 7810 and 7811 1-7 standards
- Minimum card thickness: 0.010 inches (0.254mm)
- Maximum card thickness: 0.033 inches (0.838mm)

Dimension

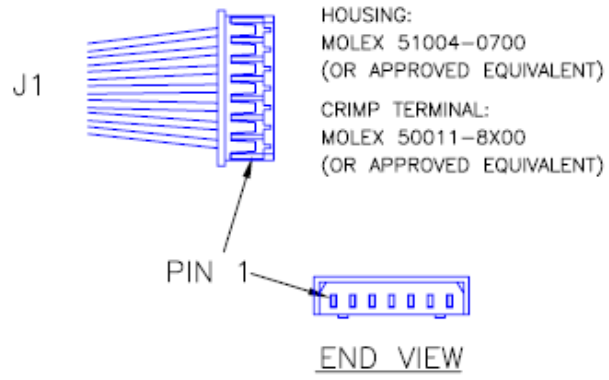
- Standard Bezel Length: 4.64 inches (117 mm). Width: 3.97 inches (101 mm). Height: .389 inches (9.88 mm)
- Compact Bezel Length: 4.2 inches (107.3 mm). Width: 2.5 inches (63 mm). Height: .87 inches (22.2 mm)
- Flush-Mount Bezel Length: 4.3 inches (109.2 mm). Width: 2.75 inches (69.9 mm). Height: 2.75 inches (69.9 mm)

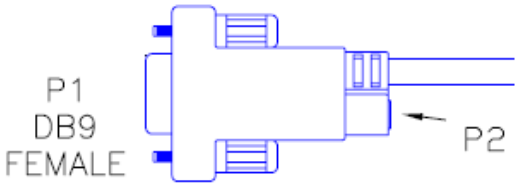
Mounting

- The reader is mounted using front flange, side mount studs, or both. The reader should be mounted with the debris slot facing down. Please refer to the mounting drawing in Appendix D.

Interface Cable and Connector

- RS232 interface
  - IDTECH standard RS232 Interface Cable (P/N: CAB 1041-1)
  - DB-9 Female connector with 2mm power jack in the housing
  - Standard cable length is 6 feet
  - Pin Out Table





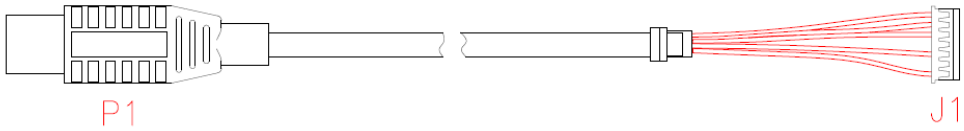
J1*	Color	Signal	P1*
1	Drain	CASE_GND	SHELL
2	White	TXD	2
3	Green	RXD	3
4	Yellow	VCC	from power jack
5	Brown	RTS	8**
6	Grey	CTS	4**
7	Black	GND	5

***J1 is the connector to PCB end and P1 is DB-9 end**
**** RTS and CTS are not used unless hardware handshaking support is enabled by Function ID 0x44 (Handshake)**

Header Description: Molex P/N: 51004-0700

- USB interface
  - IDTECH standard USB interface cable (P/N: 80035212-002)
  - Series “A” plug

- Standard cable length is 6 feet
- Pin Out Table



J1	Color	Signal	P1
1	Drain	CASE_GND	SHELL
3	Green	+DATA	3
5	Red	V_IN	1
6	White	-DATA	2
7	Black	GND	4

- Power Adapter (RS232 Units only)
  5V, 500mA
  Polarity: Inside (+)
  Warning: Any power supply (VCC) higher than 5.5 V may damage the unit

Environmental

Operating Temperature: 32°F to 140°F (0°C to 60°C)
Storage Temperature: -40°F to 140°F (-40°C to 60°C)
Humidity: Maximum 95% non-condensing
Vibration & Shock Sweep 10Hz to 50Hz/min; 294 m/s^2(30G)

Durability

Magnetic Head 500,000 card cycles
Chassis & Bezel 500,000 card cycles
Switch operations 500,000 card cycles
Magnetic Read Data: Less than one error in 500,000 bits on cards encoded with a short field to ISO 7811 1-5.

Electronics MTBF

Calculated MTBF for electronics is 300,000 POH based on Bellcore standard.
Electro-Static Discharges (ESD Meets or exceeds IEC 1000-4-2)
Electronics must survive ESD of 6kV contact & 12kV air discharge.

Materials

Plastic body meets UL94V-0 flammability rating

Outputs

CMOS levels (TTL) 0 to 5 VDC (TTL Magstripe Clock & Date format)
CARD Seated sensor CMOS output, low level when sensor is activated

CARD Present sensor	CMOS output, low level when sensor is activated
RS232	Serial interface
USB	USB interface

Agency Approvals

RoHS, FCC Class-B, UL, CE

7 COMMAND PROCESS

There are two protocols for the SecureMOIR. One is the TLP (Turbo Transport Layer Protocol-224), the other is ITP (ID TECH Transport Protocol). These two protocols have different HEADER and TRAILER, but share the same DATA. Please note that the TLP was called "MOIR protocol" and ITP was called "NGA" in previous user manual versions. To choose the reader response protocol when the reader is first powered, just send command in the protocol which you want, and the SecureMOIR will respond in the same protocol as the commands. If no commands have been sent to the reader, for secure output the reader uses the setting of ITP bit. (See configuration byte 0x2F bit 4 in section 7.3.8)

7.1 TLP Protocol for Sending Commands and Receiving Responses

Every command and response follows the same basic structure:

HEADER	DATA	TRAILER

The HEADER consists of <60> followed by <Command Length>. The <Command Length> are two bytes: most significant then least significant byte. For the setting commands(command ID 0x53), the DATA often consists of the Command ID, Function ID, Function Length, and Function Data. For get setting commands (command ID 0x52), the DATA consists of the Command ID and one Functional ID. The TRAILER consists of <LRC> followed by <ETX>. The maximum size of length is 768 (including envelope bytes).

7.1.1 Send Setting Command

Command:

60<Command Length><Command ID>><FuncSETBLOCK1>…<FuncSETBLOCKn><LRC><ETX>
Each function-setting block <FuncSETBLOCK> has following format:
<FuncID><Len><FuncData>

Where:

<Command Length> = is a two-byte count of the bytes in the DATA field

<Command ID> = is a one byte value identifying a specific command ID. See section 7.3 for command ID list. Only '0', '1' or 'S' command IDs are allowed for the send setting commands.

<FuncID> = is a one byte Function ID, which identifies the particular function or settings affected

<Len> = is a one-byte length count for the data block "<FuncData>"

<FuncData> = is the data block for the function

<LRC> = See Calculation in section below

<ETX> = 03

7.1.2 Get Setting Command

This Get Setting Command will get the reader's current setting

Host Command ⟶ Reader
Response ⟵ Status

Command: 60<Command Length><Command ID><FuncID> <LRC><ETX>

Response: 60 <Length> [<Response Data>] <Status> <LRC><ETX>

Where:

<Length> = is a two-byte counter from <Response Data> to the end of <Status>.

<Command ID> = always 'R'

<Response Data> = is the data block associated with the Response.

<Status> is a two-byte value indicating the success or failure of a command.

The overall LRC (Modulus 2 = Exclusive OR) from 60 to LRC should be zero. See example of LRC calculation below.

7.1.3 Example of LRC Calculation

LRC = Longitudinal Redundancy Check. Calculated by taking 'Exclusive OR' (Modulus 2) of all characters preceding it, total with LRC is equal to zero.
For example, the following command means "Set <Send Option> to 0x30 value".
<60><00><04><53><19><01><30><1F><03>
<1F> is the LRC character.

It is derived from the following:

Characters	#1(binary)	#2 (binary)
<60>	0110	0000
<00>	0000	0000
<04>	0000	0100
<53>	0101	0011
<19>	0001	1001
<01>	0000	0001
<30>	0011	0000
<1F>	0001	1111 <Result of Exclusive OR>

7.1.4 Communication Timing

The maximum delay for a command to be written into the reader is per configuration. Typical delay is 5ms for one setting one configuration byte.

During the command processing time, the reader will not respond to a new command. The reader will accept a new command as soon as it has responded to the previous command.

Note: Maximum delay between two characters in a command is 100ms for USB CDC interface, 30ms for USB HID and 10ms for RS232.

During command processing or the reading of a magnetic stripe, the reader will not respond to a new command. The typical delay for the reader to respond to a setting command is less than 20ms with the exception that all settings are being reset to their default settings.

Once communication between the host and the reader has been established, sending the appropriate setup commands to the reader from the host application can enter changes into the reader's settings.

Please see the following sections for the explanations and examples of the proper format and command content to send commands to the reader. All commands and characters are expressed in hex format and contained in brackets.

7.2 ITP for Sending Commands and Receiving Responses

SecureMOIR also supports ITP which is a protocol compatible with SecureMag readers, SecureHead and other swipe readers. All the commands can be sent with a different HEADER and TRAILER as described below:

HEADER	DATA	TRAILER

The HEADER includes the <STX>. The TRAILER consists of the <EXT> and <LRC>. The command protocol is specified as below:

<STX><CommandID><FuncID><Len><FuncData><ETX><LRC>

7.2.1 Send Setting Command

The setting command is a collection of one or more function setting blocks and its format is as follows.
Command:
<STX><CommandID><FuncSETBLOCK1>…<FuncSETBLOCKn><ETX><LRC>
Response: <ACK> or <NAK> for wrong command (invalid funcID, length and value)

Each function-setting block <FuncSETBLOCK> has following format:
<FuncID><Len><FuncData>

Where:

<Command ID> is a one byte value identifying a specific command ID. See section 7.3 for command ID list. Only '0', '1' or 'S' command IDs are allowed for the send setting commands.
<FuncID> is one byte identifying the setting(s) for the function.
<Len> is the length count for the following function-setting block <FuncData>.
<FuncData> is the current setting for this function. It has the same format as in the sending command for this function.

7.2.2 Get Setting Command

SecureMOIR will send the current setting to application.
Command: <STX> <'R'> <FuncID> <ETX> <LRC>
Response: <ACK> <STX> <FuncID> <Len> <FuncData> <ETX> <LRC>

<FuncID>, <Len> and <FuncData> definitions are same as described above.

Where:

Characters	Hex Value	Description
<STX>	02	Start of Text
<ETX>	03	End of Text
<ACK>	06	Acknowledge
<NAK>	15	Negative Acknowledge
<UnknownID>	16	Warning: Unsupported ID in setting
<AlreadyInPOS>	17	Warning: Reader already in OPOS mode
<R>	52	Review Setting
<S>	53	Send Setting
<LRC>	-	Xor'd all the data before LRC.

7.3 General Reader Commands Description

The reader Command IDs are listed as below:

ASCII	HEX (Command ID)	Name	Use
'$'	24	Get Reader Status	Determining card inserted, MSR data present, etc.
'0'	30	Clear configuration bit	Change one configuration bit but without affecting the other bits in a byte.
'1'	31	Set configuration bit	Set one configuration bit but without affecting the other bits in a byte.
'2'	32	Get configuration difference from default	Get all the configuration differences from default in one request
'8'	38	Copyright Report	Requests reader's copyright notice
'9'	39	Firmware Version Report	Requests version string
'F'	46	Key Loading	Special command to load encryption keys
'I'	49	Reader Reset	Reset the reader.

ASCII	HEX (Command ID)	Name	Use
			Software reset does not resend startup string (RS232 only)
'M'	4D	OPOS/ OPOS raw Command (Only RS232)	Command to enter OPOS or JPOS raw mode
'P'	50	Arm/Disarm to Read	Arm to Capture Buffer Mode MSR
'Q'	51	Read Buffered Data	Read Stored MSR Data
'R'	52	Read Reader Options	Read various reader optional settings
'S'	53	Set Reader Options	Set various reader optional functions
'U'	55	Keyboard Mode	Enter/Leave Keyboard Mode
'l'	6C	LED Functions	Turning on/off/flash the bicolor-LED

Table 1 – Reader Command ID Table

For <CommandID> 0x52, 0x53, 0x30 and 0x31, there must be a <FuncID> followed after <CommandID>. For the other <CommandID>, there is no <FuncID> followed.

7.3.1 Get Firmware Version Report [39]

TLP: 60 00 01 39 58 03
ITP: 02 39 03 <LRC>

Note: An approximately '55-byte' version description will be returned. The description and length varies somewhat by hardware and version. This function return the same result as command "52 22".

Response:
TLP: 60 00 35 <Version Description> <LRC> 03
Response Example (mixed hex and ASCII):
60 00 35 "ID TECH TM3 Secure Mag Only Insert RS232 Reader V1.00" 63 03

ITP: 02 35 <Version Description> 03< LRC>

7.3.2 Revert to Default Settings [53 18]

TLP: 60 00 02 53 18 29 03
ITP: 02 53 18 03 <LRC>

This command does not have any <FuncData>. All the unprotected function IDs in the reader will be reverted to default. See details in section 7.4.1. (Some transient statuses e.g. card report timers may not be cleared immediately if done in the middle of a card transaction). Please note the response to this command can take more than a second.

7.3.3 Host LED Control Command [6C]

TLP: 60 00 02 6C <LED State> <LRC> 03
ITP: 02 6C <LED State> 03 <LRC>

This command is used to change the color setting on the LED.
Note: Reader must have the "LED" on the reader for this command function properly.
Where <LED State> are:

'0'	30	LED will be turned off.
'1'	31	LED will be turned on green.
'2'	32	LED will be turned on red.
'3'	33	LED will be turned on amber.
'4'	34	LED will be flashing red/amber.
'5'	35	LED will be flashing green.
'6'	36	LED will be flashing red.
'7'	37	LED will be flashing amber.
'A'	41	LED will be slowly flashing green
'B'	42	LED will be slowly flashing red
'C'	43	LED will be slowly flashing amber

Example: To flash the LED green:
60 00 02 6C 35 3B 03

The successful response will be as below:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Other possible TLP response statuses:

6913	2nd byte of LED command was not 30-37, or 41-43
691D	Command length was incorrect
691F	host LED control not enabled. To configure the reader to support host see bit 4 in set reader option byte 0x11 in section 7.3.7.

7.3.4 Reader Reset Command [49]

TLP: 60 00 01 49 28 03
ITP: 02 49 03 <LRC>

This allows the host to return the reader to its default state which is the state after reader is powered on, i.e. not armed to read, no magnetic data stored, etc. The reader remains on-line. This command is not supported on USB interface reader.

The successful response will be as below:
TLP: 60 00 02 90 00 F2 03
ITP: 06

7.3.5 Get Copyright Information [38]

TLP: 60 00 01 38 59 03
ITP: 02 38 03 <LRC>

An approximately '56-byte' Copyright Notice will be returned.

Response:

TLP: 60 00 38 <Copyright String> <LRC> 03
Response Example mixed hex and ASCII:
60 00 38 Copyright (c) 2011, ID TECH <LRC> 03
ITP: 02 38 <Copyright String> 03< LRC >

7.3.6 Get Reader Status [24]

Command:
TLP: 60 00 01 24 <LRC> 03
ITP: Command: 02 24 03< LRC>

The response will be as below:
TLP: 60 00 01 <Reader Status><LRC> 03
ITP: 06 02 <Reader Status> 03< LRC>

For RS232 and USB-KB readers, a single-byte reader status will be returned.

Bit Position	0	1
B0	0(Reserved for future)	0 (Reserved for future)
B1	Card not seated	Card seated
B2	Others	Media detected*
B3	Card not present*	Card present*
B4	No magnetic data	Magnetic data present
B5	All other conditions	Card in Slot*
B6	All other conditions	Incomplete Insertion*
B7	Unused	

* Flags are available only when front switch is supported by the reader. The flag will always be 0 if an option is not supported.

7.3.7 Set Reader Option Byte [53 11]

TLP: 60 00 04 53 11 01 <Setting> <LRC> 03

ITP: 02 53 11 01 <Setting> 03 <LRC>

A single-byte setting is defined as follows:

Bit Position	0	1
B0	Card Seated Notification Off	**Card Seated Notification On***
B1	Card Removed Notification Off	**Card Removed Notification On***
B2	Card In Notification Off*	**Card In Notification On**
B3	MSR Data Envelope Off*	**MSR Data Envelope On**
B4	**LED Controlled by Reader***	LED Controlled by Host
B5	Magnetic Data Present Notification Off	**Magnetic Data Present Notification On***
B6	**Standard Decoder***	Raw Data Decoder
B7	Card Out Notification Off*	**Card Out** Notification **On**

Bold is the default for RS232 interface. * is the default for USB HID/KB interface.

A successful response will be as below:
TLP: 60 00 02 90 00 F2 03
ITP: 06

For RS232 reader, the default value is **0xAF**. For USB HID and HID KB the default is **0x23**.

B3 - After a good read, the magnetic stripe data will be sent out with an envelope if "MSR Data Envelope" is ON. Please see section 9.2.2 for the detailed TLP and ITP card data output envelops.

B5 - The "Magnetic Data Present" option is only available when the unit has been set to buffered mode.

For RS232 interface reader, after an insertion or withdrawal, a Magnetic Data Present Notification (<60><00><02><B0><Card Status><LRC><ETX>) will be issued if the “Magnetic Data Present” bit has been set to ON and magnetic data in current read direction enabled by reader. And a "Card Switch Change” notification (<60><00><02><B0><Card Status><LRC><ETX>) will be issued by the reader if "Card Seated On”, “Card Removed On”, “Card In On”, or "Card Out On" has been set to ON and the card switch have changed.

For USB_HID_KB interface reader, a Magnetic Data Present String will be issued if the “Magnetic Data Present” bit has been set to ON and magnetic data in current read direction enabled by reader. The default string is "\tMagnetic Data\t". And a card notification string (Card Seated String, Card Removed String, Card Present String or Card Out String) will be issued by the reader if "Card Seated On”, “Card Removed On”, “Card In On”, or "Card Out On" has been set to ON and the card switch was changed. The notification string can be changed by using commands in section 7.6.

B6 - The Raw Data Decoder enables raw data to be sent to the host for further processing. Two ASCII characters represent each raw data byte: The first ASCII character is for the high nibble of the hex code. The second ASCII character is for the low nibble of the hex code. For example, the characters "4" and "B" represent raw data "4Bh" (01001011).

If "Raw Data Decoder" has been set, all data will be treated as a bit string and will be sent out in hex format.Leading or trailing zeros (depending on whether the reader reads on insertion or withdrawal) will not be sent (except in KB mode where 4 bytes of trailing zeros are sent). All read track data is sent with no regard to track designation or separation.No error checking is performed. In all except KB mode a track prefix will be sent to identify which track the raw data is from. The track prefix will be 0x01 for track 1; 0x02 for track 2 and 0x03 for track 3. In KB mode, “0000” will be used to separate the tracks.

7.3.8 Set Reader Option Byte [53 2F]

Command
TLP: 60 00 04 53 2F 01 <Setting><LRC> 03
ITP: 02 53 2F 01 <Setting>03<LRC>

A single-byte setting is defined as follows:

Bit Position	0	1
B0	**Media Detected Off**	Media Detected On
B1	**No Data Notification Off**	No Data Notification On
B2	**Card in Slot Notification Off**	Card in Slot Notification On*
B3	**Incomplete Insertion Notification Off**	Incomplete Insertion Notification On*
B4	**TLP Output Format**	ITP Output Format
B5--B7	Reserved	

* Flags are only available on the reader with front switch (card present switch). The flag will always be 0 on the reader without front switch.

A successful response will be as below:
TLP: 60 00 02 90 00 F2 03
ITP: 06

For TLP, the default value is **0x00** for all the interfaces. For ITP, the default value is **0x10** for the all the interfaces.

B0 - After an insertion or withdrawal, a MEDIA DETECTED notification will be issued if its setting is ON and magnetic data in the current read direction is disabled by reader.

B1 - After an insertion or withdrawal, a NO DATA notification will be issued if B1 is set to 1. That means no data on selected tracks are detected (if Read Direction is enabled) and no magnetic data after an insertion or withdrawal time out.

B2 - After the seated switch was deactivated, a CARD IN SLOT notification will be issued if CARD PRESENT is still ON 2 seconds after the seated switch is being deactivated.

B3 - After an insertion, an INCOMPLETE INSERTION notification will be issued if CARD SEATED is still OFF 2 seconds after card present switch is activated or media is detected and card seated switch not detected.

For RS232 interface reader, a STATUS CHANGE notification (<60><00><02><B0><Card Status><LRC><ETX> TLP) will be issued by the reader if "Media Detected", "No Data", "Card In Slot", or "Incomplete Insertion" has been set to ON and the associated status was changed. Please note for ITP, the 02 B0 <Card Status> 03<LRC> will be issued.

For USB-HID-KB interface reader, a notification string (No Data String, Media Detected String, Card In Slot String or Incomplete Insertion String) will be issued by the reader if "Media Detected", "No Data", "Card In Slot", or "Incomplete Insertion" has been set to ON and the associated status was changed.

Note: If the bit 4 is set to 1, the encrypted track output will be in ITP output format (see section 9.3). If this bit is set and the host has not communicated with the reader, the readers output in non secure mode will also be in ITP mode. If the host has communicated with the reader, the reader will use the protocol that the host used to communicate.

7.4 Reader Configuration Commands Description

7.4.1 Read All Configuration Settings [52 1F]

Commands
TLP: 60 00 02 52 1F 2F 03
ITP: 02 52 1F 03<LRC>

This command does not have any <FuncData>. It retrieves all current settings.

Response:

TLP: 60 <Length> <FuncSETBLOCK1>…<FuncSETBLOCKn> LRC 03
ITP: 02 <FuncSETBLOCK1>…<FuncSETBLOCKn> 03 <LRC>

Each Function-Setting block <FuncSETBLOCK> has the following format:
<FuncID> <Len> <FuncData>

Where:

- <Length> is a two byte counter, which indicates the length of bytes of all<FuncSETBLOCK>. The most significant byte comes first.
- <FuncID> is a one byte Function ID identifying the setting(s) for the function. For a complete list of FuncIDs, see Appendix A.
- <Len> is a one-byte length count for the following function-setting block <FuncData>.
- <FuncData> is the current setting for this function. It has the same format as in the Sending Command for this function. See SENDING COMMAND LIST for details.
- <FuncSETBLOCK> are in the order of their function ID <FuncID>. There are two groups of function IDs, The first group are protected IDs set ups that don't changes with a default all. The second group do reset with a default all. The two groups are divided by the "‖" double line in the example below. (Please note in the real output, there is no ‖ which is added to the sample for explanation).

Example:

60 00 B7 23 01 30 4C 01 31 4E 09 08 00 00 00 00 00 00 00 00 77 01 03 7E 01 34 ‖ 10 01 30 11 01 8F 13 01 30 14 01 01 17 01 0D 19 01 31 1A 01 31 1B 01 30 1D 01 33 21 01 0D 24 01 30 2F 01 00 31 01 00 32 01 00 33 01 00 34 00 37 00 35 00 38 00 36 00 39 00 41 01 37 42 01 30 43 01 30 44 01 30 45 01 30 47 01 11 48 01 13 49 01 06 4A 01 03 4B 01 2A 4D 01 30 50 01 30 55 01 30 5C 01 37 5D 01 31 60 01 30 61 01 25 62 01 25 63 01 3B 64 01 25 65 01 3B 66 01 25 67 01 21 68 01 3B 69 01 3F 6C 01 25 6D 01 3B 6E 01 2B 7B 01 30 84 01 08 85 01 31 86 01 07 D2 00 D3 00 58 01 31 CD 03

Example Interpreted:
60 00 B7 ACK, length data: 00B7 hex or 183 decimal.
23 01 30
4C 01 31
4E 09 08 00 00 00 00 00 00 00 00
...
10 01 20
11 01 8F
...
CD 03 LRC, ETX.

7.4.2 Bit Setting and Clearing Commands [30 and 31]

This is a special type of setting command. For an 'S' (0x53) command that is to set the entire one configuration byte, the first byte of the command (the 'S' or 0x53) can be replaced with Command ID '0' (0x30) to clear individual bits or Command ID '1' (0x31) to set individual bits without changing the other bits in that configuration byte. These commands allow one to set or clear one or more bits of a configuration setting.
A command to clear one bit of a configuration setting is '0'.
Example:

30 11 01 80 will clear the highest bit in configuration byte 11
31 11 01 80 will set the highest bit in configuration byte 11
31 11 01 81 will set the lowest and highest bits of configuration byte 11

This simplifies the setting commands for those not familiar with hexadecimal values; there is no need to read the setting before writing the setting; and it reduces the chance of changing another setting when setting a bit value.

Limitations

- It can only be used on a one byte configuration setting.
- This cannot be used on special fields like the security level, that is no 30 7E 01 02
- This cannot be used to simultaneously turn some bits on and some bits off, so no changing 31 to 32 which is necessary to change TDES to AES.

7.4.3 Get Configuration Difference from Default [32]

This command is to get all the configuration differences from default in one request. Here is an example of the command and response for the 32 command for two readers one set for TLP protocol and one set to match a SecureMag reader in ITP protocol.
TLP: 60 00 01 32 53 03
Response: 60 00 1C 1C 01 40 4E 0B 0A 31 32 33 34 35 36 37 38 39 30 7E 01 33 AB 01 30 AC 01 01 10 03
The response indicated the difference between this reader and default is:

- Configured for dual head 1C 01 40
- Serial number 1234567890 (4E 0B 0A 31 32 33 34 35 36 37 38 39 30)
- Encryption level '3' (7E 01 33)
- The AB and AC settings are for remote key injection support (RKI)

ITP: 02 32 03 33

Resposne: 06 02 1C 01 40 4E 0B 0A 31 32 33 34 35 36 37 38 39 30 AB 01 30 AC 01 01 2F 01 10 41 01 35 03 6F
The response indicates the difference between this reader and default is:

- Configured to dual head(1C 01 40)
- Serial Number "1234567890" (4E 0B 0A 31 32 33 34 35 36 37 38 39 30)
- ITP protocol (2F 01 10)
- Baud rate 9600 (41 01 35)
- The AB and AC settings are for remote key injection support (RKI)

7.4.4 Read Specific Configuration Setting [52 nn]

All MSR reader Read Configuration Commands are listed in the following format:
TLP Response: 60 00 02 52 <FuncID>< LRC> 03
ITP Response: 02 52 <FuncID><FuncData> 03 <LRC>

For example to read the “Reader Option byte 0x11” configuration, send 60 00 02 52 11 21 03

7.4.5 Read Reader Serial Number [52 4E]

TLP: 60 00 02 52 4E 7E 03
ITP: 02 52 4E 03< LRC>

Note: An ‘8 to 10-byte’ string of serial number will be returned.

Response is as follows:

TLP: 60 00 0D 4E 0B 0A <Serial Number (10 bytes)>< LRC> 03
ITP: 06 02 4E 0B 0A <Serial Number (10 bytes)> 03 <LRC>

7.4.6 Buffered Mode Arm to Read Command [50 01 30]

TLP: 60 00 03 50 01 30 02 03
ITP: 02 50 01 30 03<LRC>

This command enables the MSR to be ready to capture a card insertion and/or removal in buffered mode.

Any previously read data will be erased and reader will wait for the next insertion or removal.

As the user inserts or removes a card, the data will be saved, but will not be sent to the host. The reader holds the data until receiving the next “Arm to Read” or “MSR Reset” command.

A notification will be sent to inform host of magnetic data presence after user card insertion and/or removal if the bit 5 in Reader Option byte0x11 has been set. See section 7.3.7.

Successful response is as follows:

TLP: 60 00 02 **90 00** F2 03
ITP: 06

Problem response is as follows:
TLP: E0 00 02 **xxxx** LRC 03
ITP: 18 if bad format; 15 if no data

Other possible TLP response statuses
- 6912 'P' command length must be 1
- 6916 'P' command data must be 0x30 or 0x32
- 6920 Reader not configured for buffered mode
- 6922 Reader not configured for magstripe read

7.4.7 Buffered Mode MSR Reset Command [50 01 32]

TLP: 60 00 03 50 01 32 00 03
ITP: 02 50 01 32 03 <LRC>

This command will disable MSR read and clear any magnetic data in buffered mode. The reader enters to a disarmed state and will ignore MSR data.

Successful response is as follows:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Problem response is as follows:
TLP: E0 00 02 xxxx LRC 03
ITP: 15 if bad format

Other possible TLP response statuses:
- 6912 'P' command length must be 1
- 6916 'P' command must be 0x30 or 0x32
- 6920 Reader not configured for buffered mode
- 6922 Reader not configured for magstripe read

7.4.8 Buffered Mode Read MSR Data Command [51 01 XX]

TLP: 60 00 03 51 01 <Track Selection Option> <LRC> 03
ITP: 02 51 01 <Track Selection Option> 03 <LRC>

The <Track Select Option> byte is defined as follows:
- ‘0’ Any Track
- ‘1’ Track 1
- ‘2’ Track 2
- ‘3’ Track 1 and Track 2
- ‘4’ Track 3
- ‘5’ Track 1 and Track 3
- ‘6’ Track 2 and Track 3
- ‘7’ Track 1, Track 2 and Track 3
- ‘8’ Track 1 and/or Track 2
- ‘9’ Track 2 and/or Track 3

This command requests card data information while in buffered mode.

The selected MSR data is sent to the host with or without envelope format, according to the operation mode setting. (See section 7.3.7)

This command does not erase the data.

Response is as follows:
TLP: 60 00 02 <Len_H><Len_L><MSR Data> LRC 03
ITP: 06 02 <MSR Data> 03 LRC

Problem response is as follows:
TLP: E0 00 02 xxxx LRC 03
ITP: 15 if no data; 18 if bad format; 16 if Bad ID
Other possible TLP response statuses:

6911	'Q' command length must be 1
6921	reader not configured for buffered mode
C000	no magstripe data available

Use of Buffered Mode with Security Level 4
When the reader is used in both buffered mode and Security level 4 it is possible to vary the order of commands and still have the reader work. The reader needs to be both armed to read and security authenticated before the card track data will be sent to the host computer as an encrypted message. In order to assure proper function reading a card under these conditions, the transaction should proceed in the following sequence (assuming the reader is already configured for Security Level 4 and configured for buffered mode): Send the Act auth command (52 80), then send the act reply command (53 82) so the reader is now allowed to send a level 4 transaction, then send an arm to read command (50 01 30). Depending on the configuration settings of the reader the host can poll the reader to determine if card data has been captured by asking for the reader status (24 and looking at the setting of B4) or asking the reader for the authentication status (52 83) and observing that the current status is 0 and the status antecedent is 2. The host computer can then request the encrypted buffered track data (50 01 30). The buffered data should not need to be re-requested, but if it is, the KSN will be updated one time for each request.

7.4.9 MSR Configuration Commands Description

All MSR reader Configuration Commands are listed in the following format:
TLP: 60 <Length> 53 <FuncID> <Len> <FuncData> <LRC> 03
ITP: 02 53 <FuncID> <Len> <FuncData> 03 <LRC>

Length is a two byte counter, which indicates length of data from 53 to end of <Func Data>. The most significant byte comes first.
Success Response in all cases
TLP: 60 00 02 90 00 F2 03
ITP: 06

7.4.10 Set MSR Transmit Mode [53 1A]

TLP : 60 00 04 53 1A 01 <MSR Transmit Mode>< LRC> 03
ITP: 02 53 1A 01 <MSR Transmit Mode> 03 <LRC>
The <MSR Transmit Mode> byte is defined as follows:

‘0’	MSR Reading Disable
‘1’	**MSR Reading Auto Transmit Mode**
‘2’	MSR Reading in Buffered Mode.
‘3’	Auto Buffered Mode

Example to enable MSR reading auto transmit mode:
60 00 04 53 1A 01 31 1D 03

7.4.11 Set MSR Read Direction [53 1D]

TLP: 60 00 04 53 1D 01 <Read Direction> <LRC> 03

ITP: 02 53 1D 01 <Read Direction> 03 <LRC>

The <Read Direction> byte is defined as follows:

‘1’ Read on both insertion and withdrawal
‘2’ Read on insertion only
‘3’ Report on withdrawal
‘4’ Read on withdrawal only

Example: 60 00 04 53 1D 01 03 28 03 report on withdrawal

Note: Unless the users are trained or the reader is a partial insert reader, about 20% of the population will not insert a card smoothly enough to be read during insertion. Nearly everyone extracts a card smoothly, but report on withdrawal feature captures, both insert and withdrawal and combines them into one read automatically outputs in one envelope

7.4.12 **Set MSR Send Option [53 19]**

This setting only applies to the reader under unencrypted mode.
TLP: 60 00 04 53 19 01 <Send Option>< LRC> 03
ITP: 02 53 19 01 <Send Option> 03 <LRC>

The <Send Option> byte is defined as follows.

Bit Position	0	1
B0	No Start/End Sentinel	Send Start/End Sentinel
B1	All Data on track 2	Account Number on track 2
B2	No bad track error report	Report error on bad track
B3	KB reader only	
	Send std control codes	send alt control codes
B4-B7	Unused	

The reader can be set to either send, or not send, the Start/End sentinels, and to send either the Track 2 account number only, or all the encoded data on Track 2. (The Track 2 account number setting does not affect the output of Track 1 and Track 3.)

<30> Do not send Start/End sentinel, do send all data on all tracks. No error notification.
<31> Send Start/End sentinel and all data on all tracks. No error notification.
<32>Do not send Start/End sentinel for any track, but do send account number on Track 2 only. No error notification.
<33> Send Start/End sentinel on Track 1, 3 and only account number on Track 2 for a credit card. No error notification.
<34> Do not send Start/End sentinel, but do send all data on all tracks. Send the error notification.
<35> Send Start/End sentinel and all data on all tracks. Send the error notification.
<36> Do not send Start/End sentinel for any track, but do send account number on Track 2 only. Send the error notification.
<37> Send Start/End sentinel on Track 1, and account number on Track 2 only for a credit card, or Send Start/End sentinel on Tracks 1 and 3 for a standard card. Send the error notification.
<38> through <3F> Send keyboard control codes in the standard form, or send the alternative control codes. And includes option <30> ~ <37> above.

The default setting for RS232 reader is **0x31**, and the default setting for the USB_HID_KB reader is **0x35**.
The response will be:
TLP: <60><00><02><90><00><F2><03>
ITP: 06

Note: If the reader is configured to send an error notification on a bad track and it is desired to suppress the start and or end sentinels on the error notification see t1ErrStart (6C), t2ErrStart (6D), and t3ErrStart (6E) and t1End (69) to set the reader not to send these.

If the reader is in Secure Level 3 or 4 the card data is sent in the same format always. These options "do not apply". The exception is a keyboard reader can send a MSR data prefix or suffix string around the data so that the host can recognize that the data came from the SecureMOIR rather than from the keyboard. The default prefix and suffix is NONE which can be set using the commands below. The other exception should be noted is that under secure mode, the output of the track LRC is set by FuncID 0x6F instead of 0x60. (See Appendix A table)

7.4.13 **Set MSR Data Terminator [53 21]**

This setting only applies to the reader under unencrypted mode.
TLP: 60 00 04 53 21 01 <Terminator Setting>< LRC> 03
ITP: 02 53 21 01 <Terminator Setting> 03< LRC>

The <Terminator Setting> byte is any one byte except 0x00:
The default is 0x0D, which is Carriage Return (CR), If 0x00 is set, the reader will send no terminator.
Example to set to send Line Feed (LF=0x0A) after the last MSR data
60 00 04 53 21 01 0A 27 03
The terminator value 30 is special it will send out two characters CRLF or OD and OA.

7.4.14 **Set MSR Data Prefix String [53 D2]**

This command works on unencrypted mode only with the exception that the reader is with keyboard interface under the secure mode.
TLP: 60 <Length> 53 D2 <Len> <Prefix String> <LRC> 03
ITP: 02 53 D2 <Len> <Prefix String> 03 <LRC>

Where:
<Prefix String> = {string length}{string}
{String length} is one byte, maximum value 15
<Len> is the number of bytes of Prefix string including string length
<Length> is a one byte counter, which indicates the number of bytes in command from 53 to the end of <Prefix String>. The most significant byte comes first.

Example to set the prefix to "TRK"
60 00 07 53 D2 04 03 54 52 4B AC 03

7.4.15 **Set MSR Data Suffix String [53 D3]**

This command works on unencrypted mode only with the exception that the reader is with keyboard interface under the secure mode.
TLP: 60 <Length> 53 D3 <Len> <Suffix String> <LRC> 03
ITP: 02 53 D3 <Len> <Suffix String> 03 <LRC>

Where:
<Suffix String> = {string length}{string}
<String length> is one byte, maximum 15
<Len> is the number of bytes of Suffix string including string length
<Length> is a one byte counter, which indicates the number of bytes in command from 53 to the end of the <Suffix String>. The most significant byte comes first.

Example to put a ‘]’ at the end of the MSR data
60 00 05 53 D3 02 01 5D BB 03

7.4.16 **Set Track 1 ID [53 31]**

This setting only applies to the reader under unencrypted mode.
This command works on unencrypted mode only.
TLP: 60 00 04 53 31 01 <Track 1 ID><LRC> 03
ITP: 02 53 31 01 <Track 1 ID> 03 <LRC>
<Track 1 ID>: ASCII code set as Track 1 ID, NULL for None.
Example: 60 00 04 53 31 01 00 07 03 Send no Track 1 ID

7.4.17 **Set Track 2 ID [53 32]**

This setting only applies to the reader under unencrypted mode.
This command works on unencrypted mode only.
TLP: 60 00 04 53 32 01 <Track 2 ID> <LRC> 03
ITP: 02 53 32 01 <Track 2 ID> 03 <LRC>
<Track 2 ID>: ASCII code set as Track 2 ID, NULL for None.
Example: 60 00 04 53 32 01 32 36 03 Send Track 2 ID of ASCII ‘2’

7.4.18 **Set Track 3 ID [53 33]**

This command works under unencrypted mode only.
TLP: 60 00 04 53 33 01 <Track 3 ID>< LRC> 03
ITP: 02 53 33 01 <Track 3 ID> 03 <LRC>
<Track 3 ID>: ASCII code set as Track 3 ID, NULL for None.
Example: 60 00 04 53 33 01 33 06 03 Send Track 3 ID of Hex ‘3’

7.4.19 **Set Track Selection [53 13]**

TLP: 60 00 04 53 13 01 <Track Selection>< LRC> 03
ITP: 02 53 13 01 <Track_Selection> 03 <LRC>
<Track_Selection>:
‘0’ Any Track
‘1’ Track 1 Only
‘2’ Track 2 Only
‘3’ Track 1 & Track 2
‘4’ Track 3 Only

‘5’ Track 1 & Track 3
‘6’ Track 2 & Track 3
‘7’ All Three Tracks
‘8’ Track 1 and/or 2
‘9’ Track 2 and/or 3

Example to select all 3 tracks and all must have valid data:
60 00 04 53 13 01 37 22 03

Note: If a track selected above (as opposed to any track), that track ‘must’ be present and good or the reader does not transmit any track information.

7.4.20 **Set Track Separator [53 17]**

This command works under unencrypted mode only.
TLP: 60 00 04 53 17 01 <Track_Separator> <LRC> 03
ITP: 02 53 17 01 <Track_Separator> 03 <LRC>

<Track_Separator> is one ASCII byte:
The default value is **CR** (Hex 0D).

Example to set the track separator to CR (carriage return):
60 00 04 53 17 01 0D 2C 03

7.4.21 **Set Track n Prefix [53 34]**

This command works under unencrypted mode only.

Characters can be added to the beginning of a track data. These can be special characters to identify the specific track to the receiving host, or any other character string. Up to six ASCII characters can be defined.

TLP: 60 00 03 53 <n><Len><Prefix><LRC>03
ITP: 02 53 <n><Len><Prefix> 03 <LRC>

Where:
n is 34h for track 1; 35h for track 2 and 36h for track 3
Len = the number of bytes of prefix string
Prefix = {string length}{string}
NOTE: String length is one byte, maximum six.

Example:
60 00 09 53 34 06 05 “Trk1=” LRC 03
Problem with configure command
E0 00 02 69 1E 95 03
See Appendix B for the list of the return status codes

7.4.22 **Set Track n Suffix [53 37]**

This command works under unencrypted mode only.

Characters can be added to the end of track data. These can be special characters to identify the specific track to the receiving host, or any other character string. Up to six ASCII characters can be defined.

TLP: 60 00 LenL 53 <n><Len><Suffix> 03 <LRC>
ITP: 02 53 <n><Len><Suffix> 03<LRC>

Where:
n is 37h for track 1; 38h for track 2 and 39h for track 3
Len = the number of bytes of suffix string
Suffix = {string length}{string}
NOTE: String length is one byte, maximum six.

Example: 60 00 09 53 38 06 05 "<End1" LRC 03

7.4.23 **Set Track 1 7-Bit Start Sentinel [53 61]**

This setting only applies to the reader under unencrypted mode.
This setting allows the user to select any single character to be output as the Track 1 start sentinel if the magnetic card's Track 1 data is 7-bit encoded.
TLP: 60 00 04 53 61 01 <Track1 7Bit Start Sentinel ><LRC> 03
ITP: 02 53 61 01<Track1 7Bit Start Sentinel > 03<LRC>

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Example: 60 00 04 53 61 01 25 72 03 (Set "%" as Start Sentinel)

7.4.24 **Set TRACK 1 5-Bit Start Sentinel [53 63]**

This setting only applies to the reader under unencrypted mode.
This setting allows the user to select any single character to be output as the Track 1 start sentinel if the magnetic card's Track 1 data is 5-bit encoded.
TLP: 60 00 04 53 63 01<Track1 5Bit Start Sentinel > <LRC> 03
ITP: 02 53 63 01<Track1 5Bit Start Sentinel > 03 <LRC>

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06
Example: 60 00 04 53 63 01 3B 6E 03 (Set ";" as Start Sentinel)

7.4.25 **Set Track 2 7-Bit Start Sentinel [53 64]**

This setting only applies to the reader under unencrypted mode.
This setting allows the user to select any single character to be output as the Track 2 start sentinel if the magnetic card's Track 2 data is 7-bit encoded.
TLP: 60 00 04 53 64 01 <Track2 7Bit Start Sentinel ><LRC>03
ITP: 02 53 64 01 <Track2 7Bit Start Sentinel >03 <LRC>

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06
Example: 60 00 04 53 64 01 25 77 03 (Set "%" as Start Sentinel)

7.4.26 **Set Track 2 5-Bit Start Sentinel [53 65]**

This setting only applies to the reader under unencrypted mode.
This setting allows the user to select any single character to be output as the Track start sentinel if the magnetic card's Track 2 data is 5-bit encoded.
TLP: 60 00 04 53 65 01 <Track2 5Bit Start Sentinel ><LRC> 03
ITP: 02 53 65 01 <Track2 5Bit Start Sentinel ><LRC> 03

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Example: 60 00 04 53 65 01 3B 68 03 (Set ";" as Start Sentinel)

7.4.27 **Set Track 3 7-Bit Start Sentinel [53 66]**

This setting only applies to the reader under unencrypted mode.
This setting allows the user to select any single character to be output as the Track 3 start sentinel if the magnetic card's Track 3 data is 7-bit encoded.
TLP: 60 00 04 53 66 01 <Track3 7Bit Start Sentinel><LRC>03
ITP: 02 53 66 01 <Track3 7Bit Start Sentinel>03 <LRC>

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Example: 60 00 04 53 66 01 23 6B 03 (Set "#" as Start Sentinel)

7.4.28 **Set Track 3 5-Bit Start Sentinel [53 68]**

This setting only applies to the reader under unencrypted mode.
This setting allows the user to select any single character to be output as the Track 3 start sentinel if the magnetic card's Track 3 data is 5-bit encoded.
TLP: 60 00 04 53 68 01<Track3 5Bit Start Sentinel><LRC>03
ITP: 02 53 68 01<Track3 5Bit Start Sentinel>03 <LRC>

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Example: 60 00 04 53 68 01 3B 65 03 (Set ";" as Start Sentinel)

7.4.29 **Set Track End Sentinel [53 69]**

This setting only applies to the reader under unencrypted mode.
This setting allows the user to select any single character to be output as the track end sentinel.

TLP: 60 00 04 53 69 01<Track End Sentinel><LRC>03
ITP: 02 53 69 01<Track End Sentinel> 03 <LRC>

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Example: 60 00 04 53 69 01 3F 60 03 (Set "?" as End Sentinel)

7.5 RS232 Reader Special Configuration Commands

For RS232 device, the serial communication parameter default setting is 38400, none, 8, 1.

7.5.1 Set Baud Rate [53 41]

The command is used to set the baud rate of serial communication between application and SecureMOIR. Reader will turn to the set baud rate after sending back a response for this setting command. Application should turn to the new baud rate after receiving the response to ensure the communication between application and SecureMOIR reader.

TLP: 60 00 04 53 41 01<Baud Rate Setting><LRC>03
ITP: 02 53 41 01<Baud Rate Setting> 03 <LRC>

The default baud rate is 38400 bits/sec.
Baud Rate Setting:
'2':1 200 bits/sec
'3': 2400 bits/sec
'4': 4800 bits/sec
'5': 9600 bits/sec
'6': 19200 bits/sec
'7': 38400 bits/sec
'8': 57600 bits/sec
'9':115200 bits/sec

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Example: 60 00 04 53 41 01 36 41 03 (Set 19200 bits/sec as baud rate)

7.5.2 Set Data Parity [53 43]

An optional parity bit follows the data bits in the character frame. This parity bit is included as a simple means of error handling. This command is used to set the data parity method of the transmission.

TLP: 60 00 04 53 43 01<Data Parity Setting ><LRC> 03
ITP: 02 53 43 01<Data Parity Setting > 03 <LRC>

The default Data Parity value is None.
Data Parity Setting:
'0': None
'1': Even

‘2’: Odd
‘3’: Mark
‘4’: Space

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Example: 60 00 04 53 43 01 32 47 03 (Set Odd as Data Parity)

7.5.3 Set Handshake Method [53 44]

TLP: 60 00 04 53 44 01<Handshake Setting ><LRC> 03
ITP: 02 53 44 01<Handshake Setting > 03 <LRC>

The command is used to set the Handshake (Flow Control) of serial communication between application and Magnetic Stripe Insert reader, where:

Handshake Setting:
‘0’: No Handshake
‘2’: Software Xon/Xoff Handshake

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06
Example: 60 00 04 53 44 01 32 70 03 (Set to software handshake)

7.5.4 Set Stop Bits [53 45]

The stop bit identifying the end of a data frame can have two different numbers: 1 or 2 bits. This command is used to set the number of stop bits in a character frame.

TLP: 60 00 04 53 45 01 <Stop Bits Setting ><LRC> <ETX>
ITP: 02 53 45 01 <Stop Bit Setting> 03<LRC>
The default Stop Bits value is 1 bit.

Stop Bits Setting:
‘0’: 1 Bit
‘1’: 2 Bits

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Example: 60 00 04 53 45 01 31 42 03 (Set to 1 stop bit)

7.5.5 Set XON ID [53 47]

This setting allows the user to select any single character to be used as the XOn ID character for software handshaking.

TLP: 60 00 04 53 47 01 <XOn ID Character><LRC>03
ITP: 02 53 47 01 <XOn ID Character> 03 <LRC>

The XOn ID can be 0x11 or 0x13. The default value is **0x11**.
The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06
Example: 60 00 04 53 47 01 12 63 03 (Set XON ID to be 0x12)

7.5.6 SET XOFF ID [53 48]

This setting allows the user to select any single character to be used as the XOff ID character for software handshaking.
TLP: 60 00 04 53 48 01 <XOff ID Character><LRC>03
ITP: 02 53 48 01 <XOff ID Character> 03 <LRC>

The XOff ID can be 0x11 or 0x13. The default value is 0x13. The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Example: 60 00 04 53 48 01 12 6C 03 (Set Xoff ID to 0x12)

7.6 USB HID or HID Keyboard Reader Special Commands

The following commands are USB HID and USB Keyboard Reader Special commands

7.6.1 Set Card Seated String [53 26]

This setting allows the user to select a character string to be output as card-seated notification. When the card seated switch changes from off to on, this string will be sent out if "Card Seated On and Off" bit in ReaderOpt byte 0x11 is set.

TLP: 60<Command Length> 53 26<Len><Card Seated String><LRC> 03
ITP: 02 53 26 <Len><Card Seated String> 03 < LRC>

In this example:
<Command Length> is a two-byte length from <53> to <Card Seated String>
<Len> is the number of bytes of the Card Seated String, but no greater than 24
<Card Seated String> is {string length}{string} (String length is one byte, maximum 23)
The default {string} is "\tCard Seated\t"

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

7.6.2 Set Card Removed String [53 27]

This setting allows the user to select a character string to be output as card removed

notification. When the card-seated switch changes from on to off, this string will be sent out if "Card Removed On and Off" bit in ReaderOpt byte 0x11 is set.

TLP: 60 <Command Length> 53 27<Len><Card Removed String><LRC>03
ITP: 02 <Command Length> 53 27<Len><Card Removed String> 03 <LRC>

In this example:
<Command Length> is a two-byte length from <53> to <Card Removed String>
<Len> is the number of bytes of the Card Removed String, but no greater than 24
<Card Removed String> is {string length}{string} (String length is one byte, maximum 23.) . The default {string} is "\tCard Removed\t"

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

7.6.3 Set Card Present String [53 28]

This setting allows the user to select a character string to be output as card present notification. When the card front switch changes from off to on, this string will be sent out if "Card In On and Off" bit in ReaderOpt byte 0x11 is set.

TLP: 60<Command Length> 53 28<Len><Card Present String><LRC>03
ITP: 02 53 28<Len><Card Present String> 03 <LRC>

In this example:
<Command Length> is a two-byte length from <53> to <Card Present String>
<Len> is the number of bytes of the Card Present String, but no greater than 24
<Card Present String> is {string length}{string} (String length is one byte, maximum 23.)
The default {string} is "\tCard Present\t".

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Please note this setting is only available for the reader which has front switch.

7.6.4 Set Card Out String [53 29]

This setting allows the user to select a character string to be output as card out notification. When the card front switch changes from on to off, this string will be sent out if "Card Out On and Off" bit in ReaderOpt byte 0x11 is set.

TLP: 60<Command Length> 53 29 <Len><Card Out String><LRC> 03
ITP: 02 53 29 <Len><Card Out String> 03 <LRC>

In this example:
<Command Length> is a two-byte length from <53> to <Card Out String>
<Len> is the number of bytes of the Card Out String, but no greater than 24
<Card Out String> is {string length}{string} (String length is one byte, maximum 23.).

The default {string} is “\tCard Out\t”.

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Please note this setting is only available for the reader which has front switch.

7.6.5 Set No Data Detected String [53 2A]

This setting allows the user to select a character string to be output as no data notification. When no magnetic data after an insertion or withdraw time out, this string will be sent out if "No Data On and Off" bit in ReaderOpt byte 0x2F is set.

TLP: 60<Command Length><53><2A><Len><No Data String><LRC> 03
ITP: 02 53 2A <Len><No Data String> 03 <LRC>

In this example:
<Command Length> is a two-byte length from <53> to <No Data String>
<Len> is the number of bytes of the No Data String, but no greater than 24
<No Data String> is {string length}{string} (String length is one byte, maximum 23.)
The default {string} is “\tCard Detected\t”.

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

7.6.6 Set Media Detected String [53 2B]

This setting allows the user to select a character string to be output as media detected notification. When capturing magnetic data in current read direction is disabled by the reader, this string will be sent out if "Media Detected On and Off" bit in ReaderOpt2ID is set.

TLP: 60<Command Length> 53 2B<Len><Media Detected String><LRC>03
ITP: 02 53 2B<Len><Media Detected String> 03 <LRC>

In this example:
<Command Length> is a two-byte length from <53> to < Media Detected String>
<Len> is the number of bytes of the Media Detected String, but no greater than 24
< Media Detected String> is {string length}{string} (String length is one byte, maximum 23.). The default {string} is “\tMedia Detected\t”.

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

7.6.7 Set Magnetic Data String [53 2C]

This setting allows the user to select a character string to be output as magnetic data notification. After an insertion or withdrawal if in buffer mode, this string will be sent out if "Magnetic Data On and Off" bit (bit 5) in ReaderOpt byte 0x11 is set.

TLP: 60<Command Length> 53 2C <Len><Magnetic Data String><LRC> 03
ITP: 02 53 2C <Len><Magnetic Data String> 03 <LRC>

Where
<Command Length> is a two-byte length from <53> to < Magnetic Data String>
<Len> is the number of bytes of the Magnetic Data String, but no greater than 24
< Magnetic Data String> is {string length}{string} (String length is one byte, maximum 23.). The default string is "\tMagnetic Data\t".

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

7.6.8 Set Card In Slot String [53 2D]

This setting allows the user to select a character string to be output as card in slot notification. When the card withdraws from the card seated switch and the card front switch is still on after 2s, this string will be sent out if "Card In Slot On and Off" bit in ReaderOpt byte 0x2F is set.

TLP: 60 <Command Length> 53 2D <Len><Card In Slot String><LRC> 03
ITP: 02 53 2D <Len><Card In Slot String> 03 <LRC>

In this example:
<Command Length> is a two-byte length from <53> to <Card In Slot String>
<Len> is the number of bytes of the Card In Slot String, but no greater than 24
<Card In slot String> is {string length}{string} (String length is one byte, maximum 23.)
The default {string} is "\tCard In Slot\t".

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Please note this setting is only available for the reader which has front switch.

7.6.9 Set Card Incomplete Insertion String [53 2E]

This setting allows the user to select a character string to be output as partial in notification. When the card is inserted through the card front switch and the card-seated switch is still off after 2s, this string will be sent out if "Incomplete Insertion On and Off" bit in ReaderOpt byte 0x2F is set.

TLP: 60 <Command Length> 53 2E <Len><Incomplete Insertion String><LRC> 03
ITP: 02 53 2E <Len><Incomplete Insertion String> 03 <LRC>

Where
<Command Length> is a two-byte length from <53> to < Incomplete Insertion String>
<Len> is the number of bytes of the Incomplete Insertion String, but no greater than 24
< Incomplete Insertion String> is {string length}{string} (String length is one byte, maximum 23). The default {string} is "\tIncomplete Insertion\t"

The successful response will be:
TLP: 60 00 02 90 00 F2 03
ITP: 06

Please note this setting is only available for the reader which has front switch.

7.7 Magnetic Card Read Modes

The SecureMOIR supports two MSR modes.

"**Auto Transmit mode**" – Reader sends data as soon as the data is available. When using "Auto Transmit Mode", the application program needs to be ready to receive data. This is the default mode. The track data is cleared as soon as it is sent.

"**Buffered Mode**" – The application program first sends an "Arm to Read" command to enable the magnetic stripe reading. The user inserts and/or removes a card, the decoded data is stored, the readers notifies the host a magstripe read occurred if enabled, and MSR is disarmed. The application program then sends a "Read MSR Data" command to retrieve the data from the buffer.

To read a magnetic stripe card, just follow these simple steps, LED indication describes LED status change when it is under the control of the reader:

Insert a card, magnetic stripe down (if not a dual head reader), into the reader until it hits a hard stop, (note if reader is configured for read on insert (the default is on withdrawal) it is important to insert the card in one continuous motion to ensure proper reading of the data). As soon as the reader detects data from magnetic stripe, the green LED indicator will go off.

Withdraw the card in one continuous motion. The green LED will go off and turn back to green very fast which can be hard to be caught by eyes. (The reader by default will read the magnetic stripe on both insertion and withdrawal, but only report the track data after the card has been withdrawn. We call this report on withdrawal.)

If the reader controls the LED, the LED will turn red (to indicate a bad read) or green (to indicate a good read) meaning it is ready for another transaction.

"Report on Withdrawal Mode" - The new standard default MSR reading option "report on withdrawal" This option is designed to maximize card read success rate. The card is read on the way in and on the way out and the two reads combined and the combination reported after the card has been removed. It is currently only supported in auto-transmit mode, it is not currently compatible with buffered mode or dual head reader.

7.8 Card Status Notification [B0 xx]

There are six notifications the reader can issue. One is an error notification, the other five are optional card seated and card unseated notification, optional card present and card removed notification and optional buffered magnetic stripe data available.

The reader can issue a card notification (60 00 02 B0 XX C2 03), if card seated, card unseated, card present, card removed, buffered magnetic stripe data available. Or there is a card that was inserted but was never seated, or that was seated and withdrawn but never fully removed from the reader. See get reader status (section 7.3.6). Each bit in the status byte holds specific information. Configuring the reader to send or not send status data is done with the Options configurations setting byte 0x11(section 7.3.7) and the Options configuration setting byte 0x2F (section 7.3.8). Please note card present and card removal notification only apply to SecureMOIR with front switch.

7.9 Set OPOS/JPOS Command [4D]

There are three forms of the command:

TLP:

60 00 03 4D 01 30 7D 03	Enter Standard Mode (Exit OPOS Mode)
60 00 03 4D 01 31 7C 03	Enter OPOS Mode
60 00 03 4D 01 32 7F 03	Enter JPOS Mode (Raw mode OPOS)

ITP:

02 4D 01 30 03 LRC	Enter Standard Mode (Exit OPOS Mode)
02 4D 01 31 03 LRC	Enter OPOS Mode
02 4D 01 32 03 LRC	Enter JPOS Mode (Raw mode OPOS)

Response is as follows:

692B	Reader already in OPOS Mode
6939	Command failure (wrong length or wrong parameter)
9000	Success for TLP
06	Success for ITP

8 SECURITY FEATURES

The SecureMOIR Reader features configurable security settings. 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 as specified in the followings:

- Security Level 0
  Security Level 0 is a special case where all DUKPT keys have been used and is set automatically when it runs out of DUKPT keys. The lifetime of DUKPT keys is 1 million. Once the key's end of life time is reached, user should inject Base Deviation Key and KSN again.

- Security Level 1
  By default, non encrypted readers from factory are configured to have this security level. There is no encryption process, no key serial number transmitted with decoded data. The reader would function as a non-encrypting reader and have decoded track data in clear text.

- 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 clear decoded track data as Level 1. To active reader from Level 2 to Level 3, please send the set TDES or AES command to active the reader to either TDES or AES. Please refer to the FuncID 0x4C in Appendix A table.

- Security Level 3
  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; however, the encrypted data format cannot be modified. For encrypted readers, this is the security level most of customer uses after key injection.

- 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. Please refer to 9.5 for the detailed information to active security level 4.

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. Once 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.

The reader can also support Data Key or PIN Key management.(See configuration byte 0x3E)

8.2 Check Card Format

- ISO/ABA (American Banking Association) Card

Encoding method

Track1 is 7 bits encoding and no other tracks.
Track1 is 7 bits encoding. Track2 is 5 bits encoding and no other tracks.
Track1 is 7 bits encoding. Track2 is 5 bits encoding. Track3 is 5 bits encoding.
Track1 is 7 bits encoding. Track3 is 5 bits encoding and no track 2.
Track2 is 5 bits encoding and no other tracks.
Track2 is 5 bits encoding. Track3 is 5 bits encoding and no track 1.
Track3 is 5 bits encoding and no other tracks.

Note: this track checking occurs after any tracks have been removed by 0x13 configuration setting.

Additional checks

Track1 2nd byte is 'B'.
There is at least one '=' in track 2 and the position of the first '=' is between 13th ~ 20th character so account number length is 12-19 digits.
Total length of track 2 is above 19 characters.
In track 1, there is a '^' between 15th ~ 22nd character (exclude space).
Total length of track 1 should be above 21 characters.
Expiration data can be omitted with an additional separator '^' or '='

T3 ISO-4909 (with PAN) checking

1. T1 and T2 should be in bank card format (Type 0, as checked above) or absent.
2. T3 2nd and 3rd characters are "01","02" and "90" – "99"
3. T3 PAN is 12 to 19 characters. The field separator is '='
4. T3 total length is from 67 to 107 characters inclusive

Note:

1. Expiration date starts 0x34 characters after the first '=' but can be changed to support cards where the offset is 0x36 for Chinese cards.

- AAMVA (American Association of Motor Vehicle Administration) Card

Encoding method

Track1 is 7 bits encoding. Track2 is 5 bits encoding. Track3 is 7 bits encoding.

- Others (Customer card)

Please note that reading JIS cards can be enabled. (See setting 0x1C bit 5)

8.3 MSR Data Masking

For encrypted ABA cards, both encrypted data and clear text data are sent.
Masked Area

The data format of each masked track is ASCII.
The clear data include start and end sentinels, separators, first N and last M digits of the PAN, and cardholder name (for Track1).
The rest of the characters should be masked using mask character.

Set PrePANClrData (N), PostPANClrData (M), MaskChar (Mask Character)

N and M are configurable and default to 4 first and 4 last digits. They follow the current PCI constraints requirements (N 6, M 4 maximum).
Mask character default value is '*'.

- Set PrePANClrDataID (N), parameter range 00h ~ 06h, default value 04h
- Set PostPANClrDataID (M), parameter range 00h ~ 04h, default value 04h
- MaskCharID (Mask Character), parameter range 20h ~ 7Eh, default value 2Ah
- DisplayExpirationDataID, parameter range '0'~'1', default value '0'

Example to configure reader as valid keyed in data

For special request to configure the reader to send masked data in a form that can be checked as if it were keyed in card data. That is if the reader needs to send valid card data in the mask field to the host, please refer to the configuration commands below:

1. The mask character has to be changed to a digit so it appears to be part of a valid account number, so if one picks '0' then send the command 53 4B 01 30
2. The host will need to verify the account number MOD10 check digit. To change the reader to set a valid MOD10 digit for the masked track data, send the command 53 55 01 31
3. The host may need to verify the card comes from an appropriate issuer (bank). To change the reader to unmask the first 6 digits (default is first 4 digits), send the command 53 49 01 06
4. The host may need to verify the masked expiration date. To reveal the expiration date send the command 53 50 01 31
5. The host may need the track LRC suppressed. To suppress the output of the track LRC in the masked and encrypted data, send the command 53 6F 01 30

Note: The reader masks the B (the second character on track 1), so customer software may need to restore the B. (Note If there was not a B, the reader would not mask track 1). There is no configuration option not to mask the B at the start of track 1.

9 OUTPUT FORMAT

This section is to describe different output formats from the reader.

9.1 Level 1 and level 2 POS Mode Data Output Format

The POS mode is a special mode the reader needs to be set by using “Set OPOS/JPOS” command. In POS mode, the USB KB reader uses the special envelope to send out card data, envelope is in the following format:
[Right Shift, Left Shift, Right Ctrl, Left Ctrl,], Read Error, Track x ID; Track x Error; Track x Data Length; Track x Data; Card Track x LEC code; Track x data LRC.
Reader will send out card data in Alt mode if its ASCII code less than H’20’.

Byte No.	Name
	Right Shift (make and break)
	Left Shift (make and break)
	Right Ctrl (make and break)
	Left Ctrl (make and break)
0	Read Error byte 1
1	Read Error byte 2 (OPOS card type)
	Remove extra line here
2*	Track x ID (track 1 is '1', 2 is '2')
3	Track x Error status
4	Track x Length 1 (high)
5	Track x Length 2 (low)
6 #	Track x Data (no extra Track ID for raw data)
	…
7 + Track x len#	Card Track x LRC
7 + Track x len +1	OPOS Track x LRC
7 + Track x len +2*	0x0D (OPOS track separator)
7 + Track x len + 3	Track y ID (start of the next track)
….	Repeat for Track y and Track z if present

Each track entry has track length + 6 bytes. And the total length is the total of the (2 bytes)+#of tracks *(6 bytes for each track + track length)+ 8 bytes for the Right Shift-Left Shift-Right Control-Left Control (all Make and Break) header

* Marks where the track data repeats and ends
# Marked fields are included in the track length

The data format is independent of MSR settings. No Track x data if track x sampling data does not exist.

OPOS header:
Only HID KB interface has the first 8 bytes <Header> [Right Shift (make & break), Left Shift (make & break), Right Ctrl (make and break), Left Ctrl (make and break)] under POS mode.
When the reader is in Security level 3 and 4 under OPOS mode, the output format is <Header> +

<Card Data>, where <Header> is the same as above. See section 9.3 and 9.4 for <Card Data>.

Read Error:

Read Error 1 byte bits:

MSB LSB

0	B6	B5	B4	B3	B2	B1	B0

B0 1: Track 1 sampling data exists (0: Track 1 sampling data does not exist)
B1 1: Track 2 sampling data exists (0: Track 2 sampling data does not exist)
B2 1: Track 3 sampling data exists (0: Track 3 sampling data does not exist)
B3 1: Track 1 decode success (0: Track 1 decode fail)
B4 1: Track 2 decode success (0: Track 2 decode fail)
B5 1: Track 3 decode success (0: Track 3 decode fail)
B6 0: if b0 to b5 are all 1, otherwise 1 (make it printable)

Read Error byte 2:

MSB LSB

0	1	B12	B11	B10	B9	B8	B7

B7 0: Track 4 sampling data does not exist
B8 0
B9, B10, B11
000: ISO Card (7, 5) or (7, 5, 5) encoding
010: AAMVA Card (7, 5, 7) encoding
110: OPOS Raw Data Output
B12 Reserved for future use
Decode flag will set to 1 (B3, B4 and B5 all set to 1) in OPOS raw data mode.

Track ID

Track ID is a byte of ID, it will be '1', '2' and '3' for track 1, 2 and 3; it is not accurate to use start sentinel to identify track.

Track x Error

Track x error is a byte of flags, it will be in format of: 0 0 1 b4, b3, b2 b1 b0
B0 1: Start sentinel error (0: Not start sentinel error)
B1 1: End sentinel error (0: Not end sentinel error)
B2 1: Parity error (0: Not parity error)
B3 1: LRC error (0: Not a LRC error)
B4 1: Other error (0: Not other error)
Track x Error is set to 0x20 in OPOS raw data mode.

Track Length

Assume actual "Track x Data Length" is hex code xy; the Track x data length for OPOS mode output will be hex code 3x, 3y.
Track x data length does not include the byte of "Track x data LRC", it is <30> <30> in case of read error on track x.

Track Data
"Card Track x LRC code" is track x card data.

Track x LRC
"Track x data LRC" is a LRC to check track x data communication; XOR all characters start from "Track x ID" to "Track x data LRC" should be 0.

9.2 Security Level 1 and Level 2 Standard Mode Output Format

9.2.1 USBHID Output Format

ID TECH HID Reader Data Structure

Offset	Usage Name
0	T1 decode status
1	T2 decode status
2	T3 decode status
3	T1 data length
4	T2 data length
5	T3 data length
6	Card encode type
7, 8	Total Output Length
9-HIDSIZE*	Output Data

In this approach, the reader will keep all of the ID TECH output format and other features like pre-amble, post-amble, etc. The output data is always HIDSIZE* bytes; the "Total Output Length" field indicates the valid data length in the output data
Note*: HIDSIZE (580 bytes as described in USB enumeration. HIDSIZE is subject to change. Software should be auto adjust in case enumeration changes).

Device Descriptor:

Field	Value	Description
Length	12	
Des type	01	
BCD USB	00 02	USB 2.0
Device Class	00	Unused
Sub Class	00	Unused
Device Protocol	00	Unused
Max Packet Size	08	
VID	0A CD	
PID	06 40 06 20 25 10 25 20	HID ID TECH Structure HID Keyboard Secure HID ID TECH Structure Secure HID Keyboard
BCD Device Release	00 01	
i-Manufacture	01	

i-Product	02	
i-Serial-Number	00	
# Configuration	01	

Configuration Descriptor:

Field	Value	Description
Length	09	
Des type	02	
Total Length	22 00	
No. Interface	01	
Configuration Value	01	
iConfiguration	00	
Attributes	80	Bus power, no remove wakeup
Power	32	100 mA

Interface Descriptor:

Field	Value	Description
Length	09	
Des type	04	
Interface No.	00	
Alternator Setting	00	
# EP	01	
Interface Class	03	HID
Sub Class	01	
Interface Protocol	01	
iInterface	00	

HID Descriptor:

Field	Value	Description
Length	09	
Des type	21	HID
bcdHID	11 01	
Control Code	00	
numDescriptors	01	Number of Class Descriptors to follow
DescriptorType	22	Report Descriptor
Descriptor Length	37 00 3D 00 52 00	HID ID TECH format HID Other format HID Keyboard format

End Pointer Descriptor:

Field	Value	Description
Length	07	
Des Type	05	End Point
EP Addr	83	EP3 – In
Attributes	03	Interrupt
MaxPacketSize	40 00	
bInterval	01	

Report Descriptor: (USB-HID)

Value	Description
06 00 FF	Usage Page (MSR)
09 01	Usage(Decoding Reader Device)
A1 01	Collection (Application)
15 00	Logical Minimum
26 FF 00	Logical Maximum
75 08	Report Size
09 20	Usage (Tk1 Decode Status)
09 21	Usage (Tk2 Decode Status)
09 22	Usage (Tk3 Decode Status)
09 28	Usage (Tk1 Data Length)
09 29	Usage (Tk2 Data Length)
09 2A	Usage (Tk3 Data Length)
09 38	Usage (Card Encode Type)
95 07	Report Count
81 02	Input (Data,Var,Abs,Bit Field)
09 30	Usage (Total Sending Length)
95 02	Report Count (2)
82 02 01	Input (Data, Var, Abs, Bit Field)
09 31	Usage (Output Data)
96 3B 02	Report Count (512 + 59=571+9=580)
82 02 01	Input (Data, Var, Abs, Bit Field)
09 20	Usage (Command Message)
95 08	Report Count
B2 02 01	Feature (Data,Var, Abs, Buffered Bytes)
C0	End Collection

Report Descriptor: (USB KB)

Value	Description
05 01	Usage Page (Generic Desktop)
09 06	Usage(Keyboard)
A1 01	Collection (Application)
05 07	Usage Page (Key Codes)
19 E0	Usage Minimum
29 E7	Usage Maximum
15 00	Logical Minimum
25 01	Logical Maximum
75 01	Report Size
95 08	Report Count
81 02	Input (Data,Variable,Absolute)
95 01	Report Count (1)
75 08	Report Size
81 01	Input Constant
95 05	Report Count

75 01	Report Size
05 08	Usage Page (LED)
19 01	Usage Minimum
29 05	Usage maximum
91 02	Output(Data Variable Absolute)
95 01	Report Count
75 03	Report Size
91 01	Output (Constant)
95 06	Report Count
75 08	Report Size
15 00	Logical Minimum
25 66	Logical Maximum (102)
05 07	Usage Page (key Code)
19 00	Usage Minimum
29 66	Usage Maximum (102)
81 00	Input(Data, Array)
06 2D FF	Usage Page (ID TECH)
95 01	Report Count
26 FF 00	Logical maximum (255)
15 01	Logical Minimum
75 08	Report Size (8)
09 20	Usage (Setup data byte)
95 08	Report Count (8)
B2 02 01	Feature (Data Var, Abs)
C0	End Collection

9.2.2 RS232, USBCDC, and USBKB Output Format

MSR output can be sent out with or without protocol envelope. By default, the envelope is included. (There is always a protocol envelope on commands and responses)

TLP Envelope:
60 <Len_H><Len_L><card data indication 1><card data indication 2>[Track 1 data][Track2 data][Track 3 data]<LRC>03

ITP Envelope:
02<card data indication 1><card data indication 2>[Track 1 data][Track2 data][Track 3 data] 03 <LRC>

<card data indication 1 > is always 0xC0.

<card data indication 2> is to indicate reading status.

Bit	0	1
B0	Track 1 decode fail	Track 1 decode success
B1	Track 2 decode fail	Track 2 decode success

B2	Track 3 decode fail	Track 3 decode success
B3	No Track 1 data	Track 1 data exists
B4	No Track 2 data	Track 2 data exists
B5	No Track 3 data	Track 3 data exists
B6-B7	Unused (set to 0)	

Note:

- The Track x decode flag will be 0 if Track x data does not exist.
- The order of magnetic data and switch change notification depends on the order in which they come to the microcontroller.This is not fixed. Where possible, the reader will try to keep the switch and data reporting consistent.

For [Track1 data], [Track2 data] and [Track 3 data], please see below
Track 1: <SS1><T1 Data><ES><CR>
Track 2: <SS2><T2 Data><ES><CR>
Track 3: <SS3><T3 Data><ES><CR>
Where: SS1(start sentinel track 1) = %
SS2 (start sentinel track 2) = ;
SS3 (start sentinel track 3) = ; for ISO, ! for CDL, % for AAMVA
ES (end sentinel all tracks) = ?

9.3 Level 3 Output Data Format

SecureMOIR has two different envelopes for the secure output format which are listed as below:

Secure output format when reader is in TLP:
<60><LenH><LenL><Card Data><CheckLRC><ETX>

Secure output format when reader is in ITP:
This format is compatible with other ID TECH swipe reader products including SecureMag, SecureHead, etc. Please note there is an exception that this output is different from ITP as this secure output format has two bytes length<LenL> and <LenH> in the HEADER in reverse order and an extra <CheckSum>.
<STX><LenL><LenH><Card Data><CheckLRC><CheckSum><ETX>
<STX> = 02h, <ETX> = 03h
<LenL><LenH> is a two byte length of <Card Data>. <LenL> is the length low byte, and <LenH> is the length high byte.
<CheckLRC> is a one byte Exclusive-OR sum calculated for all <Card Data>.
<CheckSum> is a one byte Sum value calculated for all <Card data>.

For the <CardData>, please refer to the original encryption format and enhanced encryption format listed below:

9.3.1 Original Encryption Format

<Card Data> card data format is shown below.

ISO/ABA Data Output Format:

	Data Field	**Notes**
3	Card encoding type	(00: ISO/ABA; 04: for Raw Mode)

4	Track status	(1 byte, see Notes Field 4 in 9.3.2)
5	Track 1 unencrypted length	(1 byte, 0 for no track1 data)
6	Track 2 unencrypted length	(1 byte, 0 for no track2 data)
7	Track 3 unencrypted length	(1 byte, 0 for no track3 data)
8	Track 1 masked	(Omitted if in Raw mode)
9	Track 2 masked	(Omitted if in Raw mode)
10	Track 3 data in clear	(Omitted if in Raw mode)
11	Track 1,2 encrypted	(AES/TDES encrypted data)
12	Track 3 encrypted	(only if card encoding type 04)
13	Track 1 hashed	(20 bytes SHA1-Xor)
14	Track 2 hashed	(20 bytes SHA1-Xor)
15	DUKPT serial number	(10 bytes)

Non ISO/ABA Data Output Format

	Data Field	**Notes**
3	Card encoding type	(01: AAMVA; 03: Others)
4	Track status	(1 byte, see Notes Field 4 in 9.3.2)
5	Track 1 unencrypted data length	(1 byte, 0 for no track1 data)
6	Track 2 unencrypted data length	(1 byte, 0 for no track2 data)
7	Track 3 unencrypted data length	(1 byte, 0 for no track3 data)
8	Track 1 data	
9	Track 2 data	
10	Track 3 data	

9.3.2 **Enhanced Encryption Format**

IOS/ABA card

	Data Field	**Notes**
3	Card Encode Type	(80: ISO/ABA; 84: for Raw Mode)
4	Track 1-3 Status	(1 byte, see Field 4 in Notes below)
5	T1 unencrypted data length	(1 byte, 0 for no track1 data)
6	T2 unencrypted data length	(1 byte, 0 for no track1 data)
7	T3 unencrypted data length	(1 byte, 0 for no track1 data)
8	Mask/Clear Status	(1 byte, see Field 8 in Notes below)
9	Encrypt/Hash Status	(1 byte, see Field 9 in Notes below)
10	T1 data (masked if card type 0)	(omitted if card type 84)
11	T2 data (masked if card type 0)	(omitted if card type 84)
12	T3 data unencrypted	(omitted if card type 84)
13	T1 data encrypted	(AES/TDES encrypted data)
14	T2 data encrypted	(AES/TDES encrypted data)
15	T3 data encrypted	(AES/TDES encrypted data)
16	T1-T3 hashed (if card type 0 or 4)	(20 bytes each)
17	KSN	(10 bytes)

Non ISO/ABA Data Output Format

	Data Field	Notes
3	Card Encode Type*	(81: AAMVA; 83: Others)
4	Track 1-3 Status	(1 byte, see Field 4 in Notes below)
5	T1 unencrypted data length	(1 byte, 0 for no track1 data)
6	T2 unencrypted data length	(1 byte, 0 for no track1 data)
7	T3 unencrypted data length	(1 byte, 0 for no track1 data)
8	Clear/mask data sent status	(1 byte, see Field 8 in Notes below)
9	Encrypted/Hash data sent status	(1 byte, see Field 8 in Notes below)
10	T1 clear data	
11	T2 clear data	
12	T3 clear data	

Notes:

- Card Encode Type:

Value for Original Format	Value for Enhanced Format	Encode Type	Description
00	80	ISO/ABA	ISO/ABA encode card
01	81	AAMVA	AAMVA encode card
03	83	Other	The card has a non-standard format. For example, ISO/ABA track 1 format on track 2
04	84	Raw	The card data is sent in Raw encrypted format. All tracks are encrypted and no mask data is sent
06		JIS I	JIS I encode card
07		JIS II	JIS II encode card

T1, T2 or T3 data: The length of each track data field (varies by the length of valid data in each field) is determined by the track data length field that corresponds to the track number. The track data includes all data string starting with the start sentinel and ending with the end sentinel and track LRC.

- **Field 4**: Track 1-3 Status
  - Bit 0: 0-track 1 decode fail; 1- tk1 decoded data present
  - Bit 1: 0- track 2 decode fail; 1- tk2 decoded data present
  - Bit 2: 0- track 3 decode fail; 1- track 3 decoded data present
  - Bit 3: 0- no track 1 sampling data; 1- track 1 has sampling data present
  - Bit 4: 0- no track 2 sampling data; 1- track 2 has sampling data present
  - Bit 5: 0- no track 3 sampling data; 1- track 3 has sampling data present
  - Bit 6: always 0- reserved for future use
  - Bit 7: always 0- reserved for future use

- **Field 8** Clear/mask data sent status
  - Bit 0:0-no track1 clear or masked Data; 1-track1 clear or masked Data present
  - Bit 1:0-no track2 clear or masked Data; 1-track2 clear or masked Data present
  - Bit 2:0-no track3 clear or masked Data; 1-track3 clear or masked Data present
  - Bit 3:0-DUKPT key; 1-fixed key
  - Bit 4:0-TDES; 1-AES
  - Bit 5:0-reserved for future so always 0
  - Bit 6:0-Data key; 1-PIN key
  - Bit 7: 0-no SN; 1-serial number included

- **Field 9:** Encrypted data sent status
  - Bit 0: 0- no track1 encrypted data; 1- track1 encrypted data present
  - Bit 1: 0- no track2 encrypted data; 1- track2 encrypted data present
  - Bit 2: 0- no track3 encrypted data; 1- track3 encrypted data present
  - Bit 3: 0- no track 1 hash data; 1- track 1 hash data present
  - Bit 4: 0- no track2 hash data; 1- track2 hash data present
  - Bit 5: 0- no track3 hash data; 1- track3 hash data present
  - Bit 6: 0- no session ID; 1- session ID present
  - Bit 7: 0- no KSN; 1- KSN present

- Encryption Option Setting: (for enhanced encryption format only)
- The force encryption mode is used when all tracks must be encrypted, when encrypted OPOS support is required, when the tracks must be encrypted separately, when cards other than type 0 (ABA bank cards) must be encrypted or when track 3 must be encrypted.

  Command: 53 84 01 <Encryption Option>

  Encryption Option: (**default 08h**)
  bit0: 1 – track 1 force encrypt
  bit1: 1 – track 2 force encrypt
  bit2: 1 – track 3 force encrypt
  bit3: 1 – track 3 force encrypt when card type is 0
  bit4: 1 – include mask data on ISO 4909 track 3 which will be encrypted if Type 0 card
  Note:
  1) When force encrypt is set, this track will always be encrypted, regardless of card type. No clear/mask text will be sent.
  2) If and only if in enhanced encryption format, each track is encrypted separately. Encrypted data length will round up to 8bytes for TDES or 16 bytes for AES.
  3) In original encryption format, only track 1 and track 2 of type 0 cards (ABA bank cards) will be encrypted together.

- Hash Option Setting:
  Command: 53 5C 01 <Hash Option>
  Hash Option: ('0' – **'7', default 0x07**)
  Bit0: 1 – track1 hash will be sent if data is encrypted
  Bit1: 1 – track2 hash will be sent if data is encrypted
  Bit2: 1 – track3 hash will be sent if data is encrypted

- Mask Option Setting: (for enhanced encryption format only)
  Command: 53 86 01 <Mask Option>
  Mask Option: (**Default: 0x07**)
  bit0: 1 – tk1 mask data allowed to be sent when ISO/ABA card is encrypted
  bit1: 1 – tk2 mask data allowed to be sent when ISO/ABA card is encrypted
  bit2: 1 – tk3 mask data allowed to sent when ISO/ABA card is encrypted

  When mask option bit is set – if data is encrypted (but not forced encrypted), the mask data will be sent; If mask option is not set, the mask data will not be sent under the same condition.

9.4 *Level 4 Data Output Format*

Typically, most of users use Security Level 3 after a key is injected. The Security Level 4 requires more authentication procedure, so use it with care and as appropriate.

The level 4 output format has the same envelope as level 3, please see section 9.3. The <CardData> for Level 4 are listed in sections below.

9.4.1 Level 4 Original Format

ISO/ABA Data Output Original Encrypted Format

	Date field	Notes
3	Card encoding type	(00: ISO/ABA)
4	Track status	(1 byte, see Notes Field 4 in 9.3.2)
5	Tack 1 unencrypted length	(1 byte in hex, 0 for no track1 data)
6	Track 2 unencrypted length	(1 byte in hex, 0 for no track2 data)
7	Track 3 unencrypted length	(1 byte in hex, 0 for no track3 data)
8	Track 1 masked	
9	Ttrack 2 masked	
10	Track 3 data	
11	Track 1,2,3 encrypted	(AES/TDES encrypted data, bytes)
12	SessionID encrypted	(AES/TDES encrypted data, bytes)
13	Track 1 hashed	(20 bytes SHA1-Xor)
14	Track 2 hashed	(20 bytes SHA1-Xor)
15	DUKPT serial number(KSN)	(10 bytes)

Non ISO/ABA Data Output (Non-Encrypted) Format

	Data Field	Notes
3	Card encoding type	(01: AAMVA, 03: Others)
4	Track status	(1 byte, see Notes Field 4 in 9.3.2)
5	Track 1 length	(1 byte in hex, 0 for no track1 data)
6	Track 2 length	(1 byte in hex, 0 for no track2 data)
7	Track 3 length	(1 byte in hex, 0 for no track3 data)
8	Track 1 data	
9	Track 2 data	
10	Track 3 data	

9.4.2 Level 4 Enhanced Format

For ISO card, both clear and encrypted data are sent. For other card, only clear data are sent.
A card insertion and/or removal return the following data:
Note: if all tracks are bad, an empty packet is sent.

ISO/ABA Data Output Enhanced Format:

	Data Field	Notes
3	Card encoding type	(80: ISO/ABA, 84: for Raw Mode)
4	Track status	(1 byte, see Notes Field 4 in 9.3.2)
5	Track 1 unencrypted length	(1 byte, 0 for no track1 data)
6	Track 2 unencrypted length	(1 byte, 0 for no track2 data)
7	Track 3 unencrypted length	(1 byte, 0 for no track3 data)
8	Mask/Clear Status	(1 byte, see Notes Field 8 in 9.3.2)
9	Encrypt/Hash Status	(1 byte, see Notes Field 9 in 9.3.2)
10	Track 1 masked	(Omitted if in Raw mode)
11	Track 2 masked	(Omitted if in Raw mode)
12	Track 3 data or masked data	(Omitted if in Raw mode)
13	Track 1 encrypted	(AES/TDES encrypted data)
14	Track 2 encrypted	(AES/TDES encrypted data)
15	Track 3 encrypted	(AES/TDES encrypted data)
16	SessionID encrypted	(Only in Level 4)
17	track 1 hashed (optional)	(20 bytes SHA-1-Xor)
18	track 2 hashed (optional)	(20 bytes SHA-1-Xor)
19	track 3 hashed (optional)	(20 bytes SHA-1-Xor)
20	DUKPT serial number(KSN)	(10 bytes)
21	Optional reader serial number	(10 bytes)

Non ISO/ABA Data Output Format

	Data Field	Notes
3	card encoding type	(81: AAMVA,83: Others)
4	track status	(bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling)
5	track 1 length	(1 byte, 0 for no track1 data)
6	track 2 length	(1 byte, 0 for no track2 data)
7	track 3 length	(1 byte, 0 for no track3 data)
8	track 1 data	
9	track 2 data	
10	track 3 data	

Notes:

- Card Encode Type:
  Please refer to the Card Encode Type in 9.3.2

  Description:

  Track 1 and Track 2 unencrypted Length

This one-byte value is the length of the original Track data. It indicates the number of bytes in the Track masked data field. It should be used to separate Track 1 and Track 2 data after decrypting Track encrypted data field.

Track 3 unencrypted Length
This one-byte value indicates the number of bytes in Track 3 masked data field.

Track 1 and Track 2 masked
Track data masked with the MaskCharID (default is '*'). The first PrePANID (up to 6 for BIN, default is 4) and last PostPANID (up to 4, default is 4) characters can be in the clear (unencrypted). The expiration date is masked by default but can be optionally displayed.

Track 1 and Track 2 encrypted
This field is the encrypted Track data, using either TDES-CBC or AES-CBC with initial vector of 0. If the original data is not a multiple of 8 bytes for TDES or a multiple of 16 bytes for AES, the reader right pads the data with 0 by default. The data can be padded according to PKCS #5 if Encrypt Option (0x84) bit 7 is set to 1.

The key management scheme is DUKPT and the key used for encrypting data is called the Data Key. Data Key is generated by first taking the DUKPT Derived Key exclusive or'ed with 0000000000FF0000 0000000000FF0000 to get the resulting intermediate variant key. The left side of the intermediate variant key is then TDES encrypted with the entire 16-byte variant as the key. After the same steps are preformed for the right side of the key, combine the two key parts to create the Data Key.

How to get Encrypted Data Length

The encrypted track data length is always a multiple of 8 bytes for TDES or multiple of 16 bytes for AES. This value will be zero if there was no data on both tracks or if there was an error decoding both tracks.

In the original format, Track 1 and Track 2 data are encrypted as a single block for financial card. In order to get the number of bytes for encrypted data field, we need to get Track 1 and Track 2 unencrypted length first, and add the Track 1 and Track 2 together. Round up the total length by 8 if it's TDES or 16 for AES.

In enhanced format, the tracks data are encrypted separately rather than as a group.
To calculate the encrypted track length for each track, round up the track unencrypted data length by 8 for TDES or 16 for AES. For example, to calculate the encrypted track 1 length, round up the track 1 unencrypted data length (field 5) by 8 for TDES or16 if it's AES. Please refer to section 11 Decryption Samples for detailed samples.

Track 1, 2 and 3 hashed
SecureMag reader uses SHA-1 to generate hashed data for track 1, track 2 and track 3 unencrypted data. It is 20 bytes long for each encrypted track. This is provided with two purposes in mind: One is for the host to ensure data integrity by comparing this field with a SHA-1 hash of the decrypted Track data, prevent unexpected noise in data transmission. The other purpose is to enable the host to store a token of card data for future use without keeping

the sensitive card holder data. This token may be used for comparison with the stored hash data to determine if they are from the same card.

9.5 *Level 4 Activate Authentication Sequence*

The security level changes from 3 to 4 when the device enters authentication mode successfully. Once the security level is changed to level 3 or 4, it cannot go back to a lower level.

Activate Authentication Mode Command

When the reader is in security level 4, it will only transmit the card data when it is Authenticated.

Authentication Mode Request

When sending the authentication request, the user also needs to specify a time limit for the reader to wait for the activation challenge reply command. The minimum timeout duration required is 120 seconds. If the specified time is less than the minimum, 120 seconds would be used for timeout duration. The maximum time allowed is 3600 seconds (one hour). If the reader times out while waiting for the activation challenge reply, the authentication failed.

Device Response

When authentication mode is requested, the device responds with two challenges: Challenge 1 and challenge 2. The challenges are encrypted using the current DUKPT key exclusive- or'ed with <F0F0 F0F0 F0F0 F0F0 F0F0 F0F0 F0F0 F0F0>.

The decrypted challenge 1 contains 6 bytes of random number followed by the last two bytes of KSN. The two bytes of KSN may be compared with the last two bytes of the clear text KSN sent in the message to authenticate the reader. The user should complete the Activate Authentication sequence using Activation Challenge Reply command.

Command Structure
Host -> Device:
60 00 <LenL> 52<80h><02h><Pre-Authentication Time Limit><LRC> 03

Device -> Host:
60 00 <LenH><Device Response Data><LRC><ETX> (success)
E0 00 02 6931 <LRC> 03 (fail—invalid DUKPT activation challenge)

Pre-Authentication Time Limit: 2 bytes of time in seconds
Device Response Data: 26 bytes data, consists of <Current Key Serial Number><Challenge 1><Challenge 2>

Current Key Serial Number: 10 bytes data with Initial Key Serial Number in the leftmost 59 bits and Encryption Counter in the rightmost 21 bits.
Challenge 1: 8 bytes challenge used to activate authentication. Encrypted using the key derived from the current DUKPT key.
Challenge 2: 8 bytes challenge used to deactivate authentication. Encrypted using the key derived from the current DUKPT key.

Activation Challenge Reply Command

This command serves as the second part of an Activate Authentication sequence. The host sends the first 6 bytes of Challenge 1 from the response of Activate Authenticated Mode command, two bytes of Authenticated mode timeout duration, and eight bytes Session ID encrypted with the result of current DUKPT Key exclusive- or'ed with <3C3C 3C3C 3C3C 3C3C 3C3C 3C3C 3C3C 3C3C>.

The Authenticated mode timeout duration specifies the maximum time in seconds, which the reader would remain in Authenticated Mode. A value of zero forces the reader to stay in Authenticated Mode until a card insertion and/or removal or power down occurs. The minimum timeout duration required is 120 seconds. If the specified time is less than the minimum, 120 seconds would be used for timeout duration. The maximum time allowed is 3600 seconds (one hour).

If Session ID information is included and the command is successful, the Session ID will be changed.

The Activate Authenticated Mode succeeds if the device decrypts Challenge Reply response correctly. If the device cannot decrypt Challenge Reply command, Activate Authenticated Mode fails and DUKPT KSN advances.

Command Structure
Host -> Device:
60 00 0B <S><82h><08h><Activation Data><LRC><ETX>

Device -> Host:
60 00 02 90 00 LRC 03 (success)
E0 00 02 xx xx LRC 03 (fail xxxx has the code for the reason for the failure)

Activation Data: 8 or 16 bytes, structured as <Challenge 1 Response> <Session ID>

Challenge 1 Response: 6 bytes of Challenge 1 random data with 2 bytes of Authenticated mode timeout duration. It's encrypted using the key derived from the current DUKPT key.
Session ID: Optional 8 bytes Session ID, encrypted using the key derived from the current DUKPT key.

Deactivate Authenticated Mode Command

This command is used to exit Authenticated Mode. Host needs to send the first 7 bytes of Challenge 2 (from the response of Activate Authenticated Mode command) and the Increment Flag (0x00 indicates no increment, 0x01 indicates increment of the KSN) encrypted with current DUKPT Key exclusive- or'ed with <3C3C 3C3C 3C3C 3C3C 3C3C 3C3C 3C3C 3C3C>.

If device decrypts Challenge 2 successfully, the device will exit Authenticated Mode. The KSN will increase if the Increment flag is set to 0x01. If device cannot decrypt Challenge 2 successfully, it will stay in Authenticated Mode until timeout occurs or when customer inserts and/or removes a card.

The KSN is incremented every time the authenticated mode is exited by timeout or card insertion and/or removal action. When the authenticated mode is exited by Deactivate Authenticated Mode command, the KSN will increment when the increment flag is set to 0x01.
Command Structure
Host -> Device:

60 00 0B <S><83h><08h><Deactivation Data><LRC><ETX>

Device -> Host:
60 00 02 90 00<LRC><ETX> (success)
E0 00 02 XX XX<LRC><ETX> (fail)

<Deactivation data>: 8-bytes response to Challenge 2. It contains 7 bytes of Challenge 2 with 1 byte of Increment Flag, encrypted by the specified variant of current DUKPT Key

Get Reader Authentication Status Command
Command Structure
Host -> Device:
60 00 02 <R><83h><LRC><ETX>

Device -> Host:
60 00 02 <STX><83h><02h><Current Authentication Reader Status><Pre-condition><LRC><ETX> (success)
<NAK> (fail) [6931] invalid DUKPT activation challenge

Current Reader Status: 2-bytes data with one byte of <Reader State> and one byte of <Pre-Condition>

Reader State: indicates the current state of the reader
- 0x00: The reader is waiting for Activate Authentication Mode Command. The command must be sent before the card can be read.
- 0x01: The authentication request has been sent, the reader is waiting for the Activation Challenge Reply Command.
- 0x02: The reader is waiting for a card insertion and/or removal.

Pre-condition: specifies how the reader goes to its current state as follows
- 0x00: The reader has no card insertion or removal and has not been authenticated since it was powered up.
- 0x01: Authentication Mode was activated successfully. The reader processed a valid Activation Challenge Reply command.
- 0x02: The reader receives a good card insertion and/or removal.
- 0x03: The reader receives a bad card insertion and/or removal or the card is invalid.
- 0x04: Authentication Activation Failed.
- 0x05: Authentication Deactivation Failed.
- 0x06: Authentication Activation Timed Out. The Host fails to send an Activation Challenge Reply command within the time specified in the Activate Authentication Mode command.

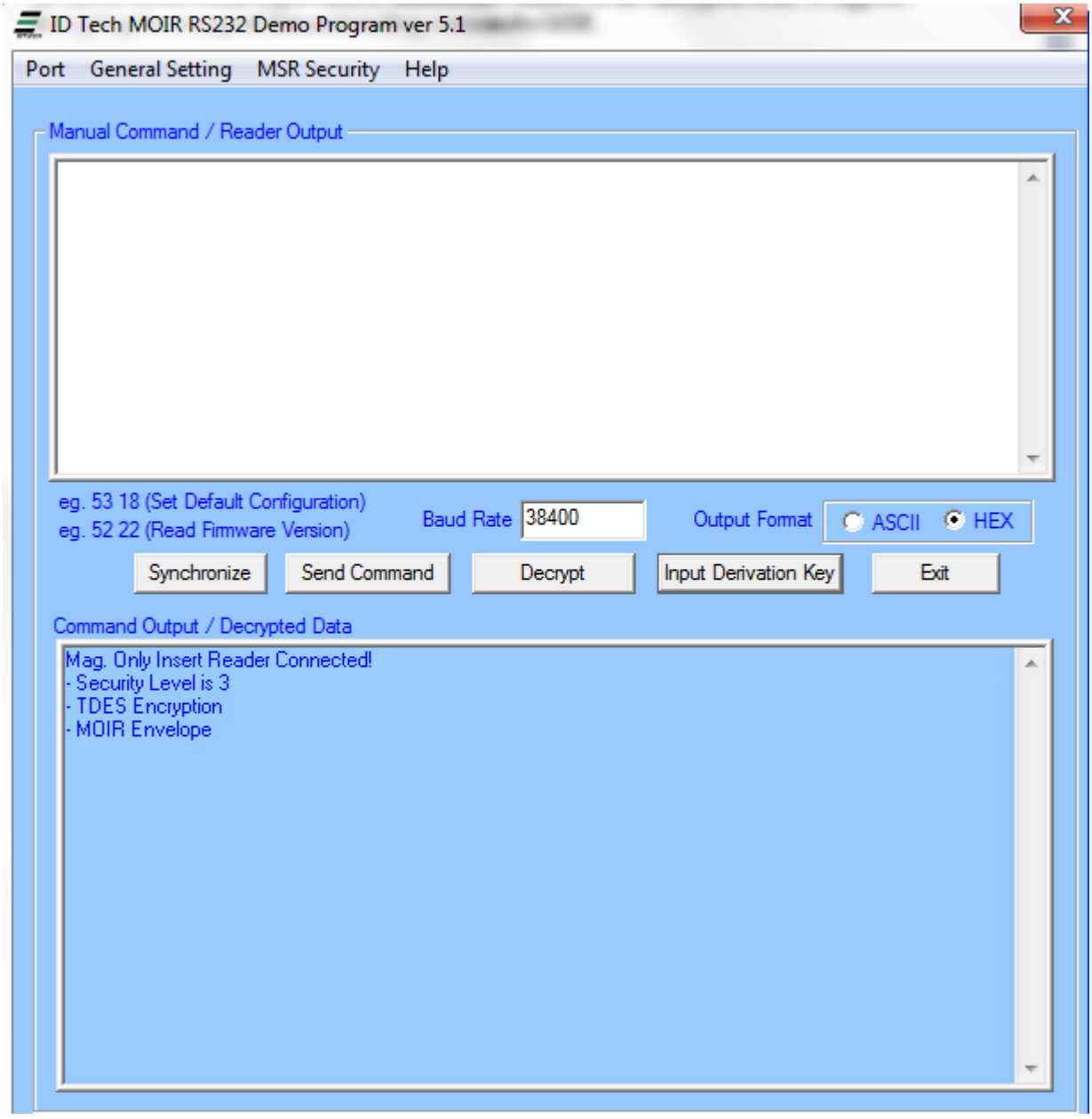
0x07: insertion and/or removal Timed Out. The user fails to insertion and/or removal a card within the time specified in the Activation Challenge Reply command

10 USING THE DEMO PROGRAM

ID TECH MOIR Demo is provided to demonstrate features of the Encrypted MSR. It supports decrypting the encrypted data and sending command to MSR.

The demo software can be downloaded from the website via the link below:
http://www.idtechproducts.com/download/insert-readers/cat_view/95-insert-readers/457-securemoir.html

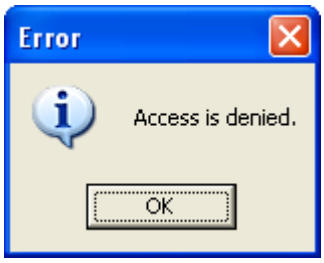
Overview of SecureMOIR Demo



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.

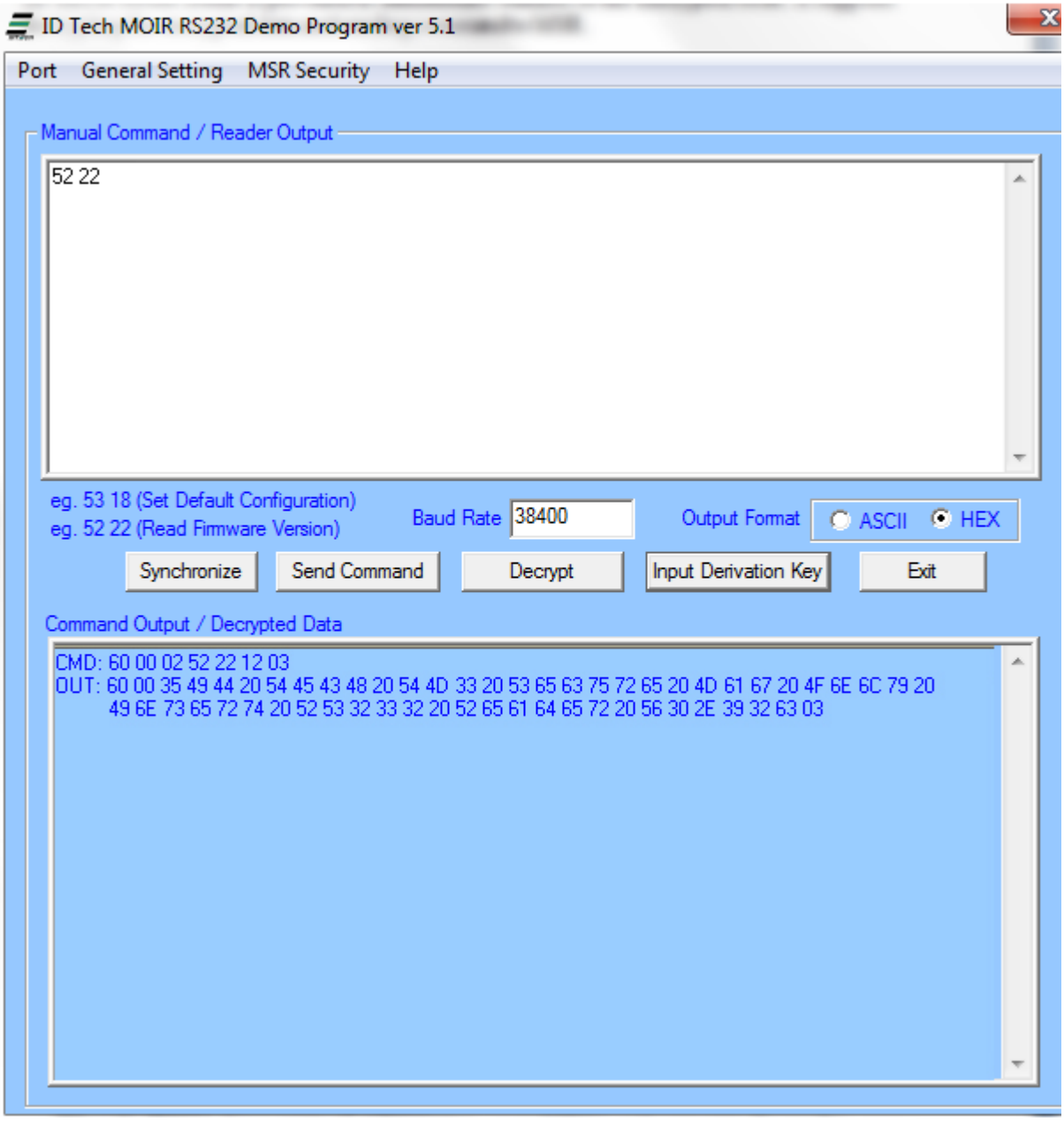
10.1 Manual Command

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

Command will be 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 before <LRC>
e.g. 60 00 02 53 18 4A 03 (Set Default Configuration)
e.g. 60 00 02 52 22 71 03 (Read Firmware Version)

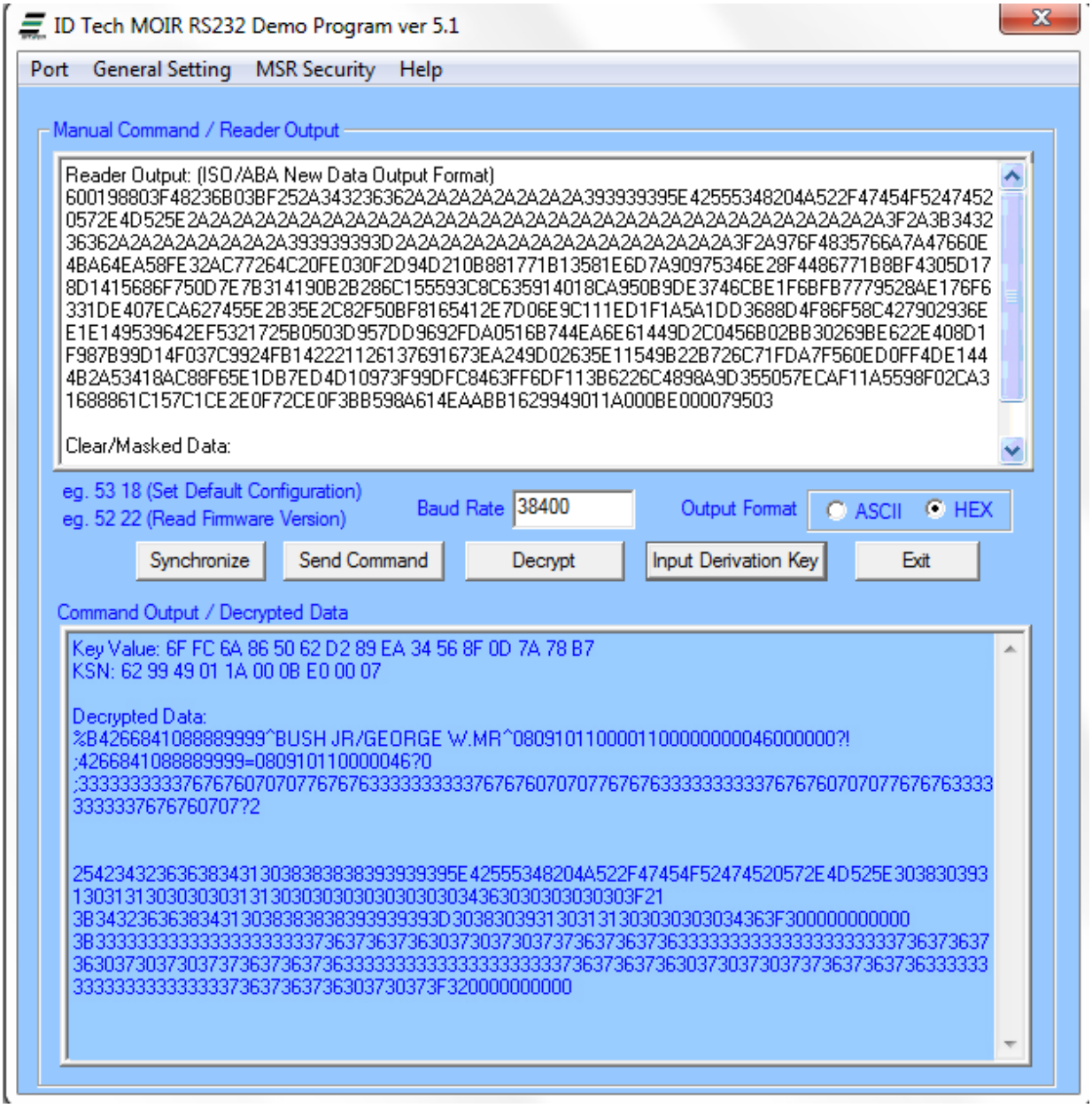
Press “Send Command”, the input and output would be shown in the lower text box.

If it is desired to use a demo to communicate in ITP, the SecureMag RS232 demo can be used. But the baud rate of the reader needs to be configured to 9600 first as the SecureMag RS232 demo uses baud rate 9600.



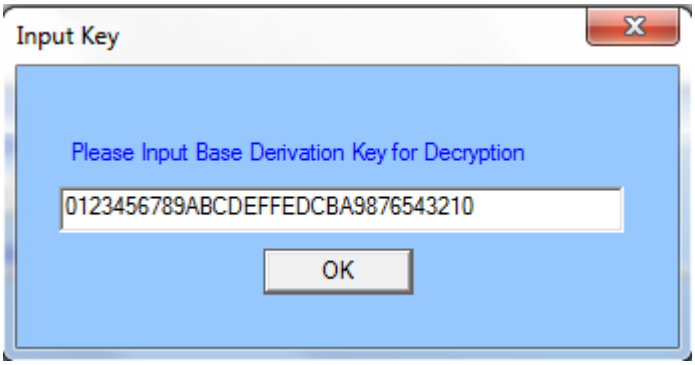
10.2 Security Level 3 Decryption

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.

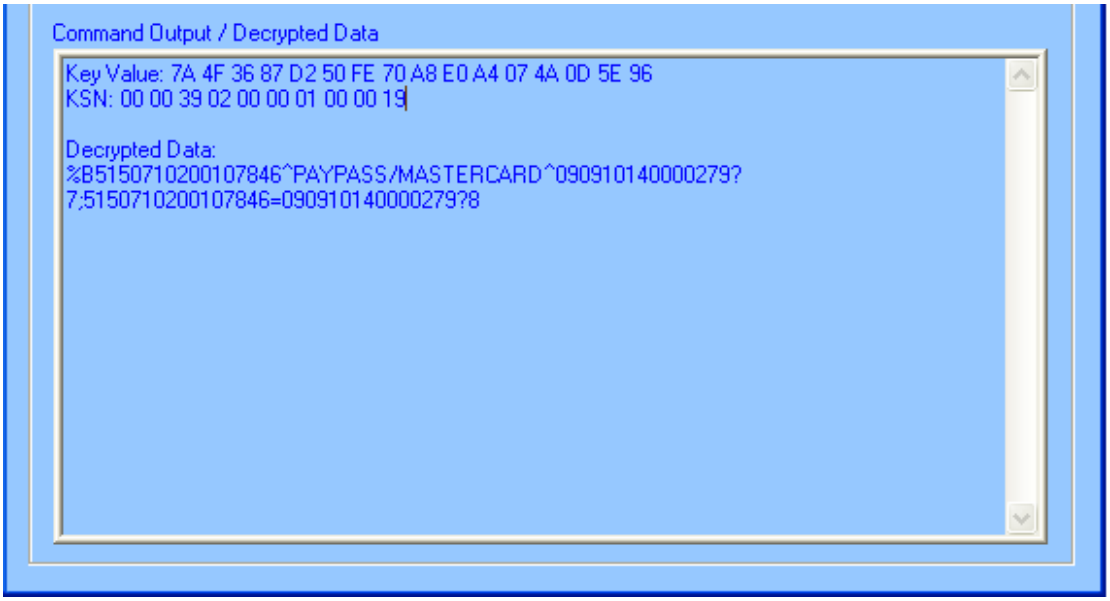


To get the decrypted data, press the “Decrypt” button and the decrypted card data will be displayed in the lower box.

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



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



10.3 **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.

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

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

Port
Select Com port and open/ close port.

Help
Provides version information of the demo software.

11 DECRYPTION EXAMPLES

BDK for all examples is
0123456789ABCDEFFEDCBA9876543210

Example Security Level 3 Decryption with default settings
Example of decryption of a three-track ABA card with the enhanced encryption format with TDES. Enhanced encryption format can be recognized because the high bit of the fourth byte underlined (80) is 1. If the reader is set to default, it will send out the card insertion and removed status that will precede and trail the encrypted card transaction data. The card status messages have been placed into separate lines in the message below to simplify interpretation. This is the block of data received from the reader that must be interpreted and decrypted.

600002B008DA03
600002B00AD803
600002B008DA03
600198<u>80</u>3F48236B03BF252A343236362A2A2A2A2A2A2A2A393939395E42555348204A522F47
454F52474520572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A
2A2A2A2A2A2A2A2A3F2A3B343236362A2A2A2A2A2A2A2A393939393D2A2A2A2A2A2A2A2A2A
2A2A2A2A2A2A2A3F2A26B03F2BD327CA087C159DEA3E77974A36B6E89CB5BC85EF92D08
FB01152089099FE2A348DF2BA8D7AFEF16A1F5F2CEA46946A92CDC2AB3B750D1AEF81279
95EE6A944E12F9DF40E46607F06C68E057DA05CC3BBB2BD68ECE1D7D89A4671423C4F6490
82106A785A62D9382968BCF4CFD0ECE3CF33449F265542CB4AE6240F99CDACD08E92744FF
C04C683834EB4D04C9CB9D2A4B4A4FFE15F7C70169C89288097C4B8BB42C67D33073CFEE6
8B95D0F88C6CF82F86BF8E7FE5909D153710399940C9DAD8BD26E929EE98BEBFA9D3C19A
AC047B61E8ED56BE52D4A7F8B5FFFA013418AC88F65E1DB7ED4D10973F99DFC8463FF6DF
113B6226C4898A9D355057ECAF11A5598F02CA31688861C157C1CE2E0F72CE0F3BB598A614
EAABB1629949011A000BE00003D703
600002B000D203

TLP protocol example separated into parts and explained:
Card present detected status
600002B008DA03

Card present and card seated status
600002B00AD803

Card present detected status
600002B008DA03

Actual start of the encrypted transaction
60, length(MSB, LSB), card type, track status, length track 1-length track 2- length track 3, mask clear status, crypt hash status
60 0198 80 3F 48-23-6B 03BF

0198 Total message length in hexadecimal
3F Track 1-3 found and properly decoded
48 Length of track 1 data is 48h (72 decimal) bytes

23 Length of track 2 data is 23h (35 decimal) bytes
6B Length of track 3 data is 6Bh (107 decimal) bytes
03 indicates tracks 1 and 2 as masked
BF Tracks 1-3 are encrypted
Tracks 1-3 are hashed
The KSN is included

Track one masked track data displayed in hexadecimal
252A343236362A2A2A2A2A2A2A2A393939395E42555348204A522F47454F52474520572E4D52
5E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2
A

Track two masked track data displayed in hexadecimal
3B343236362A2A2A2A2A2A2A2A393939393D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A

Track one encrypted track data displayed in hexadecimal
26B03F2BD327CA087C159DEA3E77974A36B6E89CB5BC85EF92D08FB011520890
99FE2A348DF2BA8D7AFEF16A1F5F2CEA46946A92CDC2AB3B750D1AEF8127995E
E6A944E12F9DF40E

Track two encrypted track data displayed in hexadecimal
46607F06C68E057DA05CC3BBB2BD68ECE1D7D89A4671423C4F649082106A785A
62D9382968BCF4CF

Track three encrypted track data displayed in hexadecimal
D0ECE3CF33449F265542CB4AE6240F99CDACD08E92744FFC04C683834EB4D04C
9CB9D2A4B4A4FFE15F7C70169C89288097C4B8BB42C67D33073CFEE68B95D0F8
8C6CF82F86BF8E7FE5909D153710399940C9DAD8BD26E929EE98BEBFA9D3C19A
AC047B61E8ED56BE52D4A7F8B5FFFA01

First 20-bytes of track one data hashed
3418AC88F65E1DB7ED4D10973F99DFC8463FF6DF

First 20-bytes of track two data hashed
113B6226C4898A9D355057ECAF11A5598F02CA31

First 20-bytes of track three data hashed
688861C157C1CE2E0F72CE0F3BB598A614EAABB1

KSN
629949011A000BE00003

LRC and ETX
D7 03

Card Removed from reader status
600002B000D203

Decrypted Data:
%B4266841088889999^BUSH JR/GEORGE W.MR^0809101100001100000000046000000?!
;4266841088889999=0809101100000046?0
;3333333337676760707077676763333333333767676070707767676333333333376767607070776767633333333337676760707077676763333333333767676070707767?2

Clear/Masked Data displayed in ASCII:
Track 1: %*4266********9999^BUSH JR/GEORGE
W.MR^********************************?*
Track 2: ;4266********9999=****************?*

Key Value: 1A 99 4C 3E 09 D9 AC EF 3E A9 BD 43 81 EF A3 34
KSN: 62 99 49 01 19 00 00 00 00 02

Decrypted Data displayed in ASCII:
%B4266841088889999^BUSH JR/GEORGE W.MR^0809101100001100000000046000000?!
;4266841088889999=0809101100000046?0
;3333333337676760707077676763333333333767676070707767676333333333376767607070776767633333333337676760707077676763333333333767676070707767?2

Track 1 decrypted data in hex including padding zeros (but there are no pad bytes here)
2542343236363834313038383838393939395E42555348204A522F47454F52474520572E4D525E30
383039313031313030303031313030303030303030303436303030303030303F21

Track 2 decrypted data in hex including padding zeros
3B34323636383431303838383838393939393D303830393130313130303030303034363F300000000000

Track 3 decrypted data in hex including padding zeros
3B33333333333333333333373637363736303730373037373637363736333333333333333333333373
6373637363037303730373736373637363633333333333333333333373637363736303730373037303737363
7363736333333333333333333333736373637363037303730373F320000000000

Example Security Level 4 decryption

Decryption example of a three track ABA card with the enhanced encryption format in AES:
This example does not include the card status reports.

6001B8803F48236B03FF252A343236362A2A2A2A2A2A2A2A393939395E42555348204A522F47
454F52474520572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A
2A2A2A2A2A2A2A2A3F2A3B343236362A2A2A2A2A2A2A2A393939393D2A2A2A2A2A2A2A2A2A
2A2A2A2A2A2A2A3F2ADBD7EFAF49EE84708053F744F288916E851789A445843030809C0E25
3E6900EEA0FFD078D51B9A7840AA5F98CC2DEADB2497DF29D6C848645E8241D4ED80AA92
ACA5D09E0F1F3669CE77D4BE332BDCE2E1295C13ADF4BE7793FA7FA24128171796A45E394
04F4A4DE137B4BA165F67719BC633087F11330F4DB2323618CEAAA40DB37773676888FF493
D82F8F9757E8148F9C05EC1BB2D2D54FB8F320C793C1F3C7D8916C693F97970DFAED98F1E
CAC6AF24BBA783BE7EDA1EB897D0CF737C6B95AF16BD15C6AE99C2C7B99EB079F2E1987
7DF3482A0CE5ABD8A8DDFED106C07A3244F0C932BF691B07023D671656B2AAB5A5B65170
A895BE90610DA284394723418AC88F65E1DB7ED4D10973F99DFC8463FF6DF113B6226C4898

A9D355057ECAF11A5598F02CA31688861C157C1CE2E0F72CE0F3BB598A614EAABB1629949
011A0003A000130003

Actual start of the encrypted transaction
60, length(MSB, LSB), card type, track status, length track 1-length track 2-length track 3, mask clear status, crypt hash status
60 01B8 80 3F 48-23-6B 03FF

01B8 Total message length in hexadecimal(0x1B8 440 decimal bytes)
80 Enhanced encryption structure (default) with ABA card
3F Tracks 1-3 found and properly decoded
48 Length of track 1 data is 48h (72 decimal) bytes
23 Length of track 2 data is 23h (35 decimal) bytes
6B Length of track 3 data is 6Bh (107 decimal) bytes
03 indicates tracks 1 and 2 as masked
FF Tracks 1-3 are encrypted
Tracks 1-3 are hashed
The KSN is included
The Session ID is included

Track one encrypted track data displayed in hexadecimal (length rounded up to next length evenly divisible by 16 (the AES block size)
DBD7EFAF49EE84708053F744F288916E851789A445843030809C0E253E6900EE
A0FFD078D51B9A7840AA5F98CC2DEADB2497DF29D6C848645E8241D4ED80AA92
ACA5D09E0F1F3669CE77D4BE332BDCE2

Track two encrypted track data displayed in hexadecimal (length rounded up to next length evenly divisible by 16 (the AES block size)
E1295C13ADF4BE7793FA7FA24128171796A45E39404F4A4DE137B4BA165F6771
9BC633087F11330F4DB2323618CEAAA4

Track three encrypted track data displayed in hexadecimal (length rounded up to next length evenly divisible by 16 (the AES block size)
0DB37773676888FF493D82F8F9757E8148F9C05EC1BB2D2D54FB8F320C793C1F
3C7D8916C693F97970DFAED98F1ECAC6AF24BBA783BE7EDA1EB897D0CF737C6B
95AF16BD15C6AE99C2C7B99EB079F2E19877DF3482A0CE5ABD8A8DDFED106C07
A3244F0C932BF691B07023D671656B2A

Session ID encrypted data displayed in hexadecimal (Only present in encryption level ‘4’)
AB5A5B65170A895BE90610DA28439472

First 20-bytes of track one data hashed (20 bytes)
3418AC88F65E1DB7ED4D10973F99DFC8463FF6DF

First 20-bytes of track two data hashed (20 bytes)
113B6226C4898A9D355057ECAF11A5598F02CA31

First 20-bytes of track three data hashed (20 bytes)

688861C157C1CE2E0F72CE0F3BB598A614EAABB1

KSN (10 bytes)
629949011A0003A00013

LRC and ETX
00 03

Clear/Masked Data in ASCII:
Track 1: %*4266********9999^BUSH JR/GEORGE
W.MR^********************************?*
Track 2: ;4266********9999=***************?*

Key Value: 8A DA 61 2E C2 8F B1 81 96 DA 34 3F CB 32 95 7E
KSN: 62 99 49 01 1A 00 03 A0 00 13
Session ID: AA AA AA AA AA AA AA AA

Decrypted Data in ASCII all three tracks:
%B4266841088889999^BUSH JR/GEORGE W.MR^0809101100001100000000046000000?!
;4266841088889999=0809101100000046?0
;33333333376767607070776767633333333337676760707077676763333333333767676070707767
67633333333337676760707?2

Track 1 decrypted data in hex including padding zeros
254234323636383431303838383839393395E42555348204A522F47454F52474520572E4D525E30
383039313031313030303031313030303030303030303436303030303030303F2100000000000000000

Track 2 decrypted data in hex including padding zeros
3B343236363834313038383838393939393D303830393130313130303030303034363F3000000000000
000000000000000000

Track 3 decrypted data in hex including padding zeros
3B333333333333333333333736373637363037303730373736373637363633333333333333333333333373
637363736303730373037373637363736363333333333333333333333736373637363037303730373736373
736373633333333333333333333373637363736303730373F320000000000

12 APPENDIX ASetting Parameters and Values

Following is a table of default setting and available settings (value within parentheses) for each function ID. Most of Function ID can be used with Command ID 52 and 53 except it's specified that some particular Function ID can ONLY be used for 52(R) or 53(S) in the table below.

Function ID	Hex	Description	Default Setting	Description	
HTypeID*	10	Terminal Type	'0' ('0'~'2','4'~'6')	PC/AT, Scan Code Set 2, 1, 3, PC/AT with external Keyboard and PC/AT without External Keyboard	u k -
ReaderOptID	11	Reader Option	AFh (RS232) /23h (KB)	Any	
ChaDelayID*	12	Character Delay	'0' ('0'-'5')	2 ms inter-character delay	k -
TrackSelectID	13	Track Selection	'0' ('0'-'9')	Any Track 0-any; 1-7—bit 1 tk1, bit 2 tk2; bit 3 tk3. '8'—tk1-2; '9' tk2-3	
PollingIntervalID	14	Polling Interval	0x01~0xFF	USB HID Polling Interval can be set between 1ms and 255ms.	u
DataFmtID	15	Data Output Format	'0' ('0'~'2')	'0' – IDT envelope '1' – UIC envelope '2' – Magtek envelope	
FmtOptionID	16	UIC, Mag-Tek	H'59'	Refer to MiniMag RS232 User's Manual	
TrackSepID	17	Track Separator	CR/Enter	CR for RS232, Enter for KB any character supported except 00, which	

				means none.	
DefaultAllID	18	Default All	None. Only apply to command ID 52.	Send 52 18. All non-security settings revert to their default values. See section 7.3.2	
SendOptionID	19	Send Option	‘1’ (‘0’~0x3F) for RS232 ‘5’ for KB	Sentinel and Account number control See section 7.4.12	
MSRReadingID	1A	MSR Reading	‘1’ (‘0’~’2’)	‘1’ Enable MSR Reading; ‘0’ MSR disable; ‘2’ Buffer Mode	
DTEnableSendID*	1B	DT Enable Send	‘0’(‘0’,’1’,’3’)	Data Editing Control	-
CustomEquipID	1C	custom equipment setting	0x00 Single Head; 0x40 Dual Head	bit 6=0: single head; bit 6=1: 0x40 dual head; bit 5=1: 0x20 support JIS Unaffected by reset all; bit 4=1: device has Card Present Switch (front switch), 0: no Card Present Switch	r
DecodingMethodID	1D	MSR Read Direction	‘3’ (‘1’~’4’)	‘1’-both ‘2’-read on insert ‘3’-report on withdrawal ‘4’-read on withdrawal	
ReviewID	1F	Review All Settings	None. Only apply to Command ID 52.	Send 52 1F to review all settings	
TerminatorID	21	MSR Terminator	0x0D(Enter/KB)	CR for RS232, Enter for KB; 0 for none; any value legal (‘0’=CRLF)	
FmVerID	22	Firmware Version	None. Only apply to Command ID 52	Send 52 22 to get firmware version	
USBHIDFmtID	23	USB HID Fmt	‘0’ USB HID ‘8’ KB (‘0’,’8’)	‘0’ for USB HID ‘8’ for USB HID KB	ur
ForeignKBID	24	Foreign KB	'0' ('0' -0x3A)	Foreign Keyboard	k
CardSeatedStrID	26	Card Seated String	[tab]Card Seated[tab]	Any String (<= 23 characters)	u
CardRemovedStrID	27	Card Removed String(not seated)	[tab]Card Removed[tab]	Any String (< = 23 characters)	u
CardInStrID	28	Card Present String	[tab]Card Present[tab]	Any String (<= 23 characters)	u
CardOutStrID	29	Card Out String(not present)	[tab]Card Out[tab]	Any String (<= 23 characters)	u
NoDataStrID	2A	No Data String	[tab]No Data[tab]	Any String (<= 23 characters)	u
MediaDetectedStrID	2B	MediaDetected String	[tab]Media Detected[tab]	Any String (<= 23 characters)	u

MagDataStrID	2C	Magnetic Data String	[tab]Magnetic Data[tab]	Any String (<= 23 characters)	u
CardInSlotStr	2D	Card In Slot String	[tab]Card In Slot[tab]	Any String (<= 23 characters)	u
PartialInStr	2E	Incomplete Insertion String	[tab]Incomplete Insertion[tab]	Any String (<= 23 characters)	u
ReaderOpt2ID	2F	Reader Option 2	00h(RS232)/03h (KB)	See section 7.3.8	
CustSetID	30	custom setting	0	0x00-none; 0x04—send serial # with encrypted transactions	
Track1ID	31	Track 1 ID	NULL	Any ASCII Code	
Track2ID	32	Track 2 ID	NULL	Any ASCII Code	
Track3ID	33	Track 3 ID	NULL	Any ASCII Code	
Track1PrefixID	34	Track 1 Prefix	None	No prefix for track 1, 6 char max	
Track2PrefixID	35	Track 2 Prefix	None	No prefix for track 2, 6 char max	
Track3PrefixID	36	Track 3 Prefix	None	No prefix for track 3, 6 char max	
Track1SuffixID	37	Track 1 Suffix	None	No suffix for track 1, 6 char max	
Track2SuffixID	38	Track 2 Suffix	None	No suffix for track 2, 6 char max	
Track3SuffixID	39	Track 3 Suffix	None	No suffix for track 3, 6 char max	
KeyTypeID	3E	Key Type	‘0’	0—data key; ‘Z’—pin key	r
EpVerID*	40		None		
BaudID	41	Baud Rate	‘7’ (‘2’~’9’)	‘7’ is 38,400 bps, ‘2’ is 1200, ‘5’ is 9600 bps; ‘9’ is 115.2 kbps	s
ParityID	43	Data Parity	‘0’ (‘0’~’4’)	Data Parity Setting: ‘0’: None ‘1’: Even ‘2’: Odd ‘3’: Mark ‘4’: Space	s
HandID	44	Hand Shake	‘0’ (‘0’,’2’)	‘0’- No handshake ‘2’- soft hand shake Only apply to RS232 interface.	s
StopID	45	Stop Bit	‘0’ (‘0’~’1’)	1-bit (1 or 2 stop bits)	s
XOnID	47	XOn Character	0x11	0x11 as XOn (0x11 or 0x13)	s

XOffID	48	XOff Character	0x13	0x13 as XOff (0x11 or 0x13)	s
PrePANID	49	lead PAN to not mask	04 (00-06)	# leading PAN digits to display	
PostPANID	4A	trail PAN to not mask	04 (00-04)	# of trailing PAN digits to display	
MaskCharID	4B	mask the PAN with this character	'*' 20-7E	any printable character	
CrypTypeID	4C	encryption type	'1' ('0'-'2')	'0'—none; '1' 3DES; '2' AES	r
SerialNumberID	4E	device serial #	any 8-10 bytes	8-10 character serial number	r
DispExpDateID,	50	mask or display expiration date	'0'; '0'-'1'	'1' don't mask expiration date	
SessionID	54	set sessionID (8 bytes)	None	Always init to all 'FF'. The sessionID in security level 4 can only be set, not review.	
Mod10ID	55	include mod10 check digit	'0' '0'-'2'	don't include mod10, '1' display mod10, '2' display wrong mod10	
KeyManageTypeID	58	DUKPT	'1'('0'-'1')	'0' fixed key; '1' DUKPT key	r
HashOptID,	5C	Hash Option	'7' ('0'-'7')	Send tk1-3 hash bit 0:1 send tk1 hash; bit 1:1 send tk2 hash; bit2:1 send tk3 hash.	
HexCaseID,	5D	Set the low/upper case of the output hex data	'1' ('0'-'1')	'0'- send out hex in lower case '1'- send out hex in upper case	k
LRCID	60	LRC character	'0' ('0'~'1')	Without LRC in output	
T17BStartID	61	Track 1 7 Bit Start Char	'%'	'%' as Track 1 7 Bit Start Sentinel	
T15BStartID	63	T15B Start	';'	';' as Track 1 5 Bit Start Sentinel	
T27BStartID	64	Track 2 7 Bit Start Char	'%'	'%' as Track 2 7 Bit Start Sentinel	
T25BStartID	65	T25BStart	';'	';' as Track 2 5 Bit Start Sentinel	
T37BStartID	66	Track 3 7 Bit Start Char	'%'	'%' as Track 3 7 Bit Start Sentinel	
T35BStartID	68	T35BStart	';'	';' as Track 3 5 Bit Start Sentinel	
T1EndID	69	AnyTrack	'?'	'?' as End Sentinel—Used for all	

		End Sentinel		tracks	
T1ERRSTARTID	6C	Track 1 error code	'%'	start sentinel if track 1 error report	
T2ERRSTARTID	6D	Track 2 error code	';'	start sentinel if track 2 error report	
T3ERRSTARTID	6E	Track 3 error code	'+'	start sentinel if track 3 error report	
SecureLRCID	6F	Send or not track LRC in secure mode	'1' ('0'-'1')	'0'- Don't send LRC in secure mode '1'- Send LRC in secure mode	
T28 B Start ID	72	JIS card track2 ID	0x00	JIS track 2 start and end sentinels	
T38 B Start ID	73	JIS card track3 ID	0x00	JIS track 3 start and end sentinels	
EquipFwID	77	feature option setting	0x00-0x03	Reader firmware configuration for ID TECH internal use only	n r
SyncCheckID	7B	check for track sync bits	'2' ('0'-2')	check leading & trailing sync bits on track data (if poorly encoded card)	
SecurityLevelID	7E	Check for security level	'0' to '4'	'0' key exhausted; '1' non-encrypted; '2' key loaded non encrypted '3' encrypted; '4' encrypted w/Authentication	n r
EncryptOptID	84	encryption options	08 encrypt trk 3 if card type 0; (0-1F)	bit 0 encrypt trk1; bit 1 encrypt trk2; bit 2 encrypt trk3; bit 3 encrypt trk3 if card type 0; bit 4 mask track 3 is ISO 4909 with PAN; bit 7 use PKCS#5 pad	
EncryptStrID	85	encrypt structure	'1'	'0' original; '1' enhanced; if 85 is not an option then always enhanced structure	r
MaskOptID	86	clear / mask data options	0x07	bit 0 send clear/mask trk1; bit 1 send clear/mask trk2; bit 2 send clear/mask trk3	
Tk3ExpDatePosID	89	Trk3 expire date position	0x34	34- or 36 are the two normal values only; 30-39 allowed	
Equip2ID	AE	special settings	00 (any)	if bit4 high send serial number during enumeration	
Master Mode	A B	Master Key loading mode	'1'	Used to process key loading	r n
MKey LoadedID	A C	Key loaded state	0x00	Used to process key loading	r n
RKI	A	RKI timeout	0x02	2- two minutes	

TimeOutID	D				
PrefixID	D2	Preamble	None	No Preamble, 15 char max	
SuffixID	D3	Postamble	None	No Postamble, 15 char max	

*Unused entries in this table were left for completeness even though unused in the MOIR reader to avoid conflicting definitions between products.

Note not all function ID are present in different hardware version of the MOIR, the last column above has some codes:
'-' feature not currently supported; exists for compatibility
's' feature available in the RS232 serial version of the reader
'u' feature available only in the USB version;
'k' feature available only in the keyboard version
'r' reset all does not affect this value
'n' not directly settable
Most function ID settings that relate to the content of formatting of the track output do not work in secure mode. Exceptions to this are Preamble and Postamble in keyboard mode only.

13 APPENDIX B STATUS CODE TABLE

Return Status and Explanations

Code	Definition
B0XX	Card status (switch, no data, media detect…) change notification
9000	Operation completed successfully (all operations)
8100	Time out
6900	Command not supported
2900	Unknown ID warning
2A00	Command received correctly, but could not be completed
C0XX	Magnetic card data with envelope
6908	cmd subtype invalid
690E	"invalid cmd" response
6911	0x51 cmd length must be 1
6913	2nd byte of LED cmd must be 30-39
6915	invalid erasing string
6916	0x50 cmd must be 0x30 or 0x32
691E	problem with config command
691F	host LED control not enabled
6920	Rdr not config for buff mode
6921	rdr not config for buff mode
6922	rdr not config for buff mode
6923	rdr not config for buff mode
692B	already in OPOS/JPOS mode
692D	invalid session ID length
692E	invalid SFR value
692F	invalid SFR selection
6930	len must be 1 or securityLevel<3
6931	invalid DUKPT activation challenge
6932	authentication failure
6933	load device key failure
6934	invalid deactivation command
6935	deactivation authorization failed
6936	invalid challenge command
6937	challenge command failure
6938	inform of failure to execute cmd
6939	warn: bad command ignored
693A	invalid configure string
693B	authentication failure

693C	load device key failure
693D	deactivation cmd disallowed
693E	invalid deactivation cmd len
69XX	command not supported

14 APPENDIX C 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

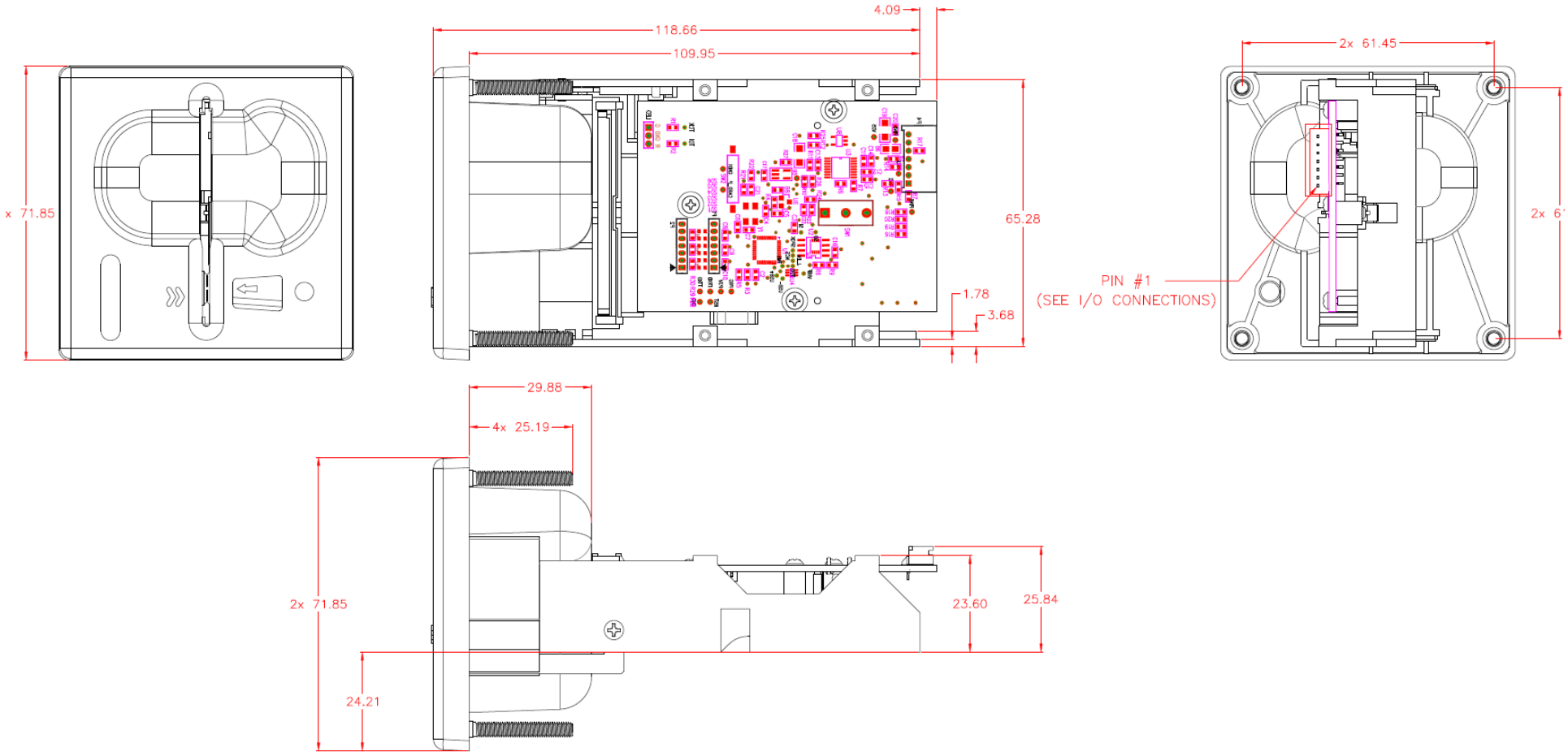
Table of Ctrl or Alt output for non printable characters

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

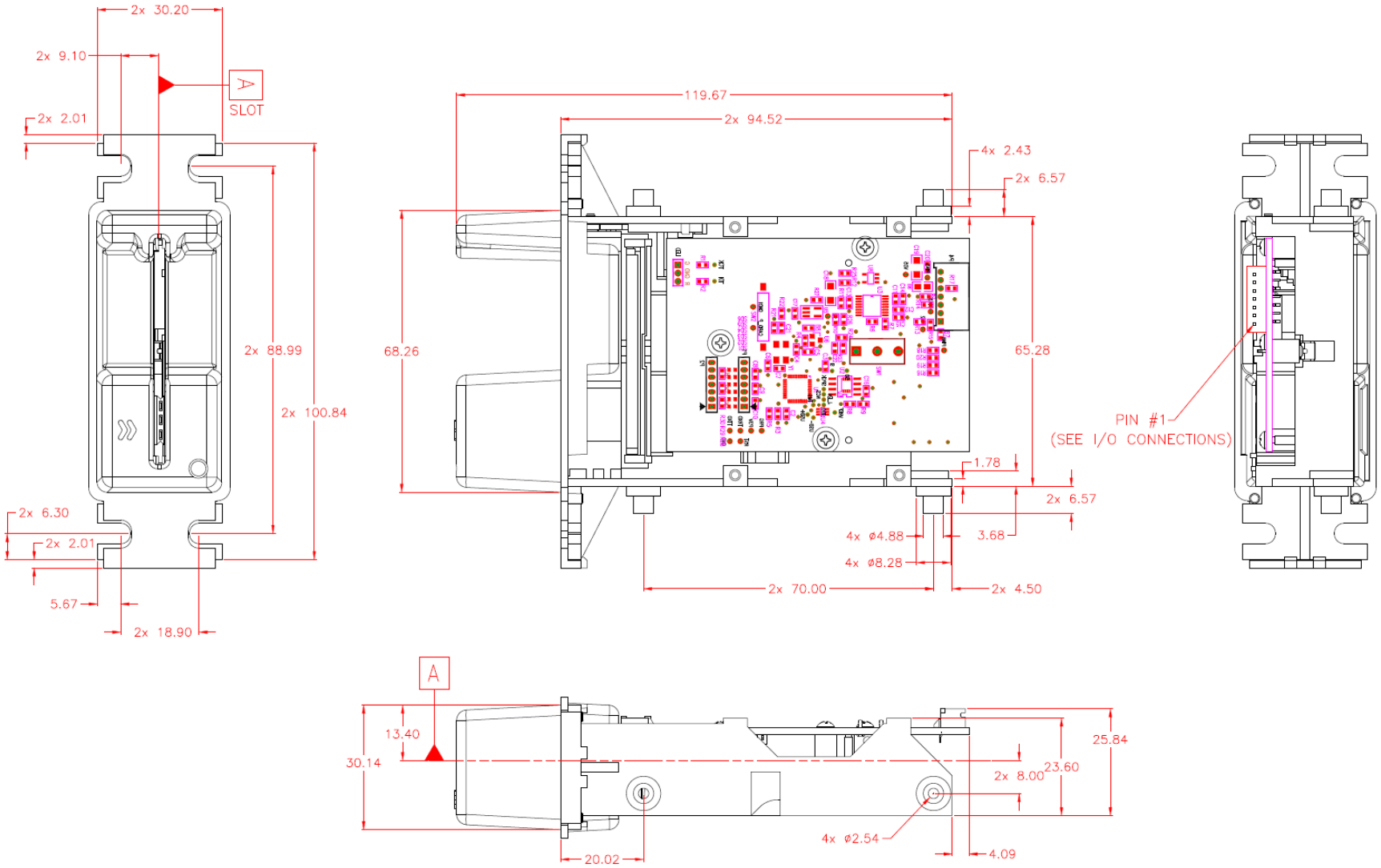
13:	Ctrl-S	Alt-019
14:	Ctrl-T	Alt-020
15:	Ctrl-U	Alt-021
16:	Ctrl-V	Alt-022
17:	Ctrl-W	Alt-023
18:	Ctrl-X	Alt-024
19:	Ctrl-Y	Alt-025
1A:	Ctrl-Z	Alt-026
1B:	ESC	Alt-027
1C:	Ctrl-\	Alt-028
1D:	Ctrl-]	Alt-029
1E:	Ctrl-6	Alt-030
1F:	Ctrl--	Alt-031

15 APPENDIX D Envelope and Mounting Drawing

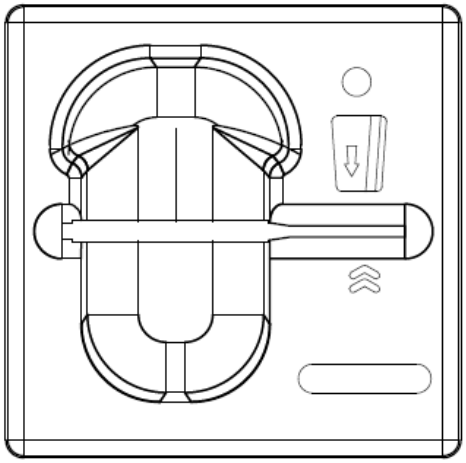
Envelope Drawing with Flush Mount Bezel

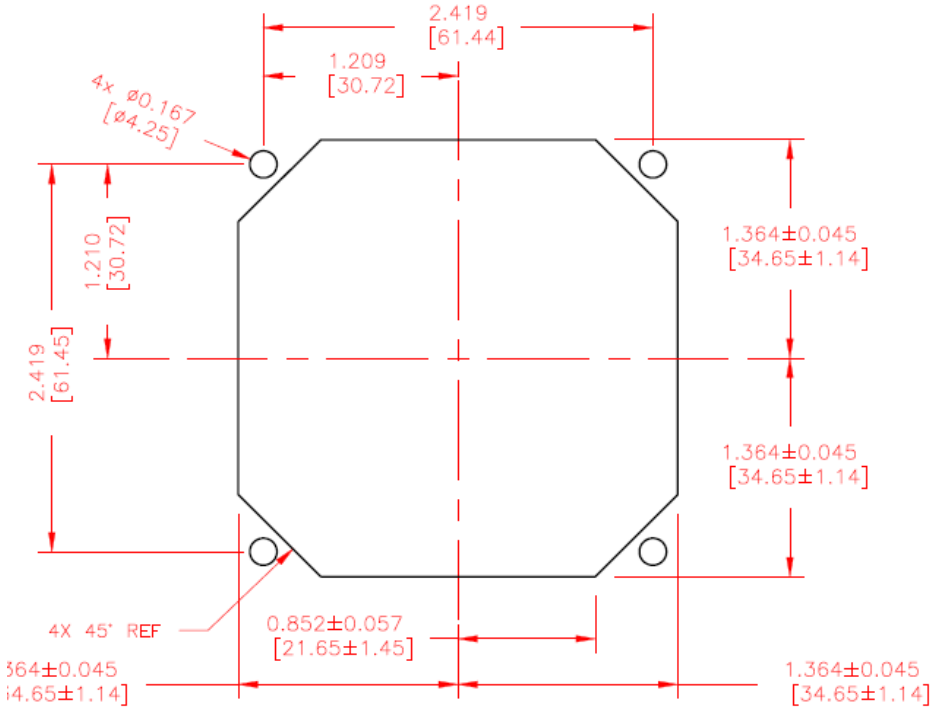


Envelope Drawing with Standard Bezel



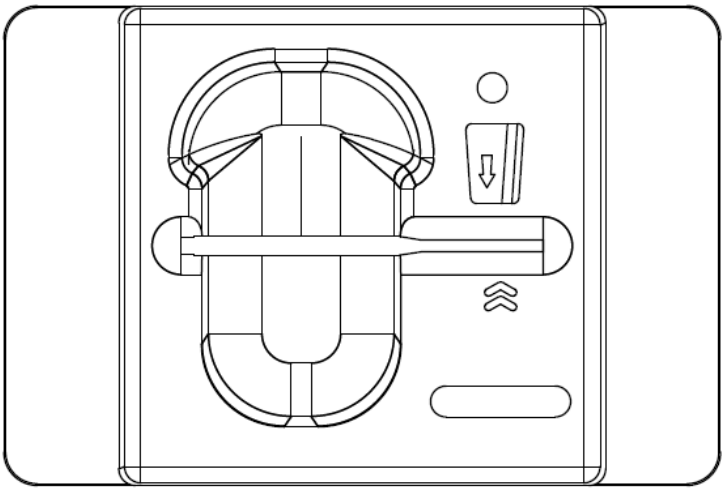
Flush Mount Bezel Mounting

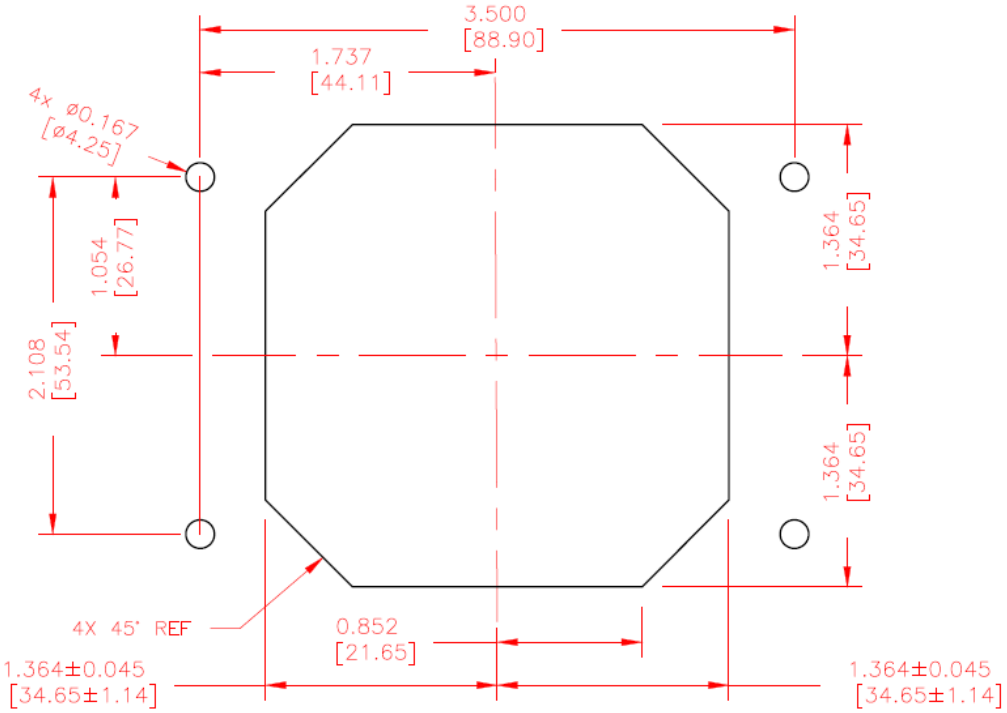




RECOMMENDED CUTOUT AND MOUNTING
FOR FLUSH MOUNTING BEZEL (80059230-001 TO -008)

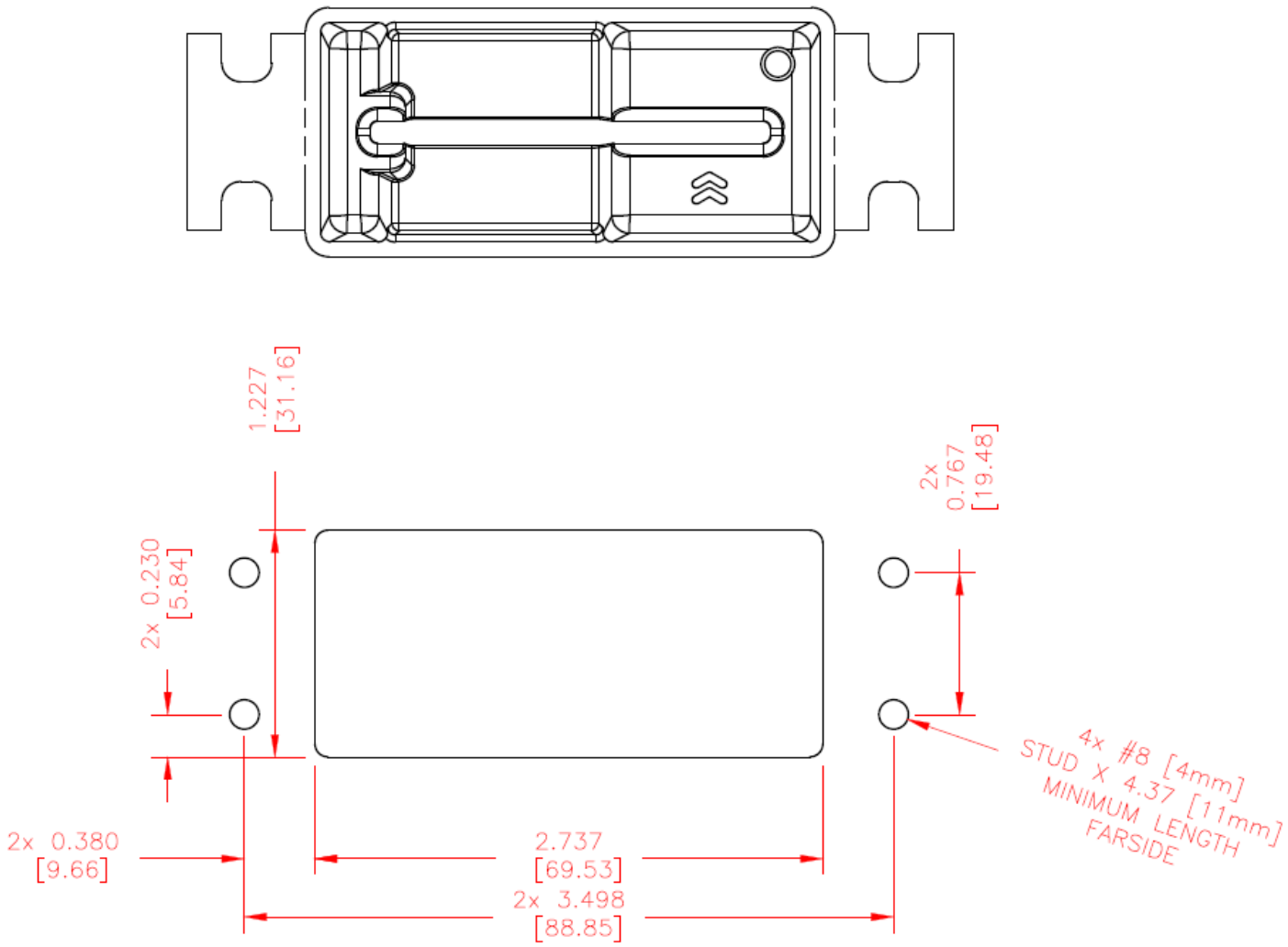
Large Flush Mount Bezel Mounting





RECOMMENDED CUTOUT AND MOUNTING
FOR FLUSH MOUNTING BEZEL (80059230-009 TO -017)

Standard Bezel Mounting



RECOMMENDED CUTOUT AND MOUNTING FOR STANDARD BEZEL