USER MANUAL

Spectrum Air

Outdoor Dual Headed Magnetic-Only Insert Reader

USB and RS232 Interfaces

ID TECH
10721 Walker Street
Cypress, CA 90630 USA

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

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

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

The information contained herein is provided to the user as a convenience. While every effort has been made to ensure accuracy, ID TECH is not responsible for damages that might occur because of errors or omissions, including any loss of profit or other commercial damage. The specifications described herein were current at the time of publication but are subject to change at any time without prior notice.
ID TECH and Value through Innovation are registered trademarks of International Technologies & Systems Corporation.

Revision History

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

Table of Contents

1. INTRODUCTION

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

2. FEATURES

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

3. ABBREVIATIONS

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

PCA	Printed Circuit Board (Assembled)
PCB	Printed circuit board bare.
PCI	Payment Card Industry
POH	Powered On Hours
POS	Point of Sale
PPMSR	Serial Port Power Magstripe Reader
P/N	Part Number
PS/2	IBM Personal System/2 Keyboard Interface
RoHS	Restriction of Hazardous Substances
RTS	Request To Send
SHA-1	Enhance Cryptographic Hash Function
SPI	Serial Peripheral Interface
T1, T2, T3	Track 1 data, Track 2 data, Track 3 data
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus
UV	Ultra Violet – spectrum of light rays

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

3.1. Formatting to designate certain data types

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

3.2. Related Documents

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

3.3. Supported Programs

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

4. INSTALLATION

4.1. Physical Installation

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

Standard Bezel
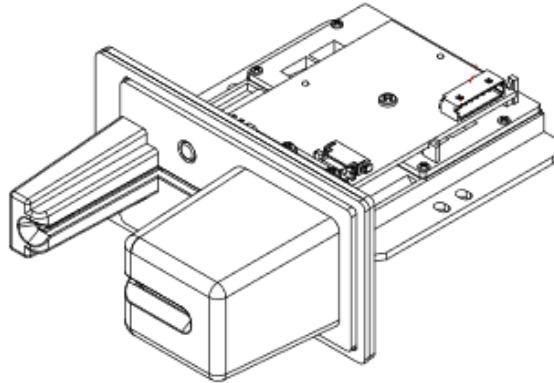
Cutout/Gasket
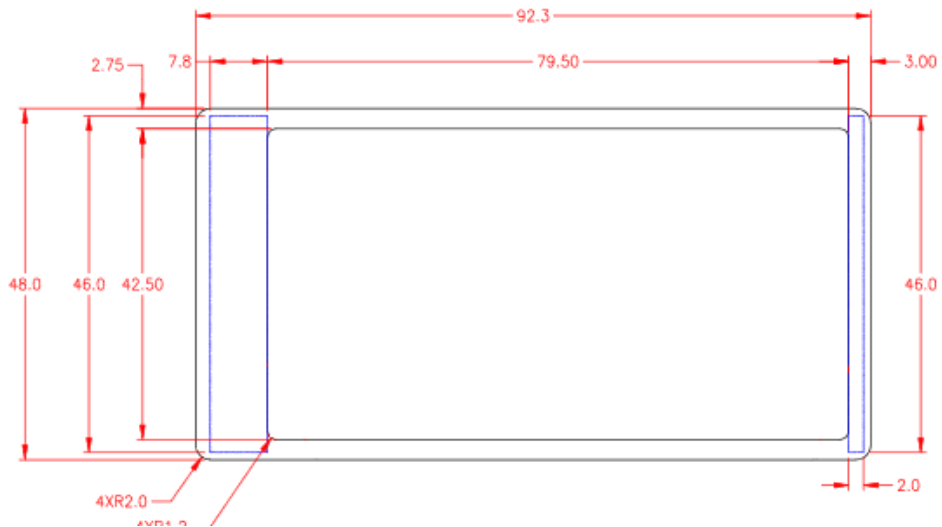
Flush Bezel
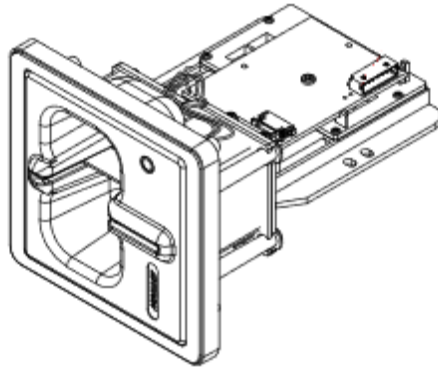
Cutout/Gasket
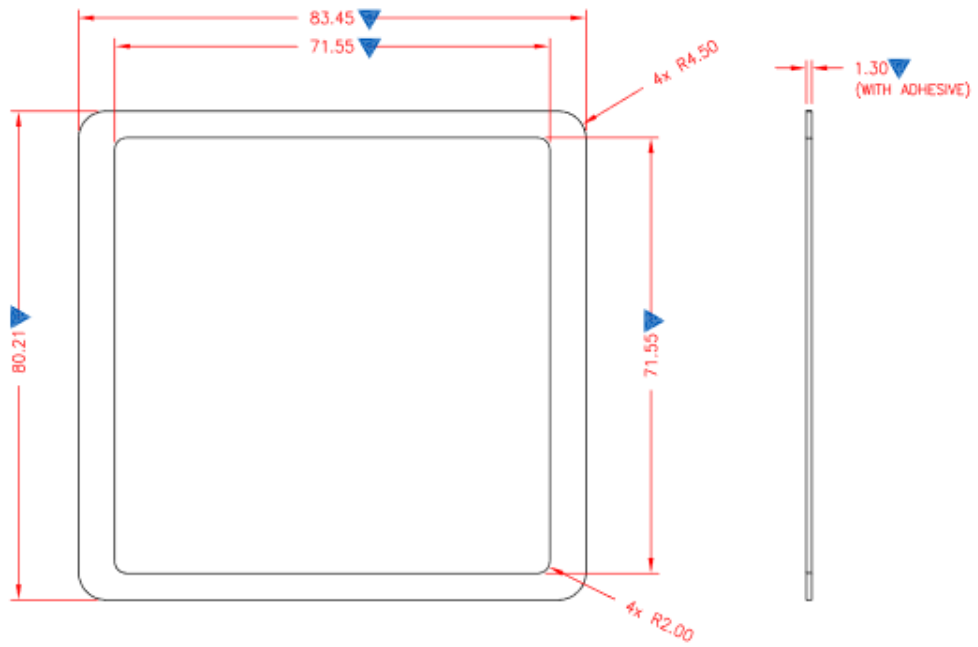
4.2. Installing a Drain Wire

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

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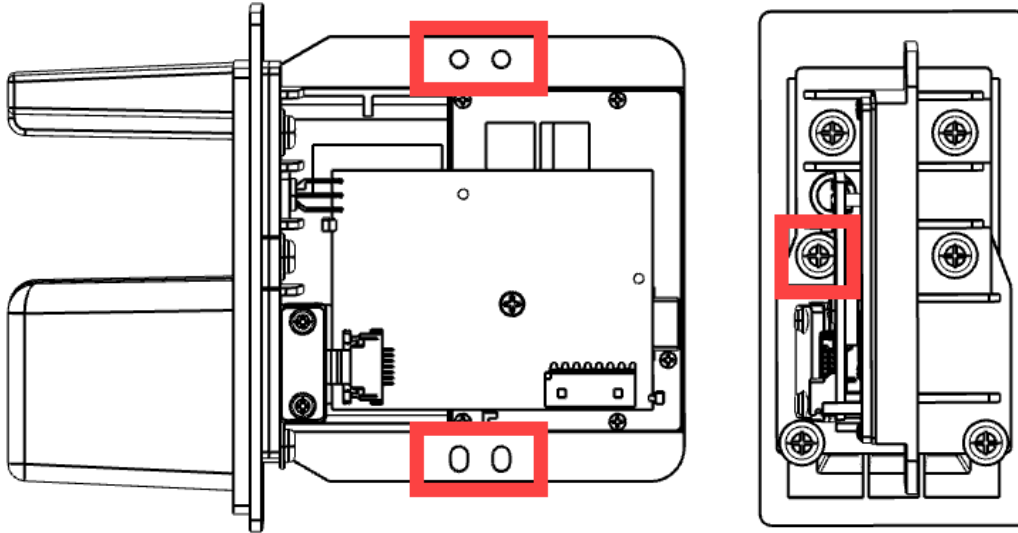
4.3. Interface

4.3.1. RS232 Interface

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

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

4.3.2. USB CDC Interface

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

4.3.3. USB HID Interface

Plug the reader into a standard USB connector on the host computer. The reader gets all needed power through the USB connector. The host will receive data from the reader as if it is coming from a USB HID

device. The host must be configured and be running an application ready to accept and process the data from the reader.

4.3.4. USB HID Keyboard Interface

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

5. OPERATION

5.1. Operating Procedure

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

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

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

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

5.2. Standard Mode (Automatic Transmit)

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

5.3. Buffered Mode

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

When the unit is armed to read in buffer mode, decoded data is retained in reader memory and an optional notice is sent to the host to indicate its presence. Data is held in memory until the reader receives the next ARM TO READ or MSR RESET command, at which point all data in memory will be erased. Refer to the specific in Buffered Mode Arm to Read [50 01 30], Buffered Mode MSR Reset Command, and Read MSR Data in Buffered Mode [51 01 xx] commands for more details.

In buffered mode, the LED is set to slowly flash green until the reader is armed to read, at which point it turns solid green. It remains green when the card track data is captured. When the host requests the

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

5.3.1. Suggested steps for buffered mode application

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

6. SPECIFICATION

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

6.1. Interfaces, signals and main components

6.1.1. USB

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

6.1.2. RS232

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

7. CONNECTOR PINOUT

7.1. RS232 Interface
Cable part number: CAB1041-1 (drawing PN 80028211)
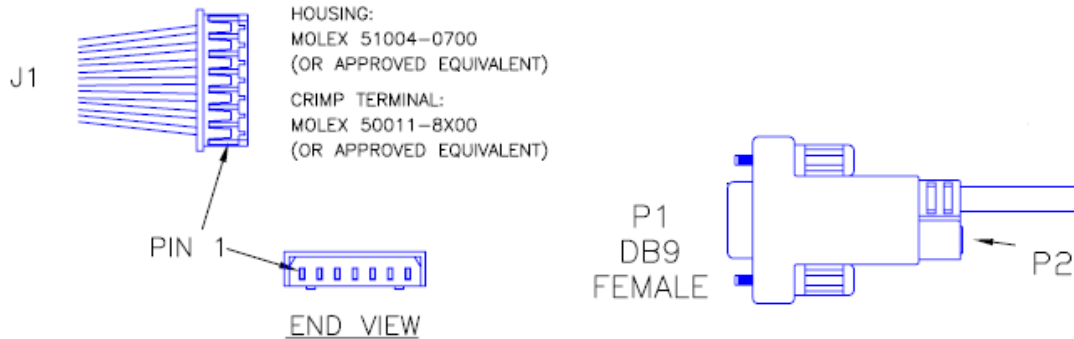
7.1.1. Wire Connection

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

7.1.2. PCA PIN Assignment

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

7.1.3. FPC Interface

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

7.1.4. LED Interface

LED1	Signal
1	Red
2	GND
3	Green

8. COMMAND PROCESS

8.1. Communication Structure

This section defines the command format for communicating with the reader.

8.2. Protocols for Sending Commands and Receiving Responses

Dual Protocol Support: The MIR supports (TLP and ITP (with NGA) protocols. The TLP is the insert reader protocol and the ITP/NGA is the swipe reader protocol, but the MIR will communicate in either of these protocols. The examples below are in TLP protocol, but if one prefers using an insert reader with an application where a swipe reader was currently supported the MIR will accommodate the ITP protocol. The MIR responds with the protocol that was first used to communicate with it when it was first powered on. See ITP Protocol for Sending Commands and Receiving Responses for more details. All commands function the same way, but the header and trailer change between the two protocols. In ITP protocol, the secure output is in NGA protocol.

All commands and responses follow the same basic structure:

HEADER	DATA	TRAILER

- The HEADER consists of <60> followed by <Command Length>; the command length is two bytes: the most significant byte followed by the least significant byte.
- The DATA often consists of the command ID, Function ID, Function Length, and Function Data.
- The TRAILER consists of <LRC> followed by <ETX>. The maximum size of length is 768 (plus envelope bytes).

8.3. Sending a Command

60<Length><Command ID>[<FuncID><Len><FuncData>…]<LRC><ETX>

Where:
- <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.
- <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 Example of LRC Calculation below for details.
- <ETX> = 03.

8.4. Protocol

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

Where:

- <Length> = is a two-byte counter from <Response Data> to the end of <Status>.
- <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) checksum (from 60 to LRC) should be zero. See Example of LRC Calculation below for details.

8.4.1. Example of LRC Calculation

The Longitudinal Redundancy Check (LRC) is calculated by taking the 'Exclusive OR' (Modulus 2) of all characters preceding it. The 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>

8.4.2. Communication Timing

The maximum delay for the reader to respond to a write configuration command is 20ms. The typical delay is 5ms.

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

Note: The maximum delay between two characters in a command is 100ms.

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.

After 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.

The following explanations and examples describe 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.

8.5. ITP Protocol for Sending Commands and Receiving Responses

Spectrum Air also supports ITP, a second protocol which is compatible with SecureMag readers. All the command can be sent with a different envelope as described below:

8.5.1. Setting Command

The setting data command is a collection of many function setting blocks and its format is as follows.

Command: <STX><S><FuncSETBLOCK1>…<FuncBLOCKn><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:
- <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.

8.5.2. Get Setting Command

This command sends the current settings to the application.
Command: <STX> <R> <FuncID> <ETX> <LRC 1>
Response: <ACK> <STX> <FuncID> <Len> <FuncData> <ETX> <LRC 2>

Where:
- <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.

Where:

Characters	Hex Value	Description
<STX>	02	Start of Text
<ETX>	03	End of Text
<ACK>	06	Acknowledge
<NAK>	15 for RS232 and USB HID interface; FD for USB KB interface	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.

8.6. General Reader Commands Description
8.6.1. Reader Command Summary
Table 1 – Reader Command Summary

ASCII	HEX	Name	Use
'8'	38	Copyright Report	Requests reader's copyright notice
'9'	39	Firmware Version Report	Requests version string
'$'	24	Get Reader Status	Determining card inserted, MSR data present, etc.
'F'	46	Key Loading	Special command to load encryption keys
'I'	49	Reader Reset	Reset the reader. Software reset does not resend startup string
'M'	4D	OPOS/ JPOS Command	Command to enter OPOS or JPOS 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
'l'	6C	LED Functions	Turning on/off/flash the bicolor-LED

8.6.2. Get Firmware Version Report [39]
60 00 01 39 58 03

Note: Returns an approximately 55-byte version description. The description and length vary somewhat by hardware and version.

Response:
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

Returns the minor version of the firmware if the version command includes 88 as the third byte:
60 00 01 39 88 88 58 03 or 60 00 03 52 22 88 9B 03
Response Example (mixed hex and ASCII):

60 00 35 "ID TECH TM3 Secure Mag Insert RS232 Reader V2.87.000" 3O 03 feature added with Version V2.89.

8.6.3. Revert to Default Settings [53 18]
60 00 02 53 18 29 03

This command does not have any <FuncData>. All non-security settings revert to their default values. (Some transient statuses, such as card report timers, may not be cleared immediately if this command runs in the middle of a card transaction).

8.6.4. Host LED Control Command [6C]
60 00 02 6C <LED State> LRC 03

This command changes the LED color settings.

Note: The reader must have the "LED" option for this command function properly.

<LED State> options:
'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

Command completed successfully response 9000 is as follows:
60 00 02 90 00 F2 03

Other possible response statuses:
6913   2nd byte of LED command was not 30-37, or 41-43 691D Command length is incorrect
691F   host LED control not enabled. To configure the reader to support host see bit 4 in set reader option section 13.6.3.

8.6.5. Reader Reset Command [49]

60 00 01 49 28 03

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

Command completed successfully response 9000 is as follows:
60 00 02 90 00 F2 03

8.6.6. Get Copyright Information [38]

60 00 01 38 59 03

Returns an approximately 26-byte Copyright Notice.

Response:
60 00 3F <Copyright String> LRC 03

Response Example mixed hex and ASCII:
60 00 3F Copyright (c) 2011, ID TECH LRC 03

8.7. Reader Configuration Commands Description

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

8.7.1. Setting Command

Command requests and responses are sent to and received from the device. For USB interface devices, the commands are sent to the device using HID class specific request Set_Report (21 09 …). The response to a command is retrieved from the device using HID class specific request GetReport (A1 01 …). These requests are sent over the default control pipe. For RS232 interface devices, please see the commands listed below.

8.7.2. Commands

The following table is a magnetic stripe reader commands summary described in this section:

HEAD	DATA	NAME	USAGE
60 00 04	53 13 01 xx	Track Selection Setting	To select the tracks on the magnetic stripe to be read.
60 00 04	5317 01 xx	Track Separator Setting	To format the data read from the card.
60 00 04	5319 01 xx	Send Option	To enable or disable the sentinel or account number on Track 2 only or sending error notification.
60 00 04	53 1A 01 xx	MSR Reading	To turn the magnetic stripe reading function off or on in either auto-transmit or buffer mode.
60 00 04	53 1D 01	Decoding Method	To read a card in a selected direction.
60 00 04	53 60 01	LRC Option	To enable or disable sending out the LRC character.
60 00 04	53 61 01	Track1 7bit start sentinel	To set the track1 start sentinel character.

60 00 04	53 62 01	Track1 6bit start sentinel	To set the track1 start sentinel character.
60 00 04	53 63 01	Track1 5bit start sentinel	To set the track1 start sentinel character.
60 00 04	53 64 01	Track2 7bit start sentinel	To set the track2 start sentinel character.
60 00 04	53 65 01	Track2 5bit start sentinel	To set the track2 start sentinel character.
60 00 04	53 66 01	Track3 7bit start sentinel	To set the track3 start sentinel character.
60 00 04	53 67 01	Track3 6bit start sentinel	To set the track3 start sentinel character.
60 00 04	53 68 01	Track3 5bit start sentinel	To set the track3 start sentinel character.
60 00 04	53 69 01	Track end sentinel	To set the track end sentinel character.
60 00 04	53 21 01 xx	Terminator Setting	To format the data read from the card.
60 00 04	53 3n 01 xx	Track 1,2, 3 ID Setting	To edit the data read from the card.
60 00 xx	53 Dx xx	Preamble and Postamble Settings	To edit the data read from the card.
60 00 03	50 01 30	Arm to Read in Buffer Mode	To enable reading in the buffer mode.
60 00 03	50 01 32	MSR Reset in Buffer Mode	To return the reader to its default settings when buffer mode is enabled.
60 00 03	51 01 xx	Read MSR Data in Buffer	To set the tracks on the magnetic stripe to be read while in the buffer mode.

8.7.3. Restore Configuration Settings to Default [53 18]
60 00 02 53 18 29 03

This command restores most settings to their default value.

Note: Executing this command does not affect the security settings, the factory options or the serial number (page 29).

Command completed successfully response 9000 is as follows:
60 00 02 90 00 F2 03

8.7.4. Read All Configuration Settings [52 1F]
60 00 02 52 1F 2F 03

This command does not have any <FuncData>. It retrieves all current settings. The MIR reader sends back a <Response>.

Response:
The current configuration data block is a collection of many Function-Setting blocks <FuncSETBLOCK> as follows:
60 <Length> <FuncSETBLOCK1>…<FuncSETBLOCKn> LRC 03

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

Where:
- <Length> is a two bytes counter, which indicates bytes of all <FuncSETBLOCK>. The most significant byte comes first.

- <FuncID> is a one byte Function ID identifies the setting(s) for the function. For a complete list of FuncID, see Appendix A, page 105.
- <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>.

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.

8.7.5. Bit Setting and Clearing Commands

This is a special type of setting command. For an 'S' (53) command that is setting only one configuration byte, the first byte of the command (the 'S' or 53) can be replaced with a '0' (31) to clear individual bits or a '1' (31) 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 01 80 will clear the highest bit in configuration byte 10
- 30 01 80 will set the highest bit in configuration byte 10
- 31 30 01 81 will set the lowest and highest bits of configuration byte 10

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, which 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.

8.7.6. Read Specific Configuration Setting [52 nn]
60 00 02 52 <Configuration> LRC 03

The <Configuration> byte corresponds to the byte from a specific configuration value. All MSR reader Read Configuration Commands are listed in the following format:
60 00 02 52 <FuncID> LRC 03

For example, to read the "Card Option" configuration, send 60 00 02 52 10 20 03.

8.7.7. Read Reader Serial Number [52 4E]
60 00 02 52 4E 7E 03

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

Response:
- 60 00 0B 4E 09 08 <Serial Number (8 bytes)> LRC 03
    - o Serial number can be 8 to 10 characters
- 60 00 0D 4E 0B 0A <Serial Number (10 bytes)> LRC 03
    - o Set Reader Serial Number [53 4E]
- 60 00 0C 53 4E 09 08 <Serial Number (8 bytes)> LRC 03
    - o Serial Number is an eight to ten-byte field containing the serial number in ASCII.

Example:
60 00 0C 53 4E 09 08 31 32 33 34 35 36 37 38 78 03

Note the byte following the 4E is serial number length +1, then the serial number length. Command completed successfully response 9000 is as follows:
60 00 02 90 00 F2 03

8.7.8. Buffered Mode Arm to Read Command [50 01 30]
60 00 03 50 01 30 02 03

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 corresponding bit in Reader Option byte has been set. See Set Reader Option [53 11] for more information.

Successful response:
60 00 02 90 00 F2 03

Problem response:
E0 00 02 xxxx LRC 03

Other possible 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

8.7.9. Buffered Mode MSR Reset Command [50 01 32]
60 00 03 50 01 32 00 03

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:
60 00 02 90 00 F2 03

Problem response:
E0 00 02 xxxx LRC 03

Other possible 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

8.7.10. Buffered Mode Read MSR Data Command [51 01 XX]
60 00 03 51 01 <Track Selection Option> LRC 03

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. This command does not erase the data.

Note: In security level 3 and 4 all track data is sent no matter which tracks are requested.

Successful response:
60 00 02 <Len_H><Len_L><MSR Data> LRC 03

Problem response:
E0 00 02 xxxx LRC 03

Other possible response statuses:
- 6911   'Q' command length must be 1
- 6921   reader not configured for buffered mode
- C000   no magstripe data available

8.7.11. 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):

1. Send the Act auth command (52 80)
2. Send the act reply command (53 82) so the reader is now allowed to send a level 4 transaction
3. 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.

8.7.12. MSR Configuration Commands Description
All MSR reader Configuration Commands are listed in the following format:
60 <Length> 53 <FuncID> <Len> <FuncData> LRC 03

Length is a two bytes counter, which indicates length of data from 53 to end of <Func Data>. The most significant byte comes first.

Successful Response:
60 00 02 90 00 F2 03

8.7.13. Set MSR Transmit Mode [53 1A]

60 00 04 53 1A 01 <MSR Transmit Mode> LRC 03

The <MSR Transmit Mode> byte is defined as follows:
- '0'   MSR Reading Disable
- '1'   MSR Reading Auto Transmit Mode (default)
- '2'   MSR Reading in Buffered Mode.*
- '3'   MSR Reading in Auto-Buffered Mode.*

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

8.7.14. Set MSR Read Direction [53 1D]

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

The <Read Direction> byte is defined as follows:
- '1'   Read on both insertion and withdrawal
- '2'   Read on insertion only
- '3'   Report on withdrawal (default)
- '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.

Report on Withdrawal Mode: the standard default MSR reading option is "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; the two reads are combined and the combination reported after the card has been removed. It is currently supported in all cases except raw for MSR mode.

> **Note**: If the reader is in Secure Level 3 or 4 the card data is sent in the same format always. The following options "do not apply". The only exception is a keyboard reader can send a MSR data prefix or postfix string (preamble and postamble) around the data so that the host can recognize that the data came from the MIR rather than from a keyboard.

8.7.15. Set MSR Send Option [53 19]

60 00 04 53 19 01 <Send Option> LRC 03

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 MIR 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 & only account number on Track 2 for a credit card or Send Start/End sentinel on Tracks 1 and 3 for a standard 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> to <3F> Send keyboard control codes in the standard form or send the alternate control codes.

The default setting for RS232 reader is 0x31, and the default setting for USB_HID_KB reader is 0x35.

Response: <60><00><02><90><00><F2><03>

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 13ErrStart (6E) and t1End (69) to set the reader not to send these.

8.7.16. Set MSR Data Terminator [53 21]

60 00 04 53 21 01 <Terminator Setting> LRC 03

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. A value of 0x00 means do not send any MSR data terminator.

8.7.17. Set MSR Data Prefix String [53 D2]

60 <length> 53 D2 <Len> <Prefix String> LRC 03

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 two bytes 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

8.7.18. Set MSR Data Postfix String [53 D3]

This command works on unencrypted mode only.

60 <length> 53 D3 <Len> <Postfix String> LRC 03

Where:
- Postfix String = {string length}{string}
- String length is one byte, maximum 15
- Len is the number of bytes of Postfix string including string length
- Length is a two bytes counter, which indicates the number of bytes in command from 53 to the end of the <Postfix 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

8.7.19. Set Track 1 ID [53 31]

This command works on unencrypted mode only.

60 00 04 53 31 01 <Track 1 ID> LRC 03
<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

8.7.20. Set Track 2 ID [53 32]

This command works on unencrypted mode only.

60 00 04 53 32 01 <Track 2 ID> LRC 03
<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'

8.7.21. Set Track 3 ID [53 33]

This command works on unencrypted mode only.

60 00 04 53 33 01 <Track 3 ID> LRC 03
<Track 3 ID>: ASCII code set as Track 3 ID, NULL for None.

Example: 60 00 04 53 33 01 03 06 03   Send Track 3 ID of Hex '3'

8.7.22. Set Track Selection [53 13]

This command works on unencrypted mode only.

60 00 04 53 13 01 <Track_Selection> LRC 03
<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 data:
60 00 04 53 13 01 07 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.

8.7.23. Set Track Separator [53 17]
This command works on unencrypted mode only.

60 00 04 53 17 01 <Track_Separator> LRC 03
<Track_Separator> is one ASCII byte; the default value is CR (Hex 0D).

Example to set the track separator to CR (carriage return)

8.7.24. Set Track n Prefix [53 34]
This command works on 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.

60 00 03 53 <n><Len><Prefix> LRC 03

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

8.7.25. Set Track n Suffix [53 37]
This command works on 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.

60 00 LenL 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

8.7.26. Set Samsung Pay Time Out [53 A0]

This command works Samsung Pay Transactions only. It does not apply before firmware version V2.89. This adds a delay after one Samsung Pay transaction occurs before another Samsung Pay transaction can occur. It does not prevent a card swipe immediately following the Samsung pay transaction

60 00 04 53 A0 01 <SpTimeOut> LRC 03

Where:

- SpTimeOut is a count of .128 second intervals before another Samsung Pay transaction can be captured. This was done because the Samsung Pay transmits the same patron information each second many times to give the reader ample opportunity to capture the data. To eliminate the timeout and accept every transaction sent by the Samsung Pay device set the SpTimeOut to 0. The default setting of 32 hex (or 50 decimal is about 6.4(=50*.128) seconds.

Note: by default, after version 2.89 Samsung Pay support5 is active, it is enabled by setting bit 4 (0x10) of CustSet2ID (0xAF). Clear this bit to disable Samsung Pay support.

Example:
60 00 04 53 A0 01 32 F2 03

8.8. Magnetic Card Read Modes

The Secure MIR supports three 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 notify the host a magstripe read occurred, 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:

1. Insert a card, magnetic stripe down(or up or down if 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 insure proper reading of the data). As soon as the reader detects data from magnetic stripe, the green LED indicator will go off.
2. Withdraw the card in one continuous motion. The green LED will go off. (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.

Configuring the reader to support auto transmit mode or buffered mode is done with Set MSR Transmit Mode [53 1A].

Auto Buffered Mode

If the reader does not have captured track data, it is ready to capture track data. The user inserts and/or removes a card, the decoded data is stored, the readers notify the host a magstripe read occurred, and MSR is disarmed. The application program then sends a "Read MSR Data" command to retrieve the data from the buffer. The reader then immediately rearms for the next MSR capture.

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:

1. Insert a card, magnetic stripe down (or up or down if 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 insure proper reading of the data). As soon as the reader detects data from magnetic stripe, the green LED indicator will go off.
2. Withdraw the card in one continuous motion. The green LED will go off. (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.

Configuring the reader to support auto transmit mode or buffered mode is done with Set MSR Transmit Mode [53 1A] page 31.

8.9. LED Handling

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.

- On powering on the reader, the LED will flash red then green to indicate a successful startup.
- The LED will turn green after reading a magstripe card to indicate a good read.
- The LED will turn red briefly after reading a magstripe card to indicate a bad read.
- The LED will turn solid amber if USB connection to host is in process or incomplete.
- The LED will flash amber on start-up if the configuration EEPROM has a problem.

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

Turn the LED off	[6C 30]
Turn the LED on Green	[6C 31]
Turn the LED on Red	[6C 32]
Turn the LED on Amber	[6C 33]
Set the LED to Green flashing	[6C 34]
Set the LED to Red flashing	[6C 35]
Set the LED to Amber Flashing	[6C 36]
Set the LED to flashing Red and Amber	[6C 37]
Set the LED to slow flashing Green	[6C 41]

Set the LED to slow flashing Red   [6C 42]
Set the LED to slow flashing Amber   [6C 43]

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 configured for RS232 and Plug-and-Play, the LED will be amber until the reader has sent its plug-and-play string to the host or if a USB reader until the enumeration process has completed. 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.

To Configure the reader to support host-controlled LED commands use the Set Reader Option command, section 13.6.3.

- RED then GREEN after Power On Self-Test.
- Solid AMBER if USB until connected.
- Solid GREEN almost always after good start up in auto mode.
- DARK during track decoding
- Slow flashing GREEN if MSR read disabled.
- Slow flashing GREEN if reader in buffered mode, but not to armed to read.
- RED for .5 second after bad card read indication in auto mode.
- If in auto mode, the LED color is determined by track options vs. card tracks.
- RED for .5 second after bad card read in buffered mode when host requests buffered data
- Solid RED: if DUKPT key is exhausted or the key is corrupt.

8.10. 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 notification. 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 set reader status section 13.6.3 on page 80. 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 and the Options 2 configuration setting byte page 82. There is a bit in configuration 0x1C bit 4 added in version 2.90 that must be set properly according to the card present hardware available in the reader. The SPTS reader has the card present signal, but not the switch so this bit must be off for this hardware to work properly.

8.11. Key Loading Command

Note: This command is normally only used by a key loading facility. This protocol is different from the normal reader protocols.

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.

KSN and Device Key loading commands and responses protocol:
When DUKPT key management is used, it is necessary to load Key Serial Number (KSN) and Initially Loaded Device Key before transaction.

The encryption key is TDES with 128-bit keys or AES encryption with double length keys (128- bit keys including parity).

KSN and Device Key loading commands and responses protocol:

Command:
<STX><'F'><'F'><Command Data (BASE64)><0x0D><0x0A><ETX><LRC>

Response:
<ACK/NAK><STX><'F'><'F'>< Respond Data(BASE64)><0x0D><0x0A><ETX> <LRC>

STX: 0x02
ETX: 0x03
ACK: 0x06
NAK: 0x15
BASE64: Data encoded with base64 algorithm
LRC: Xor'd all the data before LRC except STX

A successful key loading process includes the following steps:

1. Get Key status
      Command Data: <FF><13><01><02><LRC>
      Response Data: <FF><00><01><04><LRC>

      For Example:
      Command: \02\46\46\2F\78\4D\42\41\75\38\3D\0D\0A\03\LRC
      Response: \06\02\46\46\.........\0D\0A\03\LRC

2. Load KSN
      Command Data: <FF><0A><11><KSN#><KSN bytes><LRC>
      Response Data: <FF><00><06><RESPONSE CODE><LRC>

      Where:
- <KSN#>: TDES: 0x32   DES: 0x0A
- <KSN bytes>: 16 bytes ASCII for KSN
- <RESPONSE CODE>: 6 bytes data in ASCII format, which is converted from the first 3 cipher hex data. These cipher data are generated by encrypting KSN bytes and "00 00 00 00 00 00 00 00".

For Example:
Command:
\02\46\46\2F\77\6F\52\4D\6B\5A\47\52\6B\59\35\4F\44\63\32\4E\54\51\7A\4D\6A\45\77\5
2\54\ 43\69\0D\0A\03\5D
Response: \06\02\46\46\........\0D\0A\03\LRC

3. Load Encryption Key
Command Data: <FF><0A><LENGTH><KEY#><KEY bytes><LRC>
Response Data: <FF><00><06><RESPONSE CODE><LRC>

Where:
<LENGTH>: TDES: 0x21 DES: 0x11
<KEY#>: TDES: 0x33   DES: 0x0B
<KEY bytes>: TDES: 0x20   DES: 0x10
<RESPONSE CODE>: 6 bytes data in ASCII format, which is converted from the first 3 cipher hex
data. These cipher data are generated by encrypting KEY bytes and "00 00 00 00 00 00 00 00".

For Example:
Command:
\02\46\46\2F\77\6F\68\4D\7A\5A\42\51\7A\49\35\4D\6B\5A\42\51\54\45\7A\4D\54\56\43\
4E\45\51\34\4E\54\68\42\51\6A\4E\42\4D\30\51\33\52\44\55\35\4D\7A\4E\42\6C\51\3D\3
D\0D\0A\03\2D
Response: \06\02\46\46\........\0D\0A\03\LRC

8.12. 4. Set OPOS/JPOS Command

There are three forms of the command:
- 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)

Response:
- 692B   Reader already in OPOS Mode
- 6939   Command failure (wrong length or wrong parameter)
- 9000   Success

8.13. Read MSR Options Command

60 00 02 52 1F 03 LRC

Response:
The current setting data block is a collection of many function-setting blocks.

<FuncSETBLOCK> as follows:
<STX><FuncSETBLOCK1>…<FuncSETBLOCKn><ETX><CheckSum>

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

Where:

- <FuncID> is one byte identifying the setting(s) for the function.
- <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.
- <FuncSETBLOCK> are in the order of their Function ID<FuncID>.

9. SECURITY FEATURES

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

There are five security levels available on the reader:

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

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

9.1. 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.

9.1.1. Security Management

This reader is intended to be a secure reader. Security features include:
- Can include Device Serial Number
- Can encrypt track 1, track 2, and track 3 data for bank cards and other cards
- Provides clear text confirmation data including card holder's name and a portion of the PAN as part of the Masked Track Data for bank cards
- Optional display expiration date

- Security Level is settable
- By default setting (See AF) will allow and encrypt Samsung Pay Reader transaction (added with Version V2.89).

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

9.1.2. Review Encryption [52 nn]
60 00 02 52 <Configuration> LRC 03

The <Configuration> byte corresponds to the byte from a specific configuration value.

9.1.3. Review KSN (DUKPT Key management only) [52 51]
60 00 02 52 51 LRC 03

This command gets the DUKPT key serial number and counter.

9.1.4. Review Security Level [52 7E]
60 00 02 52 7E LRC 03

This command gets the current security level.

9.2. Check Card Format
- ISO/ABA (American Banking Association) Card (card type 0)

Encoding method:
- Track1 is 7 bits encoding.
- Track1 is 7 bits encoding. Track2 is 5 bits encoding. Track3 is 5 bits encoding. Track1 is 7 bits encoding. Track2 is 5 bits encoding.
- Track2 is 5 bits encoding.
- Track3 if present is 5-bit encoding

Additional checks:
- If there is a track 1, track1 2nd byte is 'B'.
- If there is a track 2, there is an '=' in track 2 and position of '=' is between 12th ~ 20th character.
- Total length of track 2 should above 21 characters.
- If there is a track 1, there is an '^' position of '^' is between 13th ~ 21th character.
- If enabled the reader can decode, mask and use track 3 ISO 4909 data.

9.2.1. 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.

9.2.2. Others (Customer card)

9.3. MSR Data Masking
For encrypted ABA cards, both encrypted data and clear text data are sent.
9.3.1. 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).[1]
- The rest of the characters should be masked using mask character.

9.3.2. 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'

9.4. Output Format
Generally, the output format is the same between the RS232, USB HID and USB HID KB. The output that follows is the RS232 reader because it is a subset of the other two reader interface types. The USB HID reader output is padded with zeros at the end of the secure MSR output until the length is 580 bytes. The USB HID KB reader is identical to the RS232 output described below except it is preceded by the keyboard output header and the Keyboard sends all fields that are not in ASCII in two bytes for each hex character.

The secure output is in either one of two protocols the TLP (the default protocol) or the NGA protocol. These will be described below.

The HID KB header is:
- Right Shift make
- Right Shift break
- Left Shift make
- Left Shift break
- Right Ctrl make
- Right Ctrl break
- Left Ctrl make

---

[1] If JIS card support is enabled in HID/KB mode, the JIS track sentinels are set to 0 meaning they are not sent out in encrypted or unencrypted mode. When the JIS sentinels are not sent in encrypted mode, the JIS track LRC is also suppressed.

- Left Ctrl break

9.4.1. Data Format
9.4.1.1. Original Encryption Reader Data Structure

Offset   Usage Name
If TLP protocol envelope:
     0   60
     1   Data Length high byte
     2   Data Length low byte
End TLP protocol envelope header If NGA protocol envelope:
     0   STX
     1   Data Length low byte
     2   Data Length high byte
End NGA protocol envelope header:
     3   Card Encode Type
     4   Track 1-3 Status
     5   T1 data length
     6   T2 data length
     7   T3 data length
     8   Mask/Clear Status (1 byte, see definition and example)
     9   Encrypt/Hash Status (1 byte, see definition and example)
   10   T1 data (masked if card type 0) (omitted if card type 4)
        T2 data (masked if card type 0) (omitted if card type 4)
        T3 data unencrypted (omitted if card type 4)
Encrypted section:
        T1-T2 data encrypted (if card type 0 or 4, else omitted)
        T3 data encrypted (only if card type 4)
        Session ID (8 bytes) (Only if security level 4 & card type 0 or 4)
End encrypted section
        T1-T3 hashed (if card type 0 or 4) (20 bytes each)
        KSN (10 bytes) only if card type 0 or 4)
If TLP protocol envelope
        LRC
        ETX
End TLP protocol envelope header If NGA protocol envelope
        LRC
        Check Sum
        ETX
End NGA protocol envelope header

Notes:
- Offset to the fields can be determined by adding the field length using the track data for the track field lengths. Fields are packed in the next available location.
- T1, T2 or T3 Data Length: Each byte value indicates how many bytes of decoded card data are in the track data field. This value will be zero if there was no data on the track or if there was an error decoding the track.

- The encrypted section is padded with 0 to the block size of the encryption type, 8 bytes for TDES and 16 bytes for AES.
- The hashed data may optionally be omitted.

9.4.1.2. Card Encode Type

Value	Encode Type	Description
0	ISO/ABA	ISO/ABA encode format
1	AAMVA	AAMVA encode format
3	Other	The card has a non-standard format. For example, ISO/ABA track 1 format on track 2
4	Raw	The card data is sent in Raw encrypted format. All tracks are encrypted and no mask data is sent
5	JIS II	88- (wide track, send track 2 only, -8-) if _jisIItype = 1
6	JIS I	858 855 85- 758
7	JIS II	88- (wide track, send 2 only, -8-) if _jisIItype = 0 default

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.

9.4.1.3. ID TECH Reader Data Structure

This is the format for a non-encrypted card, when encryption is enabled, and the reader is set for the original encryption structure.

Offset	Usage Name
0	STX
1	Data Length low byte
2	Data Length high byte
3	Card Encode Type (not 0 or 4)
4	Track 1-3 Status
5	T1 data length
6	T2 data length
7	T3 data length
8	T1 data unencrypted including SS, ES and LRC
	T2 data unencrypted including SS, ES and LRC
	T3 data unencrypted including SS, ES and LRC ETX
	LRC

Note: track formatting (preamble, prefix, separator, etc.) is not available in a reader set to send encrypted track data. The track data is always sent in the same format.

9.4.1.4. Enhanced Encryption Format for MIR (This is the default)

Offset   Usage Name

If TLP protocol envelope

      0   60

      1   Data Length high byte

      2   Data Length low byte

End TLP protocol envelope header

If NGA protocol envelope

      0   STX

      1   Data Length low byte

      2   Data Length high byte

End NGA protocol envelope header

      3   Card Encode Type

      4   Track 1-3 Status

      5   T1 data length

      6   T2 data length

      7   T3 data length

      8   Mask/Clear Status (1 byte, see definition and example)

      9   Encrypt/Hash Status (1 byte, see definition and example)

   10   T1 data (masked if card type 0) (omitted if card type 4)

         T2 data (masked if card type 0) (omitted if card type 4)

         T3 data unencrypted (omitted if card type 4)

Encrypted section

         T1-T2 data encrypted (if card type 0 or 4, else omitted)

         T3 data encrypted (only if card type 4)

         Session ID (8 bytes) (Only if security level 4 & card type 0 or 4)

End encrypted section

         T1-T3 hashed (if card type 0 or 4) (20 bytes each)

         KSN (10 bytes) only if card type 0 or 4

If TLP protocol envelope

         LRC

         ETX

End TLP protocol envelope header

If NGA protocol envelope

         LRC

         Check Sum

         ETX

End NGA protocol envelope header

This mode is used when all tracks must be encrypted, or encrypted OPOS support is required, or when the tracks must be encrypted separately or when cards other than type 0 (ABA bank cards) must be encrypted or when track 3 must be encrypted.

9.4.2. Encryption Option Setting (for enhanced encryption format only except bits 6-7)

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 – track 3 encrypted with card is type 0 and track 3 is ISO4904 send mask data
- if set allow credit card format tracks 1-3 to be masked even if force encrypt bit set. B4 feature added with Version V2.89.
- bit5: 0 – reserved for future use always zero bit6: 0 – reserved for future use always zero
- bit7: 1 – pad according to PKCS#5 (else pad with zeros)

Note:
- When force encrypt is set, this track will always be encrypted (unless bit3 is 1), regardless of card type. No clear/mask text will be sent.
- If and only if in enhanced encryption format, each track is encrypted separately. Encrypted data length will round up to 8bytes for DES or 16 bytes for AES.
- When force encrypt is not set, the data will be encrypted in original encryption format, that is, only track 1 and track 2 of type 0 cards (ABA bank cards) will be encrypted.

9.4.3. Hash Option Setting:

Command:

53 5C 01 <Hash Option>

Hash Option: ('0' – '7')
- 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

9.4.4. Mask Option Setting: (for enhanced encryption format only)

Command:

53 86 01 <Mask Option>

Mask Option (Default: 0x07):
- bit0: 1 – tk1 mask data allow to send when encrypted
- bit1: 1 – tk2 mask data allow to send when encrypted
- bit2: 1 – tk3 mask data allow to send when 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.

10. USING THE DEMO PROGRAM

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

10.1. Overview of Secure MIR Demo

The screenshot may reflect an older version of demo software.
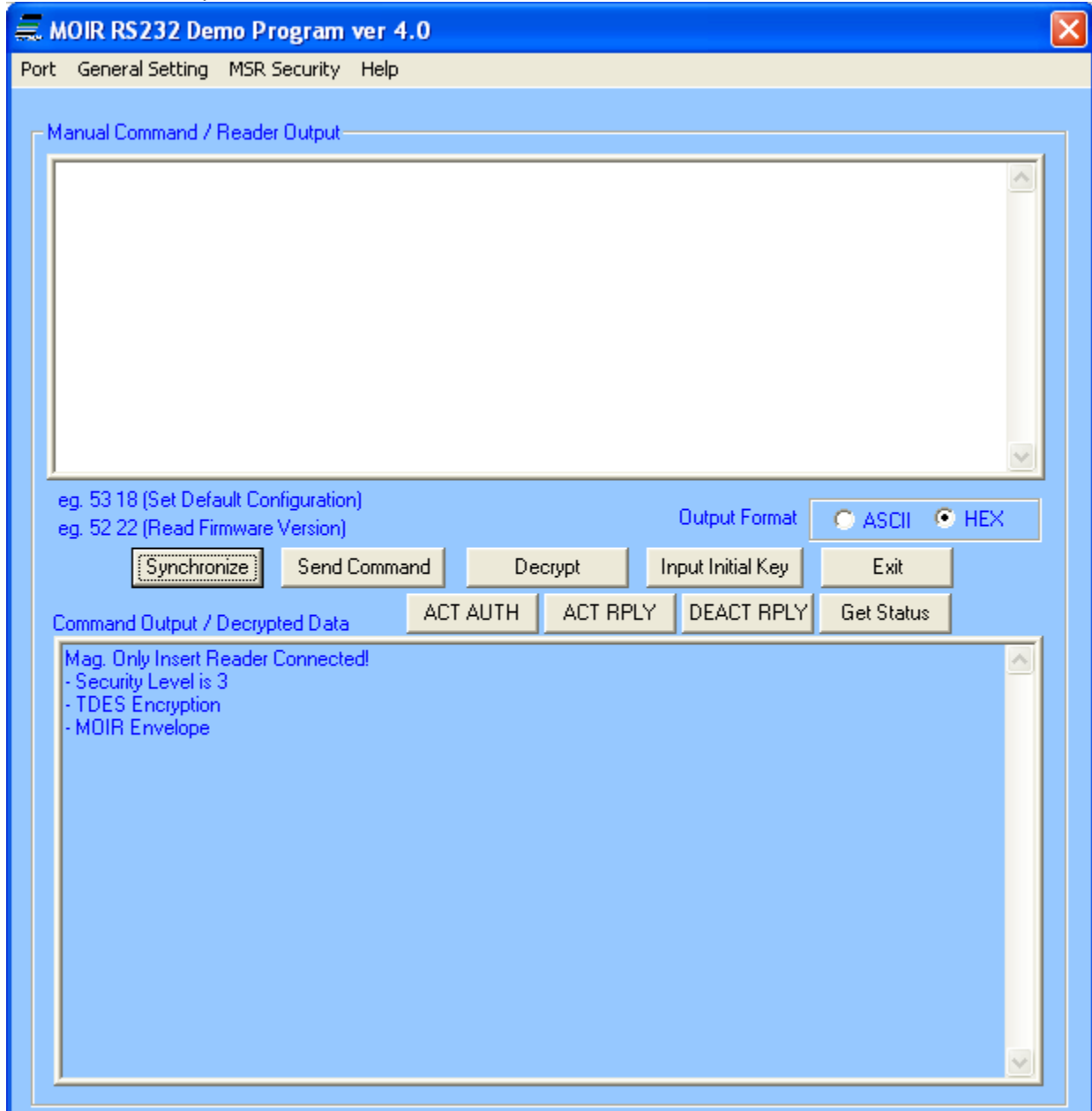
The "Synchronize" button allows the demo program to query the reader determine its security/communication setting and "synchronize" to the readers setting. This button does not

determine every possible reader feature such as baud rate, it assumes the reader is able to communicate with the demo program.

When the RS232 demo starts up, it attempts to open COM 1 and connect to the reader.
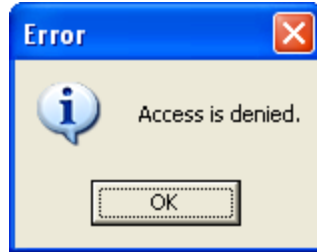
If this dialog box displays, COM 1 was either not installed or already in use. Just select the correct port under the port tab and you should be connected to the reader. A check mark next to the port and to open indicates that the port is connected.

10.2. Manual Command

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

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

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

Press **Send Command** and the input and output are shown in the lower text box.
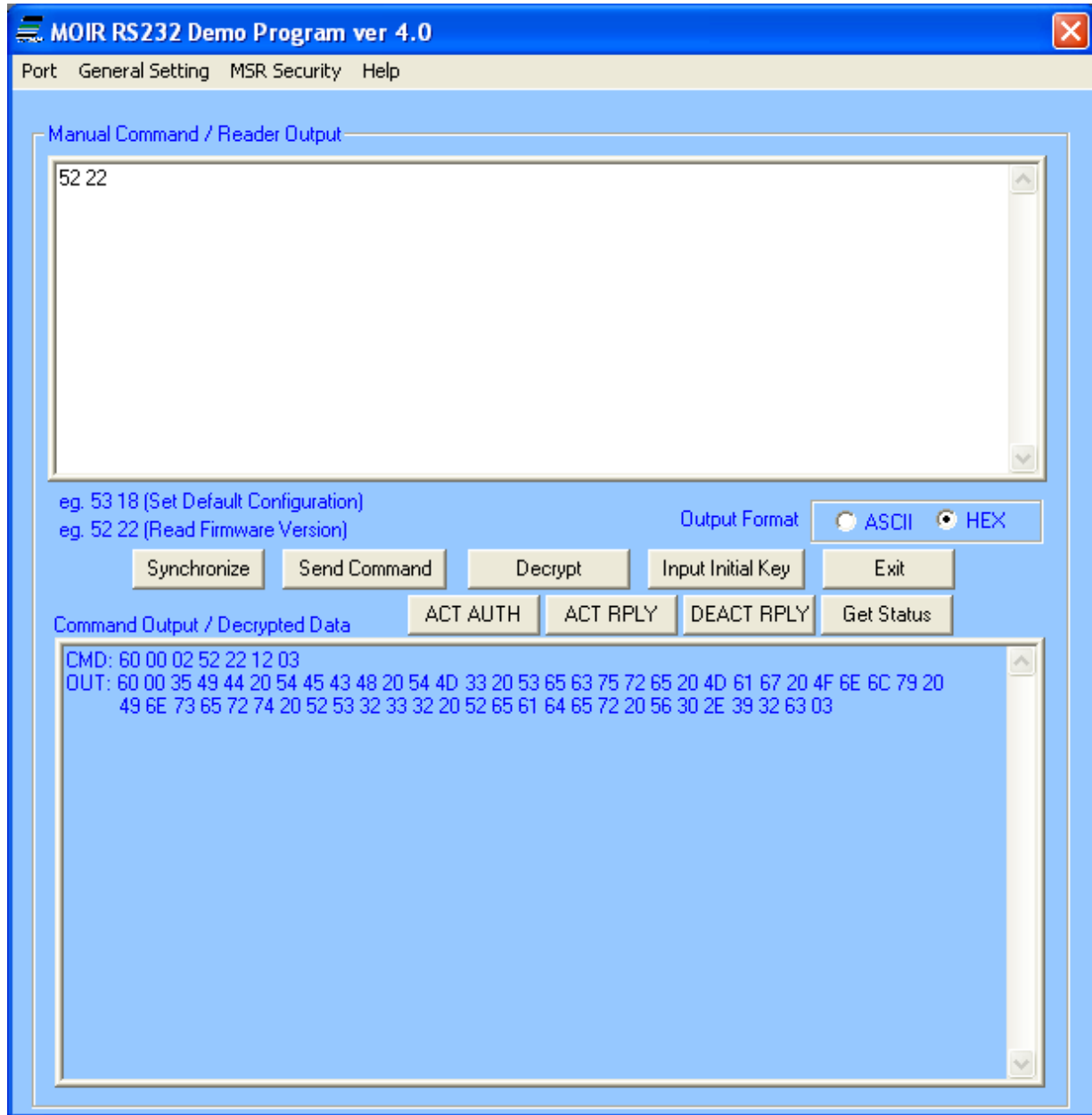
10.3. Security Level 3 Decryption

The encrypted data will show in the Manual Command / Encrypted Data textbox after a card is inserted and/or removed. By default, the cursor is in Manual Command / Encrypted Data textbox
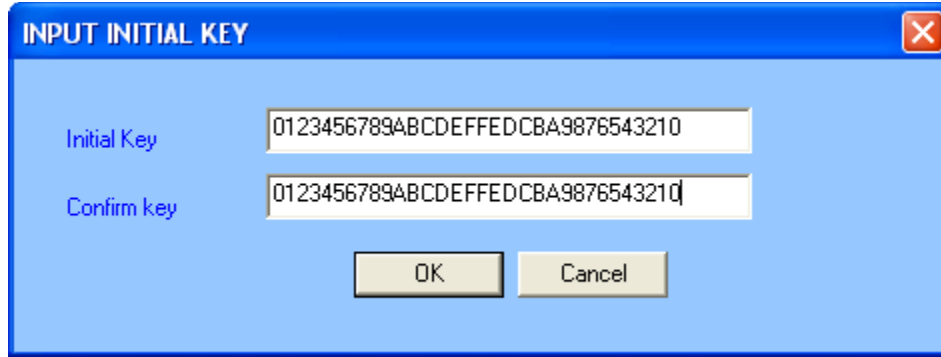
NOTE: In order to allow the demo to know that the reader is in secure mode, select the **Synchronize** button. The decrypt button will not work until this is done unless the demo is configured to match the reader.
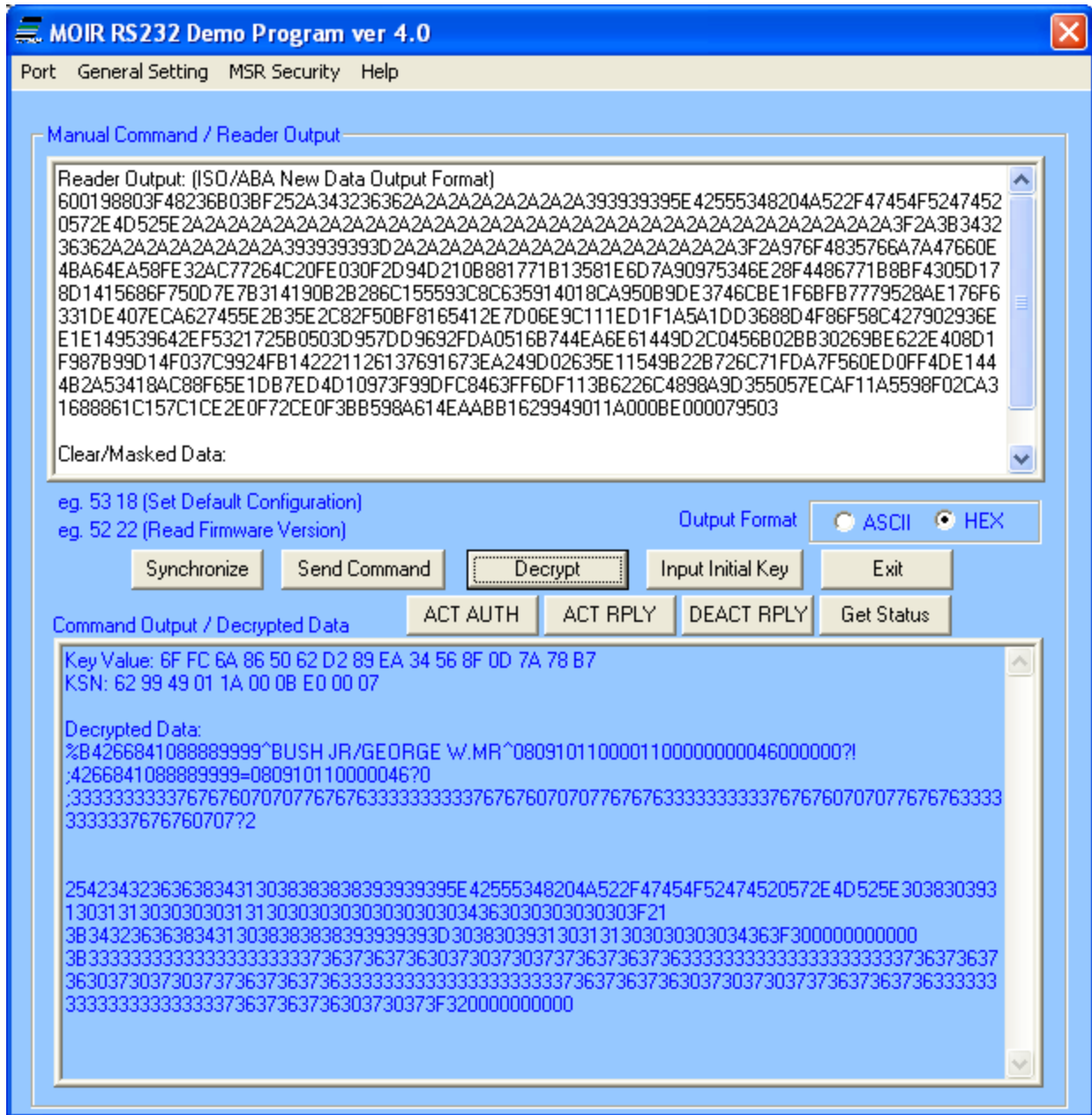
To get the decrypted data, press the **Decrypt** button and the decrypted card data will be displayed in the lower box.

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

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

10.4. Security Level 4 Features and Decryption

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

10.4.1. Activate Authentication Command

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

10.4.2. Activation Challenge Reply Command

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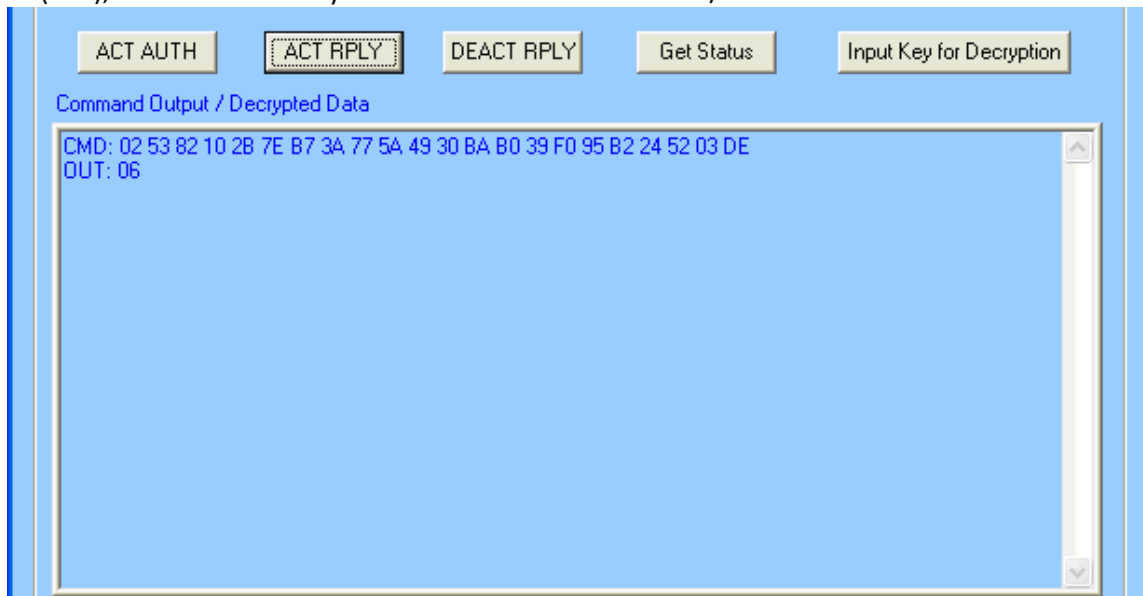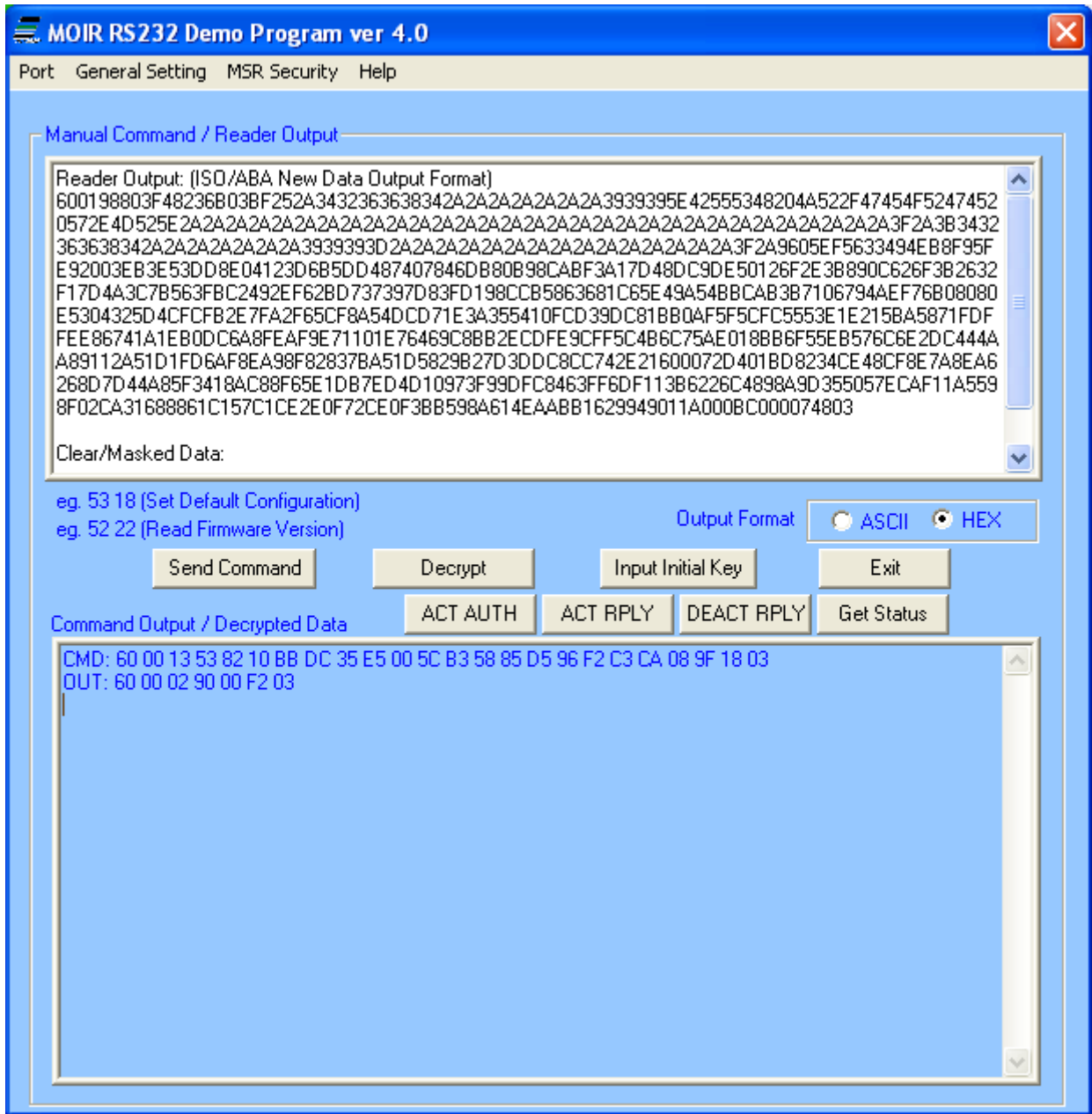
10.4.3. Deactivate Authentication Mode Command

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

10.4.4. Get Status

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

For example, 60 00 02 83 02 02 LRC 03 represents:
- Reader Status: the reader is waiting for a card insertion and/or removal
- Pre-condition: authentication mode was activated successfully. The reader processed a valid Activation Challenge Reply command.

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

10.5. Reader Operations

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

10.5.1. General Setting

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

10.5.2. MSR Security

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

10.5.3. Port

Select Com port and open/ close port.

10.5.4. Help

Provides version information of the demo software.

11.   DECRYPTION EXAMPLES

The key for all examples is:
0123456789ABCDEFFEDCBA9876543210

11.1. 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
600198803F48236B03BF252A343236362A2A2A2A2A2A2A2A2A393939395E4255534
8204A522F47454F52474520572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A
2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B343236362A2A2A2A2A2A2A39393
9393D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A26B03F2BD327CA087C159DEA3E
77974A36B6E89CB5BC85EF92D08FB01152089099FE2A348DF2BA8D7AFEF16A1F5
F2CEA46946A92CDC2AB3B750D1AEF8127995EE6A944E12F9DF40E46607F06C68E
057DA05CC3BBB2BD68ECE1D7D89A4671423C4F649082106A785A62D9382968BCF
4CFD0ECE3CF33449F265542CB4AE6240F99CDACD08E92744FFC04C683834EB4D0
4C9CB9D2A4B4A4FFE15F7C70169C89288097C4B8BB42C67D33073CFEE68B95D0F
88C6CF82F86BF8E7FE5909D153710399940C9DAD8BD26E929EE98BEBFA9D3C19A
AC047B61E8ED56BE52D4A7F8B5FFFA013418AC88F65E1DB7ED4D10973F99DFC84
63FF6DF113B6226C4898A9D355057ECAF11A5598F02CA31688861C157C1CE2E0F
72CE0F3BB598A614EAABB1629949011A000BE00003D703
600002B000D203
```

11.1.1. 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 0198 80 3F 48-23-6B 03BF

60, length(MSB, LSB), card type, track status, length track 1-length track 2- length track 3, mask clear status, crypt hash status

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
252A343236362A2A2A2A2A2A2A2A393939395E42555348204A522F47454F52474
520572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A
2A2A2A2A2A2A3F2A

Track two masked track data displayed in hexadecimal
3B343236362A2A2A2A2A2A2A2A393939393D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2
A3F2A

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

Key Value: 14 81 3F 2E DA E0 EF C0 46 0B 08 AB FA D7 95 87
KSN: 62 99 49 01 1A 00 0B E0 00 01

Decrypted Data:
%B4266841088889999^BUSH JR/GEORGE
W.MR^08091011000011000000000046000000?!
;4266841088889999=08091011000046?0
;3333333333376767607070776767633333333333376767607070776767633333333333767
67607070
77676763333333333767676760707?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^08091011000011000000000046000000?!
;4266841088889999=08091011000046?0
;3333333333376767607070776767633333333333376767607070776767633333333333767
67607070
77676763333333333767676760707?2

Track 1 decrypted data in hex including padding zeros (but there are no pad bytes here):
254234323636383431303838383839393939395E42555348204A522F47454F52474
520572E4D525E30383039313031313030303031313030303030303030303434630
30303030303F21

Track 2 decrypted data in hex including padding zeros:
3B34323636383431303838383838393939393D303830393130313130303030303034
63F300000000000

Track 3 decrypted data in hex including padding zeros:
```
3B3333333333333333333337363736373630373037303737363736373633333333
3333333333333373637363736303730373037373637363736333333333333333333
3333373637363736303730373037373637363736333333333333333333333337363
7363736303730373F320000000000
```

11.1.2. Example Security Level 4 decryption:

Example of decryption of a three-track ABA card with the enhanced encryption format with AES. This example does not include the card status reports.

```
6001B8803F48236B03FF252A343236362A2A2A2A2A2A2A2A2A393939395E4255534
8204A522F47454F524745 20572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A
2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B343236362A2A2A2A2A2A2A2A39393
9393D2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2ADBD7EFAF49EE84708053F744F2
88916E851789A445843030809C0E253E6900EEA0FFD078D51B9A7840AA5F98CC2
```

```
DEADB2497DF29D6C848645E8241D4ED80AA92ACA5D09E0F1F3669CE77D4BE332B
DCE2E1295C13ADF4BE7793FA7FA24128171796A45E39404F4A4DE137B4BA165F6
7719BC633087F11330F4DB2323618CEAAA40DB37773676888FF493D82F8F9757E
8148F9C05EC1BB2D2D54FB8F320C793C1F3C7D8916C693F97970DFAED98F1ECAC
6AF24BBA783BE7EDA1EB897D0CF737C6B95AF16BD15C6AE99C2C7B99EB079F2E1
9877DF3482A0CE5ABD8A8DDFED106C07A3244F0C932BF691B07023D671656B2AA
B5A5B65170A895BE90610DA284394723418AC88F65E1DB7ED4D10973F99DFC846
3FF6DF113B6226C4898A9D355057ECAF11A5598F02CA31688861C157C1CE2E0F7
2CE0F3BB598A614EAABB1629949011A0003A000130003
```

Actual start of the encrypted transaction:
```
60 01B8 80 3F 48-23-6B 03FF
```

60, length(MSB, LSB), card type, track status, length track 1-length track 2-length track 3, mask clear status, crypt hash status

01B8	Total message length in hexadecimal
80	Enhanced encryption structure (default) with ABA card
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
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 upto next length evenly divisible by 16 (the AES block size):
DBD7EFAF49EE84708053F744F288916E851789A445843030809C0E253E6900EE
A0FFD078D51B9A7840AA5F98CC2DEADB2497DF29D6C848645E8241D4ED80AA92
ACA5D09E0F1F3669CE77D4BE332BDCE2

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

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

Session ID encrypted data displayed in hexadecimal:
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^08091011000011000000000046000000?!
;4266841088889999=080910110000046?0
;33333333337676760707077676763333333337676760707077676763333333
33767676070707767676333333333337676760707?2
```

Track 1 decrypted data in hex including padding zeros:
```
25423432363638343130383838383939393 95E42555348204A522F47454F52474
520572E4D525E30383039313031313030303030313130303030303030303034363 0
30303030303F210000000000000000000
```

Track 2 decrypted data in hex including padding zeros:
```
3B3432363638343130383838383839393939 3D303830393130313130303030303034 3
63F3000000000000000000000000000000000
```

Track 3 decrypted data in hex including padding zeros:
```
3B3333333333333333333333736373637363037303730373736373637363333333
333333333333337363736373630373037303737363736373633333333333333333
33333373637363736303730373037373637363736333333333333333333333337363
736373630373037373F320000000000
```

12.   USB DATA FORMAT

The USB version of the reader can operate in two different modes:
- HID ID TECH mode (herein referred to as "HID mode")
- HID with Keyboard Emulation (herein referred to as "KB mode")

When the reader is operated in the HID mode, it behaves as a vendor defined HID device. A direct communication path can be established between the host application and the reader without interference from other HID devices.

12.1. USB Level 1 and level 2 Standard Mode Data Output Format

Card data is only sent to the host on the interrupt-in-pipe using an Input Report. The reader will send only one Input Report per card insertion and/or removal. If the host requests data from the reader when no data is available, the reader will send a NAK to the host to indicate that it has nothing to send.

Data Format Setting:
- USB HID Data Format, Product ID: 06 40
- USB Keyboard Format, Product ID: 06 20
- Secure HID ID TECH Structure, Product ID 25 10
- Secure HID Keyboard, Product ID 25 20

When the reader is plugged in, the firmware will read the "Data Format Setting" from non- volatile memory and send current Product ID in enumeration. After the setting is changed, the firmware will save the setting then do enumeration process.

12.1.1. USB HID Data Format

12.1.1.1. 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 data editing and other features like preamble, postamble, etc. The output data is always HIDSIZE* bytes; the "Total Output Length" field indicates the valid data length in the output data.

Note*: HIDSIZE is 580 bytes as described in USB enumeration. HIDSIZE is subject to change. Software should auto-adjust in case enumeration changes.

12.1.2. Descriptor Tables

12.1.2.1. 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	HID ID TECH Structure
	06 20	HID Keyboard
	25 10	Secure HID ID TECH Structure
	25 20	Secure HID Keyboard
BCD Device Release	00 01	
i-Manufacture	01	
i-Product	02	
i-Serial-Number	00	
# Configuration	01	

12.1.2.2. 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

12.1.2.3. 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	

12.1.2.4. 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	HID ID TECH format
	3D 00	HID Other format
	52 00	HID Keyboard format

12.1.2.5. 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	

12.1.2.6. 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 |

12.1.2.7. 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

12.2. USB Level 1 and level 2 POS Mode Data Output Format

In POS mode use 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 LRC 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
0	Right Shift
1	Left Shift
2	Right Ctrl
3	Left Ctrl
4	Read Error 1
5	Read Error 2
6	Track x ID
7	Track x Error
8	Track x Length 1
9	Track x Length 2
10	Track Data (no extra
Track ID for raw data)	
	…
10 + Track len -1	Card Track x LRC
10 + Track len	Track x LRC
10 + Track len +1	0x0D
10 + Track len + 2	Track x ID
….	Repeat Track

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

OPOS header
Only HID KB interface has [Right Shift, Left Shift, Right Ctrl, Left Ctrl] under POS mode.

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) (1 if track doesn't exist).
B4   1: Track 2 decode success (0: Track 2 decode fail) (1 if track doesn't exist).
B5   1: Track 3 decode success (0: Track 3 decode fail) (1 if track doesn't exist).
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
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   0: 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, Track x Error is set to 0x20 in OPOS raw data mode.
0x20   Success
0x30   Insufficient track data
0x21   Bad Start Sentinel
0x24   Character parity error
0x22   Bad End Sentinel
0x28   Bad track LRC or insufficient trailing synch bits

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.

12.3. Level 3 Data Output Format
For ISO card, both clear and encrypted data are sent. For other card, only clear data is sent at the default encryption setting. If the reader is in Raw mode, all tracks are sent as encrypted data.

A card insertion and/or removal returns the following data.
Note: if all tracks are bad, an empty packet is sent.

Card data is sent out in format of:
60 <LenH><LenL><Card Data><LRC><CheckSum> 03

<LenL><LenH> is a two byte length of <Card Data>.
<LRC> is a one byte Exclusive-OR sum calculated for all <Card Data>.
<CheckSum> is a one byte Sum value calculated for all <Card data>.
<Card Data> format is:

ISO/ABA Data Output Enhanced Format:

card encoding type	(80: ISO/ABA, 84: for Raw mode)
track status	(bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling)
track 1 unencrypted length	(1 byte, 0 for no track1 data)
track 2 unencrypted length	(1 byte, 0 for no track2 data)
track 3 unencrypted length	(1 byte, 0 for no track3 data)
Mask/Clear Status	(1 byte, see definition Field 8)
Encrypt/Hash Status	(1 byte, see definition Field 9)
track 1 masked	(Omitted if in raw mode)
track 2 masked	(Omitted if in raw mode)
track 3 data	(Omitted if in raw mode)
track 1 encrypted	(AES/TDES encrypted data)
track 2 encrypted	(AES/TDES encrypted data)
track 1 hashed	(20 bytes SHA1-Xor)
track 2 hashed	(20 bytes SHA1-Xor)
track 3 hashed (optional)	(20 bytes SHA1-Xor)
DUKPT serial number	(10 bytes)

ISO/ABA Data Output Original Format:

card encoding type	(0: ISO/ABA, 4: for Raw mode)
track status	(bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling)
track 1 unencrypted length	(1 byte, 0 for no track1 data)
track 2 unencrypted length	(1 byte, 0 for no track2 data)
track 3 unencrypted length	(1 byte, 0 for no track3 data)
track 1 masked	(Omitted if in raw mode)
track 2 masked	(Omitted if in raw mode)
track 3 data	(Omitted if in raw mode)
track 1 & 2 encrypted	(AES/TDES encrypted data)
track 1 hashed	(20 bytes SHA1-Xor)
track 2 hashed	(20 bytes SHA1-Xor)
track 3 hashed (optional)	(20 bytes SHA1-Xor)
DUKPT serial number	(10 bytes)

Non ISO/ABA Data Output Format:

card encoding type	(1: AAMVA, 3: Others)
track status	(bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling)
track 1 length	(1 byte, 0 for no track1 data)
track 2 length	(1 byte, 0 for no track2 data)
track 3 length	(1 byte, 0 for no track3 data)
track 1 data	
track 2 data	
track 3 data	

Note:

Field 4: Track 1-3 Status

- bit 0: if 1—tk1 decode success or no data on track
- bit 1: if 1—tk2 decode success or no data on track
- bit 2: if 1—tk3 decode success or no data on track
- bit 3: if 1—tk1 has sampling data present
- bit 4: if 1—tk2 has sampling data present
- bit 5: if 1—tk3 has sampling data present
- bit 6: if 1—reserved for future use—has been assigned in another product
- bit 7: if 1— reserved for future use

Field 8 (Clear/mask data sent status) and field 9 (Encrypted/Hash data sent status) will only be sent in new encrypt structure.

Field 8: Clear/mask data sent status byte:

- bit 0: 1—if TK1 clear/mask data present
- bit 1: 1—if TK2 clear/mask data present
- bit 2: 1—if TK3 clear/mask data present
- bit 3: 0—if other products use this DUKPT key management; 1 — fixed key; MIR indicates DUKPT by presence of KSN.
- bit 4: 0—TDES encryption; 1 — AES encryption
- bit 5: 1—if service code '2' or '6'; use ICC when possible (added V2.89)
- bit 6: 0—DATA Key see ANSI X9.24 2009 pg. 56; 1—PIN Key encryption
- bit 7: 1—if reader serial number present

Field 9: Encrypted data sent status

- bit 0: if 1—tk1 encrypted data present
- bit 1: if 1—tk2 encrypted data present
- bit 2: if 1—tk3 encrypted data present
- bit 3: if 1—tk1 hash data present
- bit 4: if 1—tk2 hash data present
- bit 5: if 1—tk3 hash data present
- bit 6: if 1—session ID present
- bit 7: if 1—KSN present

Card Type:
Value Encode Type Description
- 0 / 80 ISO/ABA format
- 1 / 81 AAMVA format
- 3 / 83 Other
- 4 / 84 Raw; un-decoded format.
- 5 / 85 JIS II-decoded format. (added with Version V2.89).
- 6 / 86 JIS I-decoded format.
- 7 / 87 JIS II-decoded format.

12.3.1. Encryption Option Setting (for enhanced encryption format only except bits 6-7)

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 – track 3 encrypted with card is type 0 and track 3 is ISO4904 send mask data
- bit5: 0 – reserved for future use always zero
- bit6: 0 – reserved for future use always zero
- bit7: 1 – pad according to PKCS#5 (else pad with zeros)

Note:
- When force encrypt is set, this track will always be encrypted, regardless of card type. No clear/mask text will be sent.
- If and only if in enhanced encryption format, each track is encrypted separately. Encrypted data length will round up to 8bytes for DES or 16 bytes for AES.
- When force encrypt is not set, the data will be encrypted in original encryption format, that is, only track 1 and track 2 of type 0 cards (ABA bank cards) will be encrypted.

12.3.2. Hash Option Setting

Command:
53 5C 01 <Hash Option>

Hash Option ('0' – '7'):
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

12.3.3. Mask Option Setting (for enhanced encryption format only)

Command:
53 86 01 <Mask Option>

Mask Option (Default: 0x07):
bit0: 1 – tk1 mask data allow to send when encrypted
bit1: 1 – tk2 mask data allow to send when encrypted
bit2: 1 – tk3 mask data allow to send when 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.

12.4. Level 4 Data Output 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 returns the following data: Note: if all tracks are bad, an empty packet is sent.

Card data is sent out in format of 60<LenL><LenH><Card Data><LRC><CheckSum> 03

- <LenL><LenH> is a two byte length of <Card Data>.
- <LRC> is a one byte Exclusive-OR sum calculated for all <Card Data>.
- <CheckSum> is a one byte Sum value calculated for all <Card data>.
- <Card Data> format is:

ISO/ABA Data Output Enhanced Format (default)

card encoding type	(80: ISO/ABA, 84: for Raw Mode)
track status	(bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling)
track 1 unencrypted length	(1 byte, 0 for no track1 data)
track 2 unencrypted length	(1 byte, 0 for no track2 data)
track 3 unencrypted length	(1 byte, 0 for no track3 data)
Mask/Clear Status	(1 byte, see definition and example)
Encrypt/Hash Status	(1 byte, see definition and example)
track 1 masked	(Omitted if in Raw mode)
track 2 masked	(Omitted if in Raw mode)
track 3 data	(Omitted if in Raw mode)
track 1 encrypted	(AES/TDES encrypted data)
track 2 encrypted	(AES/TDES encrypted data)
sessionID encrypted	(AES/TDES encrypted data)
track 1 hashed (optional)	(20 bytes SHA-1-Xor)
track 2 hashed (optional)	(20 bytes SHA-1-Xor)
track 3 hashed (optional)	(20 bytes SHA-1-Xor)
DUKPT serial number	(10 bytes)

ISO/ABA Data Output Original Format

card encoding type	(0: ISO/ABA, 4: for Raw Mode)	
track status	(bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling)	
track 1 unencrypted length	(1 byte, 0 for no track1 data)	
track 2 unencrypted length	(1 byte, 0 for no track2 data)	
track 3 unencrypted length	(1 byte, 0 for no track3 data)	
track 1 masked	(Omitted if in Raw mode)	
track 2 masked	(Omitted if in Raw mode)	
track 3 data	(Omitted if in Raw mode)	
track 1 & 2 encrypted	(AES/TDES encrypted data)	
sessionID encrypted	(AES/TDES encrypted data)	
track 1 hashed (optional)	(20 bytes SHA-1-Xor)	
track 2 hashed (optional)	(20 bytes SHA-1-Xor)	
track 3 hashed (optional)	(20 bytes SHA-1-Xor)	
DUKPT serial number	(10 bytes)	

Non ISO/ABA Data Output Format

card encoding type	(1: AAMVA, 3: Others)
track status	(bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling)
track 1 length	(1 byte, 0 for no track1 data)
track 2 length	(1 byte, 0 for no track2 data)
track 3 length	(1 byte, 0 for no track3 data)
track 1 data	
track 2 data	
track 3 data	

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.

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 pre-formed for the right side of the key, combine the two key parts to create the Data Key.

How to get Encrypted Data Length
Track 1 and Track 2 data are encrypted as a single block (in original encryption format or in separate blocks in enhanced encryption format). In order to get the number of bytes for encrypted data field, we need to get Track 1 and Track 2 unencrypted length first. The field 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. After the encrypted data is decrypted, all padding 0 need to be removed. The number of bytes of decoded track 1 data is indicated by track 1 unencrypted length field. The remaining bytes are track 2 data, the length of which is indicated by track 2 unencrypted length filed.

Track 1, 2 and 3 hashed
MIR reader uses SHA-1 to generate hashed data for both track 1, track 2 and track 3 unencrypted data. It is 20 bytes long for each 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.

12.5. Level 4 Activate Authentication Sequence
The security level changes from 3 to 4 when the device enters authentication mode successfully. After the security level is changed to level 3 or 4, it cannot go back to a lower level.

12.5.1. 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><R><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.

12.5.2. 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.

12.5.3. 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

12.5.4. Get Reader Status Command

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

Device -> Host:
60 00 02 <STX><83h><02h><Current 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.

- o 0x02: The reader receives a good card insertion and/or removal.
- o 0x03: The reader receives a bad card insertion and/or removal or the card is invalid. 0x04: Authentication Activation Failed.
- o 0x05: Authentication Deactivation Failed.
- o 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.
- o 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

12.6. General Commands

The following table is a summary of the general commands described in this section:

HEADER	DATA	NAME	USAGE
60 00 01	24	Get Reader Status	To get reader status in the form of a single byte
60 00 01	39	Get Version	To get the version of the reader's firmware
60 00 01	49	Reset the Reader	To reset the reader to its default state, No configuration change
60 00 03	50 01 30	Arm to Read in Buffer Mode	To enable reading in buffer mode
60 00 03	50 01 32	MSR Reset in Buffer Mode	To return the reader to its default settings when buffer mode is enabled
60 00 03	51 01 xx	Read MSR Data in Buffer Mode	To set the tracks on the magnetic stripe to be read while in buffer mode
60 00 02	52 1F	Review All Settings	To retrieve all current settings
60 00 02	52 <FunctionID>	Get Setting	Getting various reader optional settings
60 00 02	53 18	Default All	Setting reader optional functions to default
60 00 xx	53[<FuncID><Len><Func Data>]…	Send Setting	Setting various reader optional functions
60 00 04	53 10 01 xx	Set Terminal Type	Set terminal type of the reader
60 00 04	53 11 01 xx	Set Reader Option	Set the switch notifications, LED control, Data Envelope and Raw Data Decoding
60 00 04	53 2F 01 xx	Set Reader Option 2	Bit 0:media detect, 1:Set the notification of no data, 2:card in slot and 3:incomplete insertion;4: NGA mode; 5:alternate JIS II card type
60 00 02	6C	LED Control	To set the LED to be controlled by host

12.6.1. Get Reader Status [24]

Command:

<60><00><01><24><LRC><ETX>

Response:

<60><00><01><Reader Status><LRC><ETX>

Returns a single-byte status for RS232 and USB-KB readers.

Bit Position	0	1
B0	Unused	Unused
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	Key Block/KSN good	Key corrupt or exhausted

B7 feature added with Version V2.89.

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

12.6.2. Buffer Mode Commands [50 or 51]

Commands:

<60><00><03><50><01><30><LRC><ETX>
<60><00><03><50><01><32><LRC><ETX>
<60><00><03><51><01><Track Select Byte><LRC><ETX>

These commands are executed only when the MSR READING SETTING is in <32> MSR Reading Buffered mode. If the host sends these commands to the reader in MSR Auto- Transmission mode, the reader will send back an "E0 00" response package.

For more specific information, please refer to the descriptions under the ARM TO READ IN BUFFER MODE, MSR RESET IN BUFFER MODE, and READ MSR DATA IN BUFFER MODE commands.

12.6.3. Set Reader Option [53 11]

Command:

<60><00><04><53><11><01><Setting><LRC><ETX>

A single-byte setting is defined as follows:

Bit Position	0	1
B0	Card Seated Off	Card Seated On
B1	Card Removed Off	Card Removed On
B2	Card In Off	Card In On
B3	MSR Data Envelope Off	MSR Data Envelope On
B4	LED Controlled by Reader	LED Controlled by Host

B5	Magnetic Data Present Off	Magnetic Data Present On
B6	Standard Decoder	Raw Data Decoder
B7	Card Out Off	Card Out On

Response:
<60><00><02><90><00><LRC><ETX>

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

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.

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

After a good read, the magnetic stripe data will be sent out with an envelope if "MSR Data Envelope" is ON:
<60><Len_H> <Len_L> <Card data indication 1 > <Card data indication 2> <Magstripe data>
<LRC> <ETX>

Otherwise, magnetic stripe data will be sent out without an envelope (<Magstripe Data>).

<Card data indication 1 > (<Cx>) is an ID to indicate magnetic data.

Bit Position	Value
B0-B3	Unused
B4	'0'
B5	'0'
B6	'1'
B7	'1'

<Card data indication 2> flags the current read.

Bit Position	'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	

Note: Track x decode flag available only when track x data exist.

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 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 "[Tab]Magnetic Data[Tab]". 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.

12.6.4. Set Reader Option 2 [53 2F]

Command:
<60><00><04><53><2F><01 ><Setting><LRC><ETX>

A single-byte setting is defined as follows:

Bit Position	0	1
B0	Media Detected Off	Media Detected On
B1	No Data Off	No Data On
B2	No Card in Slot	Card in Slot On
B3	No Incomplete Insertion	Incomplete Insertion
B4	TLP Protocol for secure output	NGA protocol for secure output
B5	JIS II reports type 7/87	JIS II reports as type 5/85
B6	no corrupt key report	Report corrupt key/KSN
B7	Reserved	

B5 and B6 feature added with Version V2.89.

Response:
<60><00><02><90><00><LRC><ETX>

For RS232 reader, the default value is 0x00. For USB_HID_KB reader, the default value is 0x03.

After an insertion or withdrawal, a NO DATA notification will be issued if its setting is ON. That means no data on selected tracks (if Read Direction is enabled) and no magnetic data after an insertion or withdrawal time out.

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.

After a withdrawal, a CARD IN SLOT notification will be issued if CARD PRESENT is still ON 2 seconds after withdrawal.

After an insertion, an INCOMPLETE INSERTION notification will be issued if CARD SEATED is still OFF 2 seconds after insertion.

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

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 according status was changed.

Note: If the NGA bit is set the encrypted track output will always be in NGA protocol (that is Next Generation Architecture). If this bit is set and the host has not communicated with the reader the readers output in non secure mode will be in ITP mode. If the host has communicated with the reader, the reader will use the protocol that the host used to communicate.

12.7. RS232 Reader Special Configuration Commands

The following table is a summary of the RS232 reader special commands to configure the reader communication described in this section:

HEAD	DATA	NAME	USAGE
60 00 04 53	41 01 xx	Set Baud Rate	To set baud rate for RS232 interface reader
60 00 04 53	43 01 xx	Set Data Parity	To set Data Parity for input character frame
60 00 04 53	44 01 xx	Set Hand Shake Method	To set handshake method
60 00 04 53	45 01 xx	Set Stop Bits	To set Stop Bits for input character frame
60 00 04 53	47 01 xx	Set Xon Character	To set Xon Character
60 00 04 53	48 01 xx	Set Xoff Character	To set Xoff Character

12.7.1. Set Baud Rate

The default baud rate is 38400 bits/sec. Reader will turn to the setting baud rate after send back a response for this setting command. Application should turn to the setting baud rate after receiving the response to ensure the communication between application and hybrid reader.

Command:
<60><00><04><S><41><01><Baud Rate Setting ><LRC> <ETX>

The command is used to set the baud rate of serial communication between application and hybrid reader, where:

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

Response:
<60><00><02><90><00><F2><03> The response is sent before the BAUD rate is changed

12.7.2. Set Data Parity
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.

Set Data Parity Command:
<60><00><04><S><43><01><Data Parity Setting ><LRC> <ETX>

The default Data Parity value is None.

Data Parity Setting:
- o '0': None
- o '1': Even
- o '2': Odd
- o '3': Mark
- o '4': Space

Response: <60><00><02><90><00><F2><03>

12.7.3. Set Handshake Method
<60><00><04><S><44><01><Handshake Setting ><LRC> <ETX>

The command is used to set the Handshake (Flow Control) of serial communication between application and Magnetic Stripe Insert reader, where:
- Handshake Setting
  - o '0': No Handshake
  - o '2': Software Xon/Xoff Handshake

Response:
<60><00><02><90><00><F2><03>

12.7.4. Set Stop Bits

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

Command:
<60><00><04><S><45><01><Stop Bits Setting ><LRC> <ETX>

The default Stop Bits value is 1 bit.

Stop Bits Setting:
- '0': 1 Bit
- '1': 2 Bits

Response:
<60><00><02><90><00><F2><03>

12.7.5. Set Xon Id

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

Command:
<60><00><04><53><47><01 ><XOn ID Character><LRC><ETX>

The XOn ID can be any single ASCII character desired. The default value is 0x11.

Response:
<60><00><02><90><00><F2><03>

12.7.6. Set XOff ID

This setting allows the user to select any single character to be used as the XOff ID character.

Command:
<60><00><04><53><48><01 ><XOff ID Character><LRC><ETX>

The XOff ID can be any single ASCII character desired. The default value is 0x13.

Response:
<60><00><02><90><00><F2><03>

12.8. USB HID or HID Keyboard Reader Special Commands

The following table is a KB or USB/HID/KB Reader Special commands summary described in this section:

HEAD <60><Command Length>	DATA	NAME	USAGE
60 00 xx	53 26 xx	Set Card Seated String	To edit the string for the optional notification
60 00 xx	53 27 xx	Set Card Removed String	To edit the string for the optional notification
60 00 xx	53 28 xx	Set Card Present String	To edit the string for the optional notification
60 00 xx	53 29 xx	Set Card Out String	To edit the string for the optional notification
60 00 xx	53 2A xx	Set No Data String	To edit the string for the optional notification
60 00 xx	53 2B xx	Set Media Detected String	To edit the string for the optional notification
60 00 xx	53 2C xx	Set Magnetic Data String	To edit the string for the optional notification
60 00 xx	53 2D xx	Set Card In Slot String	To edit the string for the optional notification
60 00 xx	53 2E xx	Set Partial In String	To edit the string for the optional notification

12.8.1. Set Card Seated String

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 ReaderOptID is set.

Command:
<60><Command Length><53><26><Len><Card Seated String><LRC><ETX>

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.)

Response:
<60><00><02><90><00><F2><03>

12.8.2. Set Card Removed String

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 ReaderOptID is set.

Command:
<60><Command Length><53><27><Len><Card Removed String><LRC><ETX>

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.)

Response:
<60><00><02><90><00><F2><03>

12.8.3. Set Card Present String

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 ReaderOptID is set.

Command:
- <60><Command Length><53><28><Len><Card Present String><LRC><ETX> 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.)

Response:
<60><00><02><90><00><F2><03>

12.8.4. Set Card Out String

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 ReaderOptID is set.

Command:
<60><Command Length><53><29><Len><Card Out String><LRC><ETX>

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.)

Response:
<60><00><02><90><00><F2><03>

12.8.5. Set No Data Detected String

This setting allows the user to select a character string to be output as no data notification. When mismatch of data edit formula, no data on selected tracks, no magnetic data after an insertion or withdraw time out, this string will be sent out if "No Data On and Off" bit in ReaderOpt2ID is set.

Command:
<60><Command Length><53><2A><Len><No Data String><LRC><ETX>

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.) Response: <60><00><02><90><00><F2><03>

12.8.6. Set Media Detected String

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

Command:
<60><Command Length><53><2B><Len><Media Detected String><LRC><ETX>

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.)

Response:
<60><00><02><90><00><F2><03>

12.8.7. Set Card In Slot String

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 ReaderOpt2ID is set.

Command:
<60><Command Length><53><2D><Len><Card In Slot String><LRC><ETX>

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.)

Response:
<60><00><02><90><00><F2><03>

12.8.8. Set Partial Insertion String

This setting allows the user to select a character string to be output as partial in notification. When the card insert 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 ReaderOpt2ID is set.

Command:
<60><Command Length><53><2E><Len><Incomplete Insertion String><LRC><ETX>

In this example:
- <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.)

Response:
<60><00><02><90><00><F2><03>

12.8.9. Set Magnetic Data String
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, the magnetic data in current read direction was enabled by reader, this string will be sent out if "Magnetic Data On and Off" bit in ReaderOptID is set.

Command:
<60><Command Length><53><2C><Len><Magnetic Data String><LRC><ETX>

In this example:
- <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.)

Response:
<60><00><02><90><00><F2><03>

12.9. Magnetic Stripe Reader Configuration
12.9.1. Set Track 1 7-Bit Start Sentinel
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.

Command:
<60><00><04><53><61><01><Track1 7Bit Start Sentinel ><LRC><ETX>

Response:
<60><00><02><90><00><F2><03>

12.9.2. Set Track 1 6-Bit Start Sentinel
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 6-bit encoded.

Command:
<60><00><04><53><62><01><Track1 6Bit Start Sentinel ><LRC><ETX>

Response:
<60><00><02><90><00><F2><03>

12.9.3. Set Track 1 5-Bit Start Sentinel

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.

Command:
<60><00><04><53><63><01><Track1 5Bit Start Sentinel ><LRC><ETX>

Response:
<60><00><02><90><00><F2><03>

12.9.4. Set Track 2 7-Bit Start Sentinel

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.

Command:
<60><00><04><53><64><01><Track2 7Bit Start Sentinel ><LRC><ETX>

Response:
<60><00><02><90><00><F2><03>

12.9.5. Set Track 2 5-Bit Start Sentinel

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 5-bit encoded.

Command:
<60><00><04><53><65><01><Track2 5Bit Start Sentinel ><LRC><ETX>

Response:
<60><00><02><90><00><F2><03>

12.9.6. Set Track 3 7-Bit Start Sentinel

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.

Command:
<60><00><04><53><66><01><Track3 7Bit Start Sentinel><LRC><ETX>

Response:
<60><00><02><90><00><F2><03>

12.9.7. Set Track 3 6-Bit Start Sentinel

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 6-bit encoded.

Command:
<60><00><04><53><67><01 ><Track3 6Bit Start Sentinel ><LRC><ETX>

Response:
<60><00><02><90><00><F2><03>

12.9.8. Set Track 3 5-Bit Start Sentinel

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.

Command:
<60><00><04><53><68><01><Track3 5Bit Start Sentinel><LRC><ETX>

Response:
<60><00><02><90><00><F2><03>

12.9.9. Set Track End Sentinel

This setting allows the user to select any single character to be output as the track end sentinel.

Command:
<60><00><04><53><69><01><Track End Sentinel><LRC><ETX>

Response:
<60><00><02><90><00><F2><03>

12.9.10. Set Preamble

This setting allows the user to select a character string to be added to the beginning of magnetic stripe data. If a character string is defined, it will be sent out before any track ID or start sentinel. If no character string is defined, nothing will be sent out ahead of the track ID or start sentinel.

Command:
<60><Command Length><53><D2><Len><Preamble String><LRC><ETX>

Where:
- <Command Length> is a two-byte length from <53> to <Preamble String>
- <Len> is the number of bytes of the Preamble String, but no greater than 0x10
- <Preamble String> is {string length}{string} (String length is one byte, maximum 15.)

Response:
<60><00><02><90><00><F2><03>

12.9.11. Set Postamble

This setting allows the user to select a character string to be output at the end of magnetic stripe data. If a character string is defined, it will be sent out after the terminator ID. If no character string is defined, nothing will be sent out after the terminator ID.

Command:
<60><Command Length><53><D3><Len><Postamble String><LRC><ETX>

In this example:
- <Command Length> is a two-byte length from <53> to <Postamble String>
- <Len> is the number of bytes of Postamble String, but no greater than 0x10
- <Postamble String> is {string length}{string} (String length is one byte, maximum 15.)

Response:
<60><00><02><90><00><F2><03>

12.9.12. Envelope for Unencrypted Magnetic Stripe Data

This command adds the ID TECH envelope to magnetic stripe data before it is sent to the host.

Command:
<60><Len_H><Len_L><card data indication 1><card data indication 2>[Track 1 data][Track2 data][Track 3 data]<LRC><ETX>

<card data indication 1 >(<Cx>) is an ID to indicate magnetic data.
Bit Position

B0-B3	Unused (set to 0)
B4	'0'
B5	'0'
B6	'1'
B7	'1'

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

Bit Position	'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)	Unused (set to 0)

Note: The Track x decode flag will be 0 if Track x data does not exist.
Note: The order of magnetic data and switch change notification depends on the order in which they come to the microcontroller. This is not fixed.

12.9.13. Set Arm to Read in Buffered Mode

This command sets the reader to read magnetic stripe data and store it in memory.

Command:
<60> <00> <03> <50> <01 > <30> <LRC> <ETX>

Response:
<60> <00> <02> <90> <00> <LRC> <03>

If the reader controls the LED, the LED will turn green and the reader will send an ACK response to the host. Previously read data will be erased, and the reader will wait for the next card insertion or withdraw, depend on decoding method command. If an MSR RESET command is received, all data will be erased from memory.

When a card is inserted and withdrawn, the decoded data will be saved in memory and not sent to the host. If the reader controls the LED, the LED will turn slow flashing green. (If there was no data to read, the LED will briefly turn red and then turn to slow flashing green.) A notification will be sent to the host to indicate the presence of magnetic data. Data will be held until receiving the next ARM TO READ or MSR RESET command.

While in Buffer Mode, the reader will continue to allow the normal commands (e.g., status, LED commands).

12.9.14. MSR Reset in Buffered Mode

This command will disable MSR reading and clear any magnetic data stored in the buffer. The reader will enter a disarmed state and ignore MSR data.

Command:
<60> <00> <03><50> <01><32> <LRC> <ETX>

Response:
<60> <00> <02> <90><00> <LRC> <03>

Any stored magnetic data will be erased. The reader will send an ACK response to the host.

If the reader is configured automatically to transmit magnetic data, the reader will respond that the command is not supported. The LED will be slow flashing green.

12.9.15. Read MSR Data in Buffered Mode

There are up to three tracks of encoded data on a magnetic stripe. This setting selects the tracks to be read in Buffer Mode.

Command:
<60> <00> <03> <51 > <01 > <Track Select Byte> <LRC> <ETX>

Track Selection Settings:
- <30> Any Track
- <31> Track 1
- <32> Track 2
- <33> Track 1 & Track 2
- <34> Track 3
- <35> Track 1 & Track 3
- <36> Track 2 & Track 3
- <37> All Three Tracks
- <38> Track 1 &/or Track 2
- <39> Track 2 &/or Track 3

The data on the selected track(s) will be sent to the host either in envelope format or not, according to the Card Notification Setting, or in RAW format. The data will not be erased after this command.

13. USB HID KB DATA OUTPUT FORMAT

Level 1 and level 2 POS Mode Data Output Format

In POS mode use 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
0	Right Shift
1	Left Shift
2	Right Ctrl
3	Left Ctrl
4	Read Error 1
5	Read Error 2
6	Track x ID
7	Track x Error
8	Track x Length 1
9	Track x Length 2
10	Track Data (no extra Track ID for raw data)
…	
10 + Track len -1	Card Track x LRC
10 + Track len	Track x LRC
10 + Track len +1	0x0D
10 + Track len + 2	Track x ID
….	Repeat Track

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

OPOS header:
Only HID KB interface has [Right Shift, Left Shift, Right Ctrl, Left Ctrl] under POS mode.

Read Error:
Read Error one-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.

Card data is sent out in format of:

TLP Protocol (the default):
<60><LenH><LenL><Card Data><CheckLRC><ETX>

NGA Protocol:
<STX><LenL><LenH><Card Data><CheckLRC><CheckSum><ETX>

- <STX> = 02h
- <ETX> = 03h
- <LenL><LenH> is a two byte length of <Card Data>
- <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>

<Card Data> format is:

ISO/ABA Data Output Original Encrypted Format

card encoding type	(0: ISO/ABA)
track status	(bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling)
track 1 unencrypted length	(1 byte in binary, 0 for no track1 data)
track 2 unencrypted length	(1 byte in binary, 0 for no track2 data)
track 3 unencrypted length	(1 byte in binary, 0 for no track3 data)
track 1 masked	
track 2 masked	
track 3 data	
track 1 encrypted	(AES/TDES encrypted data, bytes)
track 2 encrypted	(AES/TDES encrypted data, bytes)
sessionID encrypted	(AES/TDES encrypted data, bytes)
track 1 hashed	(20 bytes SHA1-Xor)
track 2 hashed	(20 bytes SHA1-Xor)
DUKPT serial number	(10 bytes)

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

card encoding type	(1: AAMVA, 3: Others)
track status	(bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling)
track 1 length	(1 byte in binary, 0 for no track1 data)
track 2 length	(1 byte in binary, 0 for no track2 data)
track 3 length	(1 byte in binary, 0 for no track3 data)
track 1 data	
track 2 data	
track 3 data	

Track 1 Encrypted Data Length
This value indicates the number of bytes in the Track 1 encrypted data field. The field is always a multiple of 8 bytes in length. This value will be zero if there was no data on the track or if there was an error decoding the track. After the encrypted data is decrypted, there may be fewer bytes of decoded track data than indicated by this field. The number of bytes of decoded track data is indicated by the track 1 unencrypted length. The field is always a multiple of 8 bytes in length. This value will be zero if there was

Track 2 Encrypted Data Length
This value indicates the number of bytes in the Track 2 encrypted data field. The value will be zero if there was no data on the track or if there was an error decoding the track. After the encrypted data is decrypted, there may be fewer bytes of decoded track data than indicated by this field. The number of bytes of decoded track data is indicated by the track 2 unencrypted length.

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.

Track 1 unencrypted Length
This one-byte value indicates the number of useable bytes in the Track 1 Encrypted Data field and Track 1 masked Data field after decryption.

Track 2 unencrypted Length
This one-byte value indicates the number of useable bytes in the Track 2 Encrypted Data field and Track 2 masked Data field after decryption.

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

13.3. Level 1 and 2 Buffer Mode Output Format

Buffer Mode Operation	50 01 30: Arm to Read
	50 01 32: Buffer mode reset
Buffer Mode Output	51 01 <Track Selection Option>: Read MSR Data Track Selection Option:
	0x30 – Any Track
	0x31 – Track 1 Only
	0x32 – Track 2 Only
	0x33 – Track 1 & Track 2
	0x34 – Track 3 Only
	0x35 – Track 1 & Track 3
	0x36 – Track 2 & Track 3 0x37 – All Three Tracks0x38 – Track 1 &/or Track 2
	0x39 – Track 2 &/or Track 3

13.4. Level 4 Activate Authentication Sequence

The security level changes from 3 to 4 when the device enters authentication mode successfully. After 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 would only transmit the card data when it is in Authenticated Mode.

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. If the timeout time is set to zero, then this request has no timeout.

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 04 <R><80h><02h><Pre-Authentication Time Limit><LRC><ETX>

Device -> Host:

60 00 01 <Device Response Data><LRC><ETX> (success)
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 0A <S><82h><08h><Activation Data><LRC><ETX>

- 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 0A<S><83h><08h><Deactivation Data><LRC><ETX>

- <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 04<83h><02h><Current Reader Status><Pre-condition><LRC><ETX> (success)

- 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 removals 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 insert and/or remove a card within the time specified in the Activation Challenge Reply command

14. APPENDIX A: Setting Parameters and Values

The following table describes the default and available settings (value within parentheses) for each function ID.

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	-
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	1 (1 ~ 255)	USB HID Polling Interval	u
DataFmtID	15	Data Output Format	'0' ('0'~'2')	ID TECH Format	-
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			
SendOptionID	19	Send Option	'1' ('0'~0x3F) '5' for KB	Sentinel and Account number control. See Set MSR Send Option.	
MSRReading ID	1A	MSR Reading	'1' ('0'~'2')	Enable MSR Reading '0' MSR disable; '2' Buffer Mode See 9.4.11 page 31.	
DTEnableSendID*	1B	DT Enable Send	'0'('0','1','3')	Data Editing Control	-

Function ID	Hex	Description	Default Setting	Description	
CustomEquipID	1C	custom equipment setting	0x00, 0x10, 0x20, 0x30, 0x40, 0x50, 0x60, or 0x70	bit 6=0: single head; bit 6=1: 0x40 dual head; bit 5=1: 0x20 support JIS; bit 6=0: no card present switch; bit 6=1: card present switch present; unaffected by reset all	
DecodingMethodID	1D	MSR Read Direction	'3' ('1'~'4')	'1'-both '2'-read on insert '3'-report on withdrawal '4'-read on withdrawal. See 9.4.12 page 31.	
ReviewID	1F	Review All Settings	None		
TerminatorID	21	MSR Terminator	CR/Enter	CR for RS232, Enter for KB; 0 for none; any value legal	
FmVerID	22	Firmware Version			
USBHIDFmtID	23	USB HID Fmt	'0' USB HID '8' KB ('0','8')	'0' for USB HID '8' for USB HID KB	u r
ForeignKBID	24	Foreign KB	'0' ('0' -0x3A)	Foreign Keyboard	k
CardSeatedStrID	26	Card Seated String	[tab]Card Seated[tab]	Any String (<= 23 characters)	
CardRemovedStrID	27	Card Removed String	[tab]Card Removed[tab]	Any String (<= 23 characters)	
CardInStrID	28	Card Present String	[tab]Card Present[tab]	Any String (<= 23 characters)	
CardOutStrID	29	Card Out String	[tab]Card Out[tab]	Any String (<= 23 characters)	
NoDataStrID	2A	No Data String	[tab]No Data[tab]	Any String (<= 23 characters)	
MediaDetectedStrID	2B	MediaDetected String	[tab]Media Detected[tab]	Any String (<= 23 characters)	
MagDataStrID	2C	Magnetic Data String	[tab]Magnetic Data[tab]	Any String (<= 23 characters)	
CardInSlotSt r	2D	Card In Slot String	[tab]Card In Slot[tab]	Any String (<= 23 characters)	
PartialInStr	2E	Incomplete Insertion String	[tab]Incomplete Insertion[tab]	Any String (<= 23 characters)	
ReaderOpt2ID	2F	Reader Option 2	40h	Any See Set Reader Option 2	

Function ID	Hex	Description	Default Setting	Description	
CustSetID	30	custom setting	0	0-none; bit2—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	
CustomSetID*	30	Custom settings	0	if bit 2 high include serial number when sending enhanced encrypted tracks	-
ReaderResetID*	32		None		-
Track1PrefixID	34	Track 1 Prefix	0	No prefix for track 1, 6 char max	
Track2PrefixID	35	Track 2 Prefix	0	No prefix for track 2, 6 char max	
Track3PrefixID	36	Track 3 Prefix	0	No prefix for track 3, 6 char max	
Track1SuffixID	37	Track 1 Suffix	0	No suffix for track 1, 6 char max	
Track2SuffixID	38	Track 2 Suffix	0	No suffix for track 2, 6 char max	
Track3SuffixID	39	Track 3 Suffix	0	No suffix for track 3, 6 char max	
KeyTypeID	3E	Key Type	0	0—data key; 'Z'—pin key	
EpVerID*	40		None		
BaudID	41	Baud Rate	'7' ('2'~'9')	38,400 bps, '2' is 1200, '5' is 9600 bps; '9' is 115.2 kbps	s
ParityID	43	Data Parity	'0' ('0'~'4')	None	s
HandID	44	Hand Shake	'0' ('0'~'1')	Software (Xon/Xoff) hand shake	s
StopID	45	Stop Bit	'0' ('0'~'1')	1-bit (1 or 2 stop bits)	s
XOnID	47	XOn Character	DC1	0x11 as XOn (0x11 or 0x13)	s
XOffID	48	XOff Character	DC3	0x13 as XOff (0x11 or 0x13)	s
PrePANID	49	lead PAN to not mask	4 (0-6)	# leading PAN digits to display	
PostPANID	4A	trail PAN to not mask	4 (0-4)	# of trailing PAN digits to display	

Function ID	Hex	Description	Default Setting	Description	
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	
~~CapsCaseID*~~	~~51~~		~~None~~		
~~DataSeqID*~~	~~52~~		~~None~~		
~~StartCharID*~~	~~53~~		~~None~~		
SessionID	54	8 byte hex not stored in EEPROM	None	always init to all 'FF'	
Mod10ID	55	include mod10 check digit	'0' '0'-'2'	don't include mod10, '1' display mod10, '2' display wrong mod10	
DesKeyID	56	DES Key Value	0	internal use only	r n
AesKeyID	57	AES Key Value	0	internal use only	r n
KeyManageT ypeID	58	DUKPT	'1'('0'-'1')	'0' fixed key	
HashOptID,	5C		'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		'1' ('0'-'1')		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	

Function ID	Hex	Description	Default Setting	Description	
T1EndID	69	AnyTrack End Sentinel	'?'	'?' as End Sentinel—Used for all 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')	'1' send track LRC in secure mode; '0' don't send it	-
T28BStartID	72	JIS T12 SS/ES	None in KB mode otherwise 0x7F	none as Track 1 or 2 8 Bit Start Sentinel in keyboard mode else 0x7F	
T38BStartID	73	JIS T3 SS/ES	None in KB mode otherwise 0x7F	none as Track 3 8 Bit Start Sentinel in keyboard mode else 0x7F	
EquipFwID	77	feature option setting	0-7	Reader firmware configuration	n r
SyncCheckID	7B	check for track sync bits	'2' ('0'-2')	check leading & trailing sync bits on track data (if poorly encoded card)	
SecurityLeve lID	7E		'1' or '3'	'0' key exhausted; '1' non-encrypted; '1' key loaded non encrypted; '3' encrypted; '4'	n r
EncryptOptI D	84	encryption options	8 encrypt track 3 if card type 0; (0-FF)	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 pad according to PKCS#5	
EncryptStrID	85	encrypt structure	'0'	'0' original; '1' enhanced; if 85 is not an option then always enhanced struct	

Function ID	Hex	Description	Default Setting	Description	
MaskOptID	86	clear / mask data options	7 (0-F)	bit 0 send clear/mask trk1 bit 1 send clear/mask trk2 bit 2 send clear/mask trk3; bit 3 don't mask trk1 'B'	
Tk3ExpDatePosID	89	Trk3 expire date position	34	34- or 36 are the two normal values on30-39 allowed	
SpTimeOutID	A0	time until next Samsung Pay	50(*.128 sec) = 6.4 seconds	# of .128 sec ticks before next Samsung Pay transaction	
MasterModeID	AB		1' master key loading mode	Special for key loading	r
MKeyLoadedID	AC		0 (any)	Special for key loading	r n
RkiTimeOutID	AD	RKI timeout	2(2-255)	Remote Key Injection Timeout in minutes	
Equip2ID	AE	special settings	00 (any)	if bit4 high send serial number during enumeration	
CustSet2ID	AF		10H (any)	bit4=1 support encrypting Samsung (loop) reader transaction	
PrefixID	D2	Preamble	0	No Preamble, 15 char max	
PostfixID	D3	Postamble	0	No Postamble, 15 char max	

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

Note: not all function ID are present in different hardware version of the MIR, the last column above has some codes:
- '-' feature not currently supported; exists for compatibility
- 's' feature available on in the RS232 serial version of the reader 'u' feature available only in the USB version;
- 'k' feature available on 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.

15. APPENDIX B: STATUS/ERROR CODE TABLE

MIR Response Error Codes in TLP (ITP does not return separate error codes). The 8Axx was 69xx before MIR V2.90 because of a conflict with error codes returned by smart cards.

Code	Definition
2Axx	Command received correctly, but could not be completed
2A0D	DUKPT key exhausted
2A0E	DUKPT key blocks corrupt
8Axx or 69xx	Command not supported by reader
8A08 or 6908	invalid function ID
8A0E or 690E	"invalid command" response
8A11 or 6911	'Q' command length must be 1
8A12 or 6912	'P' command length must be 1
8A13 or 6913	2nd byte LED command must be '0'-'7','A'-'C'
8A15 or 6915	invalid erasing string
8A16 or 6916	'P' command must be 0x30 or 0x32
8A1D or 691D	command length wrong
8A1E or 691E	problem with config command
8A1F or 691F	host LED control not enabled
8A20 or 6920	reader not configured for buffered mode
8A21 or 6921	reader not configured for buff mode
8A22 or 6922	reader not configured for buffered mode
8A23 or 6923	reader not armed
8A23 or 6923	reader not armed for buff mode
8A24 or 6924	no MSR to decode
8A25 or 6924	illegal value for track selection
8A2D or 692D	invalid session ID length
8A2E or 692E	invalid SFR value
8A2F or 692F	invalid SFR selection
8A31 or 6931	invalid DUKPT activation challenge
9000	Operation completed successfully (all operations)
B0XX*	Card status (switch, no data, media detect…) change notification
C0XX*	Magnetic card data with envelope
8A32 or 6932	authentication failure
8A33 or 6933	load device key failure
8A34 or 6934	invalid deactivation command
8A35 or 6935	deactivation authorization failed
8A36 or 6936	invalid challenge command
8A37 or 6937	challenge command failure
8A38 or 6938	invalid DUKPT activation challenge
8A39 or 6939	warn: bad command ignored
8A3A or 693A	invalid configure string
8A3B or 693B	authentication failure
8A3C or 8A3C	load device key failure

8A3D or 693D	deactivation command disallowed
8A3E or 693E	invalid deactivation command length
8A3F or 693F	inform of failure to execute command
8A40 or 6940	required track(s) missing
8A41 or 6941	unsupported command
8A42 or 6942	required track(s) missing
8A50 or 6950	required track(s) missing in auto mode
8A51 or 6951	required track(s) missing in buffered mode

16. 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 char(s)	A5	\l_shift_mk	Set Shift Flag for following
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

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

ASCII Code	Control Code	Alt Code
SendOptionID	Bit 3: 0	Bit 3: 1
00:	Ctrl-2	Alt-000
01:	Ctrl-A	Alt-001
02:	Ctrl-B	Alt-002
03:	Ctrl-C	Alt-003

04:	Ctrl-D	Alt-004
05:	Ctrl-E	Alt-005
06:	Ctrl-F	Alt-006
07:	Ctrl-G	Alt-007
08:	BS	Alt-008
09:	Tab	Alt-009
0A:	Ctrl-J	Alt-010
0B:	Ctrl-K	Alt-011
0C:	Ctrl-L	Alt-012
0D:	Enter	Alt-013
0E:	Ctrl-N	Alt-014
0F:	Ctrl-O	Alt-015
10:	Ctrl-P	Alt-016
11:	Ctrl-Q	Alt-017
12:	Ctrl-R	Alt-018
13:	Ctrl-S	Alt-019
14:	Ctrl-T	Alt-020
15:	Ctrl-U	Alt-021
16:	Ctrl-V	Alt-022
17:	Ctrl-W	Alt-023
18:	Ctrl-X	Alt-024
19:	Ctrl-Y	Alt-025
1A:	Ctrl-Z	Alt-026
1B:	ESC	Alt-027
1C:	Ctrl-\	Alt-028
1D:	Ctrl-]	Alt-029
1E:	Ctrl-6	Alt-030
1F:	Ctrl--	Alt-031

17.   APPENDIX D Envelope Drawing

unit: mm, general tolerance: ±0.2mm