SecureHead™
Demo Program

SPI Interface

80101503-001 Rev. B
2 October 2019

ID TECH
10721 Walker Street, Cypress, CA 90630-4720
Tel: (714) 761-6368 Fax (714) 761-8880
www.idtechproducts.com support@idtechproducts.com

ID TECH
10721 Walker Street
Cypress, CA 90630
(714) 761-6368
www.idtechproducts.com

This document, as well as the hardware and software it describes, is furnished under license and may only be used in accordance with the terms of such license. The content of this paper is furnished for informational use, subject to change without notice, and not to be construed as a commitment by ID TECH. ID TECH assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

Except as permitted by such license, no part of this publication may be reproduced or transmitted by electronic, mechanical, recorded, or any other method, or translated into another language or language form without the express written consent of ID TECH. ID TECH is a registered trademark of International Technologies and Systems Corporation. ViVOpay and Value through Innovation are trademarks of International Technologies and Systems Corporation. Other trademarks are the property of the respective owner.

Warranty Disclaimer
The services and hardware are provided "as is" and "as-available," and the use of these services and hardware are at the user's own risk. ID TECH does not make, and hereby disclaims, any and all other excpress or implied warranties, including, but not limited to warranties of merchantability, title, fitness for a particular purpose, and any warranties arising from any course of dealing, usage, or trade practice. ID TECH does not warrant that the services or hardware will be uninterrupted, error-free, or completely secure.

FCC warning statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The user manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: The grantee is not responsible for any changes or modifications not expressly approved by the party responsible for compliance. Such modifications could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter and must be installed to provide a separation distance of at least 20cm from all persons.

Cautions and Warnings

⚠	**Caution**: The ViVOpay Vendi should be mounted 1-2 feet away from other ViVOpay Vendi. Can be adjusted based on lane setup.
⚠	**Caution**: Danger of Explosion if battery is incorrectly replaced. Replace only with same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.
⚡	**Warning**: Avoid close proximity to radio transmitters which may reduce the ability of the reader.

Table of Contents

1. Introduction

SPI SecureHead Demo Program is used to demonstrate the functionality of encrypted MSR. It decrypts data by sending a command to MSR and loading key to MSR.

There are 4 modes available for the SPI reader:

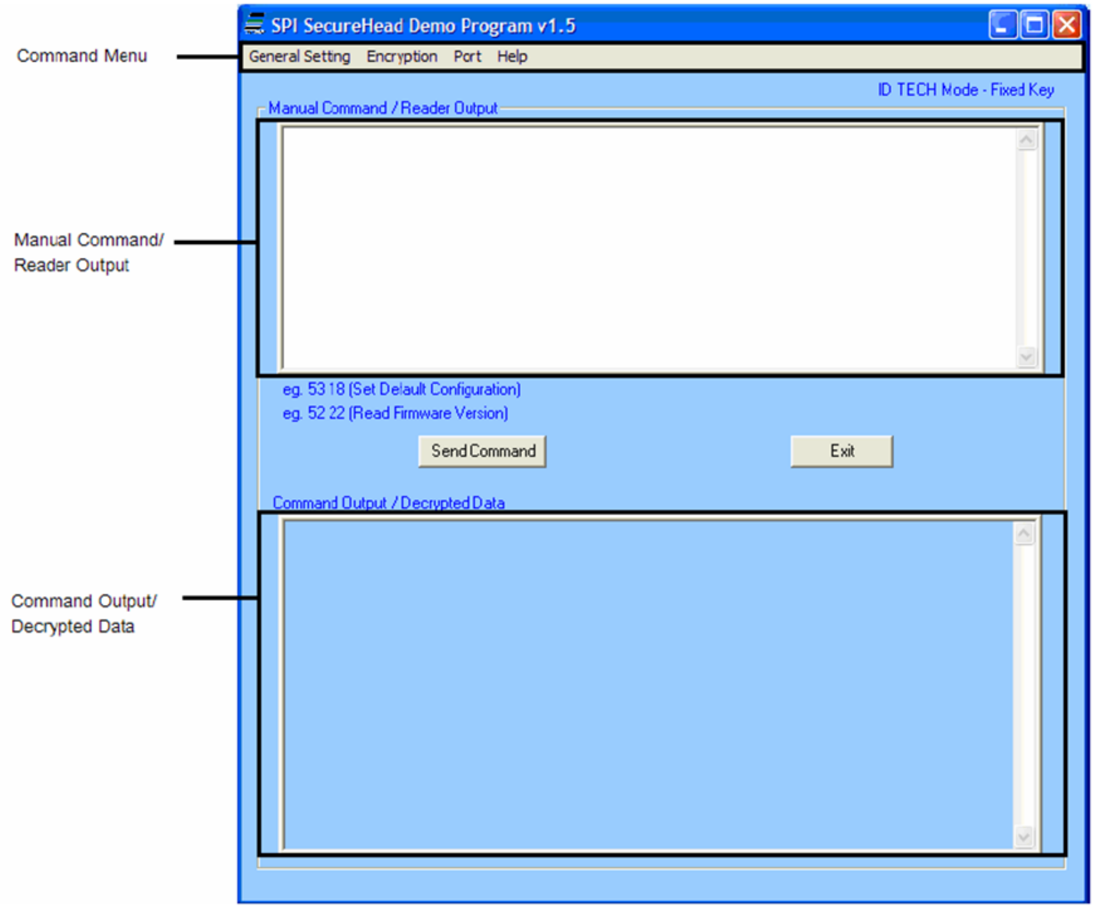
- ID TECH Mode – Fixed Key
- ID TECH Mode – DUKPT Key
- Other Mode – Fixed Key
- Non-encrypted Mode

All four modes have different data output for the format key management scheme.

2. Overview

The SPI SecureHead Demo Program consists of 3 major sections:

- **Command Menu**
- **Manual Command** and **Reader Output**
- **Command Output** and **Decrypted Data**


Command Menu
Manual Command/ Reader Output
Command Output/ Decrypted Data
SPI SecureHead Demo Program v1.5
General Setting
Encryption
Port
Help
ID TECH Mode - Fixed Key
Manual Command / Reader Output
Send Command
Exit
Command Output / Decrypted Data

eg. 53 18 (Set Default Configuration)
eg. 52 22 (Read Firmware Version)

3. Command Menu

The command menu provides MSR and encryption related settings. The settings available vary between different reader modes.

3.1. General Setting Menu

The common settings available to all modes:

Set Default Configuration

Set the reader to default settings:

MSR: Enable:

- Terminator Setting: CR
- Preamble Setting: None
- Postamble Setting: None
- Track Selected Setting: Any Track
- Sentinel and T2 Account No: Send Sentinels and all T2 data
- Data Edit Setting: Disabled
- Track 1/2/3 Prefix: None
- Track 1/2/3 Suffix: None

Note: These features are applicable in non-encrypted mode only.

Read Current Configuration

The reader outputs current configuration settings.

Read Firmware Version

The reader returns the current firmware version.

MSR Enable

This command enables the MSR.

MSR Disable

This command disables the MSR. The reader does not send out data after a card swipe when the MSR is disabled.

Clear Reader Output

This command clears the reader output text field.

ID TECH has several decoding options for non-encrypted mode:

- ID TECH Raw Format
- ID TECH Decoded – both directions

- ID TECH Decoded – forward direction only
- ID TECH Decoded – backward direction only

When decoded format is selected, the reader can be configured to send out data in either raw or decoded format from a card swipe.

3.2. Encryption Menu

This menu is to set security related features. See the encryption settings in each reader mode.

ID TECH Mode: Fixed Key

- TDES
- AES
- Get encrypted challenge
- Send authentication data
- Load key

ID TECH Mode: DUKPT Key

- TDES
- AES
- Get security level
- Get KSN

Other Mode: Fixed Key

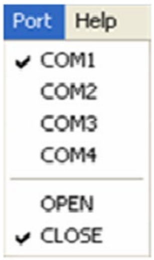
- Get encrypted challenge
- Send authentication data
- Load key
- Enable encryption
- Disable encryption

The ID TECH output format default is TDES, but the user can select TDES or AES as the encryption algorithm. For **Other** mode, the encryption algorithm is always TDES.

Use the **Get Security Level** command to verify the reader's security level under DUKPT key management. The security level is the 5th byte from the left of the **Command Response** in hex. For example, security level 3 has a command response of OUT: `06 02 7E 01 33 03 4D`.

3.3. COM Port Selection

By default, COM1 is used when the demo software is opened. If the user prefers to communicate with the reader through different serial port or close the port, the port setting can be modified in **Port Setting** menu.



3.3.1. Help

The **Help** menu displays the demo program's version information.

3.3.2. Manual Command and Reader output

In this field, a user can manually type commands to send to the reader. Click **Send Command** to send the command to the reader. The **Command** structure is described in next section.

3.3.3. Manual Command Format

Manually input commands and send settings to the device.

Command Format:

```
<STX> <ATMEL Function ID> <Len1> <Len2> <STX> <Command_Data> <ETX>
<LRC><ETX> <LRC>
                                └      SPI Protocol       ┘
└                          ATMEL Protocol                        ┘
```

where: `<STX> = 02h, <ETX> = 03h, <ATMEL Function ID> = 54h,`
`<Len1> and <Len2> are two bytes length in SPI Protocol`
`<LRC> is one-byte XOR value calculated from <STX> to <ETX>.`

The user is only required to enter the **Command_Data** parameter; the demo software automatically encapsulates the **ATMEL Protocol** and **SPI Protocol**.

For example:

Read Firmware Version

1. Enter "`52 22`" in the **Manual Command / Reader Output** window
2. Click **Send Command**. The demo software will encapsulate **ATMEL Protocol's STX, ATMEL Function ID**, two bytes length, **SPI Protocol's** STX, ETX, LRC, and **ATMEL Protocol's ETX** and LRC.

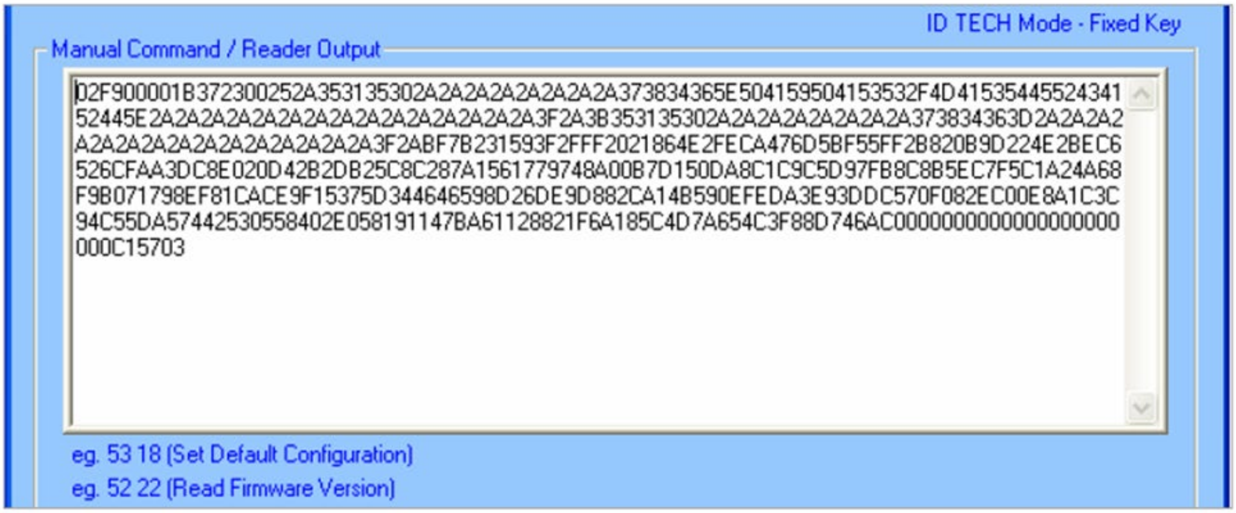
For example: `52 22 02 54 00 05 02 52 22 03 71 03 50`

For the complete command protocols, please see the SecureHead SPI manual.

3.3.4. Reader Output

This field displays the card data when a card is swiped. The field displays the unencrypted data when the reader is not encrypted. The field displays the encrypted card data when the reader is encrypted. The program shows the decrypted data in the lower field when the **Decrypt** button is selected.

Below is an example of the encrypted **MSR** data, sent by the reader in ID TECH **Fixed Key Mode**:



```
02F900001B372300252A353135302A2A2A2A2A2A2A2A373834365E504159504153532F4D41535445524341
52445E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B353135302A2A2A2A2A2A2A2A373834363D2A2A2A2
A2A2A2A2A2A2A2A2A2A2A2A3F2ABF7B231593F2FFF2021864E2FECA476D5BF55FF2B820B9D224E2BEC6
526CFAA3DC8E020D42B2DB25C8C287A1561779748A00B7D150DA8C1C9C5D97FB8C8B5EC7F5C1A24A68
F9B071798EF81CACE9F15375D344646598D26DE9D882CA14B590EFEDA3E93DDC570F082EC00E8A1C3C
94C55DA57442530558402E058191147BA61128821F6A185C4D7A654C3F88D746AC00000000000000000
000C15703
```

eg. 53 18 (Set Default Configuration)
eg. 52 22 (Read Firmware Version)

If no reader data is sent for more than 3 seconds, the current MagSwipe data in **Reader Output** window will be replaced by the next MagSwipe data. Otherwise, the new data will append after the current data.

To clear the reader output:

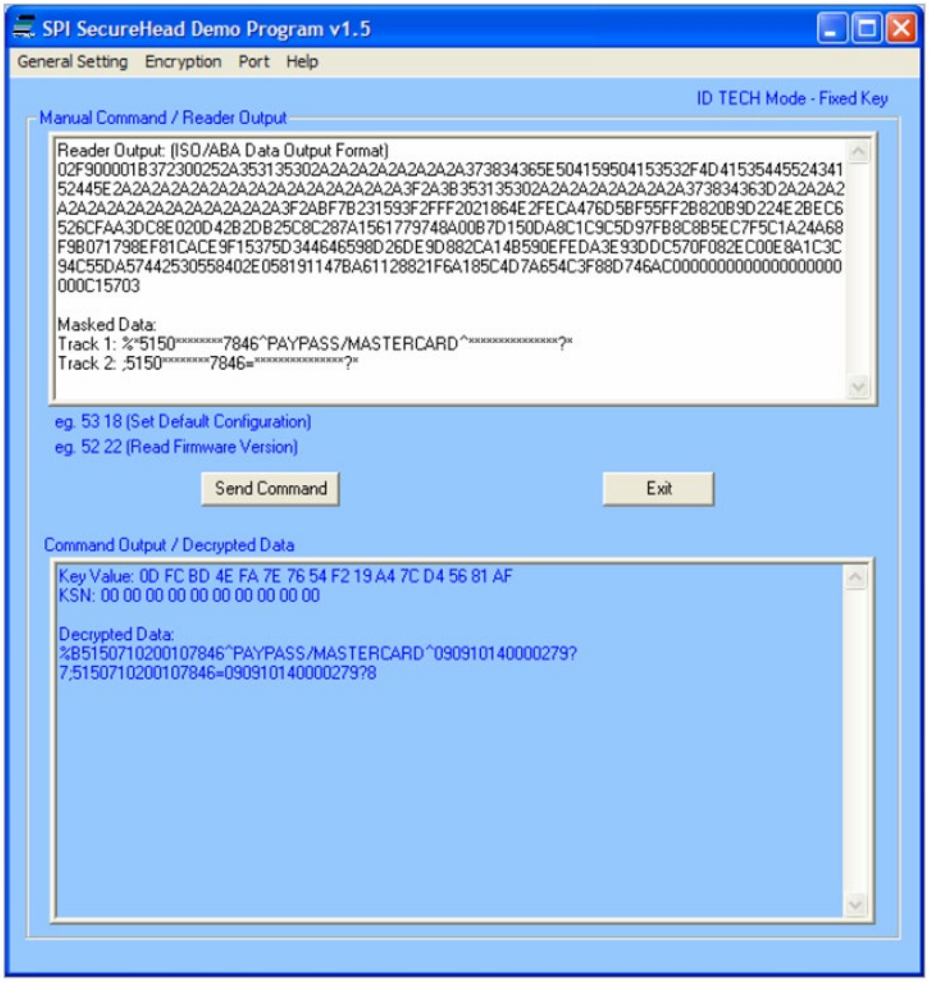
1. Navigate to **General Setting** menu
2. Select **Clear Reader Output**.

3.4. Command Output and Decrypted Data

The command sent to the reader and the command output in hex format are displayed in this section. For output command status, `06`h means command success and `15`h indicates a failure.

This section also displays decrypted MSR data with key value and KSN.

Below is an example result of decrypting an ISO standard bank card; top field displays both the reader output and the masked data, and the bottom field shows the decrypted card data.


SPI SecureHead Demo Program v1.5
General Setting
Encryption
Port
Help
ID TECH Mode - Fixed Key
Manual Command / Reader Output
Send Command
Exit
Command Output / Decrypted Data

```
Reader Output: (ISO/ABA Data Output Format)
02F900001B372300252A353135302A2A2A2A2A2A2A2A373834365E504159504153532F4D41535445524341
52445E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B353135302A2A2A2A2A2A2A2A373834363D2A2A2A2
A2A2A2A2A2A2A2A2A2A2A2A3F2ABF7B231593F2FFF2021864E2FECA476D5BF55FF2B820B9D224E2BEC6
526CFAA3DC8E020D42B2DB25C8C287A1561779748A00B7D150DA8C1C9C5D97FB8C8B5EC7F5C1A24A68
F9B071798EF81CACE9F15375D344646598D26DE9D882CA14B590EFEDA3E93DDC570F082EC00E8A1C3C
94C55DA57442530558402E058191147BA61128821F6A185C4D7A654C3F88D746AC0000000000000000000
000C15703

Masked Data:
Track 1: %*5150********7846^PAYPASS/MASTERCARD^***************?*
Track 2: ;5150********7846=***************?*
```

eg. 53 18 (Set Default Configuration)

eg. 52 22 (Read Firmware Version)

```
Key Value: 0D FC BD 4E FA 7E 76 54 F2 19 A4 7C D4 56 81 AF
KSN: 00 00 00 00 00 00 00 00 00 00

Decrypted Data:
%B5150710200107846^PAYPASS/MASTERCARD^090910140000279?
7;5150710200107846=090910140000279?8
```

4. Fixed Key Encryption

Fixed key encryption is available in ID TECH Mode or Other mode. In ID TECH Mode, the MSR data sent out can be configured as either ID TECH Decoded Format or ID TECH RAW Format. In Other mode, the MSR data sent out is always be in RAW format. The encryption algorithm will always be TDES.

4.1. Encryption Settings

An **Authentication Process** is required before a security related command is executed to ensure the device key used is correct. For example, **Authentication** is needed whenever the encryption is enabled, disabled, or the device key is changed. Until the device is restarted, this process will not be needed again.

Get Encrypt Challenge

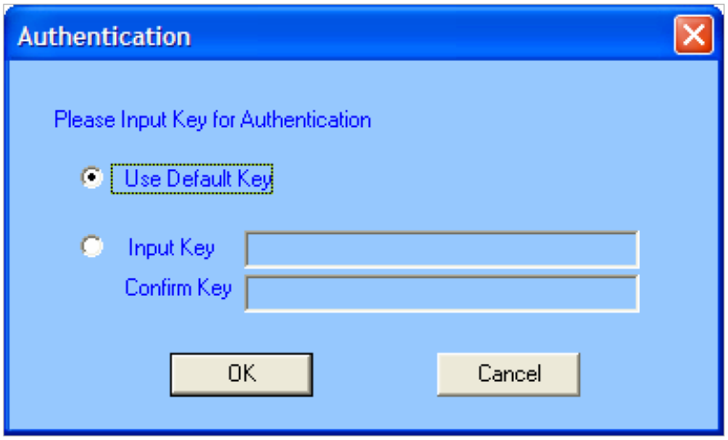
1. Navigate to the Encryption menu and select **Get Encrypt Challenge**.
2. **Get Encrypt Challenge** Command `02 54 00 05 02 52 74 03 27 03 50` is sent to the reader.
3. The reader responds with 8-byte encrypted data, `06 02 <Encrypted Data> 03 LRC`.

Send Authentication Data

The host must verify the device key used to pass the **Authentication Process**.

1. Input key. A window will display.
2. Input key for **Authentication** where prompted.
3. Enter the current encryption key to decrypt the 8-byte data
4. Select "Use Default key". (In case when the reader is using default key.)

The default key used in demo software decryption is 16 byte zero "`00000000000000000000000000000000`".



Authentication

Please Input Key for Authentication

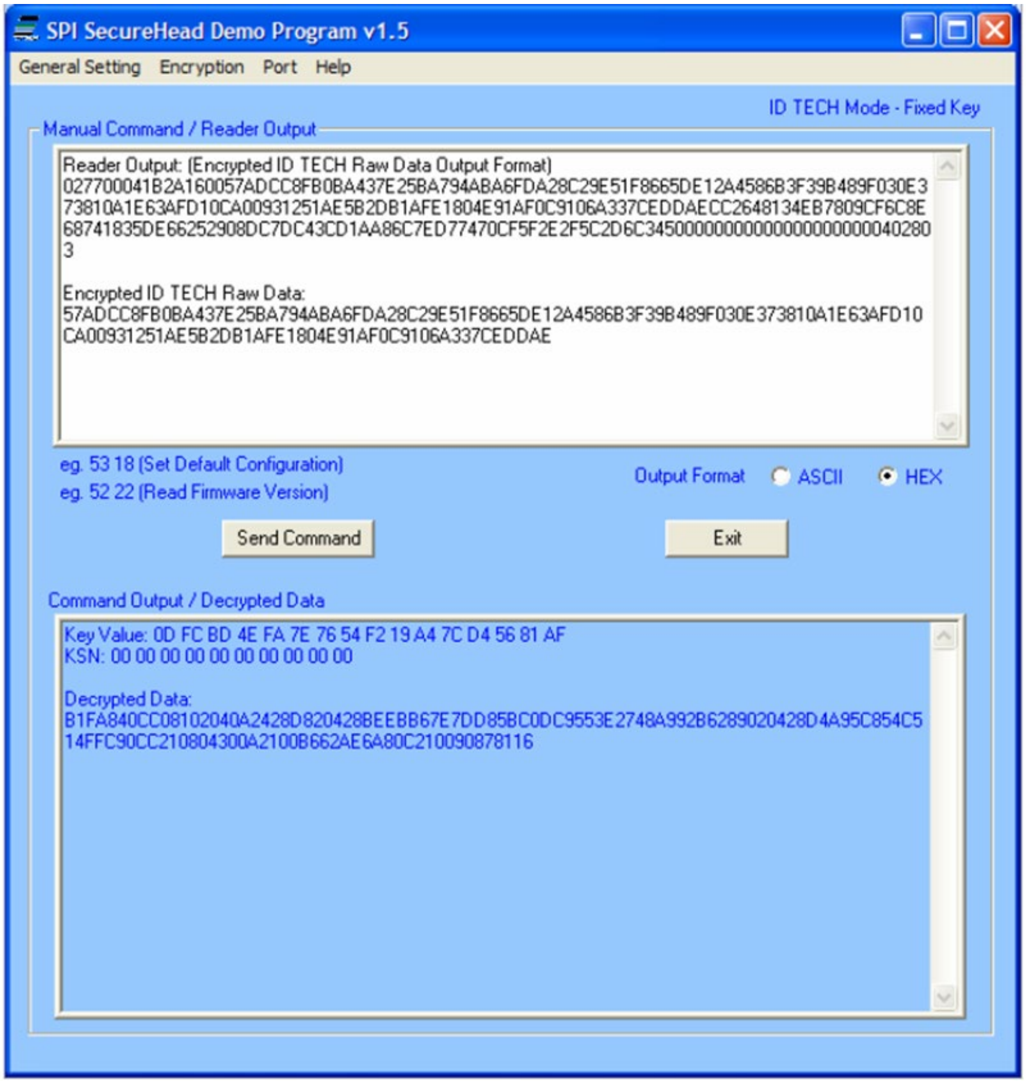
● Use Default Key

○ Input Key

Confirm Key

After inputting a new key or using the default key for decryption, the demo software will send an 8-byte decrypted data for **Authentication**. If the **Authentication** passes, the user can load a new device key for encryption.

Load Device Key
The load device key loads a 16-byte key to the device.


SPI SecureHead Demo Program v1.5
General Setting
Encryption
Port
Help
ID TECH Mode - Fixed Key
Manual Command / Reader Output
eg. 53 18 (Set Default Configuration)
eg. 52 22 (Read Firmware Version)
Output Format
○ ASCII
● HEX
Send Command
Exit
Command Output / Decrypted Data

```
Reader Output: (Encrypted ID TECH Raw Data Output Format)
027700041B2A160057ADCC8FB0BA437E25BA794ABA6FDA28C29E51F8665DE12A4586B3F39B489F030E3
73810A1E63AFD10CA00931251AE5B2DB1AFE1804E91AF0C9106A337CEDDAECC2648134EB7809CF6C8E
68741835DE66252908DC7DC43CD1AA86C7ED77470CF5F2E2F5C2D6C345000000000000000000000040280
3

Encrypted ID TECH Raw Data:
57ADCC8FB0BA437E25BA794ABA6FDA28C29E51F8665DE12A4586B3F39B489F030E373810A1E63AFD10
CA00931251AE5B2DB1AFE1804E91AF0C9106A337CEDDAE
```

```
Key Value: 0D FC BD 4E FA 7E 76 54 F2 19 A4 7C D4 56 81 AF
KSN: 00 00 00 00 00 00 00 00 00 00

Decrypted Data:
B1FA840CC08102040A2428D820428BEEBB67E7DD85BC0DC9553E2748A992B6289020428D4A95C854C5
14FFC90CC210804300A2100B662AE6A80C210090878116
```

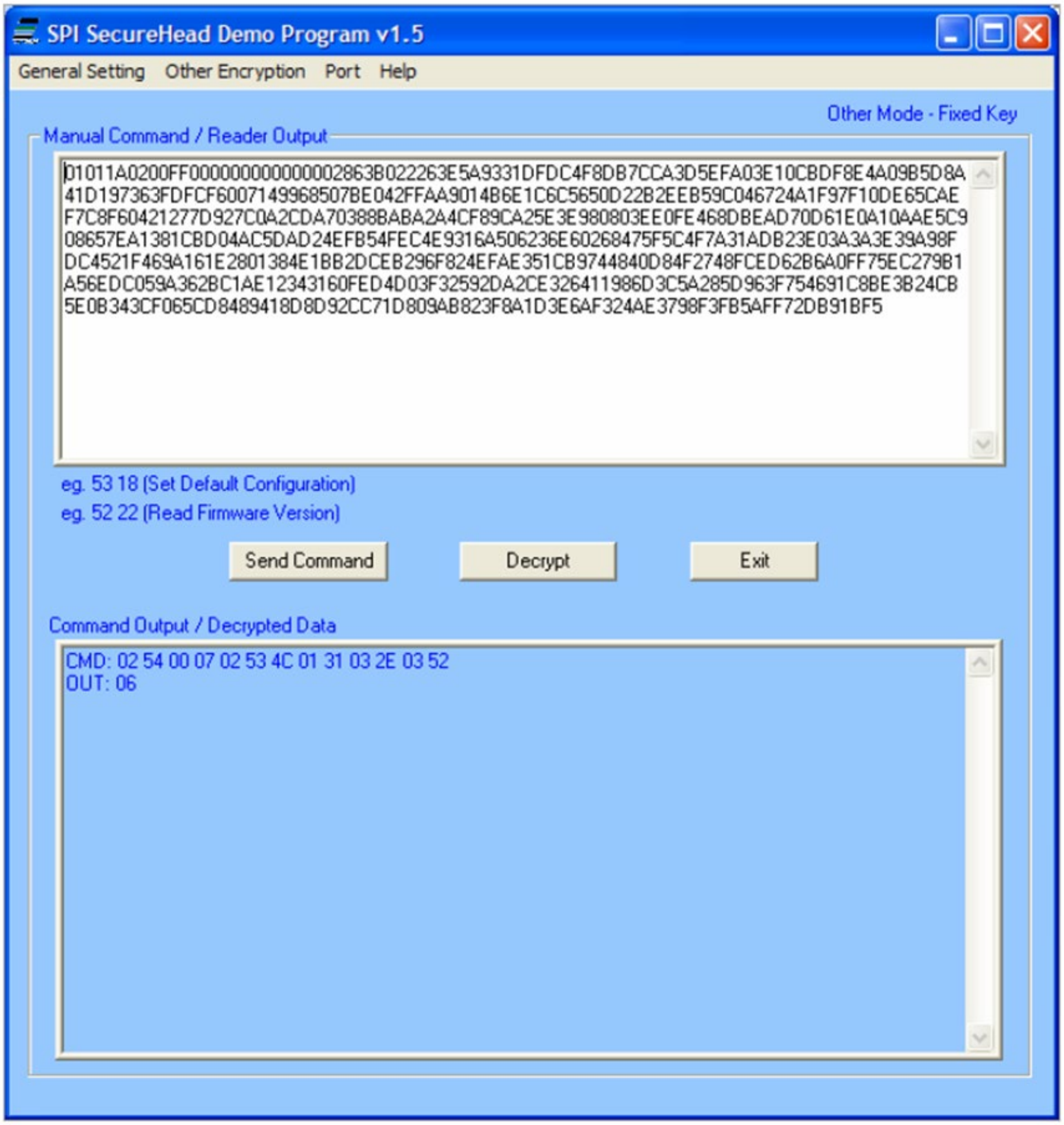
4.2. Other Mode Fixed Key Encryption

Follow the **Authentication** steps in 3.1 to change encryption setting in **Other** Mode.
Select **Encryption Enable Encryption** to enable encryption on the reader.
Go to **Encryption Disable Encryption** to disable encryption.

4.2.1. Data Decryption

1. Swipe a test card on the reader.

2. The reader will enter **Other Encryption Mode and** begin to decrypt the data mode.
3. The encrypted card data will appear in the **Reader Output** window.
4. Click “Decrypt” button to see the decrypted card data.

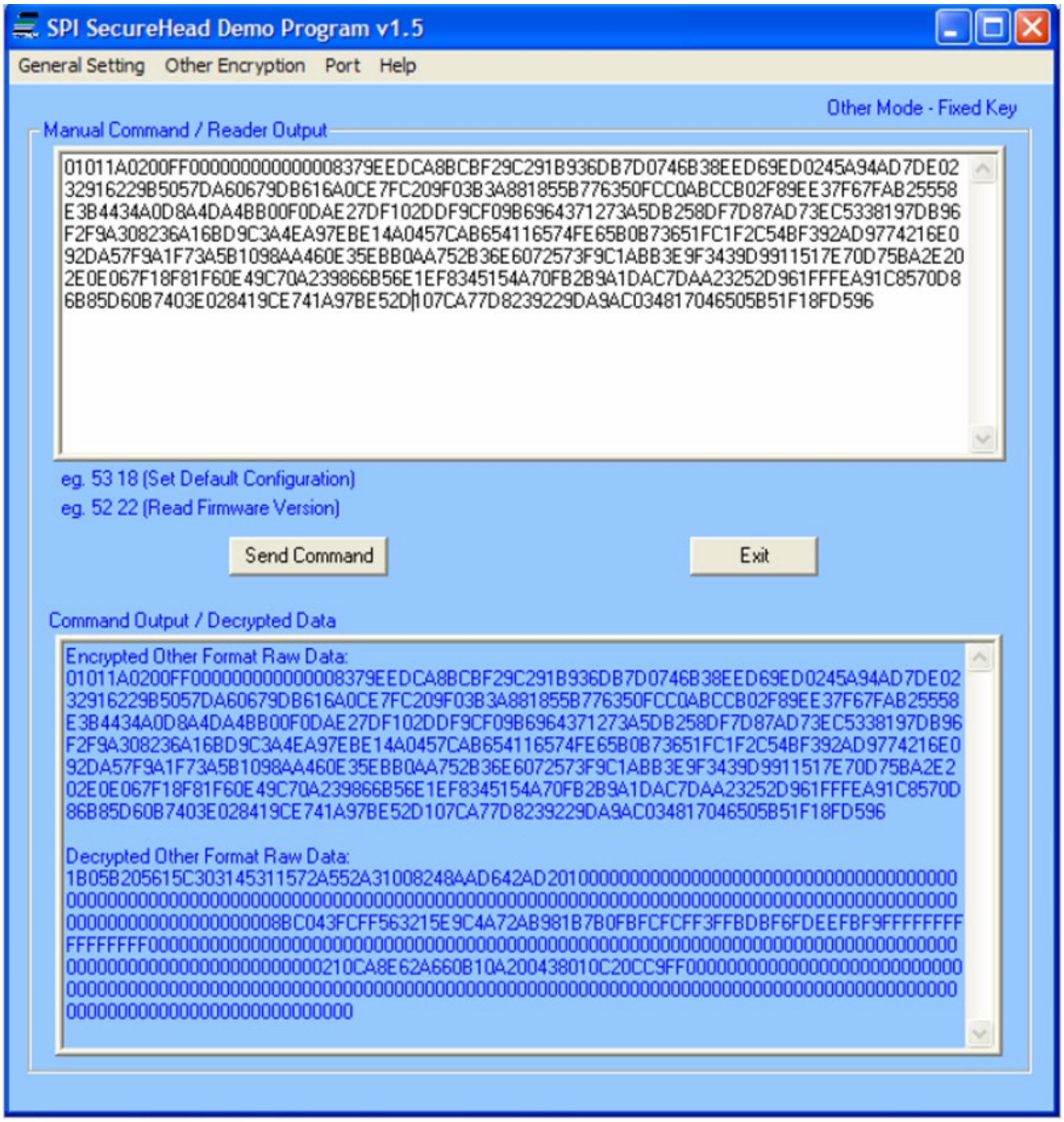

SPI SecureHead Demo Program v1.5
General Setting
Other Encryption
Port
Help
Other Mode - Fixed Key
Manual Command / Reader Output

```
01011A0200FF0000000000000002863B022263E5A9331DFDC4F8DB7CCA3D5EFA03E10CBDF8E4A09B5D8A
41D197363FDFCF6007149968507BE042FFAA9014B6E1C6C5650D22B2EEB59C046724A1F97F10DE65CAE
F7C8F60421277D927C0A2CDA70388BABA2A4CF89CA25E3E980803EE0FE468DBEAD70D61E0A10AAE5C9
08657EA1381CBD04AC5DAD24EFB54FEC4E9316A506236E60268475F5C4F7A31ADB23E03A3A3E39A98F
DC4521F469A161E2801384E1BB2DCEB296F824EFAE351CB9744840D84F2748FCED62B6A0FF75EC279B1
A56EDC059A362BC1AE12343160FED4D03F32592DA2CE326411986D3C5A285D963F754691C8BE3B24CB
5E0B343CF065CD8489418D8D92CC71D809AB823F8A1D3E6AF324AE3798F3FB5AFF72DB91BF5
```

eg. 53 18 (Set Default Configuration)
eg. 52 22 (Read Firmware Version)
Send Command
Decrypt
Exit
Command Output / Decrypted Data

```
CMD: 02 54 00 07 02 53 4C 01 31 03 2E 03 52
OUT: 06
```

Both the **Encrypted Other Format Raw Data** and **Decrypted Other Format Raw Data** are shown in the bottom text field.


SPI SecureHead Demo Program v1.5
General Setting
Other Encryption
Port
Help
Other Mode - Fixed Key
Manual Command / Reader Output

```
01011A0200FF00000000000000008379EEDCA8BCBF29C291B936DB7D0746B38EED69ED0245A94AD7DE02
32916229B5057DA60679DB616A0CE7FC209F03B3A881855B776350FCC0ABCCB02F89EE37F67FAB25558
E3B4434A0D8A4DA4BB00F0DAE27DF102DDF9CF09B6964371273A5DB258DF7D87AD73EC5338197DB96
F2F9A308236A16BD9C3A4EA97EBE14A0457CAB654116574FE65B0B73651FC1F2C54BF392AD9774216E0
92DA57F9A1F73A5B1098AA460E35EBB0AA752B36E6072573F9C1ABB3E9F3439D9911517E70D75BA2E20
2E0E067F18F81F60E49C70A239866B56E1EF8345154A70FB2B9A1DAC7DAA23252D961FFFEA91C8570D8
6B85D60B7403E028419CE741A97BE52D107CA77D8239229DA9AC034817046505B51F18FD596
```

eg. 53 18 (Set Default Configuration)

eg. 52 22 (Read Firmware Version)

```
Encrypted Other Format Raw Data:
01011A0200FF00000000000000008379EEDCA8BCBF29C291B936DB7D0746B38EED69ED0245A94AD7DE02
32916229B5057DA60679DB616A0CE7FC209F03B3A881855B776350FCC0ABCCB02F89EE37F67FAB25558
E3B4434A0D8A4DA4BB00F0DAE27DF102DDF9CF09B6964371273A5DB258DF7D87AD73EC5338197DB96
F2F9A308236A16BD9C3A4EA97EBE14A0457CAB654116574FE65B0B73651FC1F2C54BF392AD9774216E0
92DA57F9A1F73A5B1098AA460E35EBB0AA752B36E6072573F9C1ABB3E9F3439D9911517E70D75BA2E2
02E0E067F18F81F60E49C70A239866B56E1EF8345154A70FB2B9A1DAC7DAA23252D961FFFEA91C8570D
86B85D60B7403E028419CE741A97BE52D107CA77D8239229DA9AC034817046505B51F18FD596

Decrypted Other Format Raw Data:
1B05B205615C30314531157 2A552A31008248AAD642AD201000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000008BC043FCFF563215E9C4A72AB981B7B0FBFCFCFF3FFBDBF6FDEEFBF9FFFFFFFF
FFFFFFFF0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000210CA8E62A660B10A200438010C20CC9FF00000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000
```

5. IDTECH Mode- DUKPT

Before enabling ID TECH DUKPT mode, **Derivation Key** and KSN must be injected into the reader. The encryption algorithm can be either TDES or AES. The default is TDES.

5.1. Level 4 Activate Authentication Sequence

The security level changes from 3 to 4 when the device enters **Authentication Mode** successfully. To swipe a card the Level 4 **Authentication Requirement** has to be in **Authenticated Mode**.

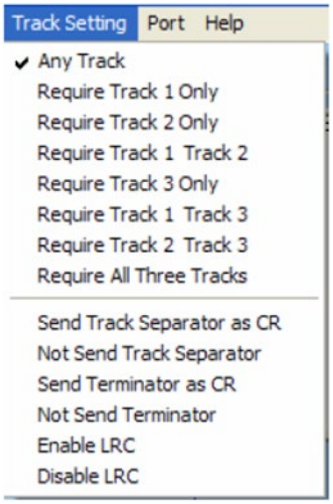
Click **ACT AUTH** (**Activate Authentication**) and **ACT RPLY** (**Activation Challenge Reply**) to enable security level 4.

1. Swipe a card.
2. The reader will enter **Authenticated Mode** and encrypted data will send.
3. Select "DEACT RPLY" to deactivates **Authentication Mode.** (Card swipes will no longer be accepted.)
4. The "Get Status" button gives the reader state and pre-condition.

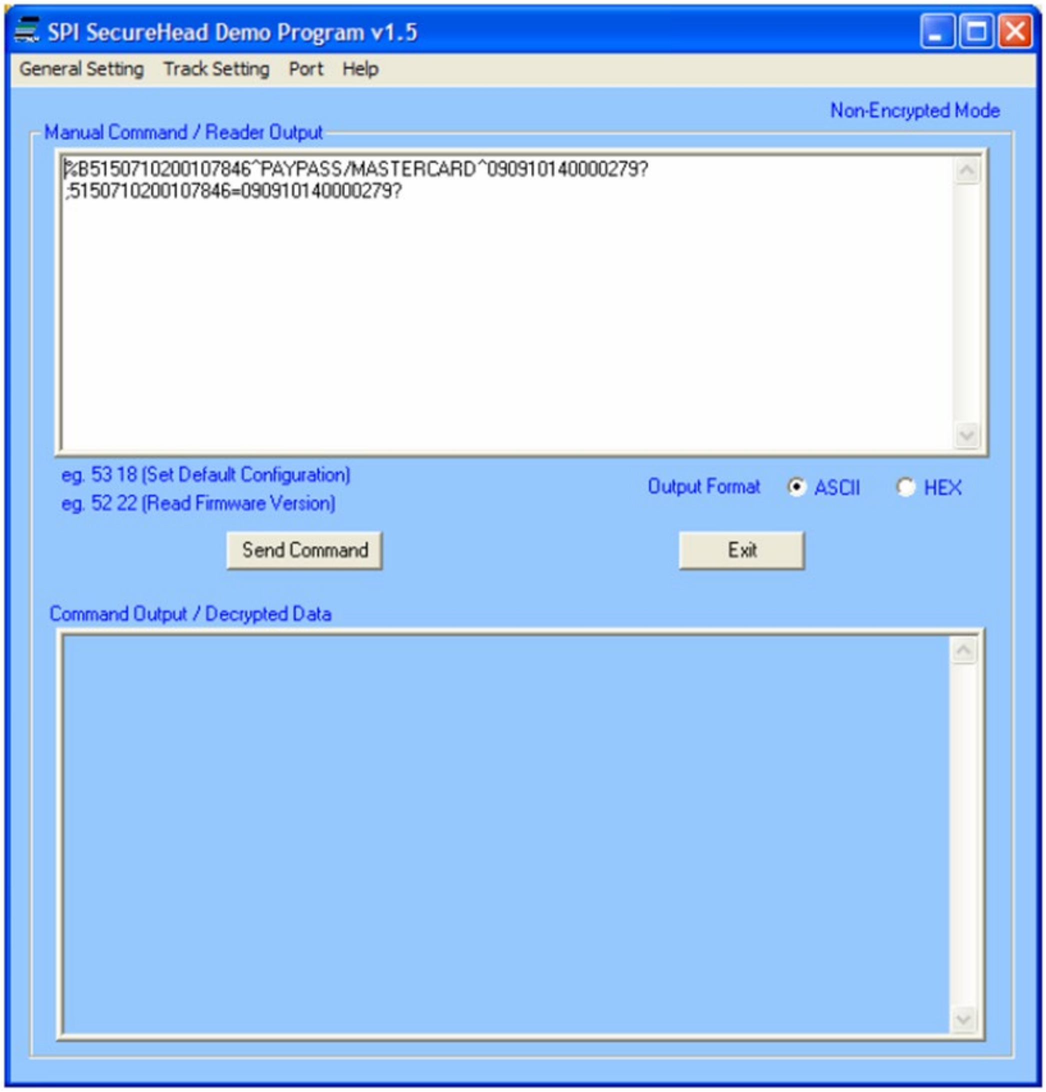
For the complete description of reader status code, please see the SPI SecureHead User Manual.

6. Non-Encrypt Mode

Track setting is available in non-encrypted mode:



When the reader is in non-encrypted mode, the card data will send in clear text, as shown below:



Non-Encrypted Mode

Manual Command / Reader Output

```
%B5150710200107846^PAYPASS/MASTERCARD^090910140000279?
;5150710200107846=090910140000279?
```

eg. 53 18 (Set Default Configuration)

eg. 52 22 (Read Firmware Version)

Output Format ● ASCII ○ HEX

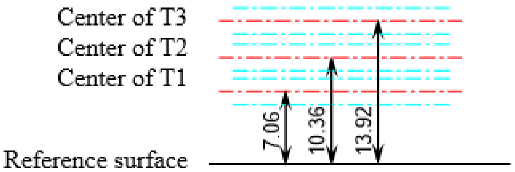
Command Output / Decrypted Data

7. Appendix A: Magnetic Heads Mechanical Design Guidelines

This installation guide is for installing ID TECH's magnetic heads with spring mounts.

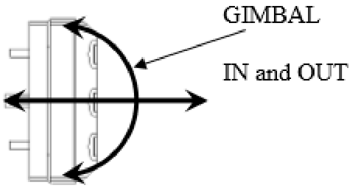
1. ISO 7810 and ISO 7811 standards define the specification for standard magnetic stripe cards. The location of each magnetic track's centerline is shown in below figure:

Note: The reference surface for the card is the edge of the card and it is the surface the card rides on when referring to the magnetic head.



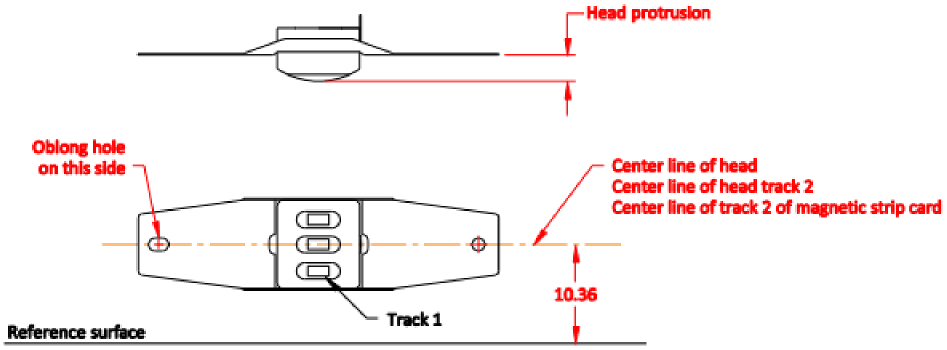
The magnetic head needs the freedom to gimbal, or rotate about Track 2's centerline, and move in and out to remain in contact with the card.

Below figure shows the rotational and linear movements that the head mounting must allow.



2. The head has to be mounted near the reference surface on which the card slides so that the magnetic tracks of the head are positioned at the same distance from the reference, the bottom of the slot, as the magnetic tracks on the card. Refer to the dimensions above.
3. A typical ID TECH magnetic head with 'spring' is shown below. The mounting holes are centered on Track 2's centerline in the spring and are used for mounting the head and positioning the track locations.

Note: the oblong hole in the spring must be oriented as shown in the drawing to locate tracks 1 through 3 properly.



The center line of head should be parallel to the reference surface.

4. The card thickness must be considered when designing the rail and head mounting. The distance between the crown of the head and the opposing slot wall should be a fraction of the minimum card thickness (0.010 inches or 0.25mm). This is so the magnetic head will always exert pressure on the card. The allows for proper contact of the head to stripe especially at high speeds and any less movement could result in an unreliable reading.

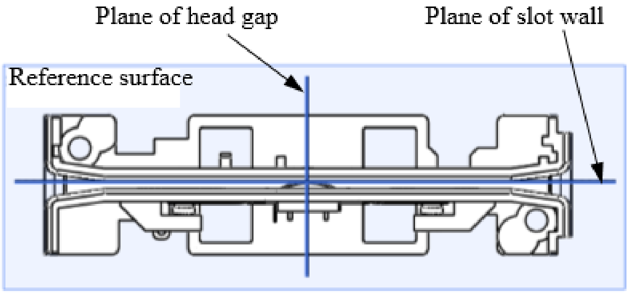
5. Standard card thickness is 0.76mm±10%. If standard cards are used, the rule should be the Apex of the head should be a maximum of 0.25mm from opposing card slot wall.
6. Adjust the distance the head is positioned from the opposing wall if a thicker or thinner card is use. Adjustment requires a unique rail design with either wider or narrower card slot width.

The minimum slot width should be maximum card thickness plus 0.15~0.30mm. The suggested minimum slot width is $1.03^{0.08}_{-0}$ when a standard card is issued.

7. The design should ensure there is no excessive force or deformation of head spring during or after the head is assembled to prevent permanent deformation of the head spring. The head spring must be mounted so that it is free to gimbal about the spring holes.

8. The bottom of the slot and the slot walls should not have any discontinuities and must instead be flat.

9. The portion of the slot wall, about 10mm on each side of the magnetic head's crown, should not have draft and must be perpendicular to the bottom of slot (reference surface). The slot width in the lead-in and lead-out area should be greater and must have gradual transition with no edges or angles to interfere with card swiping.



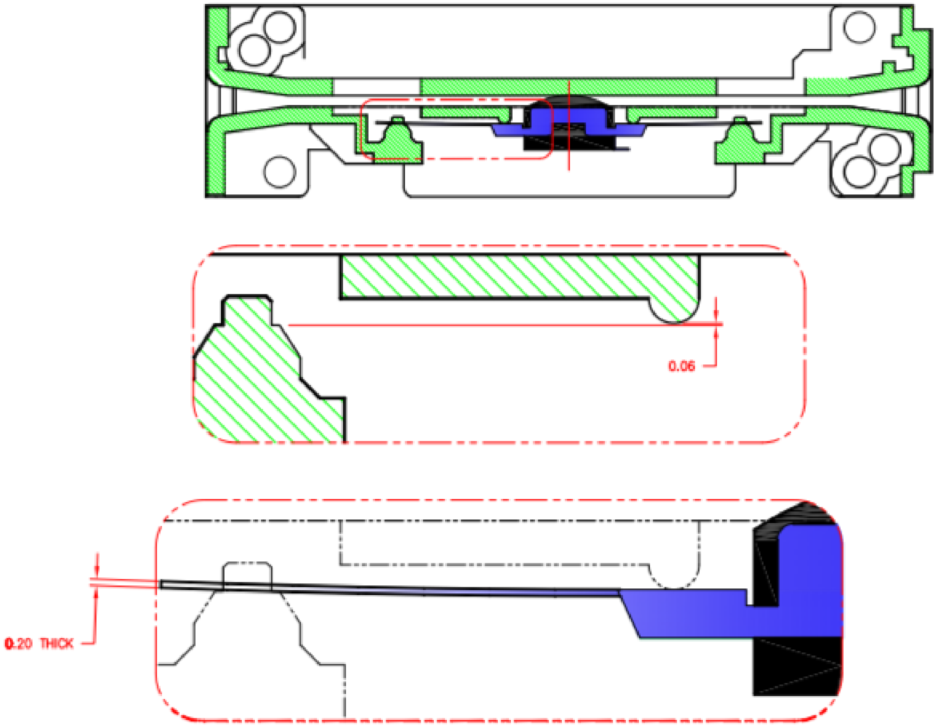
10. If the life of the reader is to be greater than 50,000 passes, the bottom of slot must embed a metal wear plate. Stainless steel is the metal of preference to avoid corrosion. The plastic material used for the slot needs to be significantly harder than the card material to ensure adequate rail life.

11. The head opening in the rail must allow room for maximum gimbal action. The back side (pin side) of magnetic head should have enough reserved space to prevent any interference during a swipe. The design must provide for a minimum of 1.25~1.52mm of space behind the head to allow for proper gimbal and head movement during card swiping.

12. When the head is installed into the rail, the spring holding the head should be slightly preloaded. Preloading the spring will ensure that the head has some stability at first card impact. This is especially important if the card is swiped at high speed. If the spring is not preloaded it will tend to vibrate when the card impacts the head and vibration causes the head to lose contact with the card.

13. ID TECH's solution to preloading the head spring is to add 2 symmetrical bumps, one on each side of the head (head window), molded into the rail (see drawing below). We recommend that the difference between the spring resting surfaces and the crown of the bumps is 0.06+/_0.03 mm. A head spring that is 0.20 mm thick will result in a 0.14+/- 0.03 mm bow. The bumps should by cylindrical and their crown parallel with the slot wall opposite to the head crown. This will ensure when the head is mounted into the rail, its crown will be parallel to the slot surface and will make good contact with the magnetic stripe on the card.

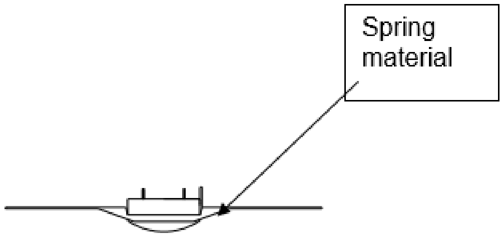
Please see the below drawing:



14. The length, width, and height of rail's slot will affect the stability of reading performance.
    a) The length of the slot is the maximum permitted by dimensional constraints. If possible, it should be 2 times the length of the card.
    b) The slot width is to be approximately 0.20 mm bigger than the maximum thickness of the card being swiped.
    c) The height of the slot should be as big as dimensional constraints allow but not extend over the embossing area of the card unless there is a provision (recess) in the rail wall design allowed.

The amount of head travel and head protrusion determines the clearance between the head and the wall of the rail window depends. The distance from the crown of the head to the surface of the spring. For a standard rail with $1.03^{0.08}_{-0}$ mm wide slot and a standard ID TECH head with 3.50 head protrusion minimum 1.25 mm clearance must be allowed on all sides of the head.

Note: Guideline does not apply when low profile heads are used. The window must allow clearance for the portion of the spring welded to the magnetic head as shown in figure below.



ID TECH can provide samples of a rail and magnetic head for design reference. Order these through your local sales representative using the following part numbers: 90mm rail 80006248-001 and Standard wing spring head 80027236-001.