IDTECH®
Value through Innovation

# User Manual

# UniMag
# Magnetic Stripe Reader
# For Mobile Devices

**80110505-001-G**
**07/27/2011**

# IDTECH UniMag User Manual

**Revision History**

| Revision | Description | Date |
|---|---|---|
| A | Initial Release | 12/10/2010 |
| B | Updated UniMag supported device | 12/22/2010 |
| C | Added encrypted output format and removed Android platform support | 02/25/2011 |
| D | Added Android platform support and updated demo software instructions | 03/21/2011 |
| E | Updated Android platform demo instruction<br>Revised encrypted output format | 06/10/2011 |
| F | Updated per Android SDK v1.15 | 07/08/2011 |
| G | Added information about XML configuration file and sampling/ decode bits. | 07/27/2011 |

**Table of Contents**

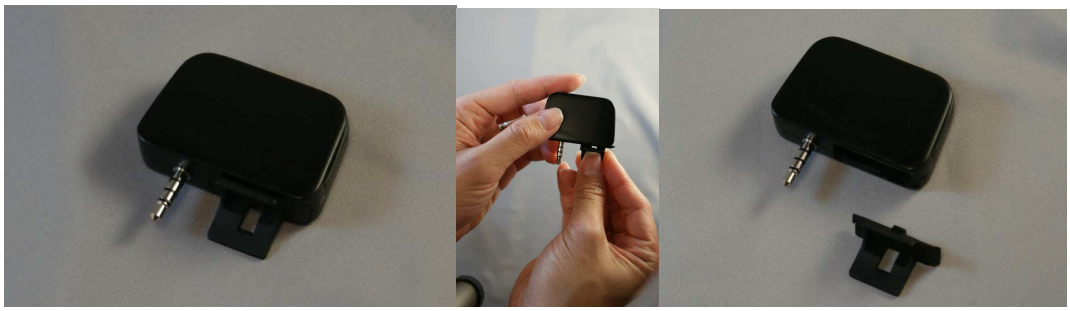
# 1. Introduction

The UniMag is a compact MagStripe reader designed for mobile devices. UniMag works on Apple iPod Touch, iPhone 3G/3GS, iPhone 4 and iPad and selected Android platform devices. A complete list of supported device can be found on the ID TECH website.

There are two UniMag versions available: one non-encrypted version and encrypted version. For more information on Apple and Android SDK, please see the SDK user manual for each operating system.

# 2. Installation

The UniMag is packaged with adaptor clips that conform to the shape of the mobile devices. When testing the UniMag on a device that does not have the appropriate clip, it is recommended to remove the clip before attaching the reader to the phone. Clip removal is easy with no additional tools required. Please see the below for instructions to remove the clip.

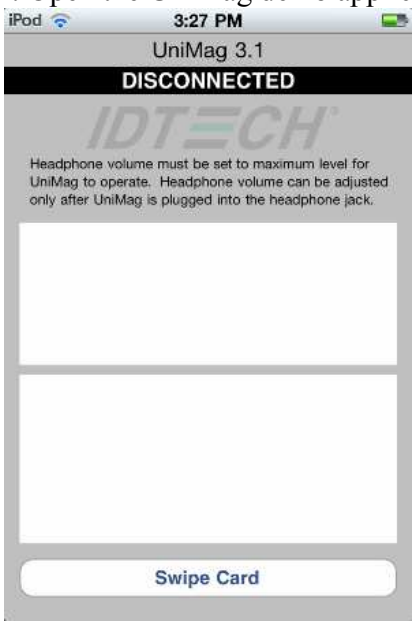


# 3. Using the Demo Software

## 3.1 Apple Platform

Please compile the demo application that comes with the SDK on Mac using Xcode. For detailed instruction, please reference to Mobile Reader SDK Compile Instruction.

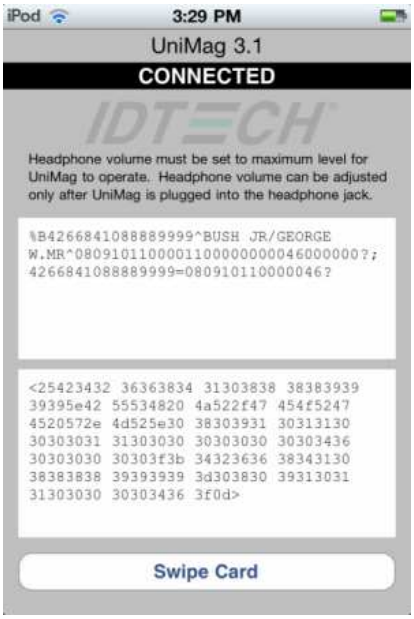
1. Open the UniMag demo application.




2. Plug the UniMag reader into the phone jack. <Power up UniMag> message will pop up, as shown below. Make sure the reader status changes to <CONNECTED> after that.


3. Click on the <SWIPE CARD> button, <Please swipe card > message box will pop up.


4. When the message box <Please swipe card> pops up, swipe a card. Card data will be displayed in the text box.



## 3.2 Android Platform

1. Install the UniMag SDK demo application on the phone

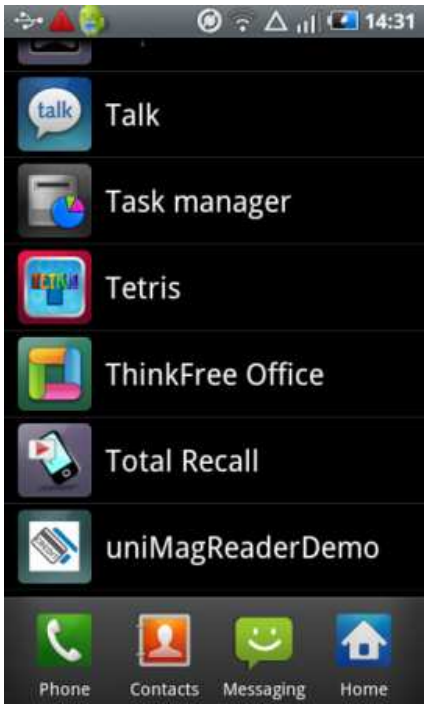
    a. Copy the **uniMagReaderDemo.apk** file to the root directory of SD card (or device memory if there is no SD card slot).

    **Note: SD card is required for current SDK structure.**

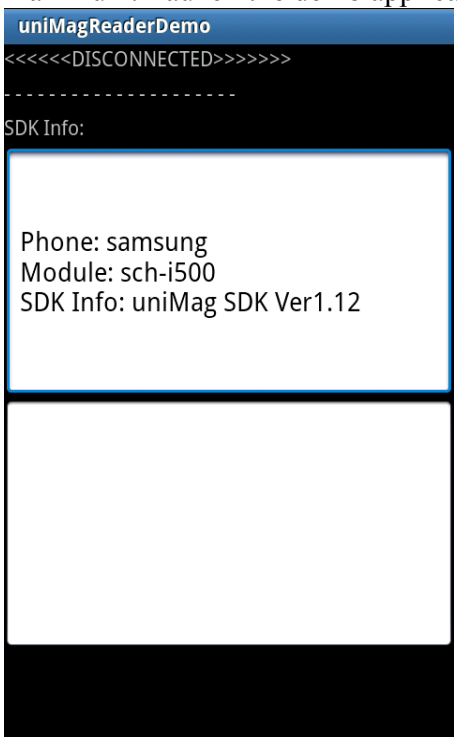
    b. Go to Android Market, search for "Apk Installer" or "Apk Manager" and then install the application.

    c. Launch ApkInstaller or Apk Manager. The application will list all APK files stored directly in the root directory of the memory card.

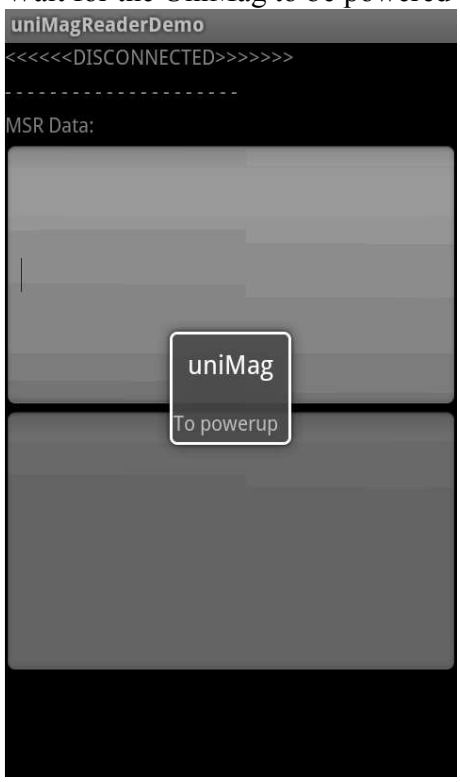

d. Click on the UniMag demo application to install.
e. UniMag demo application will be found under Applications after installed.

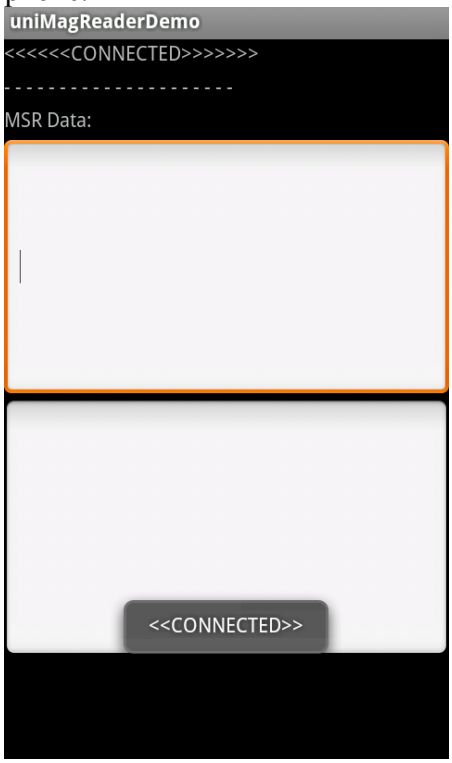
2. Plug the UniMag into the audio jack, and make sure the volume is adjusted to the maximum. Launch the demo application.



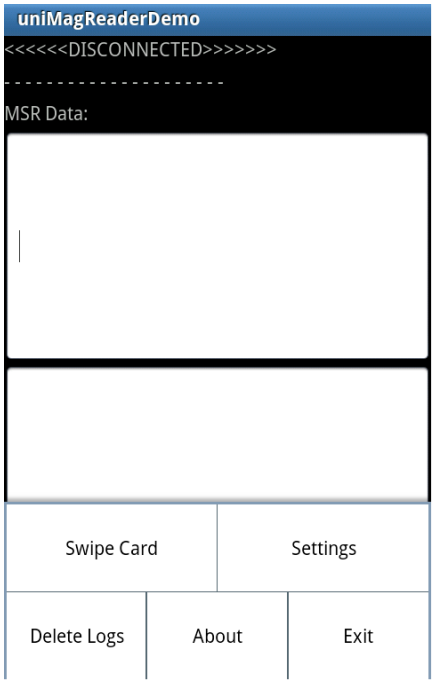

3. Wait for the UniMag to be powered up.



4. The media volume is adjusted to maximum when the UniMag is powered up. Check the device status and make sure the UniMag is properly connected to the phone.

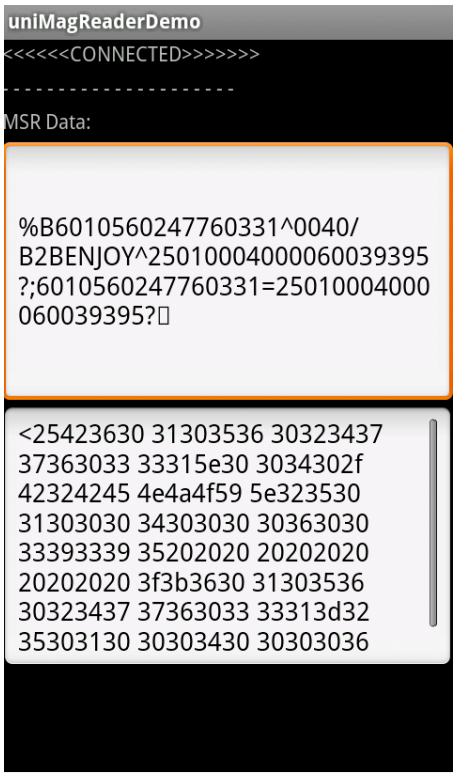



5. Click on the “menu” button and select “swipe card”

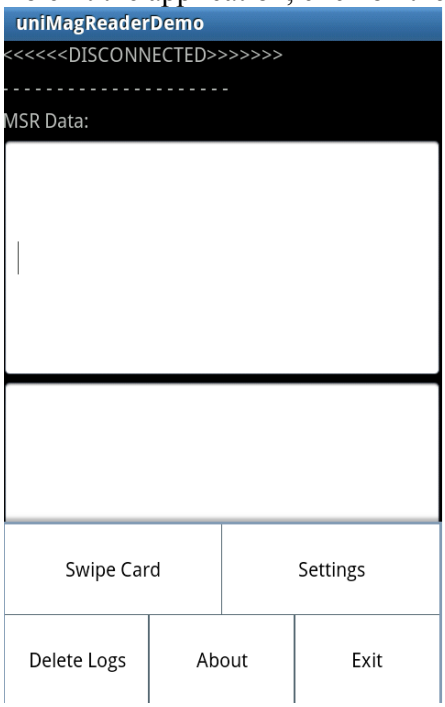


6. Wait for the card swipe icon to show up. Swipe the card


7. After the card swipe, the volume level will be restored. The card data will show up on the screen



8. To enable the event log, click on the menu button and select ‘Settings’. The log file will be saved in the SD Card root directory.
9. To delete the log, click on the menu button and select ‘Delete Logs’.
10. To exit the application, click on the menu button and select “Exit”




11. The Demo application uses the default XML configuration file located in the res/raw folder of the SDK. You can get the updated XML file from the website ‘www.idtechproducts.com’ and set updated the XML file as your default XML file.

# 4. Data Output Format

## 4.1 UniMag Unencrypted Data Output Format

Track 1: <Start Sentinel 1><$T_1$ Data><End Sentinel><Track Separator>
Track 2: <Start Sentinel 2><$T_2$ Data><End Sentinel><Track Separator>
Track 3: <Start Sentinel 3><$T_3$ Data><End Sentinel><Terminator>

where: Start Sentinel 1 = %
Start Sentinel 2 = ;
Start Sentinel 3 = ; for ISO, % for AAMVA
End Sentinel all tracks = ?

Start or End Sentinel: Characters in encoding format which come before the first data character (start) and after the last data character (end), indicating the beginning and end, respectively, of data.

Track Separator: A designated character which separates data tracks. The default character is CR (Carriage Return).

Terminator: A designated character which comes at the end of the last track of data, to separate card reads. The default character is CR (Carriage Return).

For example:

%B4352378366824999^TFSTEST /THIRTYONE
^0510201100008820088200000?<CR>;4352378366824999=051020110000882?<CR>

## 4.2 UniMag Encrypted Data Output Format

UniMag uses ID TECH enhanced data encryption format. In this format, all tracks of the data are encrypted.

Output Format:

<STX><LenL><LenH><Card Data><CheckLRC><CheckSum><ETX>

| | |
|---|---|
| 0 | STX |
| 1 | Data Length low byte |
| 2 | Data Length high byte |
| 3 | Card Encode Type[1] |
| 4 | Track 1-3 Status[2] |
| 5 | T1 data length |

| | |
|---|---|
| 6 | T2 data length |
| 7 | T3 data length |
| 8 | Clear/mask data sent status[3] |
| 9 | Encrypted/Hash data sent status [4] |
| 10 | T1 clear/mask data |
| | T2 clear/mask data |
| | T3 clear/mask data |
| | T1 encrypted data |
| | T2 encrypted data |
| | T3 encrypted data |
| | Session ID (8 bytes) (Security level 4 only, not used here) |
| | T1 hashed (20 bytes each) (if encrypted and hash tk1 allowed) |
| | T2 hashed (20 bytes each) (if encrypted and hash tk2 allowed) |
| | T3 hashed (20 bytes each) (if encrypted and hash tk3 allowed) |
| | KSN (10 bytes) |
| | CheckLRC |
| | CheckSum |
| | ETX |

Where <STX> = 02h, <ETX> = 03h

**Note 1 : Card Encode Type**

Card Type will be 8x for enhanced encryption format and 0x for original encryption format

| Value | Encode Type Description |
|---|---|
| 00h / 80h | ISO/ABA format |
| 01h / 81h | AAMVA format |
| 03h / 83h | Other |
| 04h / 84h | Raw; un-decoded format |

For Type 04 or 84 Raw data format, all tracks are encrypted and no mask data is sent. No track indicator ‘01’, ‘02’ or ‘03’ in front of each track. Track indicator ‘01’,’02’ and ‘03’ will still exist for non-encrypted mode.

**Note 2: Track 1-3 status byte**

Field 4:
Bit 0: 1— track 1 decoded data present
Bit 1: 1— track 2 decoded data present
Bit 2: 1— track 3 decoded data present
Bit 3: 1— track 1 sampling data present
Bit 4: 1— track 2 sampling data present
Bit 5: 1— track 3 sampling data present
Bit 6, 7 — Reserved for future use

Decoded bit: 1 for decode success or no sampling data; 0 for decode error (with sampled data but failed to decode)
Sampling bit: 1 for sample data exist; 0 for sample data does not exist

**Note 3: Clear/mask data sent status**

Field 8 (Clear/mask data sent status) and field 9 (Encrypted/Hash data sent status) will be sent out in enhanced encryption format, which is the default iMag/ iMag Pro output format.

Field 8: Clear/masked data sent status byte:
Bit 0: 1 —track 1 clear/mask data present
Bit 1: 1— track 2 clear/mask data present
Bit 2: 1— track 3 clear/mask data present
Bit 3: 0— reserved for future use
Bit 4: 0— reserved for future use
Bit 5: 0— reserved for future use

**Note 4: Encrypted/Hash data sent status**

Field 9: Encrypted data sent status
Bit 0: 1— track 1 encrypted data present
Bit 1: 1— track 2 encrypted data present
Bit 2: 1— track 3 encrypted data present
Bit 3: 1— track 1 hash data present
Bit 4: 1— track 2 hash data present
Bit 5: 1— track 3 hash data present
Bit 6: 1—session ID present
Bit 7: 1—KSN present

General concept for each track:
1. If encrypted, no clear data will be sent
2. Clear data always sent if no encrypted data
3. If not encrypted, hash will never be send

**Example:**

5559695555695555AAA6595595A699A555A9AAA596659995A655A595A695A695999599
9599959995999599599959995A965A965A965A9666A965596666665A65955955659966595
9AA656A656665AA6659656A65665955666A59A965A6665966A9599959995999599599959995
9995999599959995999599599599599599599599599599599599599599599599599599599959
9959995999599599599599599995AAA59995A9A5A655A595A695A695999599599995999599
9599959995995A965A965A965A965AA659995999599959995999599599599599599599599995
9995999599599599959995AAA599969A66AA6669A595565A65A666A96699665A9566595AA
5AAA9A59666966666565A65A66955966A99995969A995A55A5966969A65A655A695A5666
6569AAA669659AA969666A9A69995699A966599656AA99AAAA6AA69655A65A59A5A9
9556A66A6A6A65695AA695669A95956AA56A959555A959AA55A99A666AA9669A5565
A956A566A6A9AA69596655596A69959A99659996995656666 55AA955556A55956AAA9569
966599A99995A65AA69A5A699A9956559AA565A6659A596A6A56A5695959AAA9A5955
96A569969A9555956999966696565A9A6666696A9A55596A5999AAA5696AA5A699A6559
59A599595556699A6595996A5965569A59A69996669565A9A6656556669A65AA5A55695
A6A6A5A65A5AA66555A5699AA656A66A699AA596AA55695959956996A6A5659696555
56569A9999559655A9965695965A9AA559996659A9A6A66669AA95A969A9966666659AA
555A56659556AA55565A95AA559569A69A69959996595AA5959666AA6A569966569A69
AAA9AA5956AAA5A569596A966A5959A9666659AAA6A5A555AA65556A965655A5666
66965656A965565A6A99A999A6665965655666696A999956A66655965965996A66966AA9
A596A66A6695995A65569599A59595AA6966A956A69A6AA9A665A65655966A5AAA969
6A6AAA59565695AAAAA69A6AA56565A9A69595969A5659596959996A65A666655666A
A9A599AA56569966669695AA5559A5995A56699595956956A556666AA556A5A959A955
AA6A59A5A955AA5A9A9A66969599695665A999999A9A566959969665965556569655555
55555555555555A6A699699555A

This format needs to be “converted” to a “packed” output format as the followings:

packed uniMag output example:

029801803F48236B03BF252A343236362A2A2A2A2A2A2A393939395E42555348204A5
22F47454F52474520572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A
2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B343236362A2A2A2A2A2A2A2A393939393D2A2A
2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A6D7D5B204D3579694E148F3FB2565544D35825
EA89BA30C966D34363151BF592F995EDA86B94A47EBFDF6434CB3A075DDD18F616E2
1F1E2038BC3AD5F96C1387177BD89409DA2E92A684543E007087F8694AEA8D3DB36BA
10BC4D4B2771C622FEC8271A6E021AA5644ED559EC09CABF19F36B422CA2016B48A7
241B2DA9584ED4415B4F30637734CF5031AF475DAF27C188A1A771264011BAA090E918
93BC2A52EDD56F8E6E9554BC0C5207C04E3C21B6DA2A48F2257DC6946DBFBC87F318
9E5C8B954BF7303D01E443155911E4137AEAD52441567AA1D50924A7597EC9D758A341
8AC88F65E1DB7ED4D10973F99DFC8463FF6DF113B6226C4898A9D355057ECAF11A559
8F02CA31688861C157C1CE2E0F72CE0F3BB598A614EAABB16299490119000000000376 9
A03

02—STX character
98—low byte of total length
01—high byte of total length

80—card type byte (interpretation new format ABA card)
3F—3 tracks of data all good
48—length of track 1
23—length of track 2
6B—length of track 3
03—tracks 1 and 2 have masked/clear data
BF—bit 7=1—KSN included
Bit 6=0—no Session ID included
Bit 5=1—track 3 hash data present
Bit 4=1—track 2 hash data present
Bit 3-1—track 1 hash data present
Bit 2=1—track 3 encrypted data present
Bit 1=1—track 2 encrypted data present
Bit 0=1—track 1 encrypted data present

Reader Output: (ISO/ABA New Data Output Format)
Clear/Masked Data:
Track 1: %*4266********9999^BUSH JR/GEORGE
W.MR^********************************?*
Track 2: ;4266********9999=****************?*

Key Value: 89 52 50 33 61 75 51 5C 41 20 CF 45 F4 1A BF 1C
KSN: 62 99 49 01 19 00 00 00 00 03

Decrypted Data:
%B4266841088889999^BUSH JR/GEORGE W.MR^0809101100001100000000046000000?!
;4266841088889999=0809101100000046?0
;3333333337676760707077676763333333337676760707077676763333333337676760707
07767676333333337676760707?2

Decrypted data including pad characters
2542343236363834313038383838393939395E42555348204A522F47454F52474520572E4D5
25E3038303931303131303030303131303030303030303030343630303030303F21
3B3432363638343130383838393939393D3038303931303131303030303034363F30000000
0000
3B3333333333333333333337363736373630373037303737363736373633333333333333333
3337363736373630373037303737363736373633333333333333333333337363736373630373037
730373736373637363333333333333333333337363736373630373037F320000000000