User Manual

UniMag II/ Shuttle

Magnetic Stripe Reader
For Mobile Devices

80110509-001-E
03/13/2013

IDTECH UniMag II/ Shuttle User Manual

Revision History

Revision	Description	Date
50	Initial draft	08/15/2011
51	Updated for UniMag II Android SDK v2.0	10/07/2011
52	Revised encrypted data output format and example	10/11/2011
53	Updated Android demo screenshots, revised data output format	10/21/2011
54	Added more information on the data output format	10/31/2011
A	Updated Apple demo screenshots. Initial release.	11/16/2011
A1	Updated for UniMag II Android SDK v2.4	12/05/2011
B	Updated for UniMag II Android SDK v2.6 and iOS SDK v5.11	04/23/2012
C	Updated for Android Demo v2.12 and iOS Demo v5.13	11/19/2012
D	Add iPhone5/iPadMini/iPad4/iPodTouch5 Update with new Android demo v3.0 new functions and IOS demo v7.1 Update with auto configuration features	12/26/2012
E	Updated for new Android demo v3.6 and IOS demo v7.2	03/13/2013

Table of Contents

1. Introduction

The UniMag II/ Shuttle is a compact MagStripe reader designed for mobile devices. UniMag II reads up to 2 tracks of MagStripe data with encryption capability. It works on Apple iPod Touch, iPhone 3G/3GS/4/4S/5, iPad1/2/3/4/Mini, and selected Android platform devices. A complete list of supported device can be found on the ID TECH website.

For more information on Apple and Android SDK, please see the SDK user manual for each operating system.

2. Using the Demo Software

The following screenshots might not reflect the latest demo software version, please contact ID TECH for the most up-to-date demo software.

2.1. Apple Platform

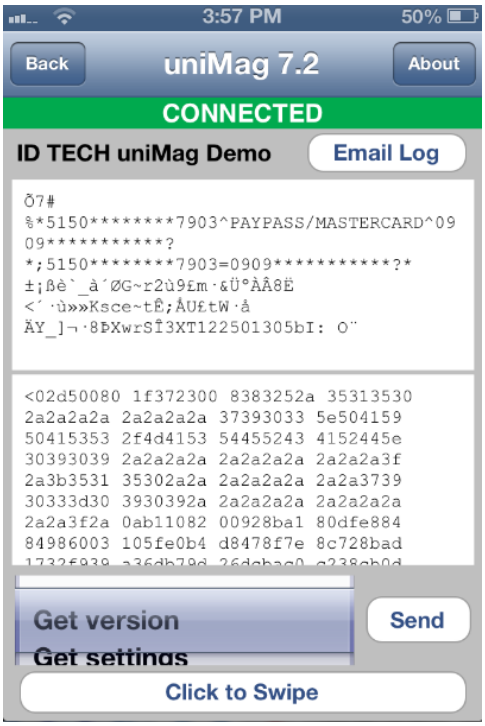
Please compile the demo application that comes with the SDK on Mac using Xcode. For detailed instruction, please reference to UniMag Apple iOS SDK User Manual.

1. Plug in Shuttle/Unimag II device and launch the UniMag II demo application, make sure the volume is set to the maximum and click on "OK".

2. <Connecting with uniMag> message will pop up, as shown below. Make sure the reader status changes to <CONNECTED> after that.

3. Click on the <Click to Swipe> 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.



2.2.Android Platform

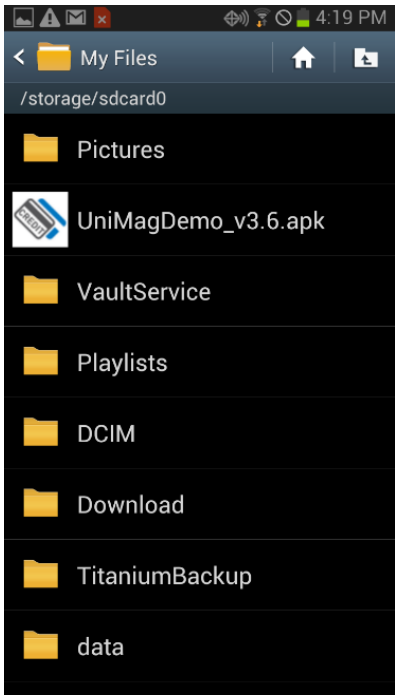
1. Install the UniMag II SDK demo application on the phone

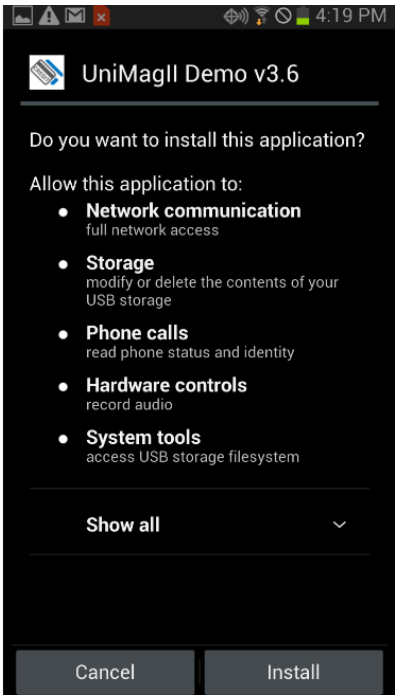
   a. Copy the **demo "*.APK"** file to the root directory of SD card (or device memory if there is no SD card slot).

   Note: SD card/internal memory is required for current SDK structure.

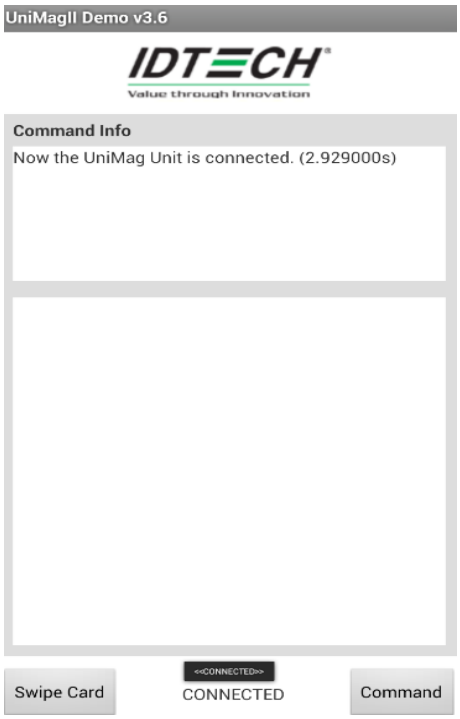
   b. Go to Android Market, search for "File Manager" or "Apk Installer" or "Apk Manager" and then install the application.

   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 demo "*.apk" file to install demo application.
   e. UniMag II demo application will be found under Applications after installed.

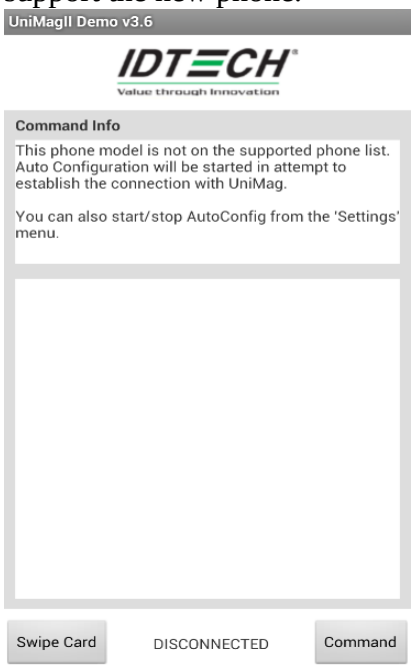




2. Adjust audio volume to maximum and plug the reader into the audio jack. Launch the demo application.
    a. If the phone is supported by the SDK, the phone would power up the reader when it's plugged in.

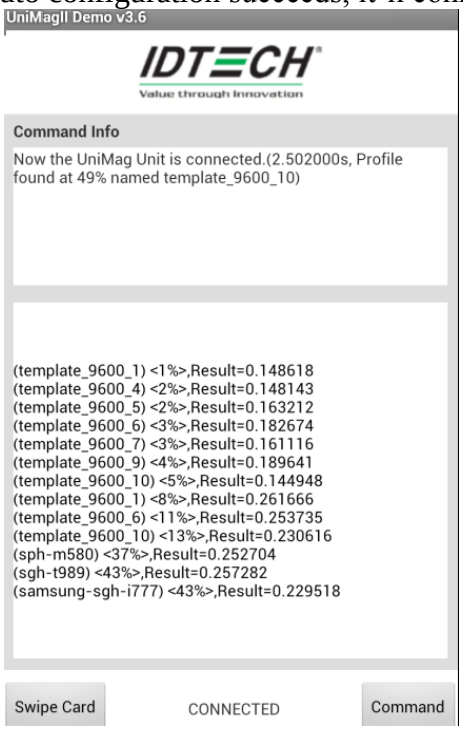


b. If the phone is not supported by the SDK, the following screen would show up. And you could run the auto configuration function to see if it can help support the new phone.



Here are few steps to run auto configuration function:

i. Click [Android Menu button] => [Settings] => [Start AutoConfig].
ii. It'll take a while to process the auto configuration function.
iii. If auto configuration succeeds, it'll connect with reader as below.



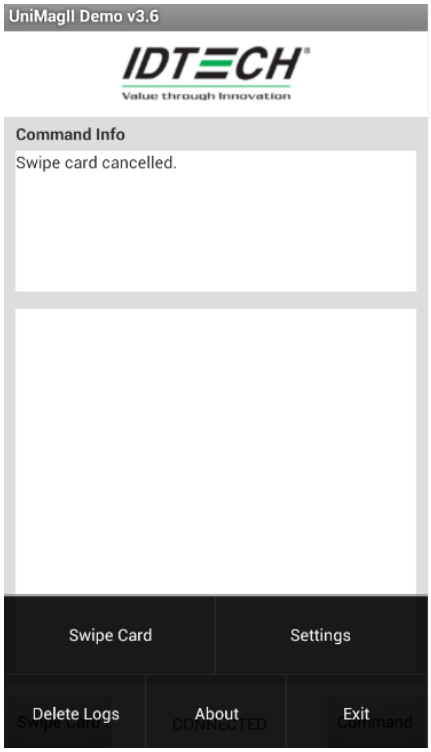
iv. Please swipe a card a few times to make sure the result is working stably
v. The next time you launch the demo, please click [Android Menu button] => [Settings] => Check [Use AutoConfig profile]

3. Click on the "swipe card" button. Wait for the card swipe message to come up and then swipe a card.

4. After a card swipe, the card data will show up on the screen.

5. To send commands to UniMag, click on the button ‘Command’ and select the command to send.

6. To enable the event log, click [Android menu button] => [Settings] => [Save Log Option]. The log file will be saved in the SD Card root directory.



7. To delete the log, click on the menu button and select ‘Delete Logs’.

8. To exit the application, click on the menu button and select “Exit”. The volume level will be restored after the demo is exited.

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

3. Data Output Format

3.1. UniMag II Unencrypted Data Output Format

Track 1: <Start Sentinel 1><T_1 Data><End Sentinel>
Track 2: <Start Sentinel 2><T_2 Data><End Sentinel><Terminator>

where: Start Sentinel 1 = %
Start Sentinel 2 = ;
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.

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?;4352378366824999=051020110000882?<CR>

3.2. UniMag II Encrypted Data Output Format

UniMag II 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>

Field	Usage Name
0	STX
1	Data Length low byte
2	Data Length high byte
3	Card Encode Type
4	Track Status
5	T1 data length
6	T2 data length
7	0
8	Field Byte 1 (see Notes)
9	Field Byte 2 (see Notes)

10 T1 data (masked if card type 80)
T2 data (masked if card type 80)
Encrypted section
T1 data encrypted (if card type 80, or force encrypt track 1 setting) else omitted.
T2 data encrypted (if card type 80, or force encrypt track 2 setting) else omitted.
End encrypted section
SN (10 bytes) padding '0' at the beginning if not 10 bytes
KSN (10 bytes) only if card data encrypted on any track
LRC
Check Sum
ETX

where
<LRC> is a one byte Exclusive-OR sum calculated for all <Card Data>.
<Check Sum> is a one byte Sum value calculated for all <Card data>.

Note:

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

2) Field 8:
   Bit 0: 1— if track 1 clear/mask data present
   Bit 1: 1— if track 2 clear/mask data present
   Bit 2: always 0
   Bit 3: 0 — Reserved for future use
   Bit 5, 4: 00 TDES; 01 AES encryption
   Bit 6: 0 — Reserved for future use
   Bit 7:1 — if serial # available

3) Field 9:
   Bit 0: if 1—track 1 encrypted data present
   Bit 1: if 1—track 2 encrypted data present
   Bit 2: always 0
   Bit 3: 0 — Reserved for future use
   Bit 4: 0 — Reserved for future use

Bit 5: 0 — Reserved for future use
Bit 6: 0 — Reserved for future use
Bit 7: if 1—KSN present

4) Card Type:

Value	Encode Type Description
80	ISO/ABA format
83	Other

5) Field Description:

Track 1, 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 for ISO/ABA format cards or plain text for other (type 83) cards.

Track 1 and Track 2 Masked

Track data masked with '*'. The first 4 and last 4 characters in PAN can be in the clear (unmasked). For type 83 cards, plain text data will be shown.

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 before encryption with 0.

The key management scheme is DUKPT. 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.

Example:

02D500801F3723008383252A353135302A2A2A2A2A2A2A373836315E50415950415353
2F4D41535445524341524 45E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B35313530
2A2A2A2A2A2A2A2A373836313D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2AA096A
6F5D1DCBE45B5F77EB2559FEE0411013232E3F42044C0397E3E9E6D9B3A11FB8ADE07
12AFD097C23AA86DFDC9DBA0E73A6FD698FD2F80800C0E1E9ED1BEED5EEA9840DA
53F41254FDB79E89B76B127C25FE44AE7524BAEB5BDAACF777FA313233343536373839
30FFFF9876543210E0004ABBF903

ISO/ABA Data Output Format

STX: 02
Data Length Low Byte: D5
Data Length High Byte: 00
Total Data Length: 0x00D5 (in HEX) 213 (in DECIMAL)
Card Encode Type: 80
Track Status: 1F

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

Track 1 Unencrypted Data Length: 37 (hex)
Track 2 Unencrypted Data Length: 23 (hex)
Always 00 (hex) byte
Field Byte 1: 83

- Bit 0: 1 — track 1 clear/mask data present
- Bit 1: 1 — track 2 clear/mask data present
- Bit 2: 0 — always 0
- Bit 3: 0 — not used
- Bit 5, 4: 00 —TDES encryption
- Bit 6: 0 — not used
- Bit 7: 1 — serial # is available

Field Byte 2: 83

- Bit 0: 1— track 1 encrypted data present
- Bit 1: 1— track 2 encrypted data present
- Bit 2: 0 —always 0
- Bit 3: 0 — not used
- Bit 4: 0 — not used
- Bit 5: 0 — not used

Bit 6: 0 — not used
Bit 7: 1 —KSN present

Track 1 Clear / Masked Data:
%*5150********7861^PAYPASS/MASTERCARD^****************?*

Track 2 Clear / Masked Data:
;5150********7861=****************?*

Account Number: 5150********7861

Card Holder Name: PAYPASS/MASTERCARD

Expiration Date:****

Track 1 Encrypted Data: Track 1 encrypted length = track 1 unencrypted length 37h rounded up by 8 bytes -> 38h = 56 bytes decimal

A096A6F5D1DCBE45B5F77EB2559FEE0411013232E3F42044C0397E3E9E6D9B3A11FB8
ADE0712AFD097C23AA86DFDC9DBA0E73A6FD698FD2F

Track 2 Encrypted Data: Track 2 encrypted length = track 2 unencrypted length 23h rounded up by 8 bytes -> 28h = 40 bytes decimal

80800C0E1E9ED1BEED5EEA9840DA53F41254FDB79E89B76B127C25FE44AE7524BAEB
5BDAACF777FA

Device Serial Number: 31323334353637383930

Key Serial Number: FFFF9876543210E0004A

LRC: BB
CheckSum: F9
ETX: 03