IDTECH®

Value through Innovation

User Manual

UniMag II
Magnetic Stripe Reader
For Mobile Devices

80110509-001-53
10/21/2011

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

Table of Contents

1. Introduction

The UniMag II 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, iPad, iPad 2 and selected Android platform devices. A complete list of supported device can be found on the ID TECH website.

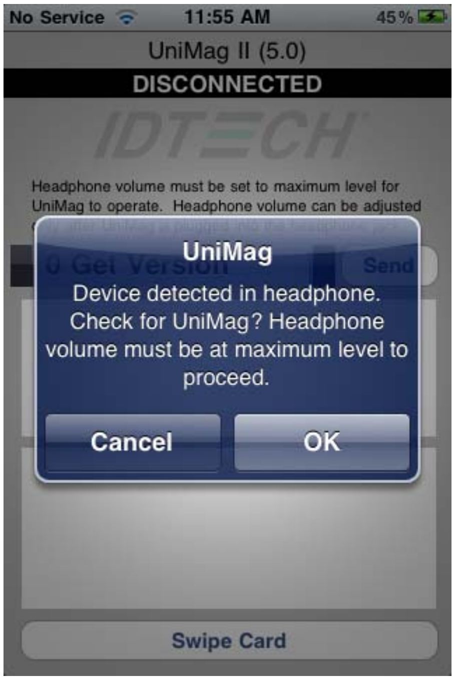
For more information on Apple and Android SDK, please see the SDK user manual for each operating system.

2. Using the Demo Software

3.1 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 the UniMag II device and launch the UniMag II demo application, make sure the volume is set to the maximum and click on "OK".

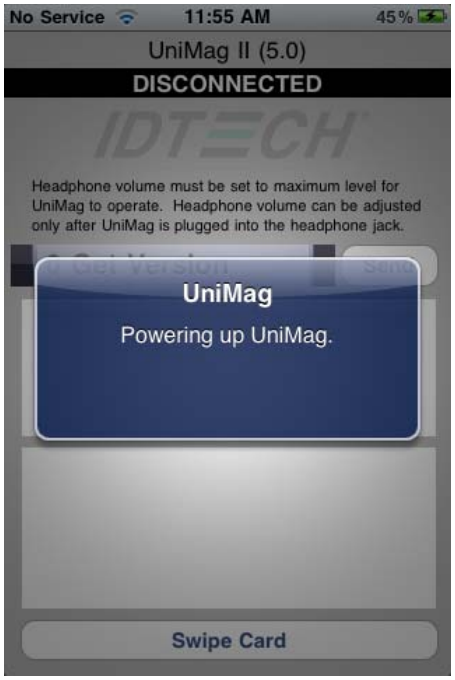


Headphone volume must be set to maximum level for UniMag to operate. Headphone volume can be adjusted

UniMag

Device detected in headphone. Check for UniMag? Headphone volume must be at maximum level to proceed.

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



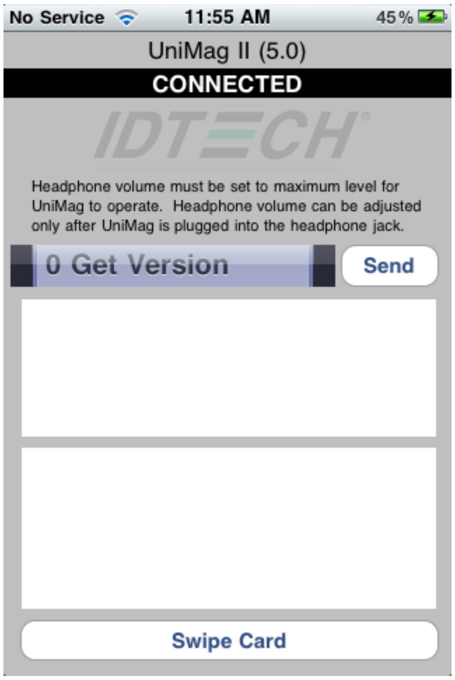
UniMag II (5.0)

DISCONNECTED

Headphone volume must be set to maximum level for UniMag to operate. Headphone volume can be adjusted only after UniMag is plugged into the headphone jack.

UniMag

Powering up UniMag.

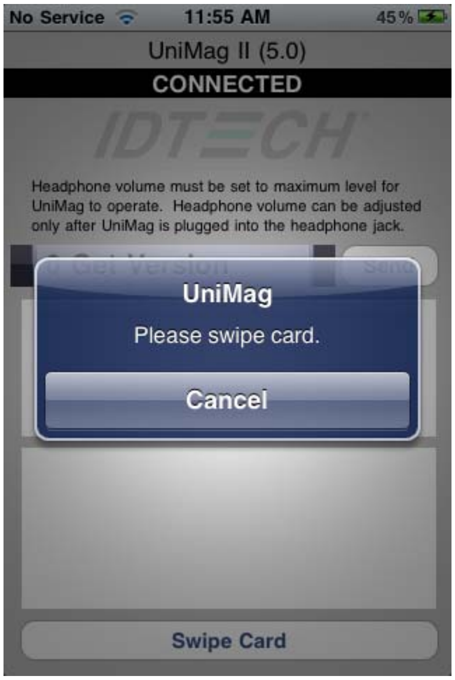


UniMag II (5.0)

CONNECTED

Headphone volume must be set to maximum level for UniMag to operate. Headphone volume can be adjusted only after UniMag is plugged into the headphone jack.

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



UniMag II (5.0)

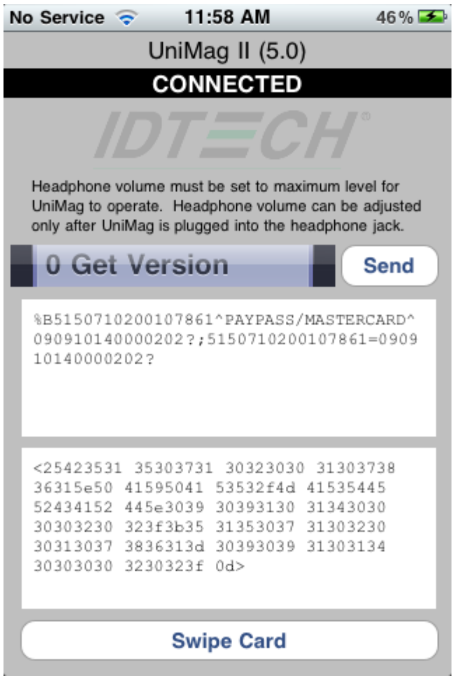
CONNECTED

Headphone volume must be set to maximum level for UniMag to operate. Headphone volume can be adjusted only after UniMag is plugged into the headphone jack.

UniMag

Please swipe card.

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



Headphone volume must be set to maximum level for UniMag to operate. Headphone volume can be adjusted only after UniMag is plugged into the headphone jack.

```
%B5150710200107861^PAYPASS/MASTERCARD^
090910140000202?;5150710200107861=0909
10140000202?
```

```
<25423531 35303731 30323030 31303738
36315e50 41595041 53532f4d 41535445
52434152 445e3039 30393130 31343030
30303230 323f3b35 31353037 31303230
30313037 3836313d 30393039 31303134
30303030 3230323f 0d>
```

3.2 Android Platform

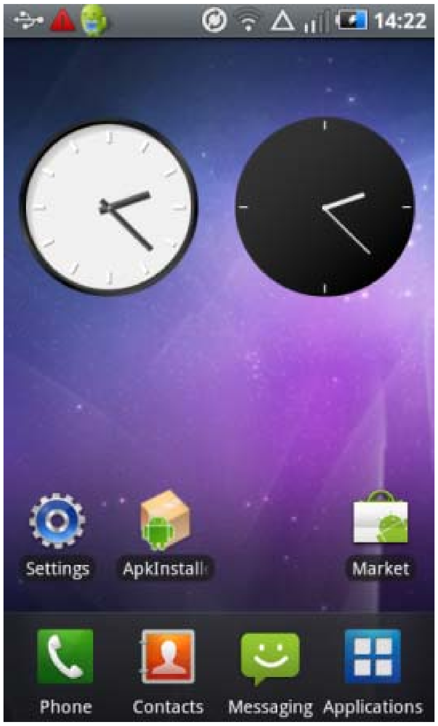
1. Install the UniMag II SDK demo application on the phone

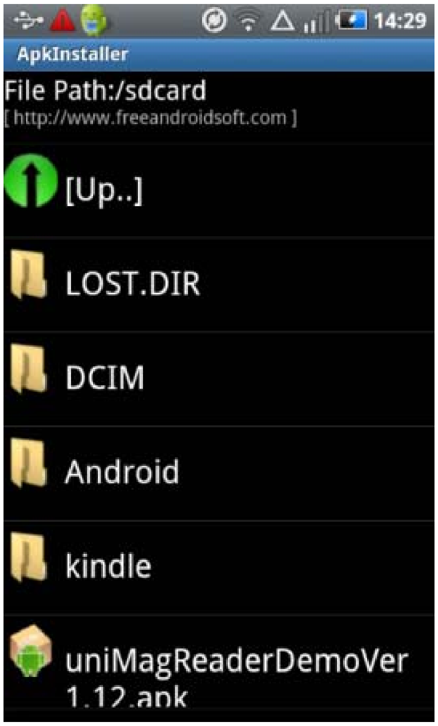
   a. Copy the **uniMagReaderDemo.apk** file to the root directory of SD card (or device memory if there is no SD card slot).

   Note: SD card is required for current SDK structure.

   b. Go to Android Market, search for “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.




14:29

ApkInstaller

File Path:/sdcard
[http://www.freeandroidsoft.com]

[Up..]

LOST.DIR

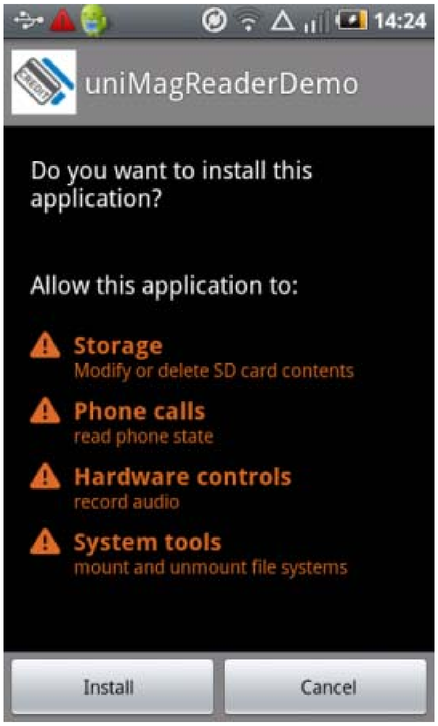
DCIM

Android

kindle

uniMagReaderDemoVer 1.12.apk

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


14:24

uniMagReaderDemo

Do you want to install this application?

Allow this application to:

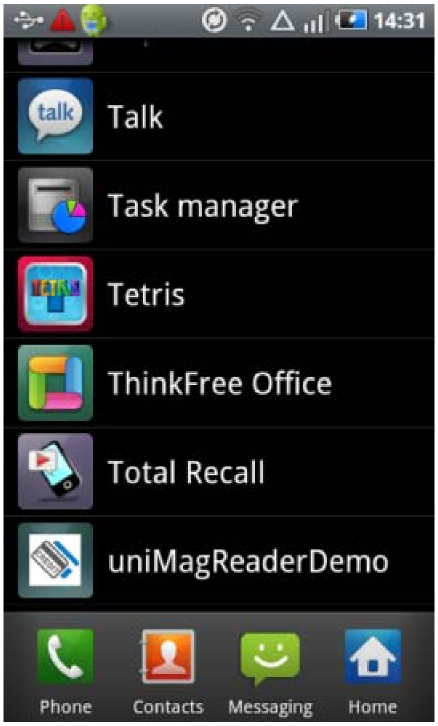
Storage
Modify or delete SD card contents

Phone calls
read phone state

Hardware controls
record audio

System tools
mount and unmount file systems

Install | Cancel


14:31

Talk

Task manager

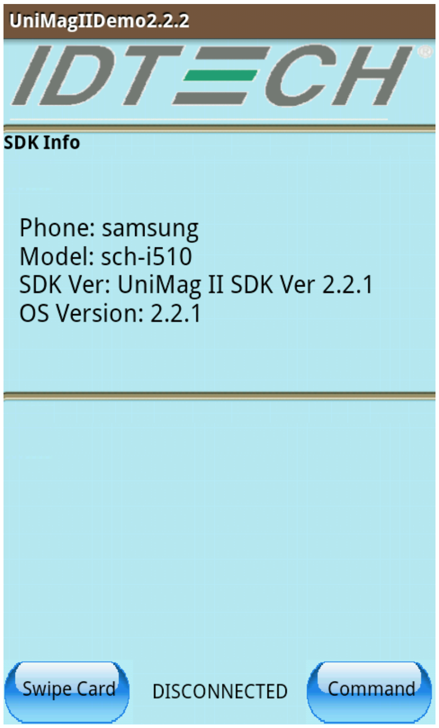
Tetris

ThinkFree Office

Total Recall

uniMagReaderDemo

2. Plug the UniMag into the audio jack. Launch the demo application.



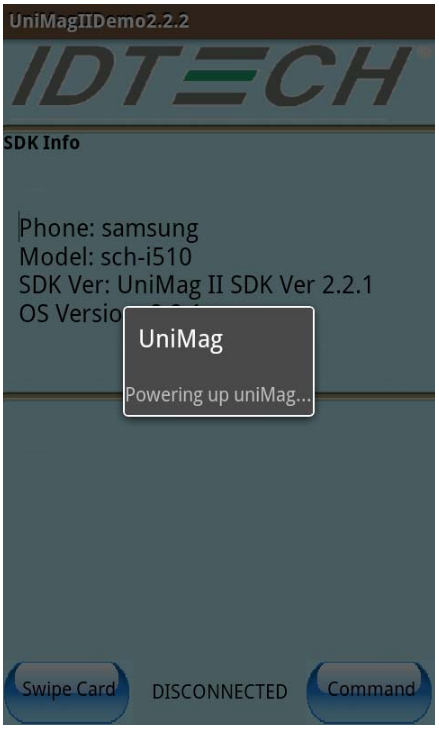
UniMagIIDemo2.2.2

SDK Info

Phone: samsung
Model: sch-i510
SDK Ver: UniMag II SDK Ver 2.2.1
OS Version: 2.2.1

DISCONNECTED

3. Wait for the UniMag to be powered up.



UniMagIIDemo2.2.2

SDK Info

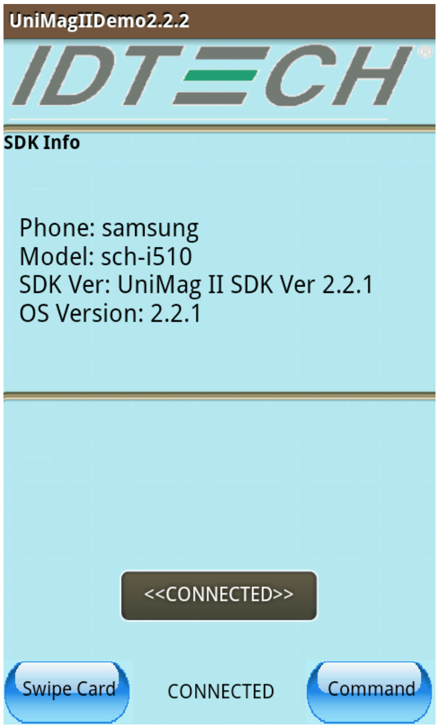
Phone: samsung
Model: sch-i510
SDK Ver: UniMag II SDK Ver 2.2.1
OS Versio

UniMag

Powering up uniMag...

DISCONNECTED

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.



UniMagIIDemo2.2.2

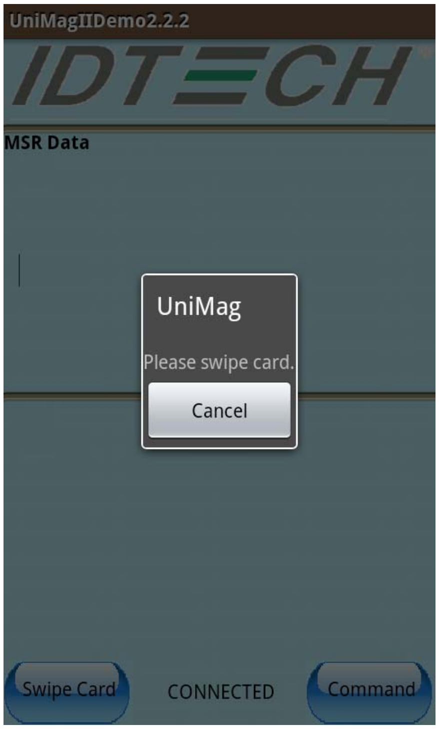
SDK Info

Phone: samsung
Model: sch-i510
SDK Ver: UniMag II SDK Ver 2.2.1
OS Version: 2.2.1

<<CONNECTED>>

CONNECTED

5. Click on the “swipe card” button. Wait for the card swipe message to come up and then swipe a card.



UniMagIIDemo2.2.2

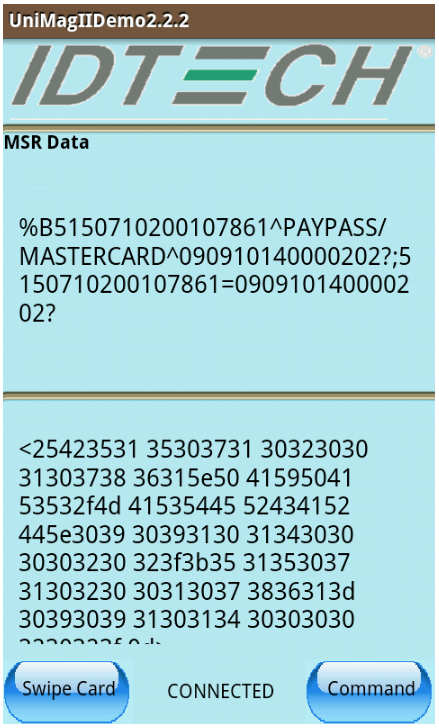
MSR Data

UniMag

Please swipe card.

CONNECTED

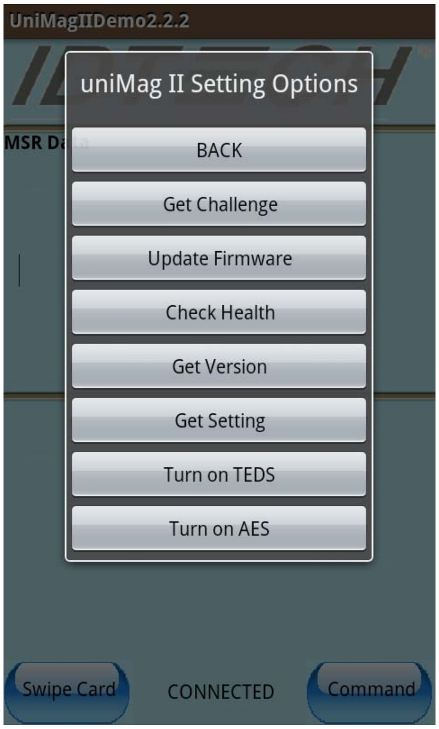
6. After a card swipe, the card data will show up on the screen. The volume level will be restored.



```
%B5150710200107861^PAYPASS/
MASTERCARD^090910140000202?;5
150710200107861=0909101400002
02?
```

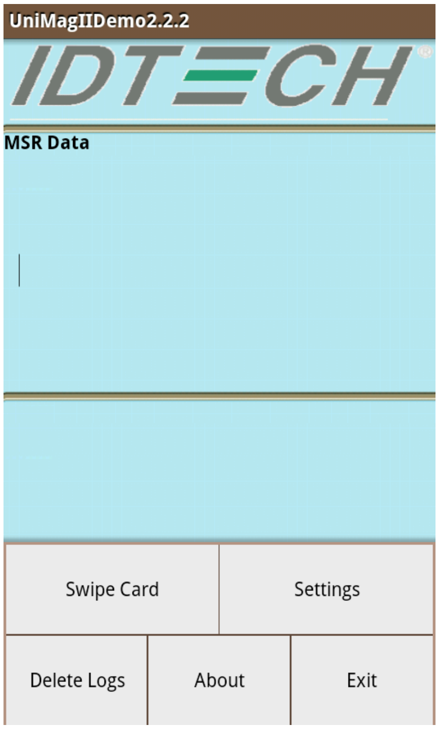
```
<25423531 35303731 30323030
31303738 36315e50 41595041
53532f4d 41535445 52434152
445e3039 30393130 31343030
30303230 323f3b35 31353037
31303230 30313037 3836313d
30393039 31303134 30303030
```

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



A key needs to be injected to the UniMag reader before "Turn on TDES" and "Turn on AES" settings to be effective. After encryption is enabled, the encryption algorithm can be switched between TDES and AES.

8. To enable the event log, click on the menu button on the phone 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.

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
^05102011000088200882000000?;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

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.

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).

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. 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.

Encrypted Data Length

Track 1 and Track 2 data are encrypted as a single block. 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. Once 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.

Example:

```
02D500801F3723008383252A353135302A2A2A2A2A2A2A373836315E50415950415353
2F4D4153544552434152445E2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B35313530
2A2A2A2A2A2A2A373836313D2A2A2A2A2A2A2A2A2A2A2A2A2A3F2AA096A
6F5D1DCBE45B5F77EB2559FEE0411013232E3F42044C0397E3E9E6D9B3A11FB8ADE07
12AFD097C23AA86DFDC9DBA0E73A6FD698FD2F80800C0E1E9ED1BEED5EEA9840DA
53F41254FDB79E89B76B127C25FE44AE7524BAEB5BDAACF777FA313233343536373839
30FFFF9876543210E0004ABBF903
```

<u>ISO/ABA Data Output Format</u>

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