IDTECH®
Value through Innovation

USER MANUAL

iMag, iMag Pro (II)

Magnetic Stripe Reader for Apple Devices

80097503-001-F
10/24/2013

Revision History

Rev	Date	Description of Changes	By
A	10/12/2010	Initial Release	JW
B	06/10/2011	-Updated manual to include iMag Pro readers -Revised specifications and encrypted output format -Removed security level 4 information	JW
C	08/17/2011	-Added information on decoded and sampling bits -Revised unencrypted output format -Removed more security level 4 related information	JW
D	07/19/2012	-Removed key management ID information	JW
E	10/12/2012	-Added iMag Pro outline drawing -Added iMag Pro Micro USB charging feature	JW
F	10/24/2013	-Added iMag Pro II	CH

Table of Contents

1 Introduction 3
2 Features and Benefits 3
3 Specifications 3
4 iMag/ iMag Pro/iMag Pro II Firmware Command 4
4.1 Setting Command 4
4.2 Get Firmware Version 4
4.3 Get Setting 5
4.4 Function ID Table 5
4.4.1 EncryptionID 5
4.4.2 Read SecurityLevelID 6
4.4.3 Get Firmware Version 6
5 Data Output Format 7
5.1 iMag/ iMag Pro(II) Unencrypted Data Output Format 7
5.2 iMag/ iMag Pro(II) Encrypted Data Output Format 8
5.3 Decryption Example 10
Appendix A iMag Pro Envelope Drawing 14
Appendix B iMag Pro II Envelope Drawing 15

1 Introduction

ID TECH iMag is a snap-on magnetic stripe reader designed to work with iPhone and iPod Touch. iMag Pro works with all Apple mobile devices including the iPad. The reader delivers superior reading performance with the ability to encrypt sensitive card data. The data encryption process prevents card holder information from being accessed when the data is stored or in transit, so the data remains secure from end to end. The reader fully supports TDES and AES data encryption using DUKPT key management method.

2 Features and Benefits

- Small form factor for comfort and mobility
- No external power supply required
- Mini USB port enables Apple devices to be charged through an external cable
- Bi-directional card reading
- Reads encoded data that meets ANSI/ISO/AAMVA standards and some custom formats such as ISO track 1 format on track 2 or 3
- Reads up to three tracks of card data
- Provides clear text confirmation data including card holder's name and a portion of the PAN as part of the Masked Track Data

3 Specifications

Communication Interface:	UART
Power Consumption:	5 mA during card swipe, 3 mA when idle
Magnetic Stripe Reader:	3 track bi-directional reading capabilities
Operating Life:	100,000 cycle minimum
Operating Environment:	0 ℃ to 55 ℃ (32 ℉ to 131 ℉) non-condensing
Storage Environment:	-30 ℃ to 70 ℃ (-22 ℉ to 158 ℉) non-condensing
Dimensions:	iMag: 95 mm (L) x 30 mm (H) x 71 mm (W) iMag Pro: 59mm (L) x 14 mm (H) x 32 mm (W) iMag ProII: 59.2mm(L) x 13.1mm(H) x 32.6mm(W)

4 iMag/ iMag Pro/iMag Pro II Firmware Command

4.1 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> for successful settings
or <NAK> for wrong commands such as invalid funcID, length and value

Each function-setting block <FuncSETBLOCK> has following format:

<FuncID><Len><FuncData>

Where:
<FuncID> is the one byte ID identifying the function being set
<Len> is a one byte length count for the 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.

Example:
Set DUKPT key management
CMD: \02\53\58\01\31\03\3A
OUT: 06

4.2 Get Firmware Version

Sending Get Firmware Version command returns the firmware version back to the application.

Command
<STX><R><FmVerID><ETX><LRC 1>

Response
<ACK> <STX><Version String><ETX><LRC 2>

Version String will be in format of "ID TECH iMag Swipe Reader x.y.z" x.y.z is the major and minor version number.

4.3 Get Setting

This command will send current setting to application.

Command
<STX> <R> <ReviewID> <ETX> <LRC 1>

Response
<ACK> <STX> <FuncID> <Len> <FuncData> <ETX> <LRC 2>

<FuncID>, <Len> and <FuncData> definition are same as described above.

Example:
Review all setting
CMD: \02\52\1F\03\4C
OUT: \06\02\7E\01\31\4C\01\31\58\01\31\03\5B

4.4 Function ID Table

The following table shows the available Function IDs with the default setting shown in **bold**.

Function Name	Function ID	Description
EncryptionID	0x4C	Security Algorithm **'0' Clear Text** '1' Triple DES '2' AES
SecurityLevelID	0x7E	Security Level (Read Only) '0' ~ '3" **Default value '1'**
GetFirmwareVersion	0x22	returns current firmware version

4.4.1 EncryptionID

Set clear text:
CMD: 02 53 4C 01 30 03 2F
OUT: 06
Read EncryptionID:
CMD: 02 52 4C 03 1F
OUT: 06 02 4C 01 30 03 7C

Set Triple DES:
CMD: 02 53 4C 01 31 03 2E

OUT: 06
Read EncryptionID:
CMD: 02 52 4C 03 1F
OUT: 06 02 4C 01 31 03 7D

Set AES
CMD: 02 53 4C 01 32 03 2D
OUT: 06
Read EncryptionID:
CMD: 02 52 4C 03 1F
OUT: 06 02 4C 01 32 03 7E

4.4.2 Read SecurityLevelID

CMD: 02 52 7E 03 2D
OUT: 06 02 7E 01 33 03 4D

4.4.3 Get Firmware Version

CMD: 02 52 22 03 71
OUT: 06 02 49 44 20 54 45 43 48 20 69 4D 61 67 00 31 31 30 03 04
Firmware Version: ID TECH iMag110

5 Data Output Format

5.1 iMag/ iMag Pro(II) 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 NULL.

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^0510201100008820088200000000?;4352378366824999=051020110000882?
```

5.2 iMag/ iMag Pro(II) Encrypted Data Output Format

iMag/ iMag Pro 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

5.3 Decryption Example

Key for all examples is
0123456789ABCDEFFEDCBA9876543210

Example of decryption of a three track ABA card

Enhanced encryption Format (this can be recognized because the high bit of the fourth byte underlined (80) is 1.

029801<u>80</u>3F48236B03BF252A343236362A2A2A2A2A2A2A2A393939395E42555348
204A522F47454F52474520572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A
A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B343236362A2A2A2A2A2A2A2A2
A393939393D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2ADA7F2A52BD3F6DD
8B96C50FC39C7E6AF22F06ED1F033BE0FB23D6BD33DC5A1F808512F7AE18D47
A60CC3F4559B1B093563BE7E07459072ABF8FAAB5338C6CC8815FF87797AE3A7
BEAB3B10A3FBC230FBFB941FAC9E82649981AE79F2632156E775A06AEDAFAF6
F0A184318C5209E55AD44A9CCF6A78AC240F791B63284E15B4019102BA6C50581
4B585816CA3C2D2F42A99B1B9773EF1B116E005B7CD8681860D174E6AD316A0E
CDBC687115FC89360AEE7E430140A7B791589CCAADB6D6872B78433C3A25DA9
DDAE83F12FEFAB530CE405B701131D2FBAAD970248A456000933418AC88F65E1
DB7ED4D10973F99DFC8463FF6DF113B6226C4898A9D355057ECAF11A5598F02C
A31688861C157C1CE2E0F72CE0F3BB598A614EAABB162994901190000000000206E
203

STX, Length(LSB, MSB), card type, track status, length track 1, length track 2, length track 3
02 9801 80 3F 48-23-6B 03BF

The above broken down and interpreted
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 so not level 4 encryption
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

Track 1 data masked (length 0x48)
252A343236362A2A2A2A2A2A2A393939395E42555348204A522F47454F5247452
0572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2
A2A2A2A2A2A2A3F2A

Track 1 masked data in ASCII
%*4266********9999^BUSH JR/GEORGE
W.MR^********************************?*

Track 2 data in hex masked (length 0x23)
3B343236362A2A2A2A2A2A2A393939393D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2
A2A2A3F2A

Track2 masked data in ASCII
;4266********9999=****************?*

In this example there is no Track 3 data either clear or masked (encrypted and hashed data is below)

Track 1 encrypted length 0x48 rounded up to 8 bytes = 0x48 (72 decimal)
DA7F2A52BD3F6DD8B96C50FC39C7E6AF22F06ED1F033BE0FB23D6BD33DC5A1
F8
08512F7AE18D47A60CC3F4559B1B093563BE7E07459072ABF8FAAB5338C6CC88
15FF87797AE3A7BE

Track 2 encrypted length 0x32 rounded up to 8 bytes =0x38 (56 decimal)
AB3B10A3FBC230FBFB941FAC9E82649981AE79F2632156E775A06AEDAFAF6F0
A

184318C5209E55AD

Track 3 encrypted length 0x6B rounded up to 8 bytes =0x70 (64 decimal)
44A9CCF6A78AC240F791B63284E15B4019102BA6C505814B585816CA3C2D2F42
A99B1B9773EF1B116E005B7CD8681860D174E6AD316A0ECDBC687115FC89360A
EE7E430140A7B791589CCAADB6D6872B78433C3A25DA9DDAE83F12FEFAB530
CE
405B701131D2FBAAD970248A45600093

Track 1 data hashed length 20 bytes
3418AC88F65E1DB7ED4D10973F99DFC8463FF6DF

Track 2 data hashed length 20 bytes
113B6226C4898A9D355057ECAF11A5598F02CA31

Track 3 data hashed length 20 bytes
688861C157C1CE2E0F72CE0F3BB598A614EAABB1

KSN length 10 bytes
62994901190000000002

LCR, check sum and ETX
06E203

Clear/Masked Data 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:
Track 1 decrypted
%B4266841088889999^BUSH JR/GEORGE
W.MR^0809101100001100000000046000000?!
Track 2 decrypted
;4266841088889999=0809101100000046?0
Track 3 decrypted
;3333333337676760707077676763333333333767676070707767676333333333376767
607070776767633333333337676760707?2

Track 1 decrypted data in hex including padding zeros (but there are no pad bytes here)

2542343236363834313038383838393939395E42555348204A522F47454F52474520572
E4D525E303830393130313130303030313130303030303030303034363030303030303F
21

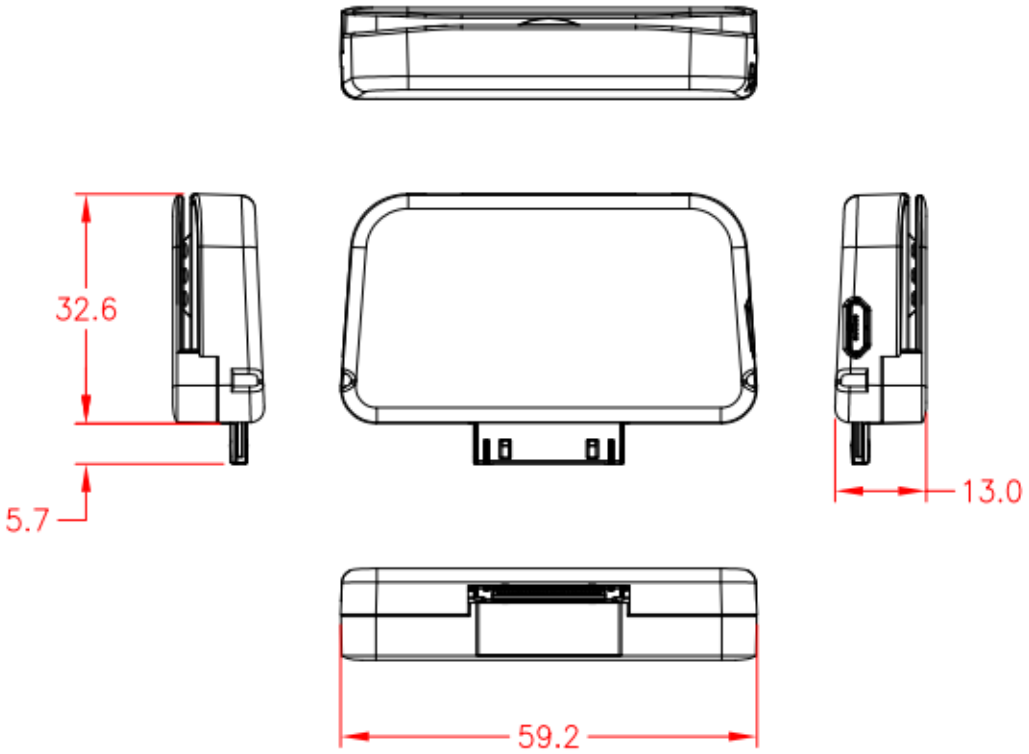
Track 2 decrypted data in hex including padding zeros

3B343236363834313038383838393939393D303830393130313130303030303034363F300
000000000

Track 3 decrypted data in hex including padding zeros

3B333333333333333333333736373637363037303730373736373637363333333333333
333333337363736373630373037303737363736373633333333333333333333373637363
736303730373037373637363736333333333333333333333736373637363037303373F32
0000000000

Appendix A iMag Pro Envelope Drawing



Appendix B iMag Pro II Envelope Drawing