IDTECH®
Value through Innovation

USER MANUAL

UniPay

Audio Jack
MSR and Chip Card Reader

80131505-001-C
3/12/2018

Revision History

Rev	Date	Description of Changes	By
A	11/8/2013	Initial Release	CH
B	12/1/2014	Revised version	CH
C	3/12/2018	Add 72 53 01 04 01 command	KT

Table of Contents

1 Introduction

ID TECH's UniPay is a compact mobile audio jack card reader that supports smart card reading (EMV), with proven and reliable magnetic stripe decoding. Its small form factor and audio jack interface make it ideal for mobile applications where either magnetic stripe and/or smart card reading are required. UniPay has the ability to work with Android and iOS mobile devices and tablets.

For the latest downloads and updates, please visit our public Knowledge Base at https://atlassian.idtechproducts.com/confluence/display/KB/Downloads+-+Home (no registration required).

2 Features and Benefits

- Audio jack interface
- No external power required
- Small form factor for comfort and mobility
- Support Android and IOS mobile devices
- Bidirectional MSR reading support up to 3 tracks
- EMV Level 1 certified
- Operates with ISO 7816 microprocessor cards
- Support TDES and AES encryption method with DUKPT key management

3 Abbrevation

APDU	Application Protocol Data Unit
ATR	Answer to Reset
CLA	Class
EMV	Europay, MasterCard and Visa
ETX	End of Text
ICC	Integrated Circuit Card
INS	Instruction
LRC	Longitudinal Redundancy Check
PPS	Protocol and Parameter Select
STX	Start of Text

4 Specifications

- Electro-Static Discharges (ESD)
  - 4kV contact, and 8kV air discharge
  - Magnetic Head Life: 300,000 cycles
  - Smart Card Contact Life: 50,000 cycles minimum
  - Rail and Cover Life: 300,000 cycles minimum
  - MTBF: 90,000 POH or depends on the electronics

- Environmental Temperature range:
  - Operating 0 to 55° C (32 to 131° F) [non-condensing]
  - Storage -30 to 70° C (-22 to 158° F) [non-condensing]

- Relative humidity
  - Maximum 95% (non-condensing)

- Size and Weight
  - Main Body size: 60.0mm(L) x38.0mm(W) x16.0mm(H)
  - Interface adapter: 52.0mm(L) x19.2mm(W) x15.2mm(H)

- Mounting method:
  - Clip: Used as the adapter to integrate with a variety of mobile devices.
  - Spacer foot: 2 spacers used to avoid the unit to conflict with the power switch of the mobile device.

- LED Indicator
  - No USB Cable connected to Host or No Power Cable connect Voltage State:

LED indicator	Invoke Method	Description
All Closed	Finish All Process and delay 2 seconds.	Sleep Mode
Solid Green 2 seconds	Finish a common command.	Process OK

Solid Green 2 seconds	Enable swiping MSR Card command and Read Card OK	MSR Good Read
Solid Green 2 seconds	Power Off ICC	Chip Card Powered off
Solid Red 2 seconds	Enable swiping MSR Card command and Read Card Bad.	MSR Bad Read
Flash Amber	Power On ICC Successfully	Chip Card Powered on. Warn the customer not to remove chip card until card is powered off.
Flash Green & Amber	Battery is Low, No Charging	Need Connect Host or Power via USB Cable
Flash Red, Green, & Amber	Enable Key Loading	Waiting for Key Loading

- USB Cable connected to Host or Power Cable connect Voltage State:

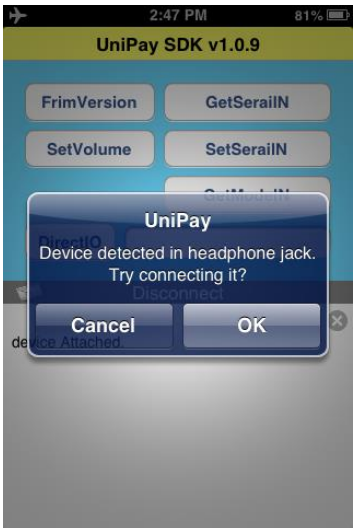
LED indicator	Invoke Method	Description
Solid Amber	Battery is Low	Charging
Solid Green	Battery is Full	Stop Charging

5 Demo software

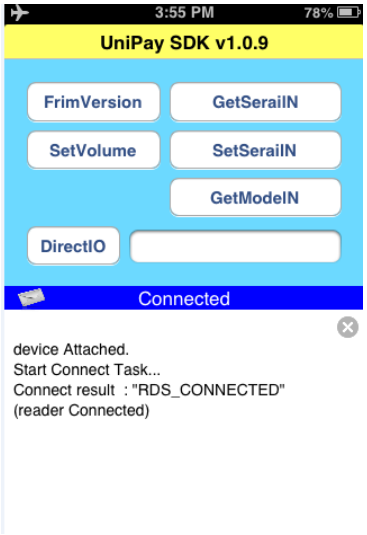
Please consult https://atlassian.idtechproducts.com/confluence/display/KB/Downloads+-+Home for the latest updates, demos, utilities, and SDKs.

5.1 iOS Demo

- Open iOS UniPay demo and plug UniPay to the iOS device.



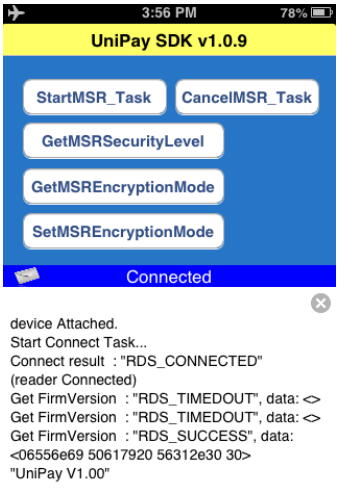
- Press OK to build the connection. After connection succeeds, it will show "RDS_CONNECTED" as below



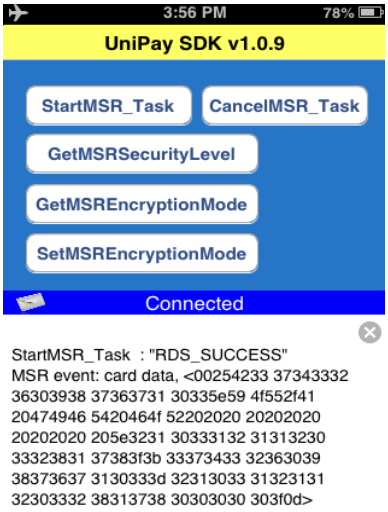
- Customer can also press other buttons on this page to get more information from the device as below:

[FirmVersion] Get firmware version from the device
[GetSerialN] Get the serial number from device
[SetVolume] Set the phone or tablet's audio output volume to communicate with
[SetSerailN] Set serial number to device
[DirectIO] Send command directly to the device

- By sliding the upper window, the demo can be switched to different function pages

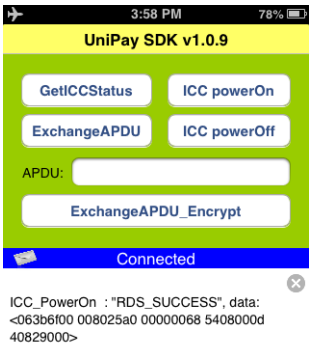


- Press [StartMSR_Task] to swipe a card. The swipe data will be showed in the lower window as below

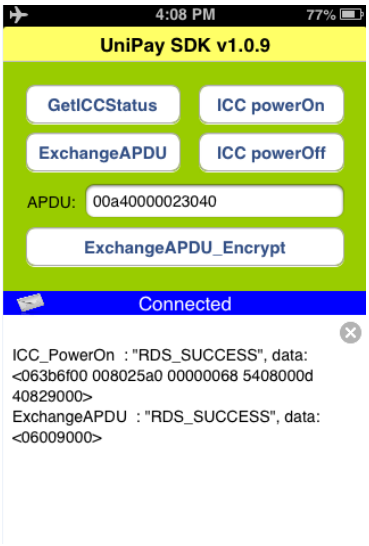


[GetMSRSecurityLevel]: get the security level from device
[GetMSREncryptionMode]: Get the encryption from device
[GetMSREncryptionMode]: Set device to TDES or AES

- Slide the upper window to get the page for smart card reader. Insert ID TECH T=0 CPU test card that comes with the evaluation kit. Click on [ICCPowerOn] button to power on the card. Check the status of the power on command.



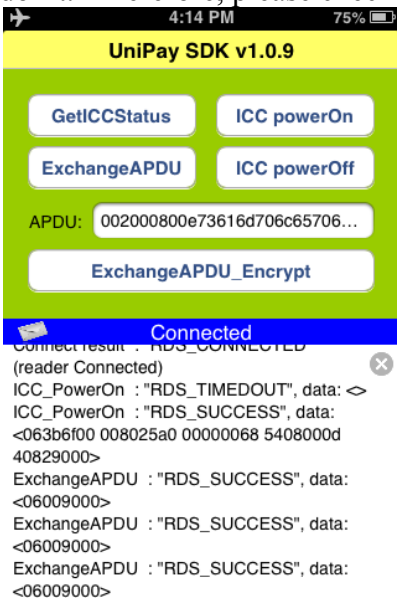
- Run the select APDU. Input a valid APDU, then click [Send APDU to CPU Card] command and. Such as the input value '00a40000023040' is the select APDU: "0x00,0xA4,0x00,0x00,0x02,0x30,0x40" for ID TECH T=0 CPU testing card.



The response code '9000' indicates a successful command.

- Run a verify APDU.

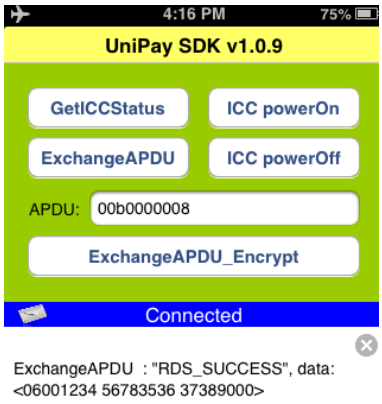
  Input another APDU “002000800e73616d706c6570617373776f7264”, and then tap on [Send APDU to CPU Card] button to verify the password “samplepassword”. Password for ID TECH T=0 testing card is “samplepassword”. Please note that some cards require password, while some don’t. Therefore, please check with card manufacturer for details.



  The response code ‘9000’ indicates a successful command.

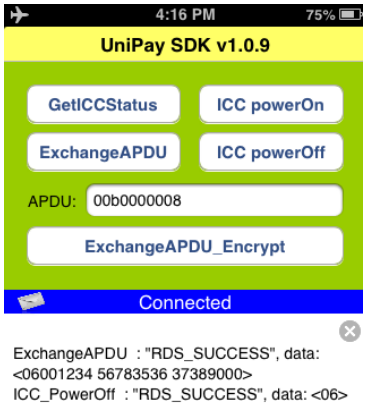
- Run a read APDU. Enter the read APDU “00b0000008” (length 08 for 8 bytes),

then tap on [Send APDU to CPU Card] button.



The last 2 bytes of response code is '9000', indicates a successful command.

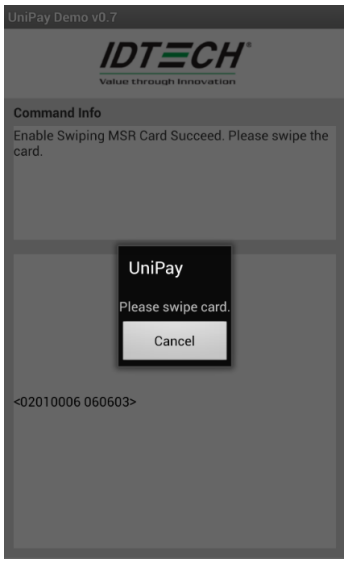
- Tap [ICC powerOff] to power off the card.

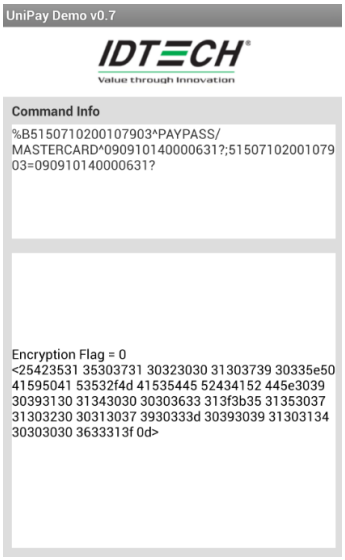


5.2 Android Audio Jack Demo

- Open the demo software and plug in UniPay. The demo will show power on and connect with UniPay.

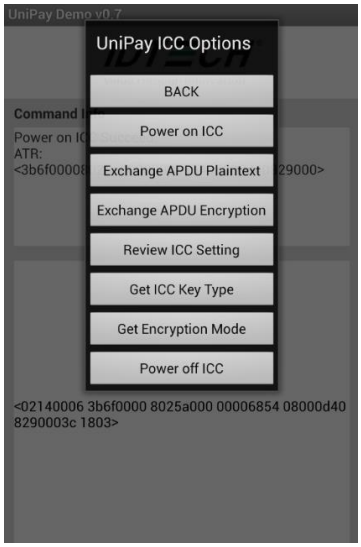
- Press [Swipe Card] button and swipe a card. The swipe data will show in the swipe





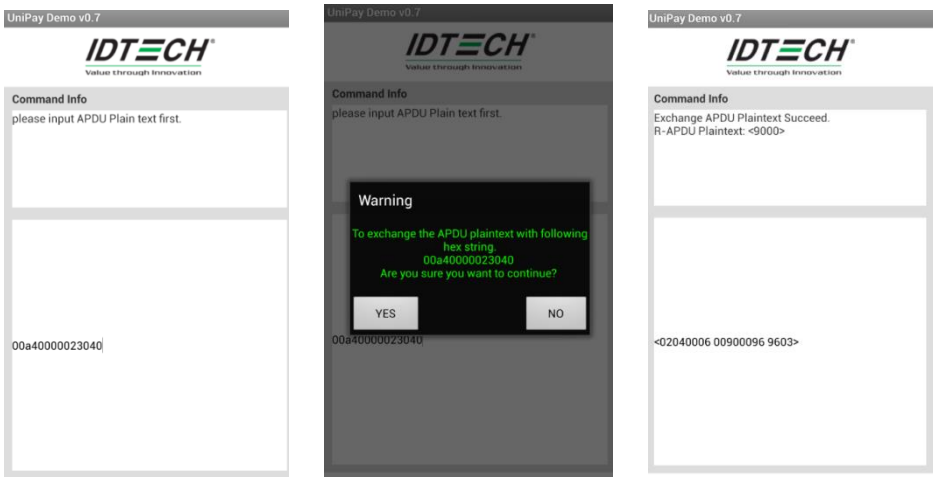
- Click [MSR] button to get more MSR options

- Click [ICC] button to get the operations with iSmart reader.



- Click [Power on ICC] to power on chip card. After power on successfully, it will show the message as below:

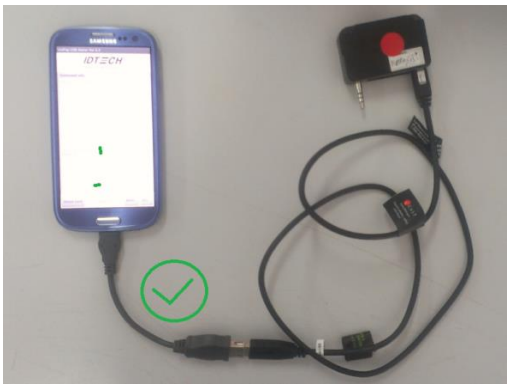
- To exchange APDU with smart card, please type in APDU in the lower window. Then click [ICC] => [Exchange APDU Plaintext]. If it's encrypted APDU, please click [Exchange APDU Encryption]. For example, run the select APDU "00a40000023040", after exchange APDU successfully, it will return 9000 as below.



5.3 Android USB Demo

Please refer to the notes below to make the sure the way to connect UniPay with Android device is right

- The Android OS version should be v3.1 or above
- The Android device should support USB Host
- The tablet or phone should be able to provide power to UniPay, as UniPay needs 100mA to be charged.
- The USB cable should be connected as the following methods, as the shorter cable should connect to Android device.



- The USB cable should NOT be connected like following method, the short transition cable

should NOT connect to the UniPay device.

- If the Tablet/Phone is not able to connect to UniPay, a USB Hub may be required to supply the external power. Please refer to following connect method:

How to use the demo software:

- **Connect/Disconnect the UniPay**

  When connect the UniPay, the status will show “CONNECTED”,
  When plug out the UniPay, the status will show “DISCONNECTED”

- **Swipe MSR card**

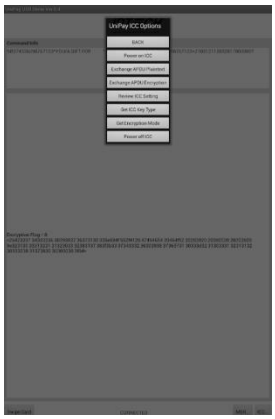
  Press “Swipe card” button, and it will pop the dialog to show “please swipe card”, then swipe card and get the MSR card.

  The swipe can also be canceled when you want to stop operation. If you don’t swipe card and you will get time out message after about 30s.

- **Command test**

  For more MSR commands, please click “MSR” button and it will pop out UniPay MSR options dialog.

  For the smart card operations, please click the [ICC] button at the right bottom of the demo



6 Firmware Commands

6.1 Command Body and Response Body

6.1.1 General Group (Task)

6.1.1.1 Get Firmware Release Version

Command Body is 78 46 01
Response Body is 06 & some bytes Ascii codes

6.1.1.2 Get Serial Number

Command Body is 78 46 02

Response Body is 06 + 9 bytes / 10 bytes ASCII code Serial Number Or
15 62 00 – No Serial Number

6.1.1.3 Get Model Number

Command Body is 78 46 20

Response Body is 06 + Model Number

6.1.1.4 Reset

Command Body is 78 46 49

Response Body is 06

Note:
Device will Reset (Re-Start) after it response ACK Response Body.
It is Highest Priority Command in device except that Key Loading State.

6.1.2 Smart Card Group (Task)

6.1.2.1 Get ICC Reader Status

Command Body is 72 46 24

Response Body is 06 + <Reader status> (1 byte)

Bit Position	'0'	'1'
0	ICC Power not ready	ICC Powered
1	Card not seated	Card seated
2~7		

6.1.2.2 Power On (Get ATR)

Command Body is 72 46 6E
1. This Command is used to power up the currently selected microprocessor card. It follows the ISO7816-3 power up sequence and returns the ATR as its response.
2. After Unit receives this command successfully, Unit should response a special Error Code (68 01) for MSR group commands.

Response Body is 06 + <ATR String>

6.1.2.3 Power Off

Command Body is 72 46 4D
After Unit receives this command successfully, Unit should process MSR group commands normally.

Response Body is 06

6.1.2.4 Exchange APDU Plaintext

Command Body is 72 46 41 <C-APDU>

Response Body is 06 + 00 + <R-APDU>

6.1.2.5 Exchange APDU Encryption for special case

Command Body is 72 46 61 <C-APDU>

Response Body is
06 + 00 + <Plaintext R-APDU> or
06 + 01 + <Encryption R-APDU>

Note:

1. For this command, the <R-APDU> of some special case could be encrypted by ICC DUKPT Key.
2. If ICC DUKPT Key was not loaded, Unit should response Error Code (04 00) for this command.
3. If ICC DUKPT Key was end its useful life, Unit should response Error Code (72 00) for this command.
4. The format of <Encryption R-APDU> is below:

- For TDES mode: 10 bytes KSN + n bytes Encrypted Data (n can be multiple of 8).
- For AES mode: 10 bytes KSN + n bytes Encrypted Data (n can be multiple of 16).

5. The format of Raw Data of Encrypted Data is below:

- For TDES mode: the raw data length of R-APDU should be multiple of 8. If it was not multiple of 8, unit should padded 0x00 bytes automatically.
- For AES mode: the raw data length of R-APDU should be multiple of 16. If it was not multiple of 16, unit should padded 0x00 bytes automatically.

6.1.2.6 Set Key Type for ICC DUKPT Key

Command Body is 72 53 01 01 01 <Option>

Key Type	Option
Data type Key	**0x00**
PIN type Key	0x01

Note: ICC Group (Task) only support A Fun of Setting/Review command except for Default All & Review All.

Response Body is 06

6.1.2.7 Get Key Type for ICC DUKPT Key

Command Body is 72 52 01 01

Response Body is 06 72 01 01 <Option>

6.1.2.8 Set Encryption Mode for ICC DUKPT Key

Command Body is 72 53 01 02 01 <Option>

Encryption Mode	Option
TDES	0x00
AES	0x01

Note:
ICC Group (Task) only supports A Fun of Setting/Review command except for Default All & Review All.

Response Body is
06 (ICC DUKPT Key existed) or
15 6A 00 (NAK + Unsupported Command Error Code) (ICC DUKPT Key did not exist)

6.1.2.9 Get Encryption Mode for ICC DUKPT Key

Command Body is 72 52 01 02

Response Body is 06 72 02 01 <Option>

Encryption Mode	Option
No ICC DUKPT Key	0xFF
TDES	0x00
AES	0x01

6.1.2.10 Default ICC Group All Setting

Command Body is 72 53 00

Response Body is 06

Below Setting should be reset to default value:

Function Name	Default Value
Key Type	Data Key
Encryption Mode	DES/TDES (ICC DUKPT Key existed) No change (ICC DUKPT Key did not exist)

6.1.2.11 Set Card Type (EMV or ISO)

Command Body is 72 53 01 04 01. Complete command with header and trailer is 02 06 00 72 53 01 04 01 00 25 CB 03 to set the device into ISO mode.

Card Type	**Option**
EMV	0xFF
ISO	0x00

Response is 06.

6.1.2.12 Review ICC Group All Setting

Command Body is 72 52 00

Response Body is 06 72 02 01 <Key Type Option> 02 01 <Encryption Mode Option>

6.1.3 MSR Card Group (Task)

6.1.3.1 Enable swiping MSR card

Command Body is 73 46 51<Ascii Char>

Track Selection Option	Ascii Char
Any Track	**0**
Track 1 Only	1
Track 2 Only	2
Track 1 & Track 2	3
Track 3 Only	4
Track 1 & Track 3	5
Track 2 & Track 3	6
All three Tracks	7

Response Body is 06 + <Track Data>

Note：
1. If device received this command, it should response ACK Response Body and enter into Waiting for Swiping MSR Card State. The waiting time is about 30 seconds.
2. In Waiting for Swiping MSR Card State, device only process Cancel Swiping MSR Card command.
3. If device did not read any MSR Card while Waiting State, device should quit the State and response “Time Out” Response Body after Time out.
4. If device read MSR Card but decoded Data Failed in Waiting State, device should response “No Card Data” Response Body and quit the State immediately.

6.1.3.2 Cancel swiping MSR card

Command Body is 73 46 19

Response Body is 06

6.1.3.3 Review MSR All Setting

Command Body is 73 52 00

Response Body is 06 + 73 + BlockNums + <FuncBlock1>[…<FuncBlockn>]
Where:
BlockNums is the number of <FuncBlock>
<FuncBlock> format is <FuncID><FuncLen><FuncData>

- <FuncID> - 1 byte Identify
- <FuncLen> - 1 byte Length of <FuncData>
- <FuncData> - <FuncLen> bytes data of this function Setting.

6.1.3.4 Default MSR All Setting

Command Body is 73 53 00

Response Body is 06

Note: Function ID 0x49, 0x50, 0x84, and 0x86 can be default.

6.1.3.5 Get Common Setting

Command Body is 73 52 01 <Function ID>

Response Body is 06 73 01 <Function ID> 01 <Setting Value>

6.1.3.6 Set Common Setting

Command Body is 73 53 01 <Function ID> 01 <Setting Value>

Function ID	Hex	Description	Setting Value	Description	
PrePANID	49	PAN to not mask	4 (0-6)	# leading PAN digits to display	e

DispExpDateID,	50	mask or display expiration date	'0"0'-'1'	'1' don't mask expiration date	e
CrypTypeID	4C	encryption type	'1' ('1'-'2')	'1' 3DES '2' AES	r e
SecurityLevelID	7E				nr
EnOptionID	84	Encryption Option (Forced encryption or not)	08	Bit 0: T1 force encrypt Bit 1 : T2 force encrypt Bit 2 : T3 force encrypt Bit3 : T3 force encrypt when card type is 0	e
MaskOptID	86	Masked / clear data sending option	0x07	Bit0: T1 mask allowed Bit1: T2 mask allowed Bit2: T3 mask allowed	e

Response Body is 06

Example:

6.1.3.6.1 Encrypt Option Setting

Command Body is 73 53 01 84 01 <Encrypt Opt>
Where:
<Encrypt Opt>:
bit0: 1 – TK1 force encrypt *
bit1: 1 – TK2 force encrypt *
bit2: 1 – TK3 force encrypt *
bit3: 1 – TK3 force encrypt when card type is 0

Response Body is 06

Note:

- When force encrypt is set, this track will always be encrypt, regardless of card type. No clear/mask text will be sent.
- If and only if in new encrypt structure, each track encryption is separated, encrypted data length will round up to 8 or 16 bytes.
- When force encrypt is not set, it encrypts data just like old structure, that is, only T1 and T2 in type zero will be encrypted.

6.1.3.6.2 Mask Option Setting

Command Body is 73 53 01 86 01 <Mask Opt>

Where:
<Mask Opt>:
bit0: 1 – TK1 mask data allow to send when encrypted.
bit1: 1 – TK2 mask data allow to send when encrypted.
bit2: 1 – TK3 mask data allow to send when encrypted.

Response Body is 06

6.2 Magstripe Card Data Output Format

6.2.1 Clear MSR Data Output Format

In Level 1 or Level 2, MSR Data Output Format is Plaintext:

Magnetic Track Basic Decoded Data Format

Track 1: <Expanded Card Encode Type><SS1><T1 Data><ES><Track Separator>
Track 2: <Expanded Card Encode Type><SS2><T2 Data><ES><Track Separator>
Track 3: <Expanded Card Encode Type> <SS3><T3 Data><ES><Terminator>

Where:
<Expanded Card Encode Type> is one byte with the following bits:
Bit 7~3: Always 0
Bit 2: Encryption On 1 or Off 0
Bit 1: AES 1 or TDES 0
Bit 0: Always 0
SS1 (start sentinel track 1) = %
SS2 (start sentinel track 2) = ;
SS3 (start sentinel track 3) = ; for ISO, % for AAMVA
ES (end sentinel all tracks) = ?
Track Separator = Carriage Return
Terminator = Carriage Return

Magnetic Track Basic Raw Data Format

Track 1: <Expanded Card Encode Type><T1 Raw Data><Track Separator>
Track 2: <Expanded Card Encode Type><T2 Raw Data><CR>

Track 3: <Expanded Card Encode Type><T3 Raw Data><CR>

Where: Track Separator = Carriage Return
Terminator = Carriage Return

Language: US English

6.2.2 Encrypted MSR Data Output Enhance structure

In Level 3, MSR output data is encrypted as the format below::

<Expanded Card Encode Type><02> <Len_Low><Len_High> <Card Data> <CheckLRC> <CheckSUM> <03>
Where:

- < Expanded Card Encode Type > is one byte with the following bits:
  Bit 7~3: Always 0
  Bit 2: Encryption On 1 or Off 0
  Bit 1: AES 1 or TDES 0
  Bit 0: Always 0
- <Len_Low><Len_High> is length of <Card Data>
- <CheckLRC> is LRC of <Card Data>
- <CheckSUM> is SUM of <Card Data>
- <Card Data> format is shown below.
  - 1 Data Length low byte
  - 2 Data Length high byte
  - 3 Card Encode Type*
  - 4 Track 1-3 Status
  - 5 T1 data length
  - 6 T2 data length
  - 7 T3 data length
  - 8 Clear/mask data sent status *
  - 9 Encrypted/Hash data sent status *
  - 10 T1 clear/mask data
  - 11 T2 clear/mask data
  - 12 T3 clear/mask data
  - 13 T1 encrypted data (Pin key/Data key)
  - 14 T2 encrypted data (Pin key/Data key)
  - 15 T3 encrypted data (Pin key/Data key)
  - 16 Session ID (8 bytes) (Security level 4 only)
  - 17 T1 hashed (20 bytes each) (if encrypted and hash tk1 allowed)

- 18 T2 hashed (20 bytes each) (if encrypted and hash tk2 allowed)
- 19 T3 hashed (20 bytes each) (if encrypted and hash tk3 allowed)
- 20 KSN (10 bytes)

Note:

1. Field 8 (Clear/mask data sent status) and field 9 (Encrypted/Hash data sent status) will only be sent in new encrypt structure

2. Field 4 Track 1-3 Status

- 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

3. Field 8: Clear/mask data sent status byte, this filed can be set by Function ID 0x86,

- Bit 0: 1--- if TK1 clear/mask data present
- Bit 1: 1--- if TK2 clear/mask data present
- Bit 2: 1--- if TK3 clear/mask data present
- Bit 3: 0--- 0 reserved future use
- Bit 4: 0--- 0 reserved future use
- Bit 5: 0--- 0 reserved future use

4. Field 9: Encrypted data sent status, this filed can be set by Function ID 0x84,

- Bit 0: if 1—tk1 encrypted data present
- Bit 1: if 1—tk2 encrypted data present
- Bit 2: if 1—tk3 encrypted data present
- Bit 3: if 1—tk1 hash data present
- Bit 4: if 1—tk2 hash data present
- Bit 5: if 1—tk3 hash data present
- Bit 6: if 1—session ID present
- Bit 7: if 1—KSN present

5. Card Type: Value Encode Type Description

0 / 80 ISO/ABA format
1 / 81 AAMVA format

3 / 83 Other
4 / 84 Raw; un-decoded format

Note:

- Card Type will be 8x in new structure and 0x for old structure
- Type 4 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. ('01','02' and '03' will still exist for none secured mode raw output when security level < 3)

6.3 Error Code

Error Code	Definition
0x0400	Related Key was not loaded
0x0702	PAN is Error
0x0F00	Encryption Or Decryption Failed
0x1000	Battery Low Warning (It is High Priority Response while Battery is Low.)
0x5500	No Admin DUKPT Key
0x5501	Admin DUKPT Key STOP
0x5504	Validate Authentication Code Error
0x5505	Encrypt Or Decrypt data failed
0x5506	Not Support the New Key Type
0x5507	New Key Index is Error
0x5508	Step Error
0x5509	Remote Key Injection Timeout (Latest Command is Timeout)
0x550A	MAC Error
0x550B	Key Usage Error
0x550C	Mode Of Use Error
0x550F	Other Error
0x6000	Save or Config Failed / Or Read Config Error
0x6200	No Serial Number
0x6900	Invalid Command – Protocol is right, but task ID is invalid
0x6A00	Unsupported Command – Protocol and task ID are right, but command is invalid
0x6A01	Unsupported Command – Protocol and task ID are right, but command is invalid – In this State
0x6B00	Unknown parameter in command – Protocol task ID and command are right, but parameter is invalid
0x6C00	Unknown parameter in command – Protocol task ID and command are right, but length is out of the requirement.
0x7300	MSR/ICC/Admin DUKPT is STOP (21 bit 1)
0x8100	Timeout

0x8200	Wrong operate step
0x8300	No Card Data
0x8400	TriMagII no Response
0x2C02	No Microprocessor ICC seated
0x2C06	No card seated to request ATR
0x8B10	ICC error on power-up
0xE313	IO line low -- Card error after session start
0xF002	ICC communication timeout
0xF003	ICC communication Error