80137503-001

SREDKey

User Manual

Rev. F

Revised: 08/04/2017

International Technologies & Systems Corporation
10721 Walker Street, Cypress, CA 90630-4720; Tel: (714) 761-6368; Fax: (714) 761-8880

www.idtechproducts.com

Revision	Date	Description	By
A	05/07/2014	Initial Release	Candy Han
B	06/20/2014	Added data sample for original format Added commands bytes	Candy Han
C	05/26/2015	Added LRC calculation Added Card Format check	Candy Han
D	07/20/2015	Added Battery Life info. Added Enable/Disable Admin Key	Ginger Wu
E	09/15/2015	Updated "KeyedOptID" Section in Appendix A on page 11 Updated Manually-Keyed Conf. Options on page 6	Ginger Wu
F	08/04/2017	Add Foreign Language options (Command 24)	Kas Thomas

ID TECH

10721 Walker Street, Cypress, CA90630 Voice: (714) 761-6368 Fax: (714) 761-8880

Visit us at http://www.ID TECHproducts.com

The information contained herein is provided to the user as a convenience. While every effort has been made to ensure accuracy, ID TECH is not responsible for damages that might occur because of errors or omissions, including any loss of profit or other commercial damage, nor for any infringements or patents or other rights of third parties that may result from its use. The specifications described herein were current at the time of publication, but are subject to change at any time without prior notice.

LIMITED WARRANTY

ID TECH warrants to the original purchaser for a period of 12 months from the date of invoice that this product is in good working order and free from defects in material and workmanship under normal use and service. ID TECH's obligation under this warranty is limited to, at its option, replacing, repairing, or giving credit for any product that returned to the factory of origin with the warranty period and with transportation charges and insurance prepaid, and which is, after examination, disclosed to ID TECH's satisfaction to be defective. The expense of removal and reinstallation of any item or items of equipment is not included in this warranty. No person, firm, or corporation is authorized to assume for ID TECH any other liabilities in connection with the sales of any product. In no event shall ID TECH be liable for any special, incidental or consequential damages to purchaser or any third party caused by any defective item of equipment, whether that defect is warranted against or not. Purchaser's sole and exclusive remedy for defective equipment, which does not conform to the requirements of sales, is to have such equipment replaced or repaired by ID TECH. For limited warranty service during the warranty period, please contact ID TECH to obtain a Return Material Authorization (RMA) number & instructions for returning the product.

THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE. THERE ARE NO OTHER WARRANTIES OR GUARANTEES, EXPRESS OR IMPLIED, OTHER THAN THOSE HEREIN STATED. THIS PRODUCT IS SOLD AS IS. IN NO EVENT SHALL ID TECH BE LIABLE FOR CLAIMS BASED UPON BREACH OF EXPRESS OR IMPLIED WARRANTY OF NEGLIGENCE OF ANY OTHER DAMAGES WHETHER DIRECT, IMMEDIATE, FORESEEABLE, CONSEQUENTIAL OR SPECIAL OR FOR ANY EXPENSE INCURRED BY REASON OF THE USE OR MISUSE, SALE OR FABRICATIONS OF PRODUCTS WHICH DO NOT CONFORM TO THE TERMS AND CONDITIONS OF THE CONTRACT.

Contents

1 Introduction

SREDKey™ by ID TECH is an encrypted key pad with an LCD and an encrypted MagStripe reader that offers retailers a complete and reliable security solution that meets the PCI 3.0 certification. This intelligent reader delivers superior reading performance while encrypting sensitive MagStripe and keyed-in data so as to reduce the PCI-DSS scope. The SREDKey ensures all data transactions are protected through secure point-to-point encryption, reducing fraud and protecting against data compromise.

2 Product Configurations

Model Number	Configuration
IDSK-534833AEB	USB-KB;AES;Enhanced Encryption;Black
IDSK-534833TEB	USB-KB;TDES;Enhanced Encryption;Black

3 Features

- Encrypted numeric keypad with 2x20 LCD and optional encrypted MSR
- 1,000,000 swipe, industry proven Magnetic Stripe Reader
- 1,000,000 manual key entry
- 4,000,000 key operations for each key
- Meets FCC Class B & CE regulatory requirements
- Plug-n-Play operation for USB-Keyboard and USB-HID interface
- PCI 3.0 certified with SRED function supported
- ROHS 2 and REACH certified
- Mounting option
- TDES/AES with DUKPT Key Management
- MSR support Track 1,2,3 reading
- MSR support ISO 7810 and 7811-1 through -6 cards. Reads AAMVA driver license cards
- Minimum Battery Life of 5-Years

4 Definition of Terms & Applicable Documents

ANSI American National Standard Institute
ESD Electrostatic Discharge
HOST A Personal Computer or Similar Computing Device
ISO International Standards Organization
MTBF Mean Time Between Failures
USB Universal Serial Bus
SRED Secure Reading and Exchange of Data
ISO/IEC 7813 – Identification cards, Physical Characteristic
ISO/IEC 7811 – Identification cards, Recording Techniques, Magnetic Stripe

5 Function & Operation

On power-on the device will go into its data capture mode. In data capture mode the device will prompt the user to enter data.

The device will display "Key is not injected!" if the device is not key-injected with encryption enabled after a key is pressed. The evaluation unit is injected with the ID TECH demo key by default and the data can be decrypted using the ID TECH SecureKey demo software.

5.1 **Function Keys Operation:**

Clear:

- Pressing the "Clear" key allows users to remove all entered data at the current level. The current transaction would not be cancelled.

BS:

- Pressing the "BS" (backspace) key allows users to remove the entered data one character at a time.

#Admin:

- Pressing the "#Admin" key when the screen displays "Swipe or Hand-Key Card Number" or "Enter Card Number then press Enter" allows user to enter the Admin Menu. Pressing the "#Admin" key in other screens puts the device in the Help Mode.

Cancel:

- Pressing the "Cancel" key once allows users to remove all the input in the current as well as the previous level. The device then goes back to the previous prompt of the current transaction. If the "Cancel" key is pressed twice, the current transaction would be cancelled and the device goes back to the initial mode.

5.2 **Admin Menu**

When the "Admin" key is pressed, the screen will display **"Select manual config 1-6"** to prompt the user to select one of six manual entry modes.

Manually-Keyed Configuration Options

Configuration #1: Card Number, Expiration Date
Configuration #2: Card Number, Expiration Date, Zip Code
Configuration #3: Card Number, Expiration Date, Street Number of the Address, Zip Code
Configuration #4: Card Number/Expiration Date/Security Code/Zip Code
Configuration #5: Card Number/Expiration Date/Security Code/Street Number/Zip Code
Configuration #6: Card Number/Expiration Date/Security Code

6 Firmware Commands

6.1 Command Structure

1. Commands sent to keypad/reader:

a. Setting Command:
<STX><S>[<FuncID><Len><FuncData>…]<ETX><LRC>

b. Read Status Command:
<STX><R><FuncID><ETX><LRC>

c. Function Command:
<STX>[<FuncID><Len><FuncData>…]<ETX><LRC>

2. Response from SREDKey:
a. Setting Command

Host		**SREDKey**
Setting Command	→	
	←	<ACK> if OK
	or	
	←	<NAK> if Error

b. Read Status Command

Host		**SREDKey**
Read Status Command	→	
	←	<ACK> and <Response> if OK
	or	
	←	<NAK> if Error

c. Other Commands

Host		**SREDKey**
Other Command	→	
	←	<ACK> and <Response> if OK
	or	
	←	<NAK> if Error

<Response> format:
The current setting data block is a collection of many function-setting blocks <FuncSETBLOCK> as follows:

<STX><FuncSETBLOCK1>…<FuncSETBLOCKn><ETX><LRC>
Each function-setting block <FuncSETBLOCK> has the following format:
<FuncID><Len><FuncData>

Where:
<FuncID> is one byte identifying the setting(s) for the function.
<Len> is a one byte length count for the following 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.
<FuncSETBLOCK> are in the order of their Function ID<FuncID>

Where:

<STX>	02h
<S>	Indicates setting commands. 53h
<R>	Indicates read setting commands. 52h
<FuncID>	One byte Function ID identifies the particular function or settings affected.
<Len>	One byte length count for the following data block<FuncData>
<FuncData>	data block for the function
<ETX>	03h
<LRC>	LRC: The overall Modulo 2 (Exclusive OR) sum (from <STX> to <LRC>) should be zero.
<ACK>	06h
<NAK>	15h

6.2 General Commands

The SREDKey is shipped from the factory with the default settings already programmed.
In the following sections, the default settings are shown in **boldface**.
For a table of default settings, see Appendix A.
This group of configuration settings defines the basic operating parameters of SREDKey.

Enable/Disable Admin Key

Enable Admin Key
CMD: 02 30 8F 01 20 03 9F
OUT: 06

Disable Admin Key
CMD: 02 31 8F 01 20 03 9E
OUT: 06

Note: Admin Key Enabled is the Default

Change to Default Settings
Command: <STX><S><18h><ETX><LRC>
Response: <ACK> if OK, <NAK> if Error
This command does not have any <FuncData>. It returns most settings to their default values.

MSR Reading Settings
Command: <STX><S><1Ah><01h><MSR Reading Settings><ETX><LRC>
Response: <ACK> if OK, <NAK> if Error
Enable or Disable the SREDKey swipe reader. If the swipe reader is disabled, no data will be sent out to the host.

<MSR Reading Settings>:

0x30 MSR Reading Disabled
0x31 MSR Reading Enabled

MSR Swipe Direction Settings
Command: <STX><S><1Dh><01h><Option><ETX><LRC>
Responde : <ACK> if OK, <NAK> if Error

<Option>:

0x30 Raw Data Decoding in Both Directions.
0x31 Decode in Both directions.
0x32 Moving Stripe Along Head in Direction of Encoding.
0x33 Moving Stripe Along Head Against Direction of Encoding.

Review Settings
Command: <STX><R><1Fh><ETX><LRC>
Response <ACK> and <Response>
This command does not have any <FuncData>.

Security Level
Command: <STX><R><7Eh><ETX><LRC>
Response: <ACK> and <Response>
<Response>: <STX><7Eh><Len>< security level><ETX><LRC>
< security level>:
0x30 - Security level 1 No key injected and no encryption
0x31 - Security level 3 encrypted reader with key injected

Review Serial Number
Command: <STX><R><4Eh><ETX><LRC>

Response: <ACK> and <Response>
<Response>: <STX><4Eh><total length><Length of Serial Number>< Serial Number ><ETX><LRC>
This command is to get device serial number.

Preamble Setting
Command: <STX><S><D2h><Len><Preamble><ETX><LRC>
Response: <ACK> if OK, <NAK> if Error

Where:
<Len> is the number of bytes of preamble string
<Preamble> is {string length}{string}
Where, {string} is 0x20~0x7E.
Note: String length is one byte, maximum fifteen <0Fh>. **Default is 0x00.**

Postamble Setting
Command : <STX><S><D3h><Len><Postamble><ETX><LRC>
Response: <ACK> if OK, <NAK> if Error

Where:
<Len> is the number of bytes of postamble string
<Postamble> is {string length}{string}
Where, {string} is 0x20~0x7E, 0x0D(carriage return)
NOTE: String length is one byte, maximum fifteen <0Fh>. **Default is 0x00.**

Review KSN (DUKPT Key management only)
Command : <STX><R><51h><ETX><LRC>
Response: <ACK> and <Response>
<Response>: <ACK><STX><51h><Len of KSN>< KSN ><ETX><LRC>

This command is to review DUKPT key KSN.

Leading PAN digit to display
Command: <STX><S><49h><01h><N ><ETX><LRC>
Response: <ACK> if OK, <NAK> if Error

N: 00~06h, **default 04h**
First N Digits in PAN which can be clear data.

Trailing PAN digits to display
Command: <STX><S><4Ah><01h><M ><ETX><LRC>

Response: <ACK> if OK, <NAK> if Error

M: 00~04h, **default 04h**
Last M Digits in PAN which can be clear data.
MASKChar
Command: <STX><S><4Bh><01h><Maskcharactor ><ETX><LRC>
Response: <ACK> if OK, <NAK> if Error

maskcharactor: 20h~7Eh, **default 2Ah**
Set the mask character to for the PAN number in the output. The default is "*".

Encryption Settings
NOTE: AES/3DES can only be set once in factory. Once the encryption is turned on, the encryption method cannot be changed, otherwise it will return error code 15h 03h 01h.

Display Expiration Date
Command: <STX><S><50h><01h>< Expiration Settings><ETX><LRC>
Response: <ACK> if OK, <NAK> if Error

Expiration Settings:
0x30 Display expiration data as mask data
0x31 Display expiration data as clear data

Hash Option
Command: <STX><S><5Ch><01h>< Hash Settings><ETX><LRC>
Response: <ACK> if OK, <NAK> if Error
Hash Settings:
0x30 not send hash
0x31 send tk1 hash
0x32 send tk2 hash
0x33 send tk1 & tk2 hash
0x34 send tk3 hash
0x35 send tk1 & tk3 hash
0x36 send tk2 & tk3 hash
0x37 send tk1 & tk2 & tk3 hash
Note: The hash data will be all zeros to reserve the hash data space in output data, which is also called null hash data later.

Encryption Option Setting (for enhanced encryption format only)
Command: <STX><S><84h><01h><Encrypt Settings><ETX><LRC>
Responde : <ACK> if OK, <NAK> if Error

<Encrypt Settings>(0 – 0x1F)
bit0: 1 – track 1 force encrypt

bit1: 1 – track 2 force encrypt
bit2: 1 – forces encryption on track 3 and there would be no mask data
bit3: 1 – encrypt trk3 if card type 0
bit4 : 1 – encrypt trk3 if card type 0 only and allow trk1, trk 2, trk3 masked data to be sent as well.

Note:

1) When force encrypt is set, this track will always be encrypted, regardless of card type. No clear/mask text will be sent.
2) If and only if in enhanced encryption format, each track is encrypted separately. Encrypted data length will round up to 8 or 16 bytes.
3) When force encrypt is not set, non-bank card will be sent in clear text. For all type 0 cards (ABA/ISO bank cards) , all tracks will be encrypted.
4)Bit 2 is valaid for all type cards.
5) When bit4 is set to 1:
If bank card and track 3 is ISO-4909 with PAN format, T3 will have mask data.
If bank card and track 3 is not ISO-4909 without PAN format, T3 mask data can not be sent .

Typical settings:
1) 00 (**default**):
Bank card: All three tracks will be encrypted. T1 and T2 can have mask. If bank card and track 3 is ISO-4909 with PAN format, T3 will have mask data. If bank card and track 3 is not ISO-4909 without PAN format, T3 mask data can not be sent .
Non-bank card: Will be sent in clear text.

2) 07
Force encryption for all type cards. All three tracks will be encrypted without mask/clear,

2) 17
Bank card: All three tracks will be encrypted. T1 and T2 can have mask. If bank card and track 3 is ISO-4909 with PAN format, T3 will have mask data. If bank card and track 3 is not ISO-4909 without PAN format, T3 mask data can not be sent .
Non-bank card: All three tracks will be encrypted.

Swipe Encrypt Structure
Command: <STX><S><85h><01h><Encrypt Settings><ETX><LRC>
Response: <ACK> if OK, <NAK> if Error

<Encrypt Settings>:

0x30	original
0x31	enhanced

Note: setting will be different based different part numbers. For any new development, please choose the part number with enhanced format.

Manual Entry Encrypt Structure
Configuration byte 8F controls Keyed in options
Command: <STX><S><8Fh><01h>< Settings Option><ETX><LRC>
Responde : <ACK> if OK, <NAK> if Error

< Settings Option> :
0x00 Original manual entry format
0x01 Enhanced manual entry format
Note: Setting will be different based on different part numbers. For any new development, please use enhanced output.

Mask Option
Command: <STX><S><86h><01h>< Mask Settings><ETX><LRC>
Response: <ACK> if OK, <NAK> if Error

< Mask Settings>:
0x00 not send mask data
0x01 send mask trk1
0x02 send mask trk2
0x03 send mask tk1 & tk2
0z04 send mask trk3
0x05 send mask tk1 & tk3
0x06 send mask tk2 & tk3
0x07 send mask tk1 & tk2 & tk 3

Firmware Version
Command: <STX><R><22h><ETX><LRC>
Response : <ACK> <STX><firmware version string><ETX><LRC>
<firmware version>: For example,
ID TECH SREDKey USB HID KB Reader V 1.00

Serial Number Settings
Command: <STX><S><30h><01h>< Settings Option><ETX><LRC>
Response: <ACK> if OK, <NAK> if Error

< Settings Option>:
bit0-Level 3/4 Non-CC send as Level 1
bit1-Level3: No empty pkt when not enough sampling bits
bit2- Enhanced Secured Output will have SN after hash
Default is 04.

Get MiniFirmware Version(NGA Format)
Command: <02><03><00><78><46><31><0F><EF><03>
Response : <STX><Len_L> <Len_H><06h><minifirmware version><CheckLRC> <CheckSUM><ETX>

<minifirmware version>: For example,
ID TECH SREDKey USB HID KB Reader V 1.00.01

Get Model Number (NGA Format)
Command: <02><03><00><78><46><20><CheckLRC> <CheckSUM><03>
Response : <STX> <Len_L> <Len_H><06h>< model number><CheckLRC> <CheckSUM><ETX>
< model number>:

IDSK-534833AOB	USB-KB;AES;Original format;Black
IDSK-534833AEB	USB-KB;AES;Enhanced Encryption;Black
IDSK-534833TOB	USB-KB;TDES;Original format;Black
IDSK-534833TEB	USB-KB;TDES;Enhanced Encryption;Black

Restart Command(NGA Format)
Command: <02><03><00><78><46><CC><CheckLRC> <CheckSUM><03>
Response: <STX> <Len_L> <Len_H><06h><CheckLRC> <CheckSUM><ETX>

This command is to restart the device.

7 Data Output Format

SREDKey has the enhanced Magstripe reader and key in format as default.

<STX><DataLenL><DataLenH><Card Data><CheckLRC><CheckSum><ETX>

<STX> = 02h, <ETX> = 03h
<LenL><LenH> is a two byte length of <Card Data>.
<CheckLRC> is a one byte Exclusive-OR sum calculated for all <Card Data>.
<CheckSum> is a one byte sum value calculated for all <Card Data>.

7.1 ID TECH Swipe Data Original Encryption Output Format

ISO/ABA Card

0 STX (02)
1 Data Length low byte
2 Data Length high byte

3 Card Encode Type (note 1)
4 Track 1-3 Status (note 2)
5 T1 clear/mask data length
6 T2 clear/mask data length
7 T3 clear/mask data length
8 T1 clear/mask data
9 T2 clear/mask data
10 T3 clear/mask data
11 T1, T2, T3 encrypted data
12 20 bytes 0x00 (if T1 encrypted, T1 null hash data)
13 20 bytes 0x00 (if T2 encrypted, T2 null hash data)
14 20 bytes 0x00 (if T3 encrypted, T3 null hash data)
15 KSN (10 bytes)
16 CheckLRC
17 CheckSum
18 ETX (03)

- Field 10 Present only ISO-4909 card

Non-Financial Card

0 STX (02)
1 Data Length low byte
2 Data Length high byte
3 Card Encode Type (Section 7.5 note 1)
4 Track 1-3 Status (Section 7.5 note 2)
5 T1 clear data length
6 T2 clear data length
7 T3 clear data length
8 T1 clear data
9 T2 clear data
10 T3 clear data
11 CheckLRC
12 CheckSum
13 ETX (03)

7.2 ID TECH Swipe Data Enhanced Encryption Output Format

For the new development, please use enhanced encryption format.
ISO/ABA Card Data Output Format

Field	Field Description
0	STX (02)

1	Data Length low byte
2	Data Length high byte
3	Card Encode Type (Section 7.5 note 1)
4	Track 1-3 Status (Section 7.5 note 2)
5	T1 clear/mask data length
6	T2 clear/mask data length
7	T3 clear/mask data length
8	Mask data sent status (Section 7.5 note 3)
9	Encrypted/Hash data sent status (Section 7.5 note 4)
10	T1 clear/mask data
11	T2 clear/mask data
12	T3 clear/mask data
13	T1 encrypted data - (Track 1 encrypted data)
14	T2 encrypted data - (Track 2 encrypted data)
15	T3 encrypted data - (Track 3 encrypted data)
16	20 bytes 0x00 (if T1 encrypted and hash tk1 allowed, T1 null hash data)
17	20 bytes 0x00 (if T2 encrypted and hash tk2 allowed, T2 null hash data
18	20 bytes 0x00 (if T3 encrypted and hash tk3 allowed, T3 null hash data)
19	10 bytes serial number (if any track encrypted and serial number allowed)
20	KSN (10 bytes)
21	CheckLRC
22	CheckSum
23	ETX (03)

Non ISO/ABA Data Output Format

Field	Field Description
0	STX (02)
1	Data Length low byte
2	Data Length high byte
3	Card Encode Type (Section 7.5 note 1)
4	Track 1-3 Status (Section 7.5 note 2)
5	T1 unencrypted data length
6	T2 unencrypted data length
7	T3 unencrypted data length
8	Clear/mask data sent status *
9	Encrypted/Hash data sent status *
10	T1 clear data
11	T2 clear data
12	T3 clear data
13	CheckLrc
14	CheckSum
15	ETX (03)

Note:
- Field 10, 11, 12

For financial card, it will output mask data.
For non-financial card, it will output clear data.

- Field 19

If serial number is not set in the unit, this field should be padded with 0x30, and if the length of serial number is less than 10 bytes, 0x30 will be padded behind. The serial number will be sent out as default setting.

7.3 ID TECH Manual Entry Original Data Output Format

Field Usage Name
0 STX (0x02)
1 Data Length low byte
2 Data Length high byte
3 Card type always 85—keyed in (Section 7.5 note 1)
4 Always 0
5 Always 0
6 Always 0
7 Always 0
8 Status (1 byte) bit set if field is present in output (range 0-7)

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
0	0	0	0	SessionID	EXP	ADR	ZIP

9 The length of unencrypted field 10 (PAN=EXP=CVV)
10 Encrypted card data (max: 180 bytes) PAN=EXP=CVV
11 20 bytes 0x00 (Null hash data)
12 EXP one byte length+ASCII Expiration date (len: 1+4 bytes)
13 ADR one byte length+ASCII Street number (max: 1+20 bytes)
14 ZIP one byte length+ASCII Zip code (max: 1+10 bytes)
15 KSN (10 bytes)
16 CheckLrc
17 CheckSum
18 ETX (0x03)

Encrypted data sent status:

- Data Length low byte/high byte should be in length of characters.
- Data include encrypted card key-in PAN=EXP (YYMM) and 3-4 digit security code (CVV).
  The format should be:
  (Security level 3) PAN=YYMM=[CVV]

  Each field is separated by delimiter '=', this should always present even CVV is not keyed-in.
- Format of the fields: EXP, ADR and ZIP is:

1 byte field length in hex)	Data

The length byte ASCII not including length

7.4 ID TECH Manual Entry Enhanced Data Output Format

For the new development, please use enhanced encryption format.

Field Usage Name

0 STX (0x02)
1 Data Length low byte
2 Data Length high byte
3 Card Encode Type always C0 ABA format (Section 7.5 note 1)
4 Field 4 see description (0x17 track2 only) or 37 track 2 and track 3 (Section 7.5 note 2)
5 Always 00
6 Length of field 10 unencrypted manual input data PAN; EXP [and CVV]
7 Length of field 11 unencrypted manual input additional data ZIP and/or ADR
8 Field 8 see description (Section 7.5 Note 3)
9 Field 9 see description (Section 7.5 Note 4)
10 Keyed-in data presented as track-2—;PAN=EXP[:CVV]?LRC
11 Additional keyed-in data in ASCII presented as track 3 [1ADR=][0ZIP=]
12 Encrypted data of field 10
13 Null hash data (20 bytes 00)
14 Device serial number (10 bytes)
15 KSN (10 bytes)
16 LRC
17 Check Sum
18 ETX (0x03)

Note:

- Data Length low byte/high byte should be in length of characters.
- Field 11 includes encrypted PAN, EXP (YYMM) and 3-4 digit (CVV).
  The format should be:
  1) ;PAN=YYMM[:CVV]?LRC
     ';'—start sentinel
     '='—field separator between PAN and EXP
     ':'—field separator between EXP and CVV if there is a CVV
     '?'—end sentinel
- The format of the fields ADR and ZIP is:

1 byte field identifier '1'—ADR; '0'—ZIP	ASCII Data	field terminator '='

- Field 10 LRC—calculated track 2 longitudinal redundancy check from ';' to '?' This LRC is calculated on the data before conversion to ASCII as it would be

encoded on a card, so that the keyed-in data can be checked identically to the card data.

7.5 Notes

Note 1: Card Encode Type

Card Encode Type starts with 0: original encryption format
Card Encode Type starts with 8: enhanced encryption format

Value Encode Type Description
00 / 80 ISO/ABA format
01 / 81 AAMVA format
03 / 83 Other
04 / 84 Raw; un-decoded format
85 manual entry mode (default)
C0 manual entry mode (new)

Below is the method SREDKey reader uses to check the card encode type:

- ISO/ABA (American Banking Association) Card
  - Encoding method
    - Track1 is 7-bit encoding.
    - Track1 is 7-bit encoding. Track2 is 5 bits encoding. Track3 is 5-bit encoding.
    - Track1 is 7-bit encoding. Track2 is 5 bits encoding.
    - Track2 is 5-bit encoding.
    - If only track3 and it is 5 bit encoding, ISO4909 and has PAN
  - Additional checks
    - Track1 2nd byte is 'B'.
    - There is at least one '=' in track 2 and the position of '=' is between 12th ~ 20th character.
    - Total length of track 2 is above 19 characters.
    - Total of 4 digits after the separator character for expiration date or a second separator to indicate no expiration date
    - Card number range in PAN will be used to identify bank card.

- AAMVA (American Association of Motor Vehicle Administration) Card
  - Encoding method
    - Track1 is 7 bits encoding. Track2 is 5 bits encoding. Track3 is 7 bits encoding.
- Others (Customer card)

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

Note 3: Clear/mask data sent status
Field 8 (Clear/mask data sent status) and field 9 (Encrypted/Hash data sent status) will only be sent out in enhanced encryption 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 or additional data present (in manual entry mode)
Bit 3: 1—reserved for future use (always 0)
Bit 4: 0— TDES encryption; 1— AES encryption
Bit 5: 0— reserved for future use
Bit 6: 1—PIN Key encryption
Bit 7: 1— reader serial number present

Note 4: Encrypted/Null 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

7.6 Data Sample

The data sample below is encrypted with IDTECH demo key with TDES encryption method. SREDKey device is tested with USBKB interface.
Card Number: 5150 7102 0010 7903

Credit Card Swipe Original Format
028801001F372300%*5150********7903^PAYPASS/MASTERCARD^**********
?*;5150*****7903=***************?*F43947D860D5BCA3732EB67A2ECB
7CEF52644E3378CBBCB9509FF655F5E54B6C99519F0B79B785B94426C17D9427E7
DC9A10A8DFED4A45C3DC1A9CB6B339B3D8521BFC17F114BC8A2E8AF4819F75

3729726F98B9D311B9F250A0FACDE4A041ED00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000062994900000000000001181DD03

STX: 02
Data length low byte: 88
Data length high byte: 01
Card encode type: 00
Track 1-3 status: 1F
T1 length: 37=> 55 bytes in decimal
T2 length: 23=> 35 bytes in decimal
T3 length: 00
T1 clear/mask data(55 characters):
%*5150********7903^PAYPASS/MASTERCARD^****************?*
T2 clear/mask data(35 characters)
;5150********7903=****************?*
Track1&2 encrypted data(55+35 bytes=90 bytes => round up by 8=> 96 bytes):
F43947D860D5BCA3732EB67A2ECB7CEF52644E3378CBBCB9509FF655F5E54B6C99519F0B79B785B94426C17D9427E7DC9A10A8DFED4A45C3DC1A9CB6B339B3D8521BFC17F114BC8A2E8AF4819F753729726F98B9D311B9F250A0FACDE4A041ED
T1 Null hash: 0000000000000000000000000000000000000000
T2 Null hash: 0000000000000000000000000000000000000000
KSN: 62994900000000000011
LRC: 81
CheckSum: DD
ETX: 03

Decrypted Data:
%B5150710200107903^PAYPASS/MASTERCARD^090910140000631??;5150710200107903=0909101400006 31?0

Credit Card Swipe Enhanced Format
02A001801F372300839B%*5150********7903^PAYPASS/MASTERCARD^****************?*;5150********7903=****************?*2B52196519901212715ABADDA6DA18FDA5B50219A0FC9341BFB0633C3F33874FFE7B5F2B63897E0023710D5F6C6BF7BE8B937A515E3A7903182519B07422A5DFA329AF47F4B4728C5410105661B3DF35C0234582B983F7108771314DF807077D00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000030303030303030303030629949000000000000EBEEC03

STX: 02
Data length low byte: A0
Data length high byte: 01

Card encode type: 80
Track 1-3 status: 1F
T1 clear/mask data length: 37(hex) => 55 in decimal
T2 clear/mask data length: 23(hex) => 35 in decimal
T3 clear/mask data length: 00
Mask date sent status: 83
Encrypted data sent status: 9B
Track 1 clear/mask data(55 characters):
%*5150********7903^PAYPASS/MASTERCARD^****************?*
Track2 clear/mask data (35 characters):
;5150********7903=****************?*
T1 encrypted data (T1 length 55 rounded up by 8 => 56 bytes):
2B52196519901212715ABADDA6DA18FDA5B50219A0FC9341BFB0633C3F33874F
FE7B5F2B63897E0023710D5F6C6BF7BE8B937A515E3A7903
T2 encrypted data(T2 length 35 rounded up by 8 => 40 bytes):
182519B07422A5DFA329AF47F4B4728C5410105661B3DF35C0234582B983F710877
1314DF807077D
T1 Null hash: 0000000000000000000000000000000000000000
T2 Null hash: 0000000000000000000000000000000000000000
Serial Number: 30303030303030303030
KSN: 6299490000000000000E
LRC: BE
CheckSum: EC
ETX: 03

Decrypted Data:
Track1 Clear Data:
%B5150710200107903^PAYPASS/MASTERCARD^090910140000631??
Track2 Clear Data:
;5150710200107903=0909101400000631?0

Manual Entry Original Format
02840085000000000416780C3AF77E5CC55F1362DC46086A17EED23D053FD161CF
5F0000000000000000000000000000000000000000000043132313262994900000000000012
2B73303

STX: 02
Data length low byte: 84
Data length high byte: 00
Card Encode Type: 85
Always 0: 00
Always 0: 00
Always 0: 00
Always 0: 00

Status bit: 04
Length of unencrypted field 10 (PAN=EXP=CVV): 16 => 22 bytes in decimal
Encrypted Data (PAN=EXP=CVV) 22 bytes rounded up by 8 => 24 bytes:
780C3AF77E5CC55F1362DC46086A17EED23D053FD161CF5F
20 bytes Null: 0000000000000000000000000000000000000000
Length+ EXPDate: 0431323132
KSN: 62994900000000000012
CheckLRC: B7
CheckSum: 33
ETX: 03

Decrypted Data:
Data in ASCII Format
5150710200107903=1212=

Manual Entry Enhanced Format

02A600C0170018008292;5150********7903=****?*293C595E789A8E5EE184D379E
919F43A06A5911BDA9F90530000000000000000000000000000000000000000303030
303030303030306299490000000000000F035B03

STX: 02
Data length low byte: A6
Data length high byte:
Card Encode Type: C0
Track Status: 17 - Track 2 only
Field 5: Always 0
Length of Field 10: 18(hex) => 24(decimal)
Length of field 11 additional data ZIP and/or ADR: 00
Clear/Mask data status: 82
Encrypted/Hash data status: 92
Field 10 Clear/Mask data(10 characters):
;5150********7903=****?*
Encrypted field 10 data (24 rounded up by 8 => 24 bytes):
293C595E789A8E5EE184D379E919F43A06A5911BDA9F9053
Null hash data: 0000000000000000000000000000000000000000
Serial Number: 30303030303030303030
KSN : 6299490000000000000F
LRC: 03
CheckSum: 5B
EXT: 03

Encrypted Data:
293C595E789A8E5EE184D379E919F43A06A5911BDA9F9053

Decrypt data:
;5150710200107903=1212?

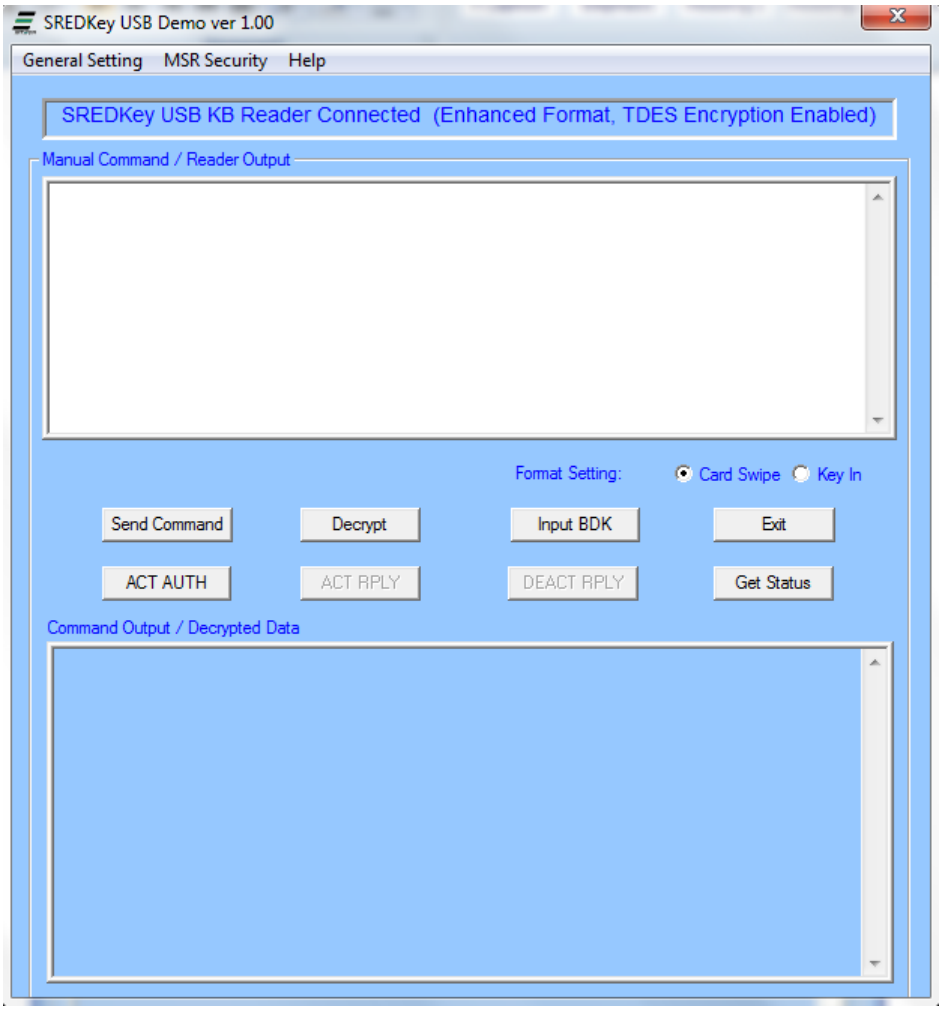
8 Demo Software

SREDkey demo software is available to demonstrate the MSR and keypad data decryption. Please see the below screenshots:

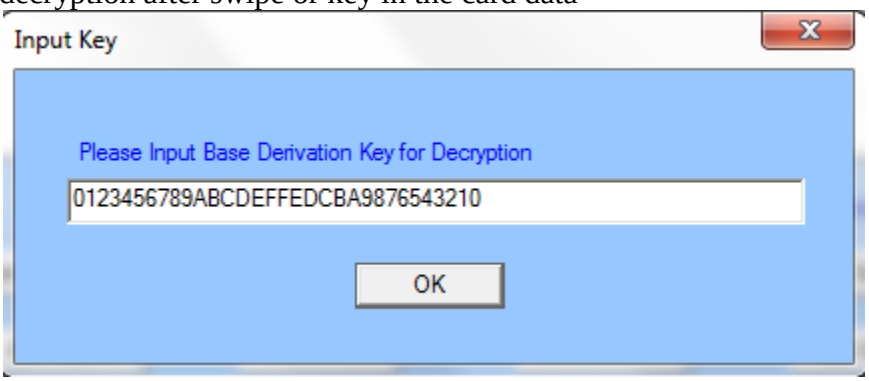
This demo software can be used for USB-HID or USB KB interface. For USB KB interface, please make sure the cursor is placed in the “manual command” window before swiping a card.

The following demo software screenshots are shown for reference and might not reflect the latest demo software version.

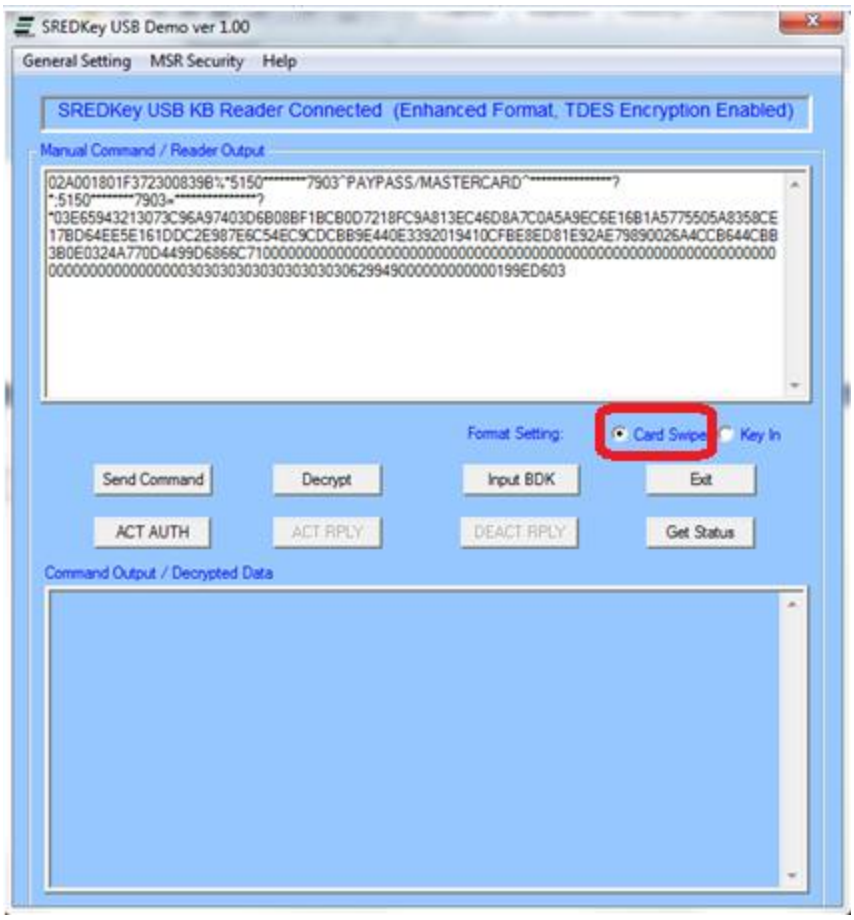
1. After plug in the SREDKey units to PC, it takes a few seconds to build the initialization between the software and SREDKey. After it’s done, the top bar on the demo software will show the units connected, encryption format and encryption method.



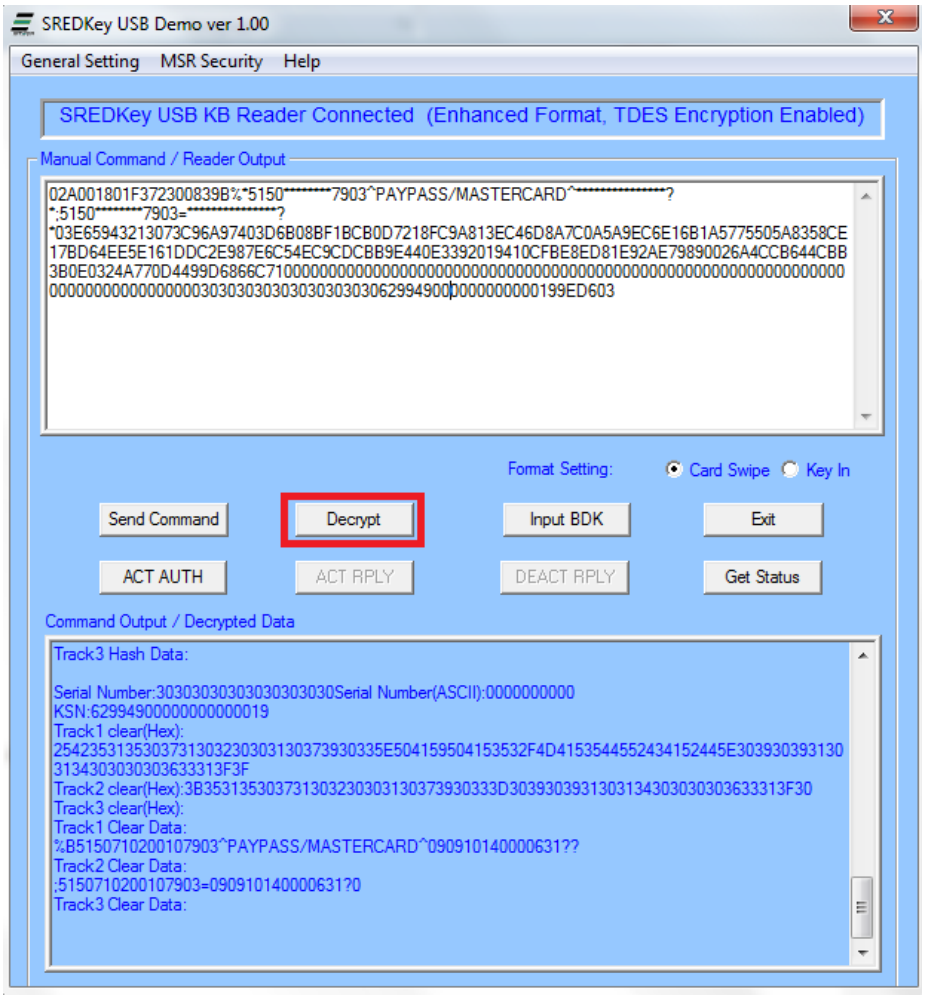
2. Input the BDK by clicking [Input BDK] button, and input the BDK to test decryption after swipe or key in the card data



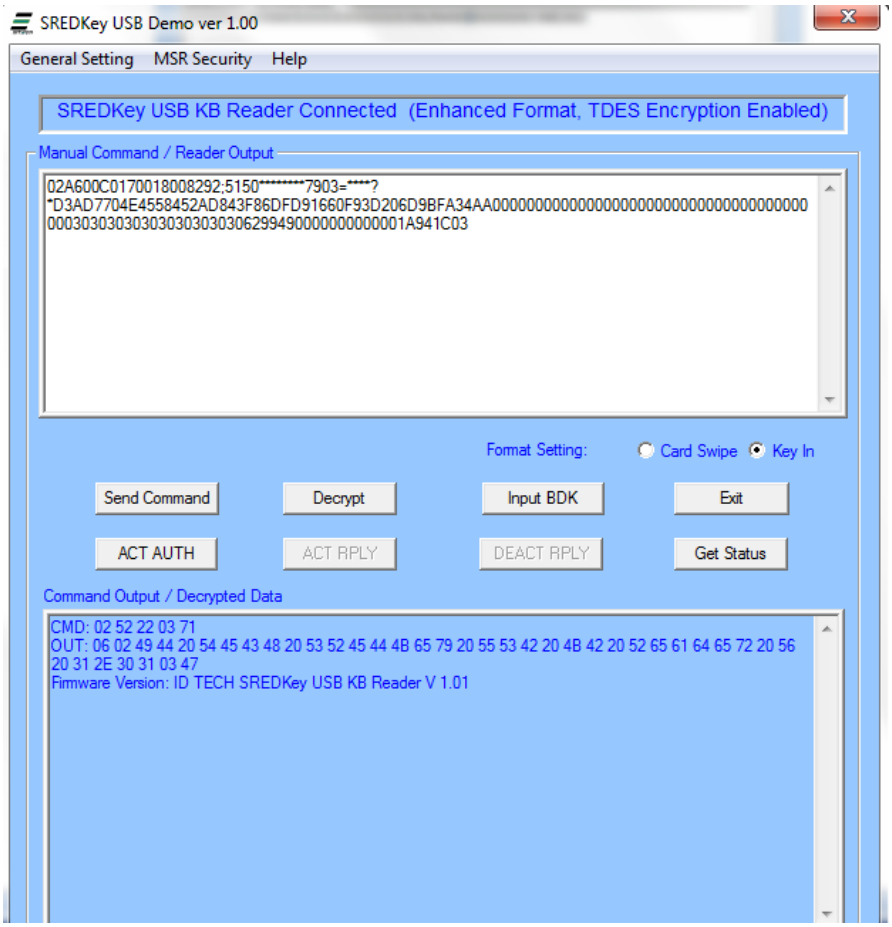
3. Swipe card
   Before swipe card, please double check the radio button [Card Swipe] is selected within the red box below.



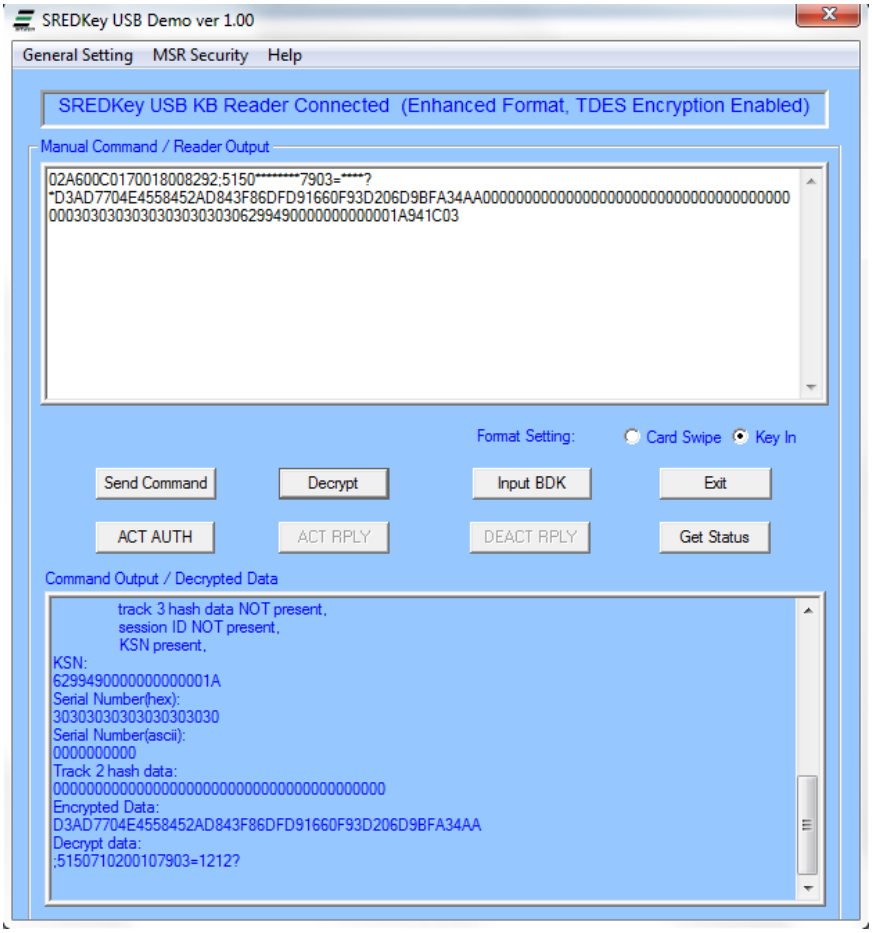
Click the [decrypt] button, the decrypted data will show in the lower window in the demo.



4. Key-in data
   Delete the swipe data in the upper window. Select the [Key In] radio button to switch to key-in format.

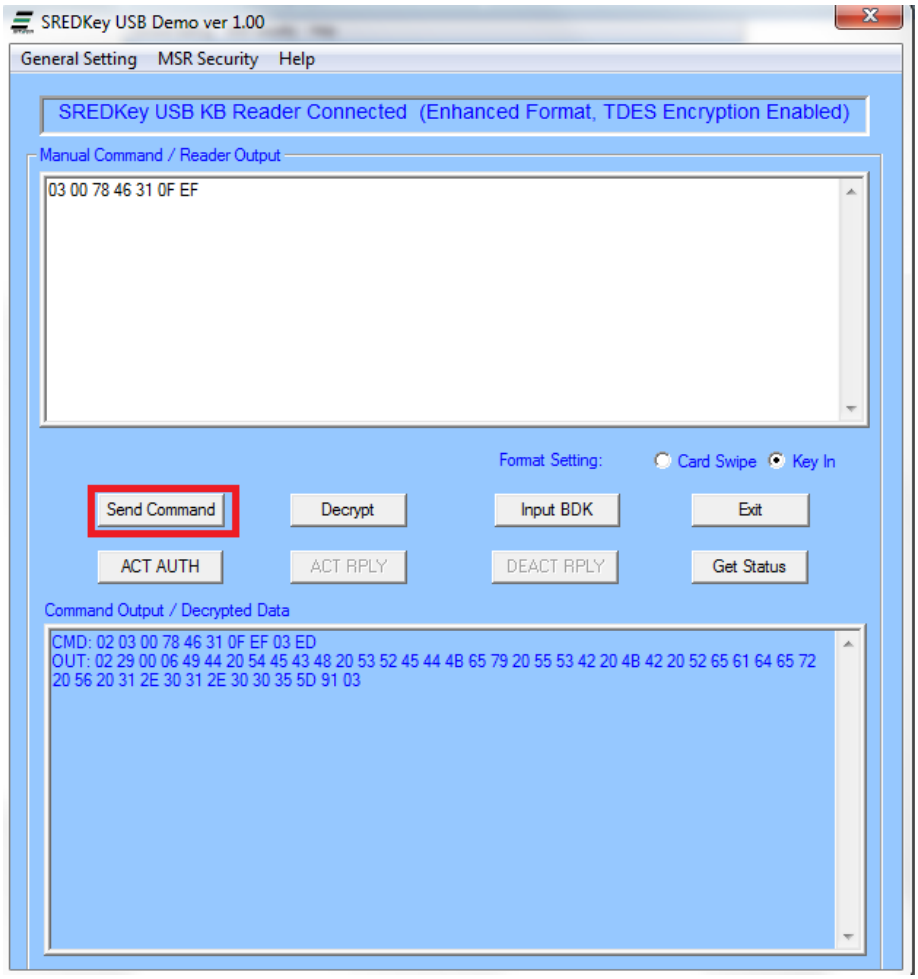


Click the [Decrypt] button.



5. Send command
   Typing in the command in the upper window excluding the STX, EXT and LRC in the upper windows, then click [Send Command] button.

   For example, send command to get the mini firmware version from device.



6. Other settings
   By click [General settings] on the top bar of the demo, there are a couple of options to change the settings or get the settings from SREDKey device.

Appendix A Setting Configuration Parameters and Values

Following is a table of default setting and available settings (value within parentheses) for each function ID.

Function ID	Hex	Description	Default Setting	Description
TrackSelectID	13	Track Selection	**‘0’**	Any Track 0-any
PollingIntervalID	14	Polling Interval	1 (1 ~ 255)	USB HID Polling Interval
TrackSepID	17	Track Separator	**0x0D=CR/Enter**	CR for RS232, Enter for KB any character supported except 00 which means none.
MSRReadingID	1A	MSR Reading Setting	‘1’ (‘0’, ‘1’)	‘0’ MSR Reading Disabled **‘1’ MSR Reading Enabled**
DecodingMethodID	1D	Decoding Direction	‘1’ (‘0’~’3’)	Reading Direction 0x30 – Raw Data Decoding in Both Directions. 0x31 – Decode in Both directions. 0x32 – Moving Stripe Along Head in Direction of Encoding. 0x33 – Moving Stripe Along Head Against Direction of Encoding.
ReviewID	1F	Review All Settings	None	
TerminatorID	21	Terminator	0x0D (any)	CR for RS232, Enter for KB; ‘0’ for CRLF
FmVerID	22	Firmware Version	None	
ForeignKBID	24	Foreign KB	'0' ('0' ~0x3A)	Foreign Language Keyboard Allowable options are: US 0x30 SWISS 0x31 SWEDISH 0x32 SPANISH_MEX 0x33 NORWAY 0x34 ITALIAN 0x35 GERMAN 0x36 FRENCH 0x37

				JAPAN 0x38 UK 0x39 UNIVERSAL 0x3A
USBHIDFmtID	23*	USB HID Fmt (HID rdr only)	‘8’ (‘0’, ‘8’)	‘0’ ID TECH Format; ‘8’ HIDKB format
CustSetID	30	Custom Customer Settings	04(00 - 07)	bit0-Level 3/4 Non-CC send as Level 1 bit1-Level3: No empty pkt when not enough sampling bits bit2- Enhanced Secured Output will have SN after hash
Track1PrefixID	34	Track 1 Prefix	0 (any string)	No prefix for track 1, 6 char max
Track2PrefixID	35	Track 2 Prefix	0 (any string)	No prefix for track 2, 6 char max
Track3PrefixID	36	Track 3 Prefix	0 (any string)	No prefix for track 3, 6 char max
Track1SuffixID	37	Track 1 Suffix	0 (any string)	No suffix for track 1, 6 char max
Track2SuffixID	38	Track 2 Suffix	0 (any string)	No suffix for track 2, 6 char max
Track3SuffixID	39	Track 3 Suffix	0 (any string)	No suffix for track 3, 6 char max
KeyTypeID	3E*	data or pin key	0	0-data key; 5A-pin key
PrePANID	49	PAN to not mask	4 (0-6)	# leading PAN digits to display
PostPANID	4A	PAN to not mask	4 (0-4)	# of trailing PAN digits to display
MaskCharID	4B	mask the PAN with this character	‘*’ 20-7E	any printable character
CrypTypeID	4C*	encryption type	‘1’ (‘1’-‘2’)	‘1’ 3DES ‘2’ AES
SerialNumberID	4E*	device serial #	any 8-10 bytes	8-10 digit serial number; Can be set only once
DispExpDateID	50	mask or display expiration date	'1"0'-'1'	‘0’ mask expiration date; ‘1’ display expiration date
SessionID	54	8 byte hex	None	always init to all ‘0xFF’
Mod10ID	55	include mod10 check digit	'0' ('0'-'2')	**‘0’ don’t include mod10,** ‘1’ display mod10, ‘2’ display wrong mod10
HashOptID,	5C		'7' (‘0’-‘7’)	Send tk1-2 hash bit 0:1 send tk1 hash; bit 1:1 send tk2

				hash; bit2:1 send tk3 hash.
T17BStartID	61	Track 1 7 Bit Start Char	**'%' (any)**	'%' as Track 1 7 Bit Start Sentinel
T15BStartID	63	T15B Start	**';' (any)**	';' as Track 1 5 Bit Start Sentinel
T27BStartID	64	Track 2 7 Bit Start Char	**'%' (any)**	'%' as Track 2 7 Bit Start Sentinel
T25BStartID	65	T25BStart	**';' (any)**	';' as Track 2 5 Bit Start Sentinel
T37BStartID	66	Track 3 7 Bit Start Char	**'%' (any)**	'%' as Track 3 7 Bit Start Sentinel
T35BStartID	68	T35BStart	**';' (any)**	';' as Track 3 5 Bit Start Sentinel
T1EndID	69	Track 1 End Sentinel	**'?' (any)**	'?' as End Sentinel
T2EndID	6A	Track 2 End Sentinel	**'?' (any)**	'?' as End Sentinel
T3EndID	6B	Track 3 End Sentinel	**'?' (any)**	'?' as End Sentinel
T1ERRSTARTID	6C	Track 1 error code	**'%' (any)**	start sentinel if track 1 error report
T2ERRSTARTID	6D	Track 2 error code	**';' (any)**	start sentinel if track 2 error report
T3ERRSTARTID	6E	Track 3 error code	**'+' (any)**	start sentinel if track 3 error report
SecureLrcID	6F	Secured output format track LRC option enhanced only	'1' ('0'-'1')	'1' to send track LRC in secured output data; '0' don't send track LRC Note: This command is valaid for level1
SyncCheckID	7B	check for track sync bits-can allow poorly encoded cards to be read	'2' ('0'-2')	check leading & trailing sync bits '0' 13 bits; '1' 13 bits, but allow if valid through track LRC; '2' 9 bits ABA; 13 bits IATA; 16 bits JIS
SecurityLevelID	7E*	Reader's encryption level	'1' or '3' ('0'-'4')	'1' no encryption; '2' key loaded; '3 encrypted reader; '0' DUKPT exhausted; '4'
EncryptOptID	84	encryption options, enhanced only	**0** encrypt card type 0; (0-1F)	bit 0: encrypt trk1; bit 1: encrypt trk2; bit 2: forces encryption on

				track 3 and there would be no mask data. It is valid both for Non – CC and card type 0; bit 3: encrypt trk3 if card type 0;; bit 4: encrypt trk3 if card type 0 only and allow trk1, trk 2, trk3 masked data to be sent as well.
EncryptStrID	85*	encrypt structure	'1'	'0' original; '1' enhanced
MaskOptID	86	clear / mask data options	7	bit 0: send clear/mask trk1 bit 1: send clear/mask trk2 bit 2: send clear/mask trk3
T3ExpDatePosID	89	expire date position	**0x34** (0x34, 0x36)	track 3 expiration date position offset
AdminLvlID	8E	Admin Level	**B,** 15, 1F, 29, 33, 3D	B-Admin 1; 15-Admin 2; 1F-Admin 3; 29-Admin 4' 33-Admin 5; 3D-Admin 6
KeyedOptID	8F*	Keyed Options	0	**bit 0:** if 0: output in original keyed output if 1: output in enhanced keyed-in output **bit 1:** if 0: allow empty CVV entry if 1: require 3 or more CVV digits **bit 2:** if 0: allow empty ZIP entry if 1: require 5 or more ZIP digits **bit 3:** if 0: allow empty ADR entry if 1: require 1 or more ADR digits **bit 4:** if 0: do mod-10 check on keyed-in PAN if 1: don't check PAN mod-10

				bits 5-7: reserve all zero **bits 5:** if 0: Admin Key Enabled if 1: Admin Key Disabled **bits 6-7:** all zero; reserved for future use
Non-fincilEncryptOptID	90*	Non-financial card encrypt options	'0'	'0' non –financial card output plaintext at level 3. '1' non –financial card output as financial card at level 3
SetDeviceColorID	91*	Set device color	'0'	'0' black '1' red
Equip2ID	AE*	special settings	special settings	If bit 4 is high, then send serial number during enumeration
PrefixID	D2	Preamble	0 (any 15)	No Preamble, 15 char max
PostfixID	D3	Postamble	0 (any 15)	No Postamble, 15 char max

* These settings do not change with a default all command.