SREDKey 2
Integration Manual

80172501- 001 Rev. J

22 February 2024

ID TECH
10721 Walker Street, Cypress, CA 90630
Voice: (714) 761-6368 Fax: (714) 761-8880
idtechproducts.com

Warranty Disclaimer

The services and hardware are provided "as is" and "as-available" and the use of the services and hardware are at its own risk. ID TECH does not make, and hereby disclaims, any and all other express or implied warranties, including, but not limited to, warranties of merchantability, fitness for a particular purpose, title, and any warranties arising from a course of dealing, usage, or trade practice. ID TECH does not warrant that the services or hardware will be uninterrupted, error-free, or completely secure.

Table of Contents

1. Introduction

ID TECH's SREDKey 2 is an encrypting keypad with an LCD and is available either with an encrypted MagStripe reader and without. The SREDKey 2 is a reliable security solution that meets PCI PTS 5.X perfect for a P2PE environment. This device delivers superior reading performance while encrypting sensitive MagStripe and keyed-in data reducing PCI-DSS scope.

2. Acronyms Used and Applicable Documents

ANSI	American National Standard Institute
ESD	Electrostatic Discharge
HOST	A Personal Computer or Similar Computing Device
ISO	International Standards Organization
USB	Universal Serial Bus
AAMVA	American Association of Motor Vehicle Administrators
SREDKEY	Secure Reading and Exchange of Data

ISO/IEC 7813: The general requirements standards are identification cards and physical characteristics.
ISO/IEC 7811: The general requirements standards are identification cards, recording techniques, and magnetic stripe.

3. Features

- Encrypted numeric keypad with 2.9" (diagonal) LCD and optional encrypted MSR
- 1,000,000 swipes: 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 PTS 5.X certified with SREDKey 2 function supported
- ROHS 2 and REACH certified
- Secure mounting option
- TDES/AES with DUKPT Key Management
- MSR support Track1,2,3 reading
- MSR support ISO 7810 and 7811-1 through -6 cards. Reads AAMVA driver license cards
- Battery Life of 5-Years
- **Operating Temperature**: 32° F to 131° F (0° C to 55° C) non-condensing
- **Storage Temperature**: -4° F to 149° F (-20° C to 65° C) non-condensing

4. Specifications

Physical	
Length	160.4mm
Width	96.7mm
Height	37.4mm
Weight	310g
Environmental	
Operating Temp	-10°C to 55°C non-condensing
Storage Temp	-20°C to 65°C non-condensing
Humidity	Maximum 90% non-condensing
Electrical	
Input	5V USB connection
Working	100 mA
Sleep	2mA
Screen	
Resolution	240x64
Size	2.9" diagonal

5. Base Functionality and Operations

When the SREDKey 2 is powered on it enters **Data Capture Mode**, prompting a user to key-in data.

If the SREDKey 2 has not been injected with a key and encryption is not enabled, it displays "Missing Transaction Keys" after the user presses any key. Evaluation units come injected with the ID TECH demo key by default, and data can be decrypted using ID TECH's Universal SDK DEMO.

5.1. Function Key Operation

- Left Arrow key ← Clicking the ← (backspace) key allows users to remove entered data one character at a time.
- **#Admin**: Clicking the **#Admin** key when the screen displays "Swipe or Hand-Key Card Number" or "Enter Card Number then press Enter" allows users to enter the **Admin Menu**. Clicking the **#Admin** key in other screens puts the device in the **Help** Mode.
- **Cancel**: Clicking the **Cancel** key once allows the users to remove all the input in the current and previous levels. The device then returns to the previous prompt for the current transaction. When the **Cancel** key is pressed twice, the current transaction is cancelled, and the device goes back to the initial mode.

Note: See Enabling and Disabling the SREDKey 2 Admin Key for instructions on turning the Admin key on and off.

5.2. Admin Menu

To select one of six manual entry modes, click the **Admin** key and the screen will display "Select manual config 1-6".

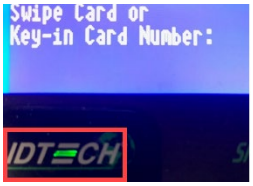
5.3. Manually Keyed Configuration Operations

Configuration #1: Card Number, Expiration Date
Configuration #2: Card Number, Expiration Date, Zip
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

5.4. SREDKey 2 LED Behavior

SREDKey 2 units have an LED below the LCD screen that indicates device status.

Device State	
Unit Ready	●
Unit Tampered	● Flashing
Unit Missing Transaction Key	●



5.5. Tamper and Failed Self-Check Indicators

The SREDKEY 2 displays the following indicators when it has been tampered or has any of the other following internal issues, such as an expired certificate, missing key, or similar fault discovered during a self-check.

Indicator	Tampered Status	Other Issue Status
LED Indicator	Red LED	Amber LED: no DEK
LCD Display Message	The screen's top line reads "Tampered" and indicates the source of the tampering on the bottom line.	If FW is downloaded at first time, show "Deactivated" If device is activated, but no LCL-KEK, show "Activated" If LCL-KEK exist but no DEK, show "Need client key"

The SREDKEY 2's LCD display can indicate the following issues in the event of a failed self-check:

- "Deactivated" indicates the reader has firmware but is not activated.
- "Activated" indicates the reader is activated but does not have an LCL-KEK.
- "Need client key" indicates the reader has an LCL-KEK, but no DEK.

6. Firmware Command Structure

The following are commands sent to keypad/reader:

- **Setting Command**: <STX><S>[<FuncID><Len><FuncData>…] <ETX><LRC>
- **Read Status Command**: <STX><R><FuncID><ETX><LRC>
- **Function Command**: <STX>[<FuncID><Len><FuncData>…] <ETX><LRC>

6.1. Response from SREDKey 2

Setting Command		
Host **Setting command**	→ ← or ←	SREDKey 2 <ACK> if OK <NAK> if Error
Read Status Command		
Host **Read Status command**	→ ← or ←	SREDKey 2 <ACK> and <Response> if OK <NAK> if Error
Other Commands		
Host **Other command**	→ ← or ←	SREDKey 2 <ACK> and <Response> if OK <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 <FuncData> function-setting block.
- <FuncData> is the current setting for this function. It has the same format as the function's sending command.
- <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>	The overall Modulo 2 (Exclusive OR) sum (from <STX> to <LRC>) should be zero
<ACK>	06h
<NAK>	15h

7. General Commands

SREDKey 2 devices use commands from both the NEO 2 and NGA protocols. SREDKey 2 devices come equipped with the default settings already programmed. See Appendix A for a table of default settings.

7.1. IDG Protocol Commands

The following commands use IDG Protocol.

IDG Protocol Command Structure

Command: <Command head><Command data><Sub command data><Length-H><Length-L><Data><CRC-L><CRC-H>
Response: <Command Head><Command data><Status code><Length-H><Length-L><Data><CRC-L><CRC-H>

Where:

- Command head is 10 bytes, including ASCII string "ViVOtech2" and 1 byte "0x00."
- Command data and Sub command data are all 1 byte.
- Length-H and Length-L describe the length value of Data.
- CRC-L and CRC-H is the calculated result data from Command Head to Data by CRC16-CCITT algorithm.

7.1.1. Get Firmware Version (29-00)

The **Get Firmware Version** command retrieves the ViVOpay firmware version number from the SREDKey 2. The SREDKey 2 returns a response frame containing the firmware version information.

Command: <ViVOtech2\0><81h><0Ch><00h><00h><CRC-L><CRC-H>
Response: <ViVOtech2\0><81h><00h><Length-H><Length-L><Key status><CRC-L><CRC-H>

7.1.2. Get Key Status (81-0C)

The **Get Key Status** command retrieves basic key information. Each pair of three bytes represents one key's parameters (index and slot).

Command: <ViVOtech2\0><81h><0Ch><00h><00h><CRC-L><CRC-H>
Response: <ViVOtech2\0><81h><00h><Length-H><Length-L><Key status><CRC-L><CRC-H>

Where:

- Key status is multi blocks, to show the key status.
- Each block contains: 1-byte Key name index, 2-byte key slot.
- The SREDKey 2 has LCL-KEK(0x14), Data Encryption Key(0x02).

For example, `0x02 0x00 0x00 0x02 0x00 0x01` represents `[KeyIndex=0x02,KeySlot=0x0000]` and `[KeyIndex=0x02,KeySlot=0x0001]`

7.1.3. Reboot Device (77-05)

The **Reboot Device** command immediately reboots the reader.

Command: <ViVOtech2\0><77h><05h><00h><00h><CRC-L><CRC-H>
Response: <ViVOtech2\0><77h><00h><00h><00h><CRC-L><CRC-H>

7.1.4. Set TransArmor Cert Data (C7-50)

The **Set TransArmor Cert Data** command sets the TransArmor Cert data for TransArmor RSA encryption functionality.

Command: <ViVOtech2\0><C7h><50h><TransArmor Cert data><CRC-L><CRC-H>
Response: <ViVOtech2\0><C7h><00h><00h><00h><CRC-L><CRC-H>

The Cert data is ASN.1 format.

7.1.5. Set TransArmor ID (C7-51)

The **Set TransArmor ID** command sets the TransArmor ID. The TransArmor ID must be 8 bytes (0x20 – 0x7F).

Command: <ViVOtech2\0><C7h><51h><Length-H><Length-L><TransArmor ID data><CRC-L><CRC-H>
Response: <ViVOtech2\0><C7h><00h><00h><00h><CRC-L><CRC-H>

The Length value is always 8. The TransArmor ID data should be ASCII code.

7.1.6. Get TransArmor ID (C7-52)

The **Get TransArmor ID** command retrieves the TransArmor ID data for TransArmor RSA encryption functionality.

The Length value is always 8. The TransArmor ID data should be ASCII code.

Command: <ViVOtech2\0><C7h><52h><00h><00h><CRC-L><CRC-H>
Response: <ViVOtech2\0><C7h><00h><Length-H><Length-L><TransArmor ID data><CRC-L><CRC-H>

7.2. NGA Protocol Commands

The following commands follow NGA Protocol.

NGA Protocol Command Structure

```
<STX><Len-Low><Len-High><Command Body / Response Body / Notification Body><Command Data><CheckLRC><CheckSUM><ETX>
```

Where:

- **<Len_Low><Len_High>:** Length of <Command Body / Response Body / Notification Body>
- **<CheckLRC>:** LRC of <Command Body / Response Body / Notification Body>
- **<CheckSUM>:** SUM of <Command Body / Response Body / Notification Body>
- **Response Body:** <Response Status> + [<Response Data>]
    - **<Response Status>:** Status of the response. 1 byte.
        - NAK: 0x15
        - ACK: 0x06
    - **<Response Data>:** Main response string.
        - If <Response Status> is ACK, several bytes needed.
        - If <Response Status> is NAK, response data is error codes (2 bytes).

7.2.1. Get Model Number (78 46 20)

The **Get Model Number** command retrieves the SREDKey 2's model number.

Command Body: 78 46 20
Response: 06 <Model Number>

Where:

- Model Number is several bytes of ASCII code; for example: "SREDKey2-xxxx."
- The Model Number must be set before it can be read; see the **Set Model Number** command.

7.2.2. Get Detailed Firmware Version (78 46 31)

The **Get Detailed Firmware Version** command retrieves the SREDKey 2's detailed firmware version.

Command Body: 78 46 31
Response: 06 <TM4 Firmware version information>

The detail firmware version is in *X.YY.ZZZ* format.

7.2.3. Reboot Device (78 46 CC)

The **Reboot Device** command immediately reboots the reader.

Command Body: 78 46 CC

Response: 06

7.2.4. Reset Device (C7 80): HID Mode

The **Reset Device** command resets the SREDKey 2 to factory default settings. Note that this command is irreversible and that device administrators must reconfigure the reader after sending this command.

Command Body: C7 80
Response: C7 00 00 00

7.3. ITP Protocol Commands

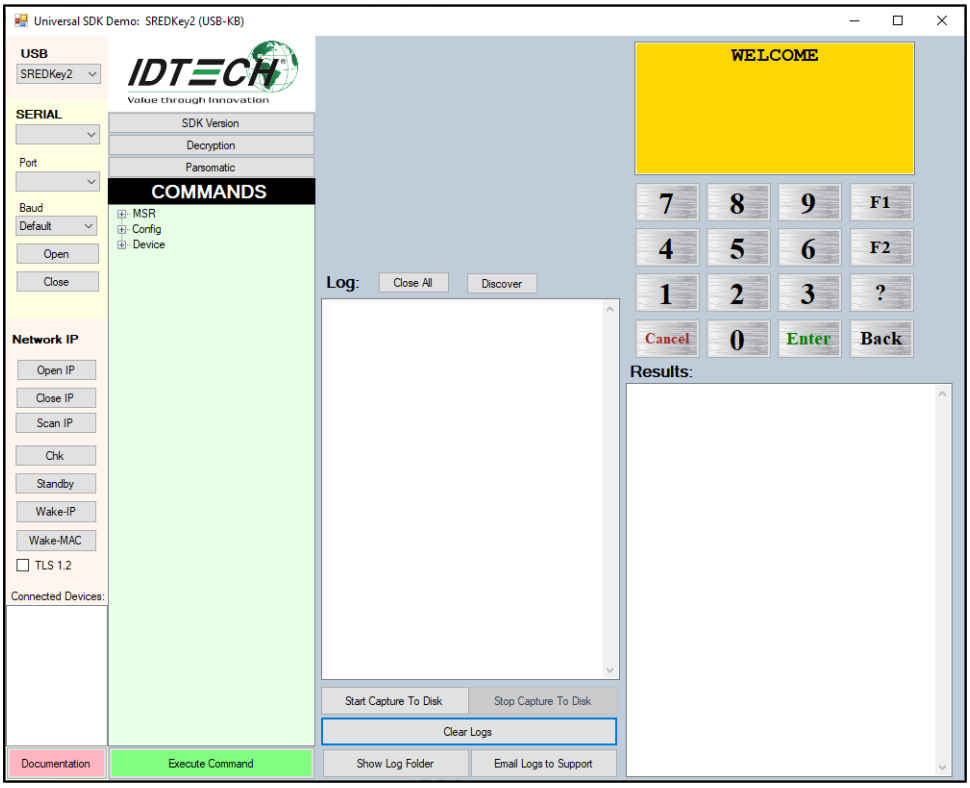
7.3.1. Reset Device (53 18): KB Mode

The **Reset Device** command resets the SREDKey 2 to factory default settings. Use this command in Keyboard Mode. Note that this command is irreversible and that device administrators must reconfigure the reader after sending this command.

Command Body: 53 18
Response: 06

8. Using the SREDKey 2 and USDK Demo Application

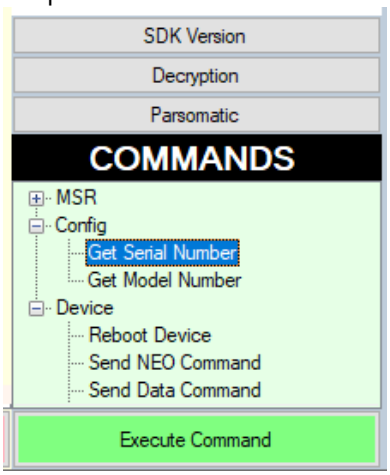
The Universal SDK Demo application is available to demonstrate SREDKey 2 **MSR** and **Keypad Data Decryption**. SREDKey 2 devices can connect to the USDK Demo app via either **USB-HID** or **USB KB Interface**. For **USB KB Interface**, make sure to place the cursor in the **Manual Command** window before swiping a card.



Note that screenshots below are for reference and may not reflect the latest software update. Screenshots may also be cropped for space.

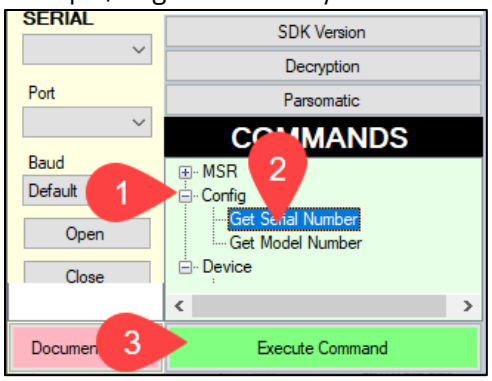
8.1. Using the Universal SDK Demo Application

Each **Command** section offers a drop-down list of sub-sections for obtaining, testing, or editing information for device status or development.



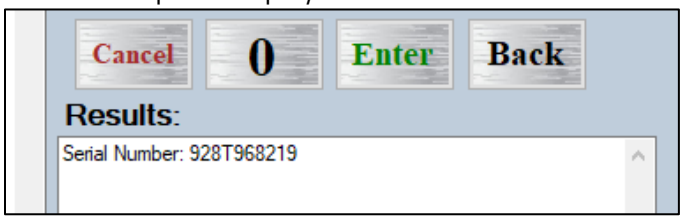
To use a command, open the **Command** tree and double-click the desired command or select a command and click **Execute.** Data displays in the **Log** panel and device results in the **Results** panel.

For example, to get a SREDKey 2's serial number:



1. Click **Config**
2. Click **Get Serial Number**
3. Click **Execute Command**.

The **Results** panel displays the device's serial number.

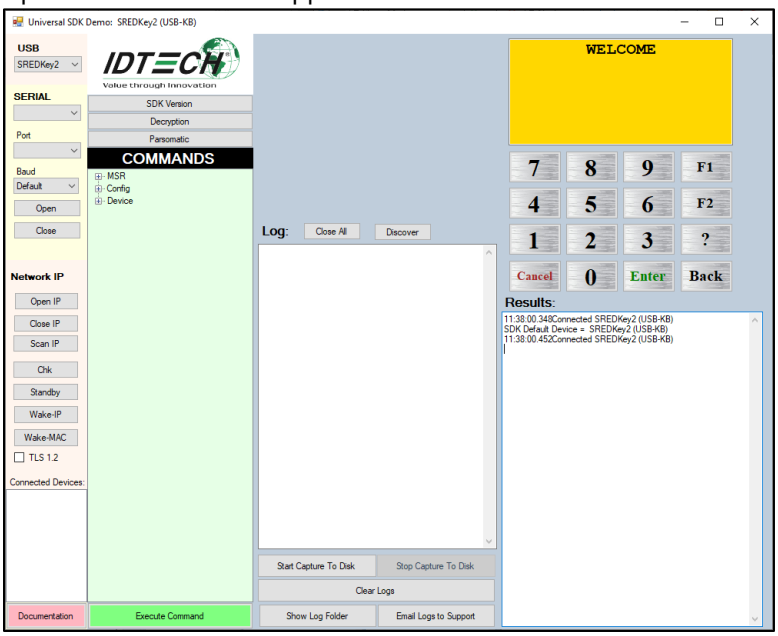


8.2. Updating SREDKey 2 Firmware

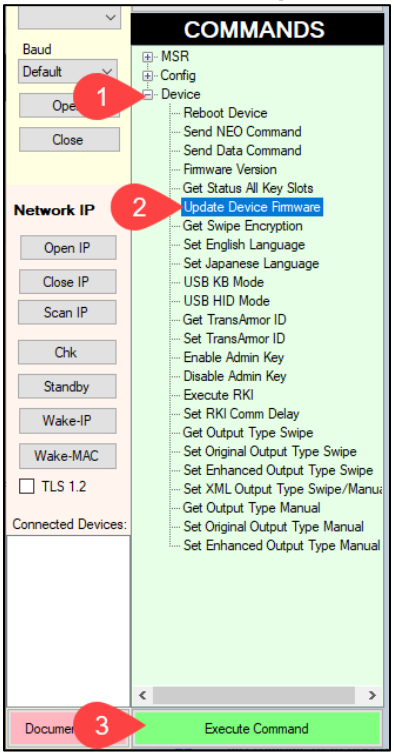
The steps below describe the process for updating SREDKey 2 firmware via the Universal SDK Demo app.

Note: Before you begin, contact your ID TECH representative to receive the most recent SREDKey 2 firmware. Download the ZIP file and extract it to your computer.

1. Connect the SREDKey 2 to your PC via USB cable.
2. Download and install the latest USDK Demo app from the ID TECH Knowledge Base (if you cannot access the link, please contact support).
3. Open the USDK Demo app from the Windows Start menu.



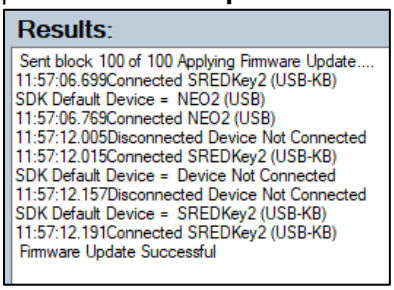
4. Under **Device**, select **Update Device Firmware**, then click **Execute Command**.



5. Navigate to and select the SREDKey 2 firmware file you downloaded earlier and click **Open**.
6. The SREDKey 2 reboots and enters the bootloader, at which point the SDK demo begins updating the device.

Note: The firmware update may take several minutes to complete

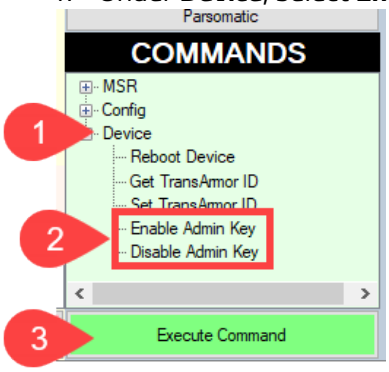
7. When the firmware update completes, the SREDKey 2 reboots again and the USDK Demo app prints **Firmware Update Successful** in the **Results** panel.



8.3. Enabling and Disabling the SREDKey 2 Admin Key

To enable or disable the Admin key:

1. Under **Device**, select **Enable Admin Key** or **Disable Admin Key**, then click **Execute Command**.

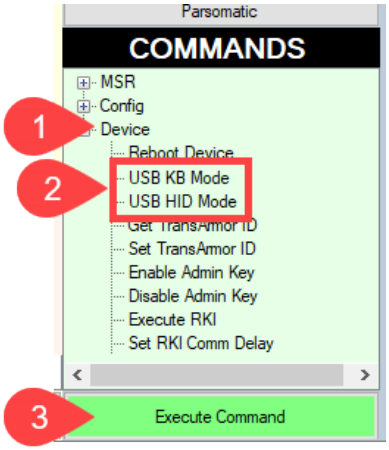


The USDK Demo app displays "Admin Key Enabled" (or disabled) in the **Results** panel.

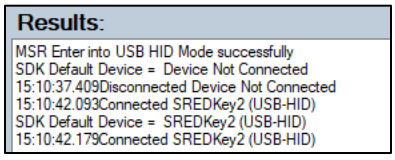
8.4. Switching a SREDKey 2 Between USB-KB and USB-HID Modes

To switch the SREDKey 2 between USB-KB and USB-HID modes:

1. Under **Device**, select the desired mode, then click **Execute Command**.

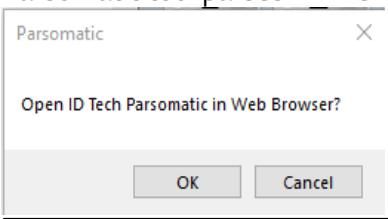


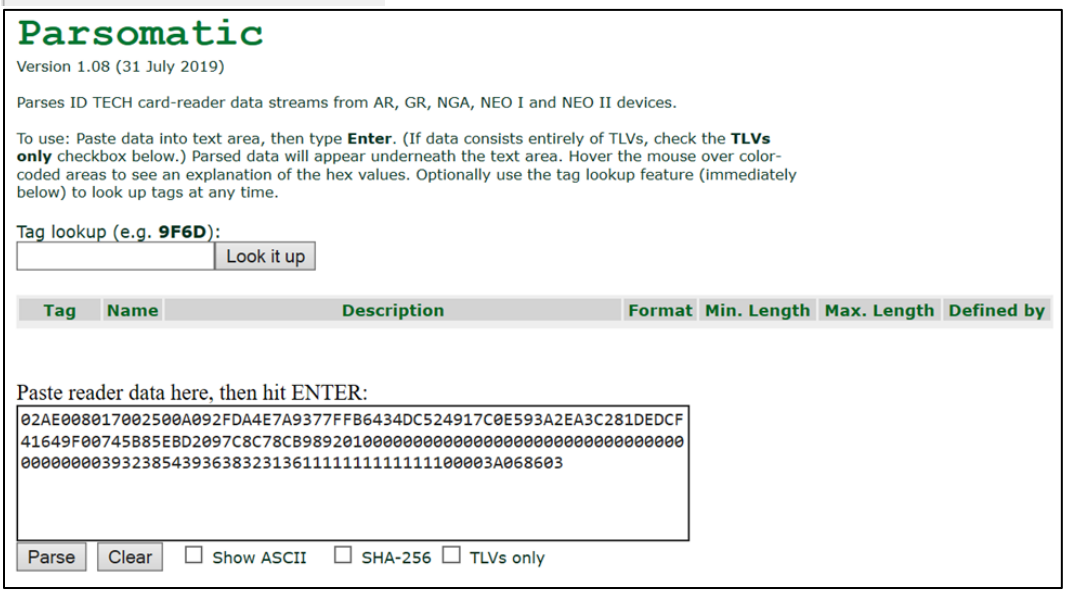
The USDK Demo app reboots the SREDKey 2; when the device reboots, the **Results** panel displays the selected USB mode:



8.5. Testing a SREDKey 2 Device

1. Connect the SREDKey 2 to the computer.
    a. If necessary, make sure the SREDKey 2 is in USB-KB mode; this setting allows the reader to directly populate Parsomatic.
2. Click **Parsomatic** and **OK** to open the ID TECH Parsomatic page in a web browser. The Parsomatic tool parses ID TECH card-reader data streams.





3. Click **Clear** at the bottom of the Parsomatic screen.
4. Keep the Parsomatic window open and swipe the demo card through the SREDKey 2; the data from the reader will populate the reader data field.
5. Click **Parse** to display the demo card's information parsed for readability.

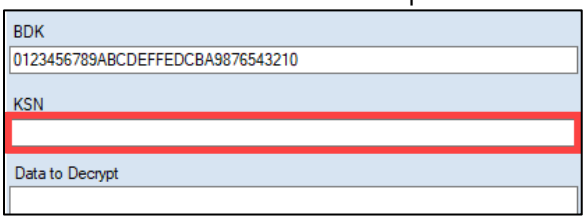
```
02 D2 01 80 1F 47 25 00 A3 9B 25 2A 34 37 36 31 2A 2A 2A 2A 2A 2A 2A
2A 30 32 36 37 5E 55 41 54 20 55 53 41 2F 54 45 53 54 20 43 41 52 44
20 30 35 20 20 20 20 20 20 5E 32 32 31 32 2A 2A 2A 2A 2A 2A 2A 2A 2A
2A 2A 2A 2A 2A 2A 2A 2A 2A 3F 2A 3B 34 37 36 31 2A 2A 2A 2A 2A 2A 2A
2A 2A 30 32 36 37 3D 32 32 31 32 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A
2A 3F 2A 21 9D 0A C5 7C 6E 8B 91 71 62 C4 39 F0 89 FF BF 89 04 78 D8
ED 2C 9C B4 70 25 2F 99 70 D6 36 F7 9E 3D 0D 08 9A 90 DB 81 77 A0 56
5F 85 0D 37 2F 76 6C BB EA C2 8E 2F 7D 35 AC C3 61 C8 AD D4 5C DE 36
87 A8 66 DF 0F 78 66 F7 4A 0D 9D 33 AE 1B 05 6B 63 13 17 FF 00 23 7A
DD D3 6C B4 7F 3B 65 90 12 4C 97 F1 18 64 D7 8E 2C 21 E5 08 0D C0 59
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 39 32 38 54 39 36
38 32 31 39 FF FF FF 02 00 00 04 60 00 55 75 1F 03
```

STX	02
LENGTH	D2 01
Card Encode Type	80
Track Status (1F)	0------- 0 Reserved for future use -0------ 1: Field 10 optional bytes length exists (0: No Field 10) --0----- 1: Track 3 sampling data exists (0: Track 3 sampling data does not exist) ---1---- 1: Track 2 sampling data exists (0: Track 2 sampling data does not exist) ----1--- 1: Track 1 sampling data exists (0: Track 1 sampling data does not exist) -----1-- 1: Track 3 decode success (0: Track 3 decode fail) ------1- 1: Track 2 decode success (0: Track 2 decode fail) -------1 1: Track 1 decode success (0: Track 1 decode fail)
Track 1 Length	47
Track 2 Length	25
Track 3 Length	00
Clear/Mask Data Sent Status (A3)	1------- Bit 7: 1 Serial Number present; 0 not present -0------ Bit 6: 1 PIN Encryption Key; 0 Data Encryption Key --1----- Bit 5: 1 Chip present on card. (First byte of service code was '2' or '6'.) Use EMV transaction if possible. ---0---- Bit 4: 0 TDES; 1 AES ----0--- Bit 3: 1 if fixed key; 0 DUKPT Key Management -----0-- Bit 2: 1 if Track3 clear/mask data present ------1- Bit 1: 1 if Track2 clear/mask data present -------1 Bit 0: 1 if Track1 clear/mask data present
Encrypted/Hash Data Sent Status (9B)	1------- Bit 7: if 1, KSN present -0------ Bit 6: if 1, session ID present --0----- Bit 5: if 1, track3 hash data (SHA digest) present ---1---- Bit 4: if 1, track2 hash data (SHA digest) present ----1--- Bit 3: if 1, track1 hash data (SHA digest) present -----0-- Bit 2: if 1, track3 encrypted data present ------1- Bit 1: if 1, track2 encrypted data present -------1 Bit 0: if 1, track1 encrypted data present
Track1 Data	25 2A 34 37 36 31 2A 2A 2A 2A 2A 2A 2A 2A 30 32 36 37 5E 55 41 54 20 55 53 41 2F 54 45 53 54 20 43 41 52 44 20 30 35 20 20 20 20 20 20 5E 32 32 31 32 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 3F 2A
Track2 Data	3B 34 37 36 31 2A 2A 2A 2A 2A 2A 2A 2A 30 32 36 37 3D 32 32 31 32 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 3F 2A
Track1 Encrypted Data	21 9D 0A C5 7C 6E 8B 91 71 62 C4 39 F0 89 FF BF 89 04 78 D8 ED 2C 9C B4 70 25 2F 99 70 D6 36 F7 9E 3D 0D 08 9A 90 DB 81 77 A0 56 5F 85 0D 37 2F 76 6C BB EA C2 8E 2F 7D 35 AC C3 61 C8 AD D4 5C DE 36 87 A8 66 DF 0F 78 Decrypt this data
Track2 Encrypted Data	66 F7 4A 0D 9D 33 AE 1B 05 6B 63 13 17 FF 00 23 7A DD D3 6C B4 7F 3B 65 90 12 4C 97 F1 18 64 D7 8E 2C 21 E5 08 0D C0 59 Decrypt this data
Track 1 Hashed	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Track 2 Hashed	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Reader Serial Number	39 32 38 54 39 36 38 32 31 39
KSN	FF FF FF 02 00 00 04 60 00 55
LRC	75
Checksum	1F
ETX	03

7. Copy the data in the **KSN** field.

Track 2 Hashed	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Reader Serial Number	39 32 38 54 39 36 38 32 31 39
KSN	FF FF FF 02 00 00 04 60 00 55
LRC	
Checksum	1F
ETX	03

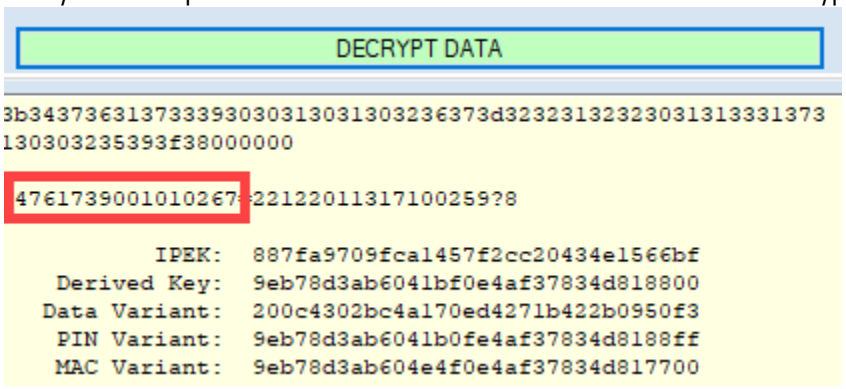
8. Return to the USDK Demo app and click **Decryption.** The ID TECH Decrypt window will appear.
9. Paste the **KSN** data into the **KSN** panel.



10. Return to the Parsomatic window and copy the **Track2 Encrypted Data** field's contents.

Track2 Data	3B 34 37 36 31 2A 2A 2A 2A 2A 2A 2A 30 32 36 37 3D 32 32 31 32 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 3F 2A
Track1 Encrypted Data	21 9D 0A C5 7C 6E 8B 91 71 62 C4 39 F0 89 FF BF 89 04 78 D8 ED 2C 9C B4 70 25 2F 99 70 D6 36 F7 9E 3D 0D 08 9A 90 DB 81 77 A0 56 5F 85 0D 37 2F 76 6C BB EA C2 8E 2F 7D 35 AC C3 61 C8 AD D4 5C DE 36 87 A8 66 DF 0F 78 Decrypt this data
Track2 Encrypted Data	66 F7 4A 0D 9D 33 AE 1B 05 6B 63 13 17 FF 00 23 7A DD D3 6C B4 7F 3B 65 90 12 4C 97 F1 18 64 D7 8E 2C 21 E5 08 0D C0 59 Decrypt this data
Track 1 Hashed	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Track 2 Hashed	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Reader Serial Number	39 32 38 54 39 36 38 32 31 39
KSN	FF FF FF 02 00 00 04 60 00 55

11. Return to the ID TECH Decrypt window, paste the Track2 Encrypted Data into the **Data to Decrypt** field, and click **Decrypt Data** and to display the decrypted data.
    a. The yellow output field shows that the card number has been decrypted by the tool:



9. Data Output Format

The SREDKey 2's default output mode is the enhanced MagStripe reader and key-in format.

```
<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>.

9.1. ID TECH Swipe Data Original Encryption Output Format

9.1.1. ISO/ABA Card

Field	Description
0	STX (02)
1	Data Length low byte
2	Data Length high byte
3	Card Encode Type (note 1)
4	Track1-3 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)

Note: Field 10 Present only ISO-4909 card.

9.1.2. Non-Financial Card

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	Track1-3 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)

9.2. ID TECH Swipe Data Enhanced Encryption Output Format

Note: For new development, please use enhanced encryption format.

9.2.1. ISO/ABA Card Data Output Format

Field	Description
1	STX
2	Data Length
3	Card Encode Type
4	Track Status
5	Track1 data length
6	Track2 data length
7	Track3 data length
8	Clear/mask data sent status
9	Encrypted/Hash data sent status
10	Optional bytes length
11	Optional bytes
12	Track1 clear/mask data
13	Track2 clear/mask data
14	Track3 clear/mask data
15	Track1 encrypted data
16	Track2 encrypted data
17	Track3 encrypted data
18	TransactionID (Session ID for Security level 4, Terminal/Merchant ID for TransArmor)
19	Track1 hashed (if encrypted)
20	Track2 hashed (if encrypted)
21	Track3 hashed (if encrypted)
22	Reader Serial Number
23	Key ID (10 bytes KSN for DUKPT, 10 bytes Key ID for fixed key, 11 bytes Key ID for TransArmor)
24	MAC Value length
25	MAC Value
26	KSN for MAC DUKPT
27	CheckLrc
28	CheckSum
29	ETX (0x03)

9.2.2. NON-ISO/ABA Data Output Format

Field	Description
1	STX
2	Data Length
3	Card Encode Type
4	Track Status
5	Track1 data length
6	Track2 data length
7	Track3 data length
8	Clear/mask data sent status
9	Encrypted/Hash data sent status
10	Optional bytes length
11	Optional bytes
12	Track1 clear/mask data
13	Track2 clear/mask data
14	Track3 clear/mask data
15	Track1 encrypted data
16	Track2 encrypted data
17	Track3 encrypted data
18	TransactionID (Session ID for Security level 4, Terminal/Merchant ID for TransArmor)
19	Track1 hashed (if encrypted)
20	Track2 hashed (if encrypted)
21	Track3 hashed (if encrypted)
22	Reader Serial Number
23	Key ID (10 bytes KSN for DUKPT, 10 bytes Key ID for fixed key, 11 bytes Key ID for TransArmor)
24	MAC Value length
25	MAC Value
26	KSN for MAC DUKPT
27	CheckLrc
28	CheckSum
29	ETX (0x03)

Note:

- **Field 12, 13, 14**
  - Financial card output is masked data.
  - Non-financial card output is clear data.
- **Field 22**
  - The serial number is sent out with the default setting.

9.3. ID TECH Manual Entry Original Data Output Format

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>0</td><td>STX (0x02)</td></tr>
<tr><td>1</td><td>Data Length low byte</td></tr>
<tr><td>2</td><td>Data Length high byte</td></tr>
<tr><td>3</td><td>Card type always 85—keyed in (Section 7.5 note 1)</td></tr>
<tr><td>4</td><td>Always 0</td></tr>
<tr><td>5</td><td>Always 0</td></tr>
<tr><td>6</td><td>Always 0</td></tr>
<tr><td>7</td><td>Always 0</td></tr>
<tr><td>8</td><td>Status (1 byte) bit set if field is present in output (range 0-7)
<table>
<tr><th>bit 7</th><th>bit 6</th><th>bit 5</th><th>bit 4</th><th>bit 3</th><th>bit 2</th><th>bit 1</th><th>bit 0</th></tr>
<tr><td>0</td><td>0</td><td>0</td><td>0</td><td>SessionID EXP</td><td>ADR</td><td>ZIP</td><td></td></tr>
</table></td></tr>
<tr><td>9</td><td>The length of unencrypted field 10 (PAN=EXP=CVV)</td></tr>
<tr><td>10</td><td>Encrypted card data (max: 180 bytes) PAN=EXP=CVV</td></tr>
<tr><td>11</td><td>20 bytes 0x00 (Null hash data)</td></tr>
<tr><td>12</td><td>EXP one-byte length+ASCII Expiration date (len: 1+4 bytes)</td></tr>
<tr><td>13</td><td>ADR one-byte length+ASCII Street number (max: 1+20 bytes)</td></tr>
<tr><td>14</td><td>ZIP one-byte length+ASCII Zip code (max: 1+10 bytes)</td></tr>
<tr><td>15</td><td>KSN (10 bytes)</td></tr>
<tr><td>16</td><td>CheckLrc</td></tr>
<tr><td>17</td><td>CheckSum</td></tr>
<tr><td>18</td><td>ETX (0x03)</td></tr>
</table>

Encrypted data sent status:

- Data Length low byte/high byte should be in length of characters.
- Data includes 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` are: 1-byte field length in hex data.
- The length byte ASCII not including length.

9.4. ID TECH Manual Entry Enhanced Data Output Format

Note: For new development, please use enhanced encryption format.

Field	Description
1	STX (0x02)
2	Data Length
3	Card Encode Type(0xC0)
4	Track Status (0x17 or 0x37)
5	Track1 data length(0x00)
6	Length of unencrypted ;PAN= EXP [:CVV]?LRC
7	Length unencrypted additional data ZIP and/or ADR
8	Clear/mask data sent status
9	Encrypted/Hash data sent status
10	Optional bytes length
11	Optional bytes
12	Empty
13	Keyed-in data presented as Track2—;PAN=EXP[:CVV]?LRC
14	Additional keyed-in data in ASCII presented as Track3 [1ADR=][0ZIP=]
15	Empty
16	Encrypted data
17	Empty
18	TransactionID (Session ID for Security level 4, Terminal/Merchant ID for TransArmor)
19	Empty
20	Hashed (present by default)
21	Empty
22	Device Serial Number (not present by default)
23	Key ID (10 bytes KSN for DUKPT, 10 bytes Key ID for fixed key, 11 bytes Key ID for TransArmor)
24	MAC Value length
25	MAC Value
26	KSN for MAC DUKPT
27	CheckLrc
28	CheckSum
29	ETX (0x03)

Note: Field 14 includes encrypted `PAN`, `EXP (YYMM)`, and `3-4 digit (CVV)`.

The format should be: `;PAN=YYMM[:CVV]?LRC`

Character	Description
;	Start sentinel
=	Field separator between PAN and expiration
:	Field separator between expiration 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 13 LRC is a calculated Track2 longitudinal redundancy check from **;** to **?**.

The LRC is calculated on the data before conversion to ASCII to be encoded on a card, so the keyed-in data can be linked to the card data.

10. Notes

10.1. Note 1: Card Encode Type

If the Card Encode Type starts with 0, it follows original encryption format.
If a Card Encode Type starts with 8, it follows enhanced encryption format.

Value	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)
86	JIS I
87	JIS II

10.1.1. Encoding Methods

The SREDKey 2 reader uses the following criteria 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 Track2 and the position of **=** is between 12th ~ 20th character.
- Total length of Track2 is greater than19 characters.
- Total of four 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 a 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.

11. Note 2: Track1-3 status byte

11.1.1. Field 4

B0:	1: Track1 decode success (0: Track1 decode fail)
B1:	1: Track2 decode success (0: Track2 decode fail)
B2:	1: Track3 decode success (0: Track3 decode fail)
B3:	1: Track1 sampling data exists (0: Track1 sampling data does not exist)
B4:	1: Track2 sampling data exists (0: Track2 sampling data does not exist)
B5:	1: Track3 sampling data exists (0: Track3 sampling data does not exist)
B6:	1: Field 10 "optional bytes length" exists (0: No Field 10)
B7:	0: Reserved for future

11.1.2. Field 10: Optional byte length

Number of optional bytes

11.1.3. Field 11: Optional status byte 1

Bit 0:	1: SHA-256. 0: SHA-1 (Note: If no optional status byte, use default SHA-1)
Bit 1:	1: Encryption type follows Field 11 bit 2 &3 &4. 0: Encryption type follows Field 8 bit 4.
Bit 4, 3, 2:	000: TransArmor RSA. 100: TransArmor 3DES-SUKPT.
Bit 5:	1: MAC Value Length, MAC Value and MAC Key KSN in Field 24, 25, and 26. 0: No MAC Value Length, MAC Value and MAC Key KSN in Field 24, 25, and 26.
Bit 6:	RFU
Bit 7:	RFU

11.2. Note 3: Clear/mask data sent status

Field 8 (Clear/mask data sent status) and field 9 (Encrypted/Hash data sent status) are only sent out in enhanced encryption format.

11.2.1. Field 8: Clear/masked data sent status byte:

Bit 0:	1: Track1 clear/mask data present
Bit 1:	1: Track2 clear/mask data present
Bit 2:	1: Track3 clear/mask data present or additional data present (in manual entry mode)
Bit 3:	1: RFU (always 0)
Bit 4:	0: TDES encryption; 1— AES encryption
Bit 5:	0: RFU
Bit 6:	1: PIN Key encryption
Bit 7:	1: reader serial number present

11.3. Note 4: Encrypted/Null Hash data sent status

11.3.1. Field 9: Encrypted data sent status

Bit 0:	1: Track1 encrypted data present
Bit 1:	1: Track2 encrypted data present
Bit 2:	1: Track3 encrypted data present
Bit 3:	1: Track1 hash data present
Bit 4:	1: Track2 hash data present
Bit 5:	1: Track3 hash data present
Bit 6:	1: session ID present
Bit 7:	1: KSN present

11.4. Data Sample

The data sample below is encrypted with an ID TECH demo key and TDES encryption method. The SREDKey 2 device is tested with USBKB interface.

Card Number: 5150 7102 0010 7903

Credit Card Swipe Original Format:
028801001F372300%*5150********7903^PAYPASS/MASTERCARD^***************?
*;5150********7903=***************?*F43947D860D5BCA3732EB67A2ECB7CEF52
644E3378CBBCB9509FF655F5E54B6C99519F0B79B785B94426C17D9427E7DC9A10A8DF
ED4A45C3DC1A9CB6B339B3D8521BFC17F114BC8A2E8AF4819F753729726F98B9D311B9
F250A0FACDE4A041ED0000000000000000000000000000000000000000000000000000
0000000000000000000000000000062994900000000000001181DD03

STX: 02
Data length low byte: 88
Data length high byte: 01
Card encode type: 00

Track1-3 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):
F43947D860D5BCA3732EB67A2ECB7CEF52644E3378CBBCB9509FF655F5E54B6C99519F
0B79B785B94426C17D9427E7DC9A10A8DFED4A45C3DC1A9CB6B339B3D8521BFC17F114
BC8A2E8AF4819F753729726F98B9D311B9F250A0FACDE4A041ED

T1 Null hash: 0000000000000000000000000000000000000000
T2 Null hash: 0000000000000000000000000000000000000000

KSN: 62994900000000000011
LRC: 81
CheckSum: DD
ETX: 03

Decrypted Data:
%B5150710200107903^PAYPASS/MASTERCARD^0909101400000631??;51507102001079
03=0909101400000631?0

Credit Card Swipe Enhanced Format
02A001801F372300839B%*5150********7903^PAYPASS/MASTERCARD^************
?*;5150*****7903=***************?*2B52196519901212715ABADDA6DA18
FDA5B50219A0FC9341BFB0633C3F33874FFE7B5F2B63897E0023710D5F6C6BF7BE8B93
7A515E3A7903182519B07422A5DFA329AF47F4B4728C5410105661B3DF35C0234582B9
83F7108771314DF807077D0000000000000000000000000000000000000000000000000
0000000000000000000000000000000003030303030303030306299490000000000000
0EBEEC03

STX: 02
Data length low byte: A0
Data length high byte: 01
Card encode type: 80
Track1-3 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

Track1 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):
2B52196519901212715ABADDA6DA18FDA5B50219A0FC9341BFB0633C3F33874FFE7B5F
2B63897E0023710D5F6C6BF7BE8B937A515E3A7903

T2 encrypted data (T2 length 35 rounded up by 8 => 40 bytes):
182519B07422A5DFA329AF47F4B4728C5410105661B3DF35C0234582B983F710877131
4DF807077D

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

11.4.1. Manual Entry Original Format

02840085000000000416780C3AF77E5CC55F1362DC46086A17EED23D053FD161CF5F00
00000000000000000000000000000000000000000431323132629949000000000000012B7
3303

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=

11.4.2. Manual Entry Enhanced Format

02A600C0170018008292;5150********7903=****?*293C595E789A8E5EE184D379E9
19F43A06A5911BDA9F90530000000000000000000000000000000000000000030303030
30303030303062994900000000000000F035B03

STX: 02
Data length low byte: A6
Data length high byte: 00
Card Encode Type: C0
Track Status: 17 - Track2 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:
00000000000000000000000000000000000000000

Serial Number:
30303030303030303030

KSN:
6299490000000000000F

LRC: 03
CheckSum: 5B
EXT: 03

Encrypted Data:
293C595E789A8E5EE184D379E919F43A06A5911BDA9F9053

Decrypt data:
;5150710200107903=1212?

12. Tamper Error Code Table

If a unit registers as tampered, the tamper **Error** code displays on-screen and the unit's LED flashes red (instead of the normal green).

Tamper Error Code in Display	Reason
BAT	Battery tamper occurred
TS0~TS7	Physical tamper occurred
TEMP	Temperature tamper occurred
VOLT	Voltage tamper occurred

13. Decommissioning SRED Devices

All PCI devices require proper decommissioning prior to device disposal in order to ensure the protection of all sensitive financial card data. For instructions on decommissioning your device, see Decommissioning of SRED Devices on the ID TECH Knowledge Base.

14. 24-Hour Device Reboot

Per PCI Requirements, this device reboots every 24 hours. Consult the *NEO 2 Interface Developer's Guide* (available from your ID TECH representative) for commands dealing with the SREDKEY 2's Real Time Clock.

15. Troubleshooting

The SREDKey 2 is designed to require minimal troubleshooting. In general, the device itself is plug-and-play and, as long as the green LED is lit, should be ready for use. If the LED is red or amber, contact your device integrator or ID TECH representative, or consult the ID TECH Knowledge Base for troubleshooting assistance.

16. For More Information

- To learn more about the SREDKey 2 and other ID TECH products, visit the ID TECH Knowledge Base.
- Visit us online at http://idtechproducts.com.
- Find more Tech Support resources at the ID TECH Tech Support home page or send an email describing any issues to support@idtechproducts.com.

17. Appendix A: Setting Configuration Parameters and Values (ITP Protocol)

The table below describes SREDKey 2 default settings and available settings (value within parentheses) for each function ID.

Function ID	Hex	Length	Name	Default	Description
TrackSelectID	13	1	Track Selection	0	Any Track 0-any
PollingIntervalID	14	1	Polling Interval	1 (1 ~ 255)	USB HID polling interval
TrackSepID	17	1	Track Separator	0x0D=CR/Enter	CR for RS232; Enter for KB any character supported except 00, which means "none"
Sentinel and Account Number controlID	19	1	Sentinel and Account Number Control	1 (0~0xF)	**Bit0** **1:** Send start/end sentinel **0:** Not send start/end sentinel **Bit1** **1:** Only send account number on Track2 **0:** Send all data on Track2 **Bit2** **1:** Send error notification **0:** No error notification **Bit3** **1:** Alt key output **0:** Control key output
MSRReadingID	1A	1	MSR Reading Setting	1 (0~1)	**0:** MSR Reading Disabled **1:** MSR Reading Enabled
DecodingMethodID	1D	1	Decoding Direction	1 (0~3)	Reading Direction **0x30:** Raw data decoding in both directions **0x31:** Decode in both directions **0x32:** Move stripe along head in direction of encoding **0x33:** Move stripe along head against direction of encoding
ReviewID	1F	1	Review All Settings	None	
FmVerID	22	1	Firmware Version	None	
USBHIDFmtID	23*	1	USB HID Format (HID reader only)	8 (0, 8)	**0:** ID TECH format **8:** HID KB format

Function ID	Hex	Length	Name	Default	Description
ForeignKBID	24	1	Foreign KB	0 (0 ~0x3A)	Foreign Keyboard; available 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
USBSuspendID	25	1	Enable/Disable USB Suspend	0(0,1)	**0:** Disable USB suspend **1:** Enable USB suspend
CustSetID	30	1	Custom Customer Settings	04(00 - 07)	**0:** Level 3/4 Non-CC sent as Level 1 **1:** Level3: No empty packet when not enough sampling bits **2:** Enhanced secured output will have SN after hash
Track1PrefixID	34	6	Track1 Prefix	0 (any string)	No prefix for Track1; six character maximum
Track2PrefixID	35	6	Track2 Prefix	0 (any string)	No prefix for Track2; six character maximum
Track3PrefixID	36	6	Track3 Prefix	0 (any string)	No prefix for Track3; six character maximum
Track1SuffixID	37	6	Track1 Suffix	0 (any string)	No suffix for Track1; six character maximum
Track2SuffixID	38	6	Track2 Suffix	0 (any string)	No suffix for Track2; six character maximum
Track3SuffixID	39	6	Track3 Suffix	0 (any string)	No suffix for Track3; six character maximum
KeyTypeID	3E*	1	Data or PIN Key	0	**0:** Data key **5A:** PIN key
PrePANID	49	1	PAN to Not Mask	4 (0-6)	Number of leading PAN digits to display
PostPANID	4A	1	PAN to Not Mask	4 (0-4)	Number of trailing PAN digits to display
MaskCharID	4B	1	Mask the PAN with This Character	* (0x20-0x7E)	Any printable character
CrypTypeID	4C*	1	Encryption Type	1 (1~3)	**1:** 3DES **2:** AES **3:** TransArmor RSA
DispExpDateID	50	1	Mask or Display Expiration Date	1(0-1)	**0:** Mask expiration date **1:** Display expiration date

Function ID	Hex	Length	Name	Default	Description
Mod10ID	55	1	Include mod10 Check Digit	0 (0-2)	**0:** Don't include mod10 **1:** Display mod10 **2:** Display wrong mod10
HashOptID	5C	1	Hash Process Option	7 (0~7)	**Send Track1-3 hash** **bit 0:**1 send Track1 hash **bit 1:** 1: send Track2 hash **bit 2:**1 send Track3 hash
UpperID	5D	1	Upper Case Option	1 (0, 1)	**0:** a~z, **1:** A~Z
LRCLv1ID	60	1	Track LRC Option in Level 1	1 (0, 1)	**1:** Send Track LRC in output data **0:** Do not send Track LRC
T17BstartID	61	1	Track1 Bit 7 Start Char	% (any)	% as Track1 Bit 7 start sentinel
T15BstartID	63	1	Track1 Bit 5 Start	; (any)	; as Track1 Bit 5 start sentinel
T27BstartID	64	1	Track2 Bit 7 Start Char	% (any)	% as Track2 Bit 7 start sentinel
T25BstartID	65	1	Track2 Bit 5 Start	; (any)	; as Track2 Bit 5 start sentinel
T37BstartID	66	1	Track3 Bit 7 Start Character	% (any)	% as Track3 Bit 7 start sentinel
T35BstartID	68	1	Track3 Bit 5 Start	; (any)	; as Track3 Bit 5 start sentinel
T1EndID	69	1	Track1 End Sentinel	? (any)	? as end sentinel
T2EndID	6A	1	Track2 End Sentinel	? (any)	? as end sentinel
T3EndID	6B	1	Track3 End Sentinel	? (any)	? as end sentinel
T1ERRSTARTID	6C	1	Track1 error Code	% (any)	Start sentinel if Track1 error report
T2ERRSTARTID	6D	1	Track2 error Code	; (any)	Start sentinel if Track2 error report
T3ERRSTARTID	6E	1	Track3 error Code	+ (any)	Start sentinel if Track3 error report
SecureLrcID	6F	1	Secured Output Format Track LRC Option Enhanced Only	1 (0, 1)	**1:** Send track LRC in secured output data **0:** Don't send track LRC **Note:** This command is valid for level3

Function ID	Hex	Length	Name	Default	Description
EquipFwID	77*	1	Feature Option Setting	0x05 (any)	Factory Reader firmware configuration; setting 77 is the firmware equipment options settings. **Bit 0:** `_secure = equipFw^0;` // Always 1 if a secure reader **Bit 1:** `_hasLED = equipFw^1;` // 1 if the reader has LED and beep support, 0 for SREDKey 2 **Bit 2:** `_hasRail = equipFw^2;` // 1 if the reader has a rail for a SecureKey reader **Bit 3:** `_xml = equipFw^3;` // 1 if XML output format, 0 for ID TECH output format **Bit 4:** `_mm = equipFw^4;` // 1 if MiniMag, always 0 for SREDKey 2 **Bit 5:** `_generic = equipFw^5;` // 1 if generic. **Bit 6 and 7:** Always 0.
SyncCheckID	7B	1	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
EncryptOptID	84	1	Encryption Options, Enhanced Only	0 encrypt card type 0; (0-1F)	**Bit 0:** Encrypt Track1 **Bit 1**: Encrypt Track2; **Bit 2:** Force encryption on Track3 and with no masked data; valid both for non-CC and card type 0 **Bit 3:** Encrypt Track3 if card type 0 **Bit 4:** Encrypt Track3 if card type 0 only and allow Track1, Track2, Track3 masked data to be sent as well **Note:** General ISO card Track3 mask is always not present, except for command 0x91. In this command, the Track3 mask is only for 4909 cards.
EncryptStrID	85*	1	Encryption Structure	1 (0~1)	**0:** Original; **1:** Enhanced
MaskOptID	86	1	Clear / Mask Data Options	7 (0~7)	**Bit 0:** Send clear/mask Track1 **Bit 1:** Send clear/mask Track2 **Bit 2:** Send clear/mask Track3
EnFmtID	88	1	Encryption Format	\02\30\34	Encryption format used in XML output format
T3ExpDatePosID	89	1	Expiration Date Position	0x34 ((0x34, 0x36)	Track3 expiration date position offset

Function ID	Hex	Length	Name	Default	Description
KeyTimeoutI D	8D	1	Timeout Value for Key Press Interval	5(20 seconds) (1~225)	Timeout = value * 4 Timeout range is from 4 to 900 seconds
AdminLvlID	8E	1	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*	1	Keyed Options	3	**bit 0** **0:** Output in original keyed output **1:** Output in enhanced keyed-in output **bit 1** **0:** Allow empty CVV entry **1:** Require three or more CVV digits **bit 2** **0:** Allow empty ZIP entry **1:** Require five or more ZIP digits **bit 3** **0:** Allow empty ADR entry **1:** Require one or more ADR digits **bit 4** **0:** Do a mod-10 check on keyed-in PAN **1:** Don't check the PAN mod-10 **bit 5** **0:** Admin enabled **1:** Admin disabled **Bits 6-7** reserved; all **0**
Non-fincilEncryptOptID	90*	1	Non-Financial Card Encryption Options	0	**0:** Non-financial card output plaintext at level 3. **1:** Non-financial card output as financial card at level 3.
Equip2ID	AE*	1	Equip Setting Byte for Different Readers or New Settings	0 (00-0xFF)	If bit4 = **1**, send serial number during USB enumeration
CustomSet3ID	B0	1	Customer Setting	0 (0, 1)	**Bit 0** **0:** Standard manual entry display **1:** Remise special display, in PAN entry mode, have hyphens every four digits, pre-PAN and post-PAN are always four digits, and masked PAN has a short delay after PAN data is displayed in clear text
CustomTimeout1	B1	1	Timeout for Plaintext Change to Mask Characters	2 (1~20)	The algorithm is **timeout = value * 0.5** (seconds), so timeout range is 1~10 seconds.

Function ID	Hex	Length	Name	Default	Description
PrefixID	D2	15	Preamble	0 (any 15)	No Preamble, 15 character maximum
PostfixID	D3	15	Postamble	0 (any 15)	No Postamble, 15 character maximum
EncryptOpt2ID	D5	1	Encrypted Option 2 Output	0 (0~1)	**Bit 0** **0:** Encrypted without MAC **1:** Encrypted with MAC Bit 1 to Bit 7 reserved; all **0**.

* These settings do not change with a default all command

17.1. Table of Legacy Function IDs

Function ID	Hex	Length	Name	Default Setting	Description
TrackSepID	17	1	Track Separator	0x0D=CR/Enter	**CR** for RS232, **Enter** for KB any character supported except **00** which means none.
Sentinel and Account number controlID	19	1	Sentinel and Account Number Control	1	**Bit 0** **1:** Send start/end sentinel **0:** Do not send start/end sentinel **Bit 1** **1:** Only send account number on Track2\ **0:** Send all data on Track2 **Bit 2** **1:** Send error notification **0:** Not error notification **Bit 3** **1:** Alt key output **0:** Control key output
Track1PrefixID	34	6	Track1 Prefix	0 (any string)	No prefix for Track1: six character maximum
Track2PrefixID	35	6	Track2 Prefix	0 (any string)	No prefix for Track2: six character maximum
Track3PrefixID	36	6	Track3 Prefix	0 (any string)	No prefix for Track3: six character maximum
Track1SuffixID	37	6	Track1 Suffix	0 (any string)	No suffix for Track1: six character maximum
Track2SuffixID	38	6	Track2 Suffix	0 (any string)	No suffix for Track2: six character maximum
Track3SuffixID	39	6	Track3 Suffix	0 (any string)	No suffix for Track3: six character maximum
LRCLv1ID	60	1	Track LRC Option in Level 1	1 (0-1)	**1:** Send track LRC in output data **0:** Don't send track LRC
T17BstartID	61	1	Track1 Bit 7 Start Character	% (any)	% as Track1 Bit 7 start sentinel
T15BstartID	63	1	Track1 Bit 5 Start	; (any)	; as Track1 5 Bit start sentinel
T27BstartID	64	1	Track2 Bit 7 Start Character	% (any)	% as Track2 Bit 7 start sentinel
T25BstartID	65	1	Track2 Bit 5 Start	; (any)	; as Track2 5 Bit start sentinel
T37BstartID	66	1	Track3 Bit 7 Start Character	% (any)	% as Track3 Bit 7 start sentinel

T35BstartID	68	1	Track3 Bit 5 Start	; (any)	; as Track3 5 Bit start sentinel
T1EndID	69	1	Track1 End Sentinel	? (any)	? as end sentinel
T2EndID	6A	1	Track2 End Sentinel	? (any)	? as end sentinel
T3EndID	6B	1	Track3 End Sentinel	? (any)	? as end sentinel
T1ERRSTARTID	6C	1	Track1 Error Code	% (any)	Start sentinel if Track1 error report
T2ERRSTARTID	6D	1	Track2 Error Code	; (any)	Start sentinel if Track2 error report
T3ERRSTARTID	6E	1	Track3 Error Code	+ (any)	Start sentinel if Track3 error report

18. Revision History

Rev	Date	Changes	Author
D	02/28/2020 03/25/2020	Renamed from SREDKey 2 User Manual Added public commands. Final adjustments for release.	CB
E	08/18/2020	Added 24 hour reset text.	CB
F	02/26/2021 03/03/2021	Setting Configuration Parameters and Values (ITP Protocol) Updated description for EncryptOptID Function ID Bits 0, 1, and 2. IDG Protocol Commands Reboot Device (77-05): Changed name from "Restart Device." NGA Protocol Commands Reboot Device (78 46 CC): Changed name from "Reset Device." Added Reset Device (C7 80 00 01 00) command. ITP Protocol Commands Added section for ITP Protocol Commands. Added Reset Device (53 18) command.	CB
H	07/26/2021	Updated 0x8F default value to 3	CB
J	02/21/2024	Updated Appendix A: Setting Configuration Parameters and Values (ITP Protocol)	CB