80128502-001

USER MANUAL

SecuRED

SRED MagStripe Reader

USB Interface

CE FC

80128502-001
Rev A 09/06/13

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

Revision History

Revision	Date	Description of Changes	By
A	09/06/2013	Initial Release	CH

Table of Contents

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.

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.

ID TECH and Value through Innovation are trademarks of International Technologies & Systems Corporation. USB (Universal Serial Bus) specification is copyright by Compaq Computer Corporation, Intel Corporation, Microsoft Corporation, and NEC Corporation. Windows is registered trademarks of Microsoft Corporation.

ID TECH
10721 Walker Street
Cypress, CA 90630
(714) 761-6368

1. Scope

SecuRED is a PCI SRED (Secure Reading and Exchange of Data) certified magnetic stripe card reader. This intelligent reader, not only encrypts payment card data as it swiped through the device, but also provides the physical security and tamper resistance needed to achieve PCI SRED standards. The document outlines the electrical, mechanical and firmware information for customer’s easy implementation.

2. Features and Benefits

- Interface includes: USB-KB, USB-HID
- Bi-directional card reading capability
- Reads up to 3 tracks of information
- Reliable for a minimum of 1,000,000 cycles
- Beeper and LED to indicate read results
- Can be used free standing or mounted
- PCI SRED certified
- TDES/AES with DUKPT Key Management

3. Abbreviation

AAMVA	American Association of Motor Vehicle Administrators
AES	Advanced Encryption Standard
DES	Data Encryption Standard
DMV	Department of Motor Vehicles
MSR	Magnetic Swipe Reader
TDES	Triple Data Encryption Standard
PCI	Payment Card Industry
POS	Point of Sale
USB	Universal Serial Bus
IPEK	Initial PIN Encryption Key

4. Applicable Document

80096401-001 SecuRED Product Requirement Specification

80128401-001 SRED Secure Card Reader Product Requirement Spec

PCI Point-to-Point Encryption: Solution Requirements – Encryption, Decryption, and Key Management within Secure Cryptographic Devices (Hardware/Hardware) V1.0

ISO 7810 – 1985	Identification Cards – Physical
ISO 7811 - 1 through 6	Identification Cards - Track 1 through 3
ISO 7816 - 1 through 4	Identification Cards - Integrated circuit cards with contacts
ISO 4909	Magnetic stripe content for track 3
ISO 7812	Identification Cards – Identification for issuers Part 1 & 2
ISO 7813	Identification Cards – Financial Transaction Cards
ANSI X.94	Retail Financial Services Symmetric Key Management

5. Operations

A card should be swiped through the reader slot when the LED is green. The magnetic stripe must face toward the magnetic read head and may be swiped in either direction. After a card is swiped, the LED will turn off temporarily until the decode process is completed. If there is no error decoding the card data then the LED will turn green. If there is any error decoding the card data, the LED will turn red for less than one second to indicate that an error occurred and then turn green.

The reader LED will be off during the data transfer and is ready to read another card when the LED returns to green. A red LED indicates an error and the beeper will also provide error indications. The beeper will beep for each correctly read track of data on the magstripe card. Depending on the security level configured, the card data might be displayed in encrypted mode.

6. Specification

6.1 Supply power

- Supply voltage: DC 5V
- Working current: Maximum 50mA (when reading card with LEDs/beeper power on)
- Sleep current: 25mA

6.2 Reliability and Environment

Reliability

- Magnetic Head Life: 1,000,000 passes minimum
- Rail and Cover Life: 1,000,000 passes minimum
- MTBF: 300,000 POH or depends on the electronics

Temperature

- operating: 0 to 55 ℃ non-condensing
- storage: -35 to 65 ℃ non-condensing

Humidity

- operating: maximum 95% non-condensing
- storage: maximum 95% non-condensing

ESD

- 4 kV direct contact, 8 kV air discharge

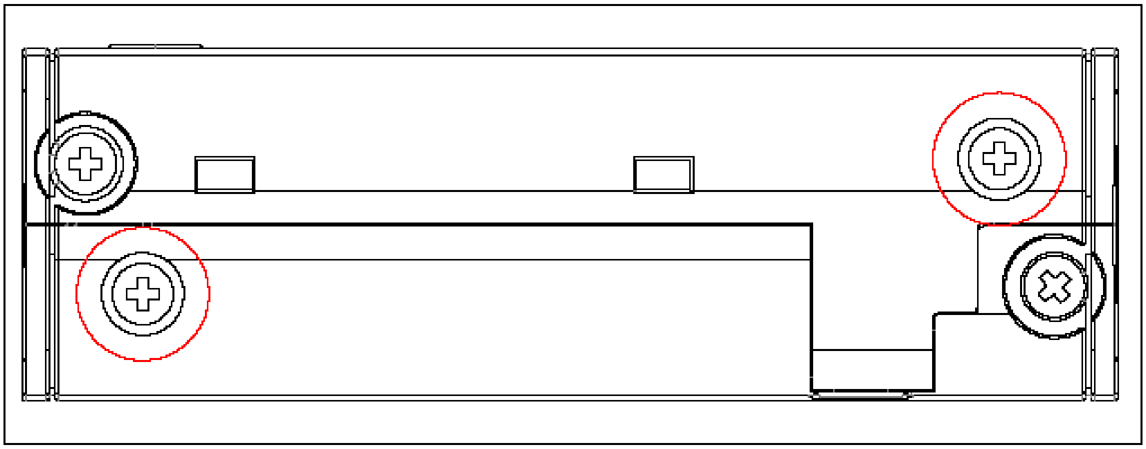
6.3 Size & weight

- Size: L*W*H:MAX 100MM*30MM*31.5MM

- Weight: 127g

6.4 Mounting method

The bottom of the reader must be flat for mounting. If the reader needs be mounted on the table, please unscrew the 2 screws showed in red below to get the two holes for mounting . The mounting nut is M3x 3.



6.5 LED Management

There are two LEDs, one is on the top of the reader and the one is on the side.

- The LED on the top flashes red if the reader is not activated.
- The top LED flashes amber for one second during the self-test after reader is powered on.
- The top LED is stable green in idle status.
- The top LED flashes dark during swiping the card, and it will go back to green if the swipe data is good. If it's a bad read, the LED will flash red.
- The red led continues flashing every second when system detects unpredictable error.

6.6 Beeper Management

- The beeper is off during idle status;
- The beeper keeps beeping when reader is not activated;
- The reader beeps once when reader is powered on
- The beeper will beep once after the card is swiped and command has been received.

7. Firmware Command

The SRED MSR reader can be appropriately configured per customer requirement. Once programmed, these configuration settings are stored in the reader's memory so the settings are not affected by the cycling of power. Command length should be less than

254 bytes. The command/response time between the reader and host is from 50ms to 6000ms.

7.1 Command Format

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

Response from SecuRED
<ACK> if setting succeeds
or
<NAK> if setting fails

b. Read Status Command:
<STX><R>[<FuncID><Len><FuncData>…]<ETX>< CheckLrc >

Response from SecuRED
<ACK>< STX ><Response><ETX>< CheckLrc > if command succeeds
Or
<NAK> if commands fail

c. Function Command:
<STX><F>[<FuncID><Data>…]<ETX>< CheckLrc >

Response from SecuRED
<ACK>< STX >[<Response>]<ETX>< CheckLrc > if command succeeds
Or
<NAK> if commands fails

Where

Characters	Hex Value	Description
<STX>	02	Start of Text
<ETX>	03	End of Text
<ACK>	06	Acknowledge
<NAK>	15 for RS232 and USB HID interface; FD for USB KB interface	Negative Acknowledge
<UnknownID>	16	Warning: Unsupported ID in setting
<AlreadyInPOS>	17	Warning: Reader already in OPOS mode
<R>	52	Review Setting
<S>	53	Send Setting
<LRC>	-	Xor'd all the data before LRC.

7.2 Get Microcontroller Firmware Version

This command is used to get firmware version from SecuRED.
Command: <STX><R><A2h><EXT><LRC1>
Response: <ACK> <STX><A2h><Len of Version String><VersionString><ETX><LRC2>

7.3 Get MSR Firmware Version

This command is used to get MSR firmware version
Command: <STX><R><52h><ETX><LRC 1>
Response: <ACK> <STX><Version String><ETX><LRC 2>

Version String will be in format of "ID TECH FirmOpt IntOpt Reader Vxx.yy. xx.yy is the major and minor version number.

7.4 Review Settings

Command: <STX> <R> <1Fh> <ETX> <LRC1>
<Response> format:
The current setting data block is a collection of many function-setting blocks <FuncSETBLOCK> as follows:
<STX><FuncSETBLOCK1>…<FuncSETBLOCKn><ETX><CheckSum>
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>

7.5 Setting Command

The setting command is a collection of many function setting blocks and its format is as follows.

Command: <STX><S><FuncSETBLOCK1>…<FuncBLOCKn><ETX><LRC>
Response: <ACK> or <NAK> for wrong command (invalid funcID, length and value)

Each function-setting block <FuncSETBLOCK> has 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.

7.6 Review Error Code

This command is used to review code data to look for root cause if pre-command fails.
Command: <STX><R><E0h><ETX><LRC1>
Respond :< ACK><STX><E0h><0x02><Error Code (2 bytes)> <ETX><LRC2>

For more error codes, please refer to Appendix B.

7.7 Review Device Status

This command is used to review status of Device.
Command: <STX><R><A6h><ETX><LRC1>
Respond:
<ACK><STX><A6h><0x01>< Status> <ETX><LRC2>
Where:
<Status>: is defined

0	Device had been attacked.
1	Device hasn’t been activated.
2	Admin Key doesn’t load.
3	Device works in idle status.
8	Check Value doesn’t load.
9	MSR key doesn’t load

For more command function ID, please refer to Appendix A.

8. Data output format

SecuRED encrypts both financial card and non-financial card. Both clear/masked data and encrypted data are sent out.

8.1 Original Encrypted Data Structure Format

This original format is maintained for customers who deployed readers before the enhanced structure was developed.

A card swipe returns the following data:

Card data is sent out in this format
<STX><LenL><LenH><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>.
<Card Data> format is

ISO/ABA Data Output Format:

- card encoding type (0: ISO/ABA; 3 For others 4: For Raw Mode)
- track status (bit 0,1,2:T1,2,3 decode*, bit 3,4,5:T1,2,3 sampling)
- track 1 unencrypted length (1 byte in binary, 0 for no track1 data)
- track 2 unencrypted length (1 byte in binary, 0 for no track2 data)
- track 3 unencrypted length (1 byte in binary, 0 for no track3 data)
- track 1 masked data (omitted if raw or force encrypted)
- track 2 masked data (omitted if raw or force encrypted)
- track 3 data (omitted if raw or force encrypted)
- track 1, 2, 3 encrypted data (AES/TDES encrypted data, bytes)
- track 1 dummy hash data* 20 bytes 0x00 reserved for future use
- track 2 dummy hash data* 20 bytes 0x00 reserved for future use
- track3 dummy hash data* 20 bytes 0x00 reserved for future use
- KSN(key serial number) 10 bytes

Note: the track 1, 2, 3 hash data can be disabled by command 53 5c 01 30. Please refer to Appendix A for details.

Except for USBKB interfaces, track formatting (preamble, prefix, separator, etc.) is not supported in a reader set to send encrypted track data. The track data is always sent in the

same format that is with no special formatting so that the program doing the decoding can know where each data field is located.
Note: For USBKB interface, preamble and postamble can be available in encrypted track data.

Offset to the fields can be determined by adding the field lengths using the track data for the track field lengths. Fields are packed in the next available location.

T1, T2 or T3 Data Length: Each byte value indicates how many bytes of decoded card data are in the track data field. This value will be zero if there is no data on the track or if there is an error decoding the track.

The encrypted section is padded with zeros to the block size of the encryption type, 8 bytes for TDES and 16 bytes for AES.

How to get Encrypted Data Length

If card encoding type high bit is not set:
The encrypted data is packed into one continuous block and then padded with zeros until the encryption block size is reached, 8 bytes for triple DES and 16 bytes for AES. The length of the encrypted data is the length of Track 1 + length of track 2 + length of track 3. This total is padded to the block length then encrypted. The field is always a multiple of 8 bytes in length if triple DES or 16 bytes if AES encryption is used. This value will be zero if there was no data on the track or if there was an error decoding the track.

The length of track 1 encrypted data is equal to track 1 encrypted data length. The length of track 2 is equal to track 2 data length. If present the length of track 3 encrypted length is equal to the length of the track 3 data length.

Once the encrypted data is decrypted, there may be fewer bytes of decoded track data than indicated by this field. The number of bytes of decoded track data is indicated by the track 1 unencrypted length.

If card encoding type high bit is set:
In this mode tracks are encrypted separately rather than as a group. The length of encrypted track 1 is the length of the track rounded up to the nearest multiple of 8 bytes if TDES encryption is used or 16 bytes if AES encryption is used. Track 2 follows the end track 1 as rounded up and follows the same rule as track 1. Track 3 follows track 2 as rounded up and again follows the same rule. If the encryption is security level 4, then the session ID follows track 3 and is eight bytes long.

Track 1 unencrypted Length

This one-byte value indicates the number of useable bytes in the track 1 encrypted data field and track 1 masked data field after decryption.
Track 2 unencrypted Length

This one-byte value indicates the number of useable bytes in the track 2 encrypted data field and track 2 masked data field after decryption.

Track 3 unencrypted Length

This one-byte value indicates the number of useable bytes in the Track 3 masked Data field.

Original Format Data Example

The example below is the decryption of a three track ABA card with the original encryption format and SecuRED Reader with default settings.

Original encryption format can be recognized because the high bit of the fourth byte underlined (00) is 0.

02F100001F372300252A353135302A2A2A2A2A2A2A373930335E5041595041535
32F4D41535445524341524 45E2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B35
3135302A2A2A2A2A2A2A373930333D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2
A3F2AEB2C43BD28846F6ADDCDB806DEBC3500328E4589AF72C7AAE09C4F714
89D6D7EDE9C3C6DA94F31288463262429D072BAA1017CB8B93DF3F7F43A8DC4
D64FF8DA7C30310A5456CC37DD6410D0463B61CE95EDC4671035D1E63C1E1C74
43FC80150000000000000000000000000000000000000000000000000000000000
0000000000000000629949012C0004600004C26603

STX, Length (LSB, MSB), card type, track status, length track 1, length track 2, length track 3
02 F100 00 1F 37 23 00
The above broken down and interpreted
02—STX character
F1—low byte of total length
00—high byte of total length
00—card type byte (interpretation old format ABA card)
1F—Track 1&2 data good
37—length of track 1
23—length of track 2
00—length of track 3

Track 1 data masked (length 0x37)
252A353135302A2A2A2A2A2A2A373930335E504159504153532F4D41535445524
34152445E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A
In Ascii:
%*5150********7903^PAYPASS/MASTERCARD^***************?*

Track 2 data in hex masked (length 0x23)

3B353135302A2A2A2A2A2A2A2A373930333D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A
In Ascii:
;5150********7903=***************?*

Track 1 & 2 encrypted length 0x37+0x23=90 in decimal -> rounded up by 8 bytes=96 bytes
EB2C43BD28846F6ADDCDB806DEBC3500328E4589AF72C7AAE09C4F71489D6D7EDE9C3C6DA94F31288463262429D072BAA1017CB8B93DF3F7F43A8DC4D64FF8DA7C30310A5456CC37DD6410D0463B61CE95EDC4671035D1E63C1E1C7443FC8015

Track1 dummy hash data
0000000000000000000000000000000000000000

Track2 dummy hash data
0000000000000000000000000000000000000000

KSN
629949012C0004600004

LRC, checksum and ETX
C2 66 03

Decrypted Data:
Data in ASCII Format
%B5150710200107903^PAYPASS/MASTERCARD^090910140000631??;5150710200107903=090910140000631?0

Data in HEX Format
25423531353037313032303031303739303335E504159504153532F4D4153544552434152445E3039303931303134303030303633313F3F3B353135303731303230303130373930333D3039303931303134303030303633313F30

8.2 Enhanced Encrypted Data Structure Format

SecuRED output structure setting:

53 85 01 encryptStructure
encryptStructure = ‘0’ Original Encryption Format
encryptStructure = ‘1’ Enhanced Encryption Format

Enhanced encrypt output structure will send bytes 8 and 9 and CardType will be 1xxxxxxx (high bit =1). Also the T1, T2 data are encrypted in separate data block.

Encrypt Option Setting: // only effect in new structure
53 84 01 encrypOpt // default 0x08
encryptOpt:
bit0: 1 – tk1 force encrypt *
bit1: 1 – tk2 force encrypt *
bit2: 1 – tk3 force encrypt *
bit3: 1 – tk3 force encrypt when card type is 0
bit4: 1 – new mask feature: see notes 4

Note:
1) When force encryption is set, all tracks will always be encrypted, regardless of card type. No clear/mask text will be sent, except bit4 “new mask feature is set (see notes).
2) If and only if in new encrypt structure, each track encryption is separated, encrypted data length will round up to 8 or 16 bytes.
3) When force encrypt and new mask feature is not set, it encrypts data just like old structure, that is, only T1 and T2 in type zero will be encrypted.
4) When new mask feature (bit4) is set,
   a) Mask data can be sent even if set to “force encrypt” (bit0-3 is set);
   b) If bank card and track 3 is iso-4909 with PAN format, T3 will be encrypted and has mask data.

Typical setting:
1) 08 (default):
   All tracks will be encrypted. Only T1 and T2 will sent out clear/mask data.
2) 07
   Force encryption. All three tracks will be encrypted without mask, regardless of card type.
3) 10
   T1 and T2 will be encrypted. If the T3 is with ISO-4909 format, it’ll be encrypted and its mask data will be sent out. Otherwise, T3 will be sent in clear text.
4) 17
   All tracks will be encrypted. T1 and T2 will send out clear/mask data. T3 will send out clear/mask data if it’s ISO 4909 format.

Dummy Hash Option Setting:
Command: 53 5C 01 <Dummy Hash Option> // default 0x37
Dummy Hash Option: (‘0’ – ‘7’)
bit0: 1 – tk1 dummy hash will be sent if data is encrypted
bit1: 1 – tk2 dummy hash will be sent if data is encrypted
bit2: 1 – tk3 dummy hash will be sent if data is encrypted

Mask Option Setting: // only effected in new structure
Command: 53 86 01 <Mask Option> // Default: 0x07
Mask Option:
bit0: 1 – tk1 mask data allow to send when encrypted
bit1: 1 – tk2 mask data allow to send when encrypted
bit2: 1 – tk3 mask data allow to send when encrypted

Note:
1) When mask option bit is set – if data is encrypted (but not forced encrypted), the mask data will be sent; If mask option is not set, the mask data will not be sent under the same condition.

Following is the output structure:

0	STX
1	Data Length low byte
2	Data Length high byte
3	Card Encode Type*
4	Track 1-3 Status
5	T1 data length
6	T2 data length
7	T3 data length
8	Clear/mask data sent status *
9	Encrypted/Hash data sent status *
10	T1 clear/mask data
	T2 clear/mask data
	T3 clear/mask data
	T1 encrypted data
	T2 encrypted data
	T3 encrypted data
	Track 1 dummy hash data* (20 bytes 0x00 reserved for future use)
	Track 2 dummy hash data* (20 bytes 0x00 reserved for future use)
	Track 3 dummy hash data* (20 bytes 0x00 reserved for future use)
	KSN (10 bytes) (DUKPT only)
	CheckLrc
	CheckSum
	ETX

Note:
1) Field 8 (Clear/mask data sent status) and field 9 (Encrypted/Hash data sent status) will only be sent in new encrypt structure.
2) Field 8: Clear/mask data sent status byte:
   bit 0: 1--- if TK1 clear/mask data present
   bit 1: 1--- if TK2 clear/mask data present
   bit 2: 1--- if TK3 clear/mask data present
   Bit 3:1— if fixed key; 0 DUKPT
   Bit 4-5: 00- TDES; 01 - AES
   Bit 6: 1-- PinKey; 0 – Data key
   Bit7: 1 – Serial # present; 0- not present

3) Field 9: Encrypted data sent status
   bit 0: if 1—tk1 encrypted data present
   bit 1: if 1—tk2 encrypted data present
   bit 2: if 1—tk3 encrypted data present
   bit 3: if 1—tk1 dummy hash data present
   bit 4: if 1—tk2 dummy hash data present
   bit 5: if 1—tk3 dummy hash data present
   Bit 6: if 1—session ID present
   Bit 7: if 1—KSN present

Card Type:

Value	Encode Type Description
0 / 80	ISO/ABA format
1 / 81	AAMVA format
3 / 83	Other
4/ 84	Raw Data format
* / 85	JIS II

Note:
1) Card Type will be 8x in new structure and 0x for old structure
2) Type 4 or 84: Raw data format; all tracks are encrypted and no mask data is sent. No track indicator ‘01’, ‘02’ or ‘03’ in front of each track. (‘01’,’02’ and ‘03’ will still exist for none secured mode raw output when security level < 3)
3) Type 85: JIS II, needs to set to Enhanced mode. Only T2 will be sent; Force encrypted, no clear text.
4) Note: the track 1, 2, 3 dummy hash data can be disabled by command 53 5c 01 30. Please refer to Appendix A for details.

Enhance Format Data Example:

Example below is the decryption of a three track ABA card with the enhanced encryption format and SecuRED is with default settings except enhanced encryption structure format.

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

02F300<u>80</u>1F372300039B252A353135302A2A2A2A2A2A2A2A373930335E504159504
153532F4D4153544552434152445E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3
B353135302A2A2A2A2A2A2A2A373930333D2A2A2A2A2A2A2A2A2A2A2A2A2A2A
2A2A3F2A277034D65F3BE450F2210B20A347DA4E307EEE546DE3677F9A584CA3
40164A82A85627E51FBD1EE81EA7F69D5560305BF0C2CBE0C77166876C3F4B21E
6C229808A9063442AC8A79FAC6B857D6B6BED94C0D664BFC97E931626F338CA
CD16F9900000000000000000000000000000000000000000000000000000000000
000000000000000000629949012C000460000670B403

STX, Length(LSB, MSB), card type, track status, length track 1, length track 2, length track 3
02 F300 <u>80 </u>1F 372300

The above broken down and interpreted
02—STX character
F3—low byte of total length
00—high byte of total length
80—card type byte (interpretation new format ABA card)
1F—Track 1&2 good
37—length of track 1
23—length of track 2
00—length of track 3
03—tracks 1 and 2 have masked/clear data
9B Encrypted/Hash data status
bit 7=1—KSN included
Bit 6=0—no Session ID included so not level 4 encryption
Bit 5=0—no track 3 dummy hash data present
Bit 4=1—track 2 dummy hash data present
Bit 3=1—track 1 dummy hash data present
Bit 2=0—no track 3 encrypted data present
Bit 1=1—track 2 encrypted data present
Bit 0=1—track 1 encrypted data present

Track 1 data masked (length 0x37)
252A353135302A2A2A2A2A2A2A2A373930335E504159504153532F4D41535445524
34152445E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A

Track 1 masked data in ASCII
%*5150********7903^PAYPASS/MASTERCARD^***************?*

Track 2 data in hex masked (length 0x23)
3B353135302A2A2A2A2A2A2A2A373930333D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A

Track2 masked data in ASCII
;5150********7903=***************?*

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

Track 1 encrypted length 0x37=55 (decimal) bytes rounded up to 8 bytes = 56(decimal) bytes277034D65F3BE450F2210B20A347DA4E307EEE546DE3677F9A584CA340164A82A85627E51FBD1EE81EA7F69D5560305BF0C2CBE0C7716687

Track 2 encrypted length 0x23= 35(decimal) bytes rounded up to 8 bytes= 40 (decimal bytes)
6C3F4B21E6C229808A9063442AC8A79FAC6B857D6B6BED94C0D664BFC97E931626F338CACD16F990

Track 1 dummy Hash Data:
0000000000000000000000000000000000000000
Track 2 dummy Hash Data:
0000000000000000000000000000000000000000

Key Serial Number:
629949012C0004600006

LCR, check sum and ETX
70 B4 03

Decrypted Data:
Data in ASCII Format
%B5150710200107903^PAYPASS/MASTERCARD^0909101400006317??
;5150710200107903=0909101400006317?0

Data in HEX Format
2542353135303731303230303130373930335E504159504153532F4D415354455243415 2445E303930393130313430303030363331373F3F
3B353135303731303230303130373930333D303930393130313430303030363331373F30

9. Security feature

The SecuRED is only working with the key injected and encryption is enabled.

9.1 Check Card Format

- ISO/ABA (American Banking Association) Card (card type 0)

  Encoding method

  Track1 is 7 bits encoding.
  Track1 is 7 bits encoding. Track2 is 5 bits encoding. Track3 is 5 bits encoding.
  Track1 is 7 bits encoding. Track2 is 5 bits encoding.
  Track2 is 5 bits encoding.

  Additional check

  Track1 2nd byte is 'B'.
  There is only one '=' in track 2 and the position of '=' is between 13th ~ 20th character so account number length is 12-19 digits.
  Total length of track 2 is above 19 characters.

- 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)

9.2 MSR Data Masking

For financial card, the clear data includes start and end sentinels, separators, first N, last M digits of the PAN, card holder name (for Track1). The rest of the characters should be masked using mask character.

Set PrePANClrData (N), PostPANClrData (M), MaskChar (Mask Character)
N and M are configurable and default to 4 first and 4 last digits. They follow the current PCI constraints requirements (N 6, M 4 maximum).
Mask character default value is '*'.

- Set PrePANClrDataID (N), parameter range 00h ~ 06h, default value 04h

- Set PostPANClrDataID (M), parameter range 00h ~ 04h, default value 04h

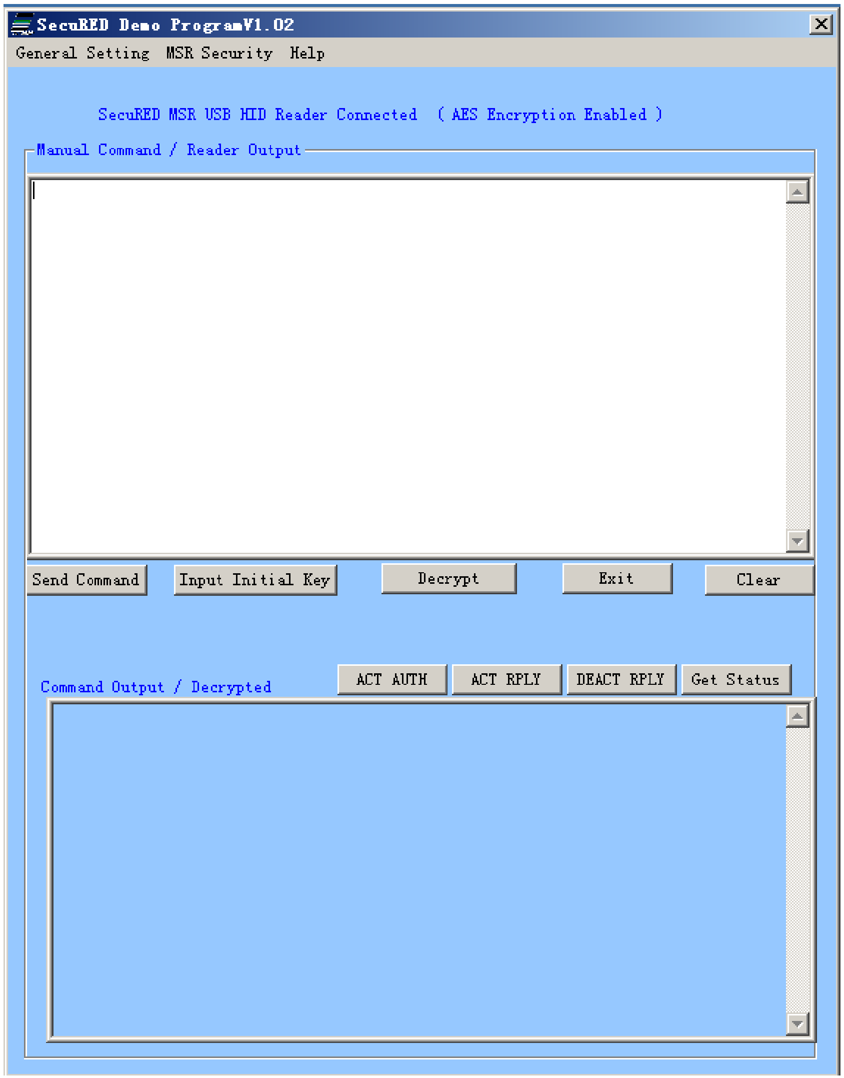
- MaskCharID (Mask Character), parameter range 20h ~ 7Eh, default value 2Ah

- DisplayExpirationDataID, parameter range '0'~'1', default value '0'

For non-financial card, the first 4 digits/characters of track data, start sentinel and end sentinel is in clear. The other data are masked with "*".

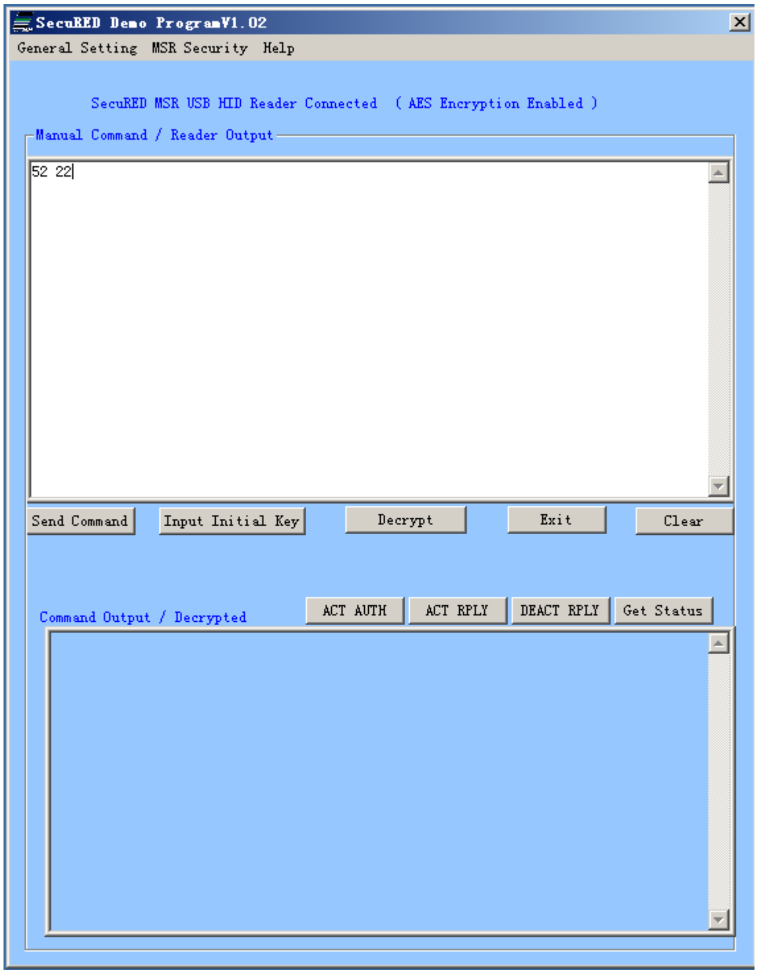
10.Use demo software

Double click executable file "SecuRED_USB_Demo.exe" after connecting the SecuRED with PC.

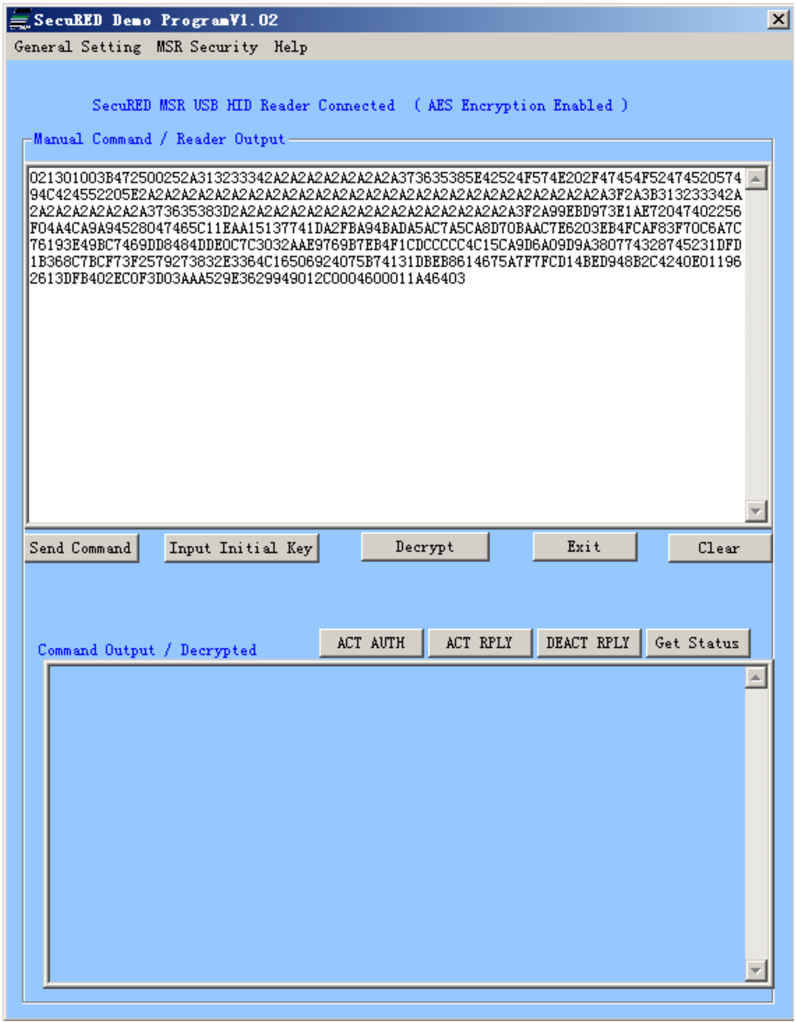


10.1 Send Command

Command can be sent to SecuRED via the demo software. The command can be typed in the upper window, such as get firmware version command below. Then click [send command] button, then the response from reader will be showed in the second window below.

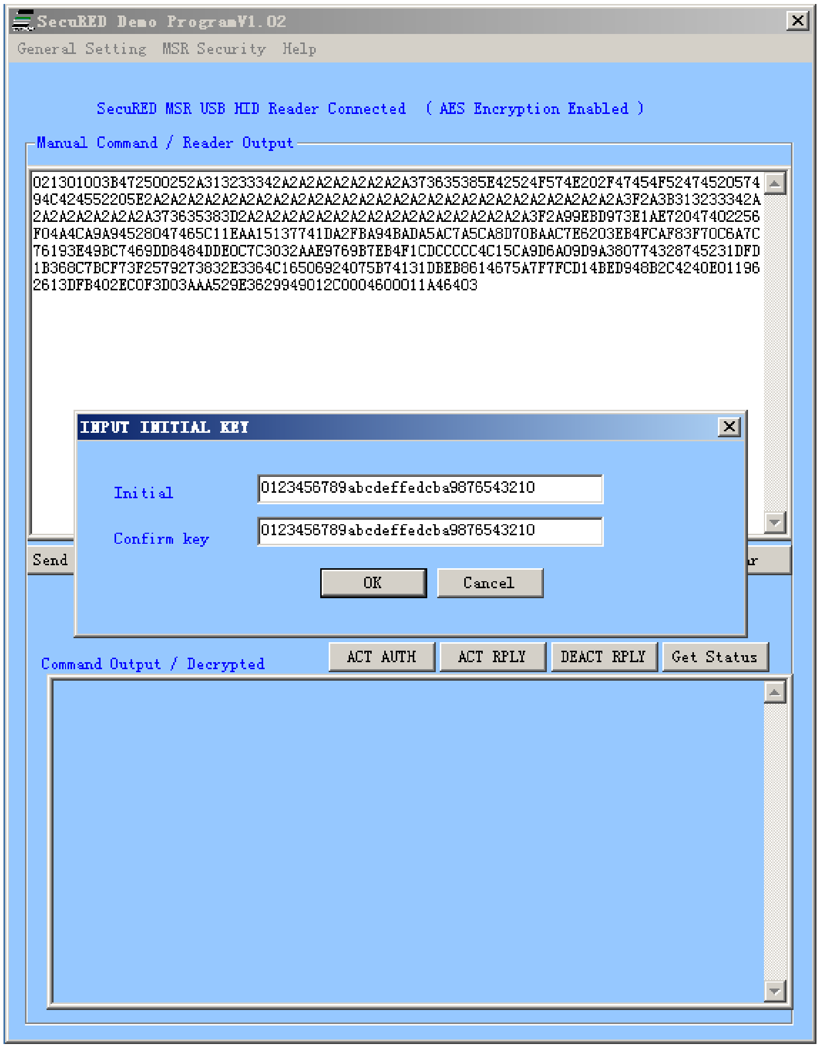

SecuRED Demo ProgramV1.02
General Setting MSR Security Help
SecuRED MSR USB HID Reader Connected (AES Encryption Enabled)
Manual Command / Reader Output
52 22
Send Command
Input Initial Key
Decrypt
Exit
Clear
Command Output / Decrypted
ACT AUTH
ACT RPLY
DEACT RPLY
Get Status

10.2 Swipe Card

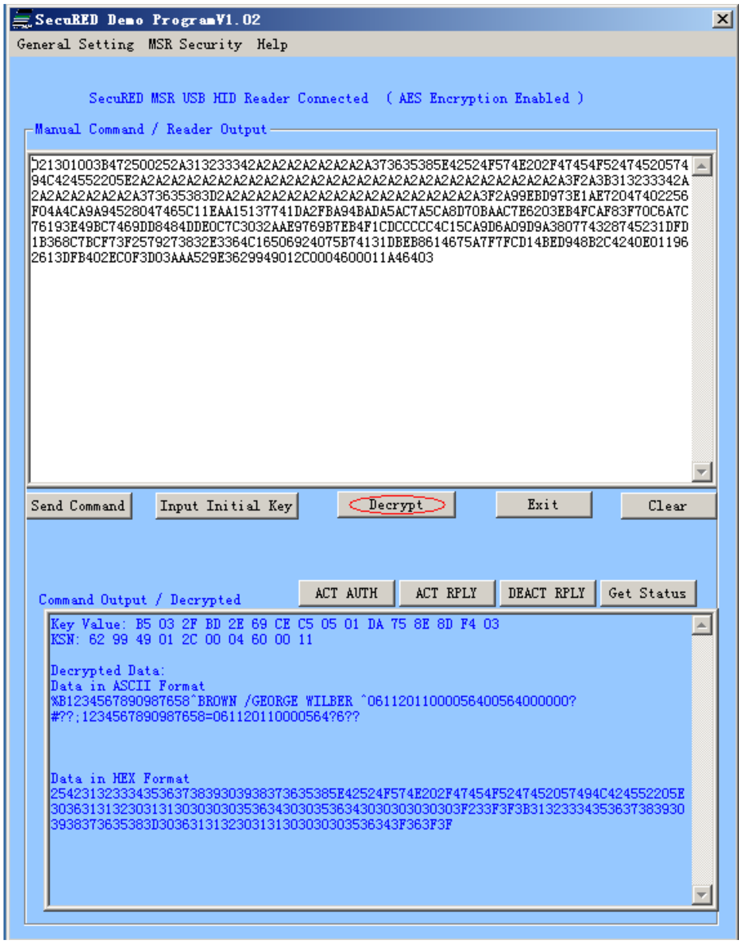


Decrypt data

Before decrypt data, please input the Base Derivation Key to decrypt data if the key injected is not ID Tech demo key "0123456789abcdeffedcba9876543210".



Then click the [Decrypt] button to decrypt data, and the decrypted card data will be showed in the lower window.



Note:

About SecuRED KB interface, please clear the Manual Command/Reader Output before swipe card in the upper window.

APPENDIX A Setting Parameters (Function ID) 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	
HTypeID*	10	Terminal Type	'0' (‘0’~’2’,'4'~'6')	PC/AT, Scan Code Set 2, 1, 3, PC/AT with external Keyboard and PC/AT without External Keyboard	k
BeepID	11	Beep Setting	‘2’ (‘0’~’4’)	Beep volume high and frequency high	
ChaDelayID	12	Character Delay	‘0’ (‘0’~’5’) ‘6’	2 ms inter-character delay ‘6 for 0 mS delay	k
TrackSelectID	13	Track Selection	‘0’ (‘0’~’9’) 0x30 – Any Track 0x31 – Track 1 Only 0x32 – Track 2 Only 0x33 – Track 1 & Track 2 0x34 – Track 3 Only 0x35 – Track 1 & Track 3 0x36 – Track 2 & Track 3 0x37 – All Three Tracks 0x38 – Track 1 Or Track 2 0x39 – Track 2 Or Track 3	Any Track 0-any; 1-7—bit 1 tk1, bit 2 tk2; bit 3 tk3. ‘8’—tk1-2; ‘9’ tk2-3	
PollingInterval ID	14	Polling Interval	1 (1 ~ 255)	USB HID Polling Interval	u
DataFmtID	15	Data Output Format	‘0’ (‘0’~’2’)	ID TECH Format;	-
FmtOptionID	16	UIC, Mag-Tek	H’59’	Refer to MiniMag RS232 User’s Manual	-
TrackSepID	17	Track Separator	CR/Enter	CR for RS232, Enter for KB any character supported except 00 which means none.	
SendOptionID	19	Send Option	‘1’ (‘0’~0x3f)	Sentinel and Account	

				number control Sentinel and Account number control 0x30 - Not send start/end sentinel and send all data on Track 2, not error notification. Control Key Output. 0x31 - Send start/end sentinel and send all data on Track 2, not send error notification. Control Key Output. 0x32 - Not send start/end sentinel and only send account number on Track 2, not send error notification. Control Key Output. 0x33 - Send start/end sentinel and only send account number on Track 2, not send error notification. Control Key Output. 0x34 - Not send start/end sentinel and send all data on Track 2, send error notification(default). Control Key Output. 0x35 - Send start/end sentinel and send all data on Track 2, send error notification. Control Key Output. 0x36 - Not send start/end sentinel and only send account number on Track 2, send error notification. Control Key Output. 0x37 - Send start/end sentinel and only send account number on Track 2, send error notification. Control Key Output. 0x38 - Not send start/end sentinel and send all data on Track 2, not error	

				notification. Alt Key Output. 0x39 - Send start/end sentinel and send all data on Track 2, not send error notification. Alt Key Output. 0x3a - Not send start/end sentinel and only send account number on Track 2, not send error notification. Alt Key Output. 0x3b - Send start/end sentinel and only send account number on Track 2, not send error notification. Alt Key Output. 0x3c - Not send start/end sentinel and send all data on Track 2, send error notification(default). Alt Key Output. 0x3d - Send start/end sentinel and send all data on Track 2, send error notification. Alt Key Output. 0x3e - Not send start/end sentinel and only send account number on Track 2, send error notification. Alt Key Output. 0x3f - Send start/end sentinel and only send account number on Track 2, send error notification. Alt Key Output.	
MSRReadingID	1A	MSR Reading	‘1’ (‘0’~’2’)	Enable/Disable MSR Reading 0x30 – MSR Reading Disabled 0x31 – MSR Reading Auto Mode Enabled 0x32 – MSR Reading Buffered Mode Enabled	
DTEnableSendID*	1B	DT Enable Send	‘0’(‘0’,’1’,’3’)	Data Editing Control 0x30 – Disable Data Edit. 0x31 – Data Edit Match mode.	d

				0x33 – Data Edit Unmatch mode	
DecodingMethodID	1D	Decoding Direction	‘1’ (‘0’~’3’)	Reading Direction 0x30 – Raw Data Decoding in Both Directions. 0x31 – Decoding 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	CR/Enter	CR for RS232, Enter for KB	
FmVerID	22	Firmware Version			
USBHIDFmtID	23	USB HID Fmt	‘0’ (‘0’~’1’)	ID TECH Format	ur
ForeignKBID	24	Foreign KB	'0' ('0' ~ '9')	Foreign Keyboard	k
SecureKeyID*	25	Obsolescent encryption	‘@’ (0x20-0x7F)	No simple encryption	
ArmtoReadID*	30				
CustSetID	30		00-07	.0 POS-X: Level 3 Non-CC send same as Level1 .1 Level3: No empty pkt when not enough sampling bits .2 Enhanced Secured Output will have SN after hash	
ReaderResetID*	32		None		
Track1PrefixID	34	Track 1 Prefix	0	No prefix for track 1, 6 char max	
Track2PrefixID	35	Track 2 Prefix	0	No prefix for track 2, 6 char max	
Track3PrefixID	36	Track 3 Prefix	0	No prefix for track 3, 6 char max	
Track1SuffixID	37	Track 1 Suffix	0	No suffix for track 1, 6 char max	
Track2SuffixID	38	Track 2 Suffix	0	No suffix for track 2, 6 char max	
Track3SuffixI	39	Track 3 Suffix	0	No suffix for track 3, 6 char	

D				max	
LZ1ID*	3C		0xD		-
Set50	3C	Set50		set MSR reg eeprom map	
LZ2ID*	3D		0xD		-
SwapT1T3ID	3D	Swap T1,T3	0x00,0x5A	0x5A:Swap T1 and T3. Will not be reset by 53 18	
LZ3ID*	3E		0xD		-
PinKeyID	3E		0x00,0x5A	0x5A– PinKey Can only set at level 1; Won't reset by 53 18;	
LZ4ID*	3F		0xD		-
EpVerID*	40		None		
BaudID	41	Baud Rate	'5' ('2'~'9')	9600 bps, '2' is 1200, '7' is 38,400 bps; '9' is 115.2 kbps	s
DataID	42	Data Bit	'0' ('0'~'1')	8 Bits required in secure mode	s
ParityID	43	Data Parity	'0' ('0'~'4')	None	s
HandID	44	Hand Shake	'0' ('0'~'1')	Software (Xon/Xoff) hand shake	s
StopID	45	Stop Bit	'0' ('0'~'1')	1 Bit	s
XOnID	47	XOn Character	DC1	0x11 as XOn	s
XOffID	48	XOff Character	DC3	0x13 as XOff	s
PrePANID	49	PAN to not mask	4 (0-6)	# leading PAN digits to display	e
PostPANID	4A	PAN to not mask	4 (0-4)	# of trailing PAN digits to display	e
MaskCharID	4B	mask the PAN with this character	'*' 20-7E	any printable character	e
CrypTypeID	4C	encryption type	'1' ('1'-'2')	'1' 3DES '2' AES	r e
OutputModeID	4D	Std, OPOS or JPOS	'0' ('0' ~ '1')	Standard mode	
SerialNumberID	4E	device serial #	any 8-10 bytes	8-10 hex serial number	r
DispExpDateID,	50	mask or display expiration date	'0''0'-'1'	'1' don't mask expiration date	e
CapsCaseID*	51		None		
DataSeqID*	52		None		
StartCharID*	53		None		
SessionID	54	8 byte hex not stored in EEPROM	None	always init to all 'FF'	e

Mod10ID	55	include mod10 check digit	'0' '0'-'2'	don’t include mod10, ‘1’ display mod10, ‘2’ display wrong mod10	e
DesKeyID	56	DES Key Value	0	internal use only	r e
AesKeyID	57	AES Key Value	0	internal use only	r e
KeyManageTypeID	58	DUKPT or Fixed key	‘1’(‘0’-‘1’)	‘0’ fixed key ‘1’ DUKPT key	-
T1GENERICFMTID*	59		None		
T2GENERICFMTID*	5A		None		
T3GENERICFMTID*	5B		None		
HashOptID,	5C		'3' (‘0’-‘7’)	Send tk1-2 hash bit 0:1 send tk1 hash; bit 1:1 send tk2 hash; bit2:1 send tk3 hash.	e
HexCaseID,	5D		'0' (‘0’-‘1’)		k
LRCID	60	LRC character	‘0’ (‘0’~’1’)	Without LRC in output	
T17BStartID	61	Track 1 7 Bit Start Char	‘%’	‘%’ as Track 1 7 Bit Start Sentinel	
T16BStartID	62	T16B Start	‘%’	‘%’ as Track 1 6 Bit Start Sentinel	
T15BStartID	63	T15B Start	‘;’	‘;’ as Track 1 5 Bit Start Sentinel	
T27BStartID	64	Track 2 7 Bit Start Char	‘%’	‘%’ as Track 2 7 Bit Start Sentinel	
T25BStartID	65	T25BStart	‘;’	‘;’ as Track 2 5 Bit Start Sentinel	
T37BStartID	66	Track 3 7 Bit Start Char	‘%’	‘%’ as Track 3 7 Bit Start Sentinel	
T36BStartID	67	T36BStart	‘!’	‘!’ as Track 3 6 Bit Start Sentinel	
T35BStartID	68	T35BStart	‘;’	‘;’ as Track 3 5 Bit Start Sentinel	
T1EndID	69	Track 1 End Sentinel	‘?’	‘?’ as End Sentinel	
T2EndID	6A	Track 2 End Sentinel	'?'	‘?’ as End Sentinel	
T3EndID	6B	Track 3 End Sentinel	'?'	‘?’ as End Sentinel	
T1ERRSTARTID	6C	Track 1 error code	‘%’	start sentinel if track 1 error report	
T2ERRSTAR	6D	Track 2 error	‘;’	start sentinel if track 2 error	

TID		code		report	
T3ERRSTAR TID	6E	Track 3 error code	‘+’	start sentinel if track 3 error report	
SecureLrcID	6F	Secured output format Lrc option	‘1’ (‘0’-‘1’)	‘1’ to send LRC in secured output data	e
BootloaderID *	70	Boot Loader Mode	None	N/A	-
T344EndID*	71		None		
T28BStartID	72	JIS T12 SS/ES	0		
T38BStartID	73	JIS T3 SS/ES	0		
FKChallenge	74	Fixed Key Challenge reply (Authenticate)	None	Not a setting command; Dynamically get challenge and authenticate commands 52 74 53 74	
SPISettingID	75		'0'		p
LoadFixKeyI D	76	Load Fixed Key	Null	All null before keyloading	
EquipFwID	77	feature option setting	3 (0-ff)	Reader firmware configuration .0 _secure .1 _hasLed .2 _asPP4; for PPMSR .3 _asITX for RS232 only .4 _mm (Data Edit) .5 _generic .6 _dualhead (HP only)	r
BeepOffComI D*	7A	Turn off Beep	‘0’ (‘0’-‘3’)		
SyncCheckID	7B	check for track sync bits	‘0’ (‘0’-2’)	check leading & trailing sync bits on track data (if poorly encoded card)	
ErrorZoneID*	7C		None		
MagTSecureL vlID	7D		‘1’ (‘0’-‘3’)		p
SecurityLevelI D	7E				n r
MagTCryptID	7F		'1'(‘0’-‘3’)		p
EnOptionID	84	Encryption Option (Forced encryption or not)	08	Bit 0: T1 force encrypt Bit 1 : T2 force encrypt Bit 2 : T3 force encrypt Bit3 : T3 force encrypt when card type is 0	e

EnStructID	85	Encryption Structure (Enhanced or original)	‘0’,(‘0’-‘1’)	‘0’ –Original Encrypt Structure ‘1’ – Enhanced Encrypt Structure	e
MaskOptID	86	Masked / clear data sending option	0x07	Bit0: T1 mask allowed Bit1: T2 mask allowed Bit2: T3 mask allowed	e
PwrStrDlyID*	87	Reserved for UNIMAG			
HashTypeID	88	Hash type selection	‘0’ (‘0’-‘1’)	‘0’ – SHA-1 20 bytes ‘1’ - SHA-2 32 bytes	e
FixKeyLeverID	8A	Review lever of the Fix key	‘1’(‘1’-‘3’)	Value from ‘1’-‘3’	
	A0				
	A1				
WinCETestID*	AA		None		
PrefixID	D2	Preamble	0	No Preamble, 15 char max	
PostfixID	D3	Postamble	0	No Postamble, 15 char max	
AddedFieldID*	FA	DE Added Field	0	No Added Field	d
SearchCmdID*	FB	DE Search Cmd	0	No Search Command	d
SendCmdID*	FC	DE Send Cmd	08 00 FF 00 FF 00 FF 00 FF	No Send Command	d
SearchCmdID2	FD	DE Search Cmd 2	0	No Search Command2	d

*Unused entries in this table were left for completeness even though unused in the Mag reader to avoid conflicting definitions between products.

Note not all function ID are present in different hardware version of the SecuRED the last column above has some codes:

‘-‘ feature not currently supported; exists for compatibility
‘s’ feature available on in the RS232 serial version of the reader
‘u’ feature available only in the USB version;
‘k’ feature available on in the keyboard version
‘p’ feature available only in the SPI version
‘r’ reset all does not affect this value
‘n’ not directly settable
‘d’ feature only for reader with data editing feature
‘e’ feature only for reader with encrypt feature

Most function ID settings that relate to the content of formatting of the track output do not work in secure mode. Exceptions to this are Preamble and Postamble in keyboard mode only.

APPENDIX B   ERROR CODE LIST TABLE

Order	Error code	Note
1	0xE0 00	No Card Account number(Paring key part).
2	0xE1 00	Paring key don’t exist. Operate related command before loading Paring key.
3	0xE2 00	Paring key has existed.
4	0xE3 00	The parameter doesn’t match. Parameter of the command doesn’t match requirement.
5	0xE4 00	Fail to decrypt data.
6	0xE5 (ID code)	Command length is error. ID code is command ID.
7	0xE6 (ID code)	Parameter is error. The parameter is out scope.
8	0xE7 (ID code)	Command is error. The device don’t support the command.
9	0xE8 00	Command LRC is error.
10	0xE9 00	Command time overflow.
11	0xEA 00	Operation is error. It is often occured by error operation order.
12	0xEB 00	Random data don`t match.
13	0xEC 00	MSR key has existed.
14	0xED 00	MSR key don`t exist.
15	0xEE 00	Secure level don`t match requirement.
16	0xEF 00	EEPROM write error.
17	0x00 00	No error

APPENDIX C Key Code Table in USB Keyboard Interface

For most characters, "Shift On" and "Without Shift" will be reverse if Caps Lock is on.

Firmware needs to check current Caps Lock status before sending out data.

For Function code B1 to BA, if "Num Lock" is not set, then set it and clear it after finishing sending out code.

For Function code BB to C2, C9 to CC, if "Num Lock" is set then clear it and set it after finishing sending out code.

Keystroke	Hex Value	Functional Code	USB KB Code
Ctrl+2	00		1F Ctrl On
Ctrl+A	01		04 Ctrl On
Ctrl+B	02		05 Ctrl On
Ctrl+C	03		06 Ctrl On
Ctrl+D	04		07 Ctrl On
Ctrl+E	05		08 Ctrl On
Ctrl+F	06		09 Ctrl On
Ctrl+G	07		0A Ctrl On
BS	08	\bs	2A
Tab	09	\tab	2B
Ctrl+J	0A		0D Ctrl On
Ctrl+K	0B		0E Ctrl On
Ctrl+L	0C		0F Ctrl On
Enter	0D	\enter	28
Ctrl+N	0E		11 Ctrl On
Ctrl+O	0F		12 Ctrl On
Ctrl+P	10		13 Ctrl On
Ctrl+Q	11		14 Ctrl On
Ctrl+R	12		15 Ctrl On
Ctrl+S	13		16 Ctrl On
Ctrl+T	14		17 Ctrl On
Ctrl+U	15		18 Ctrl On
Ctrl+V	16		19 Ctrl On
Ctrl+W	17		1A Ctrl On
Ctrl+X	18		1B Ctrl On
Ctrl+Y	19		1C Ctrl On
Ctrl+Z	1A		1D Ctrl On

ESC	1B	\esc	29
Ctrl+\	1C		31 Ctrl On
Ctrl+]	1D		30 Ctrl On
Ctrl+6	1E		23 Ctrl On
Ctrl+-	1F		2D Ctrl On
SPACE	20		2C
!	21		1E Shift On
"	22		34 Shift On
#	23		20 Shift On
$	24		21 Shift On
%	25		22 Shift On
&	26		24 Shift On
'	27		34
(	28		26 Shift On
)	29		27 Shift On
*	2A		25 Shift On
+	2B		2E Shift On
,	2C		36
-	2D		2D
.	2E		37
/	2F		38
0	30		27 Shift On
1	31		1E Shift On
2	32		1F Shift On
3	33		20 Shift On
4	34		21 Shift On
5	35		22 Shift On
6	36		23 Shift On
7	37		24 Shift On
8	38		25 Shift On
9	39		26 Shift On
:	3A		33 Shift On
;	3B		33
<	3C		36 Shift On
=	3D		2E
>	3E		37 Shift On
?	3F		38 Shift On
@	40		1F
A	41		04 Shift On
B	42		05 Shift On
C	43		06 Shift On
D	44		07 Shift On
E	45		08 Shift On

F	46		09 Shift On
G	47		0A Shift On
H	48		0B Shift On
I	49		0C Shift On
J	4A		0D Shift On
K	4B		0E Shift On
L	4C		0F Shift On
M	4D		10 Shift On
N	4E		11 Shift On
O	4F		12 Shift On
P	50		13 Shift On
Q	51		14 Shift On
R	52		15 Shift On
S	53		16 Shift On
T	54		17 Shift On
U	55		18 Shift On
V	56		19 Shift On
W	57		1A Shift On
X	58		1B Shift On
Y	59		1C Shift On
Z	5A		1D Shift On
[	5B		2F
\	5C		31
]	5D		30
^	5E		23 Shift On
_	5F		2D Shift On
`	60		35
a	61		04
b	62		05
c	63		06
d	64		07
e	65		08
f	66		09
g	67		0A
h	68		0B
i	69		0C
j	6A		0D
k	6B		0E
l	6C		0F
m	6D		10
n	6E		11
o	6F		12
p	70		13

q	71		14
r	72		15
s	73		16
t	74		17
u	75		18
v	76		19
w	77		1A
x	78		1B
y	79		1C
z	7A		1D
{	7B		2F Shift On
|	7C		31 Shift On
}	7D		30 Shift On
~	7E		35 Shift On
DEL	7F		2A
F1	81	\f1	3A
F2	82	\f2	3B
F3	83	\f3	3C
F4	84	\f4	3D
F5	85	\f5	3E
F6	86	\f6	3F
F7	87	\f7	40
F8	88	\f8	41
F9	89	\f9	42
F10	8A	\fa	43
F11	8B	\fb	44
F12	8C	\fc	45
Home	8D	\home	4A
End	8E	\end	4D
→	8F	\right	4F
←	90	\left	50
↑	91	\up	52
↓	92	\down	51
PgUp	93	\pgup	4B
PgDn	94	\pgdn	4E
Tab	95	\tab	2B
bTab	96	\btab	2B Shift On
Esc	97	\esc	29
Enter	98	\enter	28
Num_Enter	99	\num_enter	58
<u>Delete</u>	9A	\del	4C
Insert	9B	\ins	49

Backspace	9C	\bs	2A
SPACE	9D	\sp	2C
Pause	9C	\ps	48
Ctrl+[	9F	\ctr1	2F Ctrl On
Ctrl+]	A0	\ctr2	30 Ctrl On
Ctrl+\	A1	\ctr3	31 Ctrl On
Left_Ctrl_Break	A2	\l_ctrl_bk	Clear Ctrl Flag
Left_Ctrl_Make	A3	\l_ctrl_mk	Set Ctrl Flag for following char(s)
Left_Shift_Break	A4	\l_shift_bk	Clear Shift Flag
Left_Shift_Make	A5	\l_shift_mk	Set Shift Flag for following char(s)
Left_Windows	A6	\l_windows	E3 (left GUI)
Left_Alt_Break	A7	\l_alt_bk	Clear Alt Flag
Left_Alt_Make	A8	\l_alt_mk	Set Alt Flag for following char(s)
Right_Ctrl_Break	A9	\r_ctrl_bk	Clear Ctrl Flag
Right_Ctrl_Make	AA	\r_ctrl_mk	Set Ctrl Flag for following char(s)
Right_Shift_Break	AB	\r_shift_bk	Clear Shift Flag
Right_Shift_Make	AC	\r_shift_mk	Set Shift Flag for following char(s)
Right_Windows	AD	\r_windows	E7 (right GUI)
Right_Alt_Break	AE	\r_alt_bk	Clear Alt Flag
Right_Alt_Make	AF	\r_alt_mk	Set Alt Flag for following char(s)
Num_Lock	B0	\num_lock	53
Num_0	B1	\num0	62 Num Lock On
Num_1	B2	\num1	59 Num Lock On
Num_2	B3	\num2	5A Num Lock On
Num_3	B4	\num3	5B Num Lock On
Num_4	B5	\num4	5C Num Lock On
Num_5	B6	\num5	5D Num Lock On
Num_6	B7	\num6	5E Num Lock On
Num_7	B8	\num7	5F Num Lock On
Num_8	B9	\num8	60 Num Lock On
Num_9	BA	\num9	61 Num Lock On
Num_Home	BB	\num_home	5F
Num_PageUp	BC	\num_pgup	61
Num_PageDown	BD	\num_pgdn	5B
Num_End	BE	\num_end	59
Num_↑	BF	\num_up	60
Num_→	C0	\num_right	5E
Num_↓	C1	\num_down	5A
Num_←	C2	\num_left	5C

Print_Scrn	C3	\prt_sc	46
System_Request	C4	\sysrq	9A
Scroll_Lock	C5	\scroll	47
Pause	C6	\menu	76
Break	C7	\break	
Caps_Lock	C8	\caps_lock	39
Num_/	C9	\num_/	54
Num_*	CA	\num_*	55
Num_-	CB	\num_-	56
Num_+	CC	\num_+	57
Num_.	CD	\num_.	63 Num Lock On
Num_DEL	CE	\num_del	63
Num_INS	CF	\num_ins	62
Delay_100ms	D0	\delay	Delay 100 ms

Table of Ctrl or Alt output for non printable characters

ASCII Code	Control Code	Alt Code
SendOptionID	Bit 3: 0	Bit 3: 1
00:	Ctrl-2	Alt-000
01:	Ctrl-A	Alt-001
02:	Ctrl-B	Alt-002
03:	Ctrl-C	Alt-003
04:	Ctrl-D	Alt-004
05:	Ctrl-E	Alt-005
06:	Ctrl-F	Alt-006
07:	Ctrl-G	Alt-007
08:	BS	Alt-008
09:	Tab	Alt-009
0A:	Ctrl-J	Alt-010
0B:	Ctrl-K	Alt-011
0C:	Ctrl-L	Alt-012
0D:	Enter	Alt-013
0E:	Ctrl-N	Alt-014
0F:	Ctrl-O	Alt-015
10:	Ctrl-P	Alt-016
11:	Ctrl-Q	Alt-017
12:	Ctrl-R	Alt-018
13:	Ctrl-S	Alt-019
14:	Ctrl-T	Alt-020
15:	Ctrl-U	Alt-021
16:	Ctrl-V	Alt-022
17:	Ctrl-W	Alt-023
18:	Ctrl-X	Alt-024

19:	Ctrl-Y	Alt-025
1A:	Ctrl-Z	Alt-026
1B:	ESC	Alt-027
1C:	Ctrl-\	Alt-028
1D:	Ctrl-]	Alt-029
1E:	Ctrl-6	Alt-030
1F:	Ctrl--	Alt-031