USER MANUAL

SecureKey™ M100/M130
Encrypted Keypad with Optional Encrypted MSR

XML Format

80120504-001-A
July 31, 2013

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

Revision History

Revision	Description	Date
A	Initial Release	08/13/2013

Table of Contents

1.0 Introduction

ID TECH SecureKey M series is an encrypted numeric keypad with an optional Magnetic Swipe Reader (MSR). The Secure keypad allows the retailers to not only encrypt credit card data at the magnetic reader but it also encrypts a manually entered credit card number. The SecureKey M series has 15 keys (10 Numeric, 5 functional) with a 2x20 backlit LCD.

SecureKey M series keypads encrypt the data using TDES or AES algorithm format with DUKPT key management. For encrypted card reader settings and operations, please refer to 80096504-001 SecureMag User Manual.

SecureKey M series is available in USB-Keyboard and USB-HID interface.

2.0 Product Configurations

SecureKey M series include 2 main models:

- SecureKey M100: Encrypted Keypad
- SecureKey M130: Encrypted Keypad with Magstripe Card Reader

Currently we offer the following configurations:

TDES encryption default

1. IDKE-504800BL SecureKey M100 XML Format, TDES
2. IDKE-534833BL SecureKey M130 XML Format, TDES

AES encryption default

3. IDKE-504800ABL SecureKey M100 XML Format, AES
4. IDKE-534833ABL SecureKey M130 XML Format, AES

3.0 Features

- Encrypted numeric keypad with 2x20 LCD and optional encrypted MSR
- 1,000,000 swipe, industry proven Magnetic Stripe Reader
- 20,000,000 key operations for each key
- Meets FCC Class B & CE regulatory requirements
- Plug-n-Play operation for USB-Keyboard and USB-HID interface
- Keypad is encrypted using DUKPT and TDES/AES encryption.
- Optional encrypted MSR with DUKPT and TDES/AES encryption
- Works with Windows 95/98, WINME 2000, XP, Vista, & Windows 7

4.0 Terms and Abbreviations

AAMVA	American Association of Motor Vehicle Administration
ABA	American Banking Association
AES	Advanced Encryption Standard
ANSI	American National Standard Institute
ASIC	Application Specific Integrated Circuit
BPI	Bits per Inch
CE	European Safety and Emission approval authority
DES	Data Encryption Standard
DUKPT	Derived Unique Key Per Transaction
ESD	Electrostatic Discharge
GND	Signal Ground
HOST	A Personal Computer or Similar Computing Device
HID	Human Interface Device
IPS	Inches per Second
ISO	International Organization for Standardization
JIS	Japanese Industrial Standard
KSN	Key Serial Number
LRC	Longitudinal Redundancy Check Character.
MAC	Message Authentication Code
MSR	Magnetic Stripe Reader
MTBF	Mean Time Between Failures
OTP	One Time Programmable
PAN	Primary account number
PCI	Payment Card Industry
PID	USB Product ID
POS	Point of Sale
P/N	Part Number
RoHS	Restrictions of Hazardous Substances
T1,T2,T3	Track 1 data, Track 2 data, Track 3 data
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus
VID	USB Vendor ID

Note: many unusual words used in this document are defined in Appendix A Setting Configuration Parameters and Values table on page38.

5.0 Applicable Documents

ISO 7810 – 1985	Identification Cards – Physical
ISO 7811 - 1 through 6	Identification Cards - Track 1 through 3
ISO 7812	Identification Cards – Identification for issuers Part 1 & 2
ISO 7813	Identification Cards – Financial Transaction Cards
ISO 4909	Magnetic stripe content for track 3
ANSI X.94	Retail Financial Services Symmetric Key Management
USB ORG	USB Specification Rev. 2.0

Keyboard Key Code Specification Revision 1.3a, 3/16/2000, Microsoft Corporation
80096504-001 SecureMag User Manual

6.0 Function & Operation

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

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

6.1 Function Keys Operation:

Clear:

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

BS:

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

#Admin:

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

Cancel:

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

6.2 Admin Menu

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

<u>Manually-Keyed Configuration Options (Firmware Version v1.14 or below)</u>
Configuration #1: Card Number, Expiration Date
Configuration #2: Card Number, Expiration Date, Zip Code
Configuration #3: Card Number, Expiration Date, Street Number of the Address, Zip Code
Configuration #4: Card Number, Expiration Date, Zip Code, Security Code
Configuration #5: Card Number, Expiration Date, Address, Zip Code, Security Code
Configuration #6: Card Number, Expiration Date, Address, Security Code

<u>Manually-Keyed Configuration Options (Firmware Version v1.16 or above)</u>

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

When the user selects the key corresponding to a manual mode, and then selects enter, the mode will be configured and the unit will return to the data capture mode.
If the user selects more than one key, then the last key selected will be used to select the mode.
If a invalid key is selected the unit will display **"error"** then **"Select manual config 1-6"**

6.3 Help Mode

If the user selects the Admin key while in Admin mode, the unit enters the Help Mode. In the Help Mode, the unit displays short text messages of the various manual entry configurations with a 3 seconds pause between each message. Hitting any key in the Help Mode makes the unit return to the Admin Menu.

7.0 Configuration

The reader must be appropriately configured to your application. Configuration settings enable the reader to work with the host system. Once programmed, these configuration settings are stored in the reader's non-volatile memory (so they are not affected by the cycling of power).

7.1 Setup Command Structure

Commands sent to keypad/reader

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

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

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

Response from SecureKey

a. Setting Command

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

b. Read Status Command

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

c. Other Commands

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

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
<CheckSum>	Check Sum: The overall Modulo 2 (Exclusive OR) sum (from <STX> to <CheckSum>) should be zero.
<ACK>	06h
<NAK>	FD for USB KB interface 15 for all other interface

7.2 Communication Timing

The SecureKey takes time to process a command. During that processing time, it will not respond to a new command.

The typical delay for the reader to respond to a command is 20ms, the maximum delay for the reader to respond can be as much as 40ms. Caution must therefore be taken to maintain a minimum delay between two commands.

7.3 Default Settings

The SecureKey is shipped from the factory with the default settings already programmed. In the following sections, the default settings are shown in **boldface**.

For a table of default settings, see Appendix A.

7.4 General Selections

This group of configuration settings defines the basic operating parameters of SecureKey.

7.4.1 Change to Default Settings

<STX><S><18h><ETX><CheckSum>

This command does not have any <FuncData>. It returns most settings to their default values.

7.4.2 MSR Reading Settings

Enable or Disable the SecureKey swipe reader. If the swipe reader is disabled, no data will be sent out to the host.
<STX><S><1Ah><01h><MSR Reading Settings><ETX><CheckSum>

MSR Reading Settings:

"0" MSR Reading Disabled

"1" MSR Reading Enabled

7.4.3 Decoding Method Settings

The SecureKey can support four kinds of decoded directions.
<STX><S><1Dh><01h><Decoding Method Settings><ETX><CheckSum>
Decoding Method Settings:
"0" Raw Data Decoding in Both Directions,
"1" Decoding in Both Directions.
"2" Moving stripe along head in direction of encoding.
"3" Moving stripe along head against direction of encoding.

With the bi-directional method, the user can swipe the card in either direction and still read the data encoded on the magnetic stripe. Otherwise, the card can only be swiped in one specified direction to read the card. Raw Decoding just sends the card's magnetic data in groups of 4 bits per character. The head reads from the first byte of each track, starting from the most significant bit. The data starts to being collected when the first 1 bit is detected. No checking is done except to verify track has or does not have magnetic data.

7.5 Review Settings

<STX><R><1Fh><ETX><CheckSum>

This command does not have any <FuncData>. It activates the review settings command. SecureKey sends back an <ACK> and <Response>.
<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>

7.6 Review Serial Number

<STX><R><4Eh><ETX><CheckSum>

This command is to get device serial number.

7.7 Controlling Keyed-in Options

7.7.1 Configuration byte 8F controls Keyed in options

bit 0: if 0: output in original keyed output; 1: output in enhanced keyed-in output
bit 1: if 0: allow empty CVV entry; 1: require 3 or more CVV digits
bit 2: if 0: allow empty ZIP entry; 1: require 5 or more ZIP digits
bit 3: if 0: allow empty ADR entry; 1: require 1 or more ADR digits
bit 4: if 0: do mod-10 check on keyed-in PAN; 1: don't check PAN mod-10
bits 5-7: reserved all zero
Note: bits 1 through 3 are only applicable if the reader is configured for Manually-Keyed Configuration Options greater than 1 and only apply to firmware version 1.16 and above.

7.7.2 Configuration byte 8E Setting Admin Level Options

The reader can be configured to set the manually Keyed-in Configuration option in two ways first selecting the Admin key then a number from 1 to 6. For the meaning of these numbers see section 6.2 admin menu.

7.8 Message Formatting Selections

7.8.1 Preamble Setting

Characters can be added to the beginning of a string of data. These can be special characters for identifying a specific reading station, to format a message header expected by the receiving host, or any other character string. Up to fifteen ASCII characters can be defined.

<STX><S><D2h><Len><Preamble><ETX><CheckSum>

Where:
<Len>= the number of bytes of preamble string
<Preamble> = {string length}{string}
NOTE: String length is one byte, maximum fifteen <0Fh>.

7.8.2 Postamble Setting

The postamble serves the same purpose as the preamble, except it is added to the end of the data string, after any terminator characters.

<STX><S><D3h><Len><Postamble><ETX><CheckSum>

Where:
<Len> = the number of bytes of postamble string
<Postamble> = {string length}{string}
NOTE: String length is one byte, maximum fifteen <0Fh>.

7.9 Magnetic Track Selections

7.9.1 Track Selection

There are up to three tracks of encoded data on a magnetic stripe.

This option selects the tracks that will be read and decoded.

<STX><S><13h><01h><Track_Selection Settings><ETX><CheckSum>

Track_Selection Settings:

"0" Any Track this is the only setting supported

Note: If any of the required multiple tracks fail to read for any reason, no data for any track will be sent.

7.10 Set MSR Data Terminator [53 21]

<STX><S><21h><01h><Terminator Setting><ETX><CheckSum>

The <Terminator Setting> byte is any one byte except 0x00:

The default is 0x0D, which is Carriage Return (CR), If 0x00 is set the reader will send no terminator.

Example to set to send Line Feed (LF=0x0A) after the last MSR data

<STX><S><21h><01h><0Ah><ETX><CheckSum>

The terminator value 30 is special it will send out two

characters CRLF or OD and OA

A Value of 0x00 means do not send any MSR data terminator.

7.11 Security Settings

7.11.1 Encryption Settings

Encryption type output.

<STX><S><4Ch><01h><Encryption Settings><ETX><CheckSum>

Encryption Settings:

"1" Enable TDES Encryption

"2" Enable AES Encryption

7.12 Review KSN (DUKPT Key management only)

<STX><R><51h><ETX><CheckSum>

This command is to get DUKPT key serial number and counter.

Response:

<ACK><STX><51h><0Ah><10 BYTE KSN><ETX><CheckSum>

Example:
06 02 51 0A 62 99 49 01 45 00 00 00 00 1B 03 B7

7.13 Review Security Level

<STX><R><7Eh><ETX><CheckSum>

This command is to get the current security level.

Response:
<STX><7E><01><33h><ETX><CheckSum>

7.14 Control Credit Card Output when Card Swiped Lifted

<STX><S><AFh><01h><Control Settings><ETX><CheckSum>

Control Settings:

01h Disallow Credit Card swiped while lifted

00h Allow to send credit card data unencrypted when on shifted track

If a credit card is swiped, while the card is lifted, it is possible to get a good card read, where track 1 data is shifted into track 2 or track 3 and/or where track 2 data is shifted into track 3. Since the credit card data is always normally encrypted, this potentially allows the credit card data to be sent without encryption exposing the card contents. By default this is allowed. This feature was added in V1.23.

7.15 Encrypted Output for Decoded Data

7.15.1 Encrypt Functions

When a card is swiped through the Reader, the track data will be TDEA (Triple Data Encryption Algorithm, aka, Triple DES) or AES (Advanced Encryption Standard) encrypted using DUKPT (Derived Unique Key Per Transaction) key management. DUKPT key management uses a base derivation key to encrypt a key serial number that produces an initial encryption key which is injected into the Reader prior to deployment. After each transaction, the encryption key is modified per the DUKPT algorithm so that each transaction uses a unique key. Thus, the data will be encrypted with a different encryption key for each transaction.

7.15.2 Security Related Function ID

Security Related Function IDs are listed below. Their functions are described in other sections.

Characters	Hex Value	Description

PrePANID	49	First N Digits in PAN which can be clear data
PostPANID	4A	Last M Digits in PAN which can be clear data
MaskCharID	4B	Character used to mask PAN
EncryptionID	4C	Security Algorithm
Device Serial Number ID	4E	Device Serial Number (Can be write once. After that, can only be read)
DisplayExpirationDateID	50	Display expiration data as mask data or clear data
KSN and Counter ID	51	Review the Key Serial Number and Encryption Counter format v1.22) 51 0A KSN
Session ID	54	Set current Session ID
Key Management Type ID	58	Select Key Management Type
HashOptID	5C	to include or not hash data
SecurityLevelID	7E	Security Level (Read Only)
EncryptOptID	84	which tracks to encrypt
EncryptStrID	85	original or enhanced swipe encrypt structure
MaskOptID	86	which tracks to mask
EnFmtID	88	for XML
T3ExpDatePosID	89	offset to date on ISO4049 track 3
KeyedOptID	8F	original or enhanced keyed-in encrypt structure
Equip2ID	AE	unusual special settings control
CustSet2ID	AF	check for cc tracks shifted due to swipe while card lifted

Feasible settings of these new functions are listed below.

Characters	Default Setting	Description
PrePANID	04h	00h ~ 06h Allowed clear text from start of PAN Command format: 02 53 49 01 04 03 LRC
PostPANID	04h	00h ~ 04h Allowed clear text from end of PAN Command format: 02 53 4A 01 04 03 LRC
MaskCharID	‘*’	20h ~ 7Eh Command format: 02 53 4B 01 3A 03 LRC

DisplayExpirationDataID	'0'	'0' Display expiration data as mask data '1' Display expiration data as clear data
EncryptionID	'0'	'0' Clear Text '1' Triple DES '2' AES Command format: 02 53 4C 01 31 03 LRC
SecurityLevelID	'1'	'0' ~ '3' Command format: 02 52 7E 03 LRC
Device Serial Number ID	00, 00, 00, 00, 00, 00, 00, 00, 00, 00	10 bytes number: Command format: Set Serial Number: 02 53 01 4E 09 08 37 36 35 34 33 32 31 30 03 LRC Get Serial Number: 02 52 4E 03 LRC
KSN and Counter ID	00, 00, 00, 00, 00, 00, 00, 00, 00, 00	This field includes the Initial Key Serial Number in the leftmost 59 bits and a value for the Encryption Counter in the right most 21 bits. Get DUKPT KSN and Counter: 02 52 51 03 LRC
Session ID	00, 00, 00, 00, 00, 00, 00, 00	This Session ID is an eight bytes string which contains any hex data. This filed is used by the host to uniquely identify the present transaction. Its primary purpose is to prevent replays. It is only be used at Security Level 4. After a card is read, the Session ID will be encrypted, along with the card data, a supplied as part of the transaction message. The clear text version of this will never be transmitted. New Session ID stays in effect until one of the following occurs: 1. Another Set Session ID command is received. 2. The reader is powered down. 3. The reader is put into Suspend mode.
Key Management Type ID	'1'	Fixed key management by default. '1': DUKPT Key
HashOptID	'7'	hash all encrypted tracks
SecurityLevelID	'3'	Security Level (Read Only)

EncryptOptID	0	which tracks to encrypt
EncryptStrID	'1'	to use original or enhanced swipe encryption format
MaskOptID	7	which tracks may be sent masked
EnFmtID	023034	
T3ExpDatePosID	34	offset to track 3 expire date position
KeyedOptID	0 or 1	to use original or enhanced keyed in encryption format.
Equip2ID	00 (any)	if bit 4 is set high, the USB enumeration will include the reader's serial number.
CustSet2ID	**00H** (or 01H)	bit0=0 send unencrypted as other type card; bit0=1 disallow a credit card shifted 1 or 2 tracks

7.15.3 Security Management

This reader is intended to be a secure reader. Security features include:

- Can include Device Serial Number
- Can encrypt track 1, track 2, and track 3 data for bank cards and other cards
- Provides clear text confirmation data including card holder's name and a portion of the PAN as part of the Masked Track Data for bank cards
- Optional display expiration date
- Security Level is settable

The reader features configurable security settings. Before encryption can be enabled, Key Serial Number (KSN) and Base Derivation Key (BDK) must be loaded before encrypted transactions can take place. The keys are to be injected by certified key injection facility.

7.15.4 MSR Data Masking

For ABA cards needing to be encrypted, encrypted data, hash data and clear text data maybe sent.

Masked Area

The data format of each masked track is ASCII.

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

8.0 Descriptor

The USB version of the reader can be operated in two different modes:
- HID ID TECH mode (herein referred to as "***HID*** mode")
- HID with Keyboard Emulation (herein referred to as "***KB*** mode").

When the reader is operated in the HID mode, it behaves like a vendor defined HID device. A direct communication path can be established between the host application and the reader without interference from other HID devices.

8.1 Descriptor Tables

Device Descriptor:

Field	Value	Description
Length	12	
Des type	01	
bcd USB	00 02	USB 2.0
Device Class	00	Unused
Sub Class	00	Unused
Device Protocol	00	Unused
Max Packet Size	08	
VID	0A CD	
PID	26 10 26 20	HID ID TECH StructureHID Keyboard
BCD Device Release	00 01	
i-Manufacture	01	
i-Product	02	
i-Serial-Number	00	Changes to 3 if USB serial number enabled
# Configuration	01	

Configuration Descriptor:

Field	Value	Description
Length	09	
Des type	02	
Total Length	22 00	
No. Interface	01	
Configuration Value	01	
iConfiguration	00	
Attributes	80	Bus power, no remove wakeup
Power	32	100 mA

Interface Descriptor:

Field	Value	Description
Length	09	
Des type	04	
Interface No.	00	
Alternator Setting	00	
# EP	01	
Interface Class	03	HID
Sub Class	01	
Interface Protocol	01	
iInterface	00	

HID Descriptor:

Field	Value	Description
Length	09	
Des type	21	HID
bcdHID	11 01	
Control Code	00	
numDescriptors	01	Number of Class Descriptors to follow
DescriptorType	22	Report Descriptor
Descriptor Length	37 00 3D 00 52 00	HID ID TECH format HID Other format HID Keyboard format

End Pointer Descriptor:

Field	Value	Description
Length	07	
Des Type	05	End Point
EP Addr	83	EP3 – In
Attributes	03	Interrupt
MaxPacketSize	40 00	
bInterval	01	

Report Descriptor: (USB-HID Setting)

Value	Description
06 00 FF	Usage Page (MSR)
09 01	Usage(Decoding Reader Device)
A1 01	Collection (Application)
15 00	Logical Minimum
26 FF 00	Logical Maximum
75 08	Report Size
09 20	Usage (Tk1 Decode Status)
09 21	Usage (Tk2 Decode Status)
09 22	Usage (Tk3 Decode Status)
09 28	Usage (Tk1 Data Length)
09 29	Usage (Tk2 Data Length)
09 2A	Usage (Tk3 Data Length)
09 38	Usage (Card Encode Type)
95 07	Report Count
81 02	Input (Data, Var, Abs, Bit Field)
09 30	Usage (Total Sending Length)

95 02	Report Count (2)
82 02 01	Input (Data, Var, Abs, Bit Field)
09 31	Usage (Output Data)
96 9A 02	Report Count (666)
82 02 01	Input (Data, Var, Abs, Bit Field)
09 20	Usage (Command Message)
95 08	Report Count
B2 02 01	Feature (Data,Var, Abs, Buffered Bytes)
C0	End Collection

Report Descriptor: (USB KB Interface)

Value	**Description**
05 01	Usage Page (Generic Desktop)
09 06	Usage(Keyboard)
A1 01	Collection (Application)
05 07	Usage Page (Key Codes)
19 E0	Usage Minimum
29 E7	Usage Maximum
15 00	Logical Minimum
25 01	Logical Maximum
75 01	Report Size
95 08	Report Count
81 02	Input (Data, Variable, Absolute)
95 01	Report Count (1)
75 08	Report Size
81 01	Input Constant
95 05	Report Count
75 01	Report Size
05 08	Usage Page (LED)
19 01	Usage Minimum
29 05	Usage maximum
91 02	Output(Data Variable Absolute)
95 01	Report Count
75 03	Report Size
91 01	Output (Constant)
95 06	Report Count
75 08	Report Size
15 00	Logical Minimum
25 66	Logical Maximum (102)
05 07	Usage Page (key Code)
19 00	Usage Minimum

29 66	Usage Maximum (102)
81 00	Input(Data, Array)
06 2D FF	Usage Page (ID TECH)
95 01	Report Count
26 FF 00	Logical maximum (255)
15 01	Logical Minimum
75 08	Report Size (8)
09 20	Usage (Setup data byte)
95 08	Report Count (8)
B2 02 01	Feature (Data Var, Abs)
C0	End Collection

9.0 Data Output Format

9.1 XML Data Output Format

The XML data output format is as below. Messages (swiped and keyed credit, debit, other, gift, drivers licenses, etc.) need to include at least the <Addr></Addr> tag. The XML tags needs to be in the following order:

```
<DvcMsg Ver="1.1">
    <Dvc attribute list ...></Dvc>
    <Card attribute list ...></Dvc>
    <Addr attribute list ...></Dvc>
    <Tran attribute list ...></Dvc>
</DvcMsg>
```

Field Name	Attribute	Required	Max Length	Type	Description
Ver	DvcMsg	Required	10	String	Device Message Version (use 1.1)
App	Dvc	Required	50	String	Application Name
AppVer	Dvc	Required	10	String	Application Version
DvcType	Dvc	Required	40	String	Device Type (MODEL-MANUFACTURER)
DvcSN	Dvc	Required	40	String	Device Serial Number
Entry	Dvc	Required	20	String	Card Entry Method (SWIPE, MANUAL, CONTACTLESS)
CEncode	Card	Optional	2	Integer	Card Encoding Type: 0 = ISO/ABA 1 = AAMVA 2 = Keyed (Manual Keyed) 3 = Other
Trk1	Card	Optional	240	String	Track 1 (currently only used for non-financial cards)
Trk2	Card	Optional	180	String	Track 2 (currently only used for non-financial cards)
Trk3	Card	Optional	180	String	Track 3 (currently only used for non-financial cards)
ETrk1	Card	Optional	240	String	Encrypted Track 1
ETrk2	Card	Optional	180	String	Encrypted Track 2
ECData	Card	Optional	180	String	Encrypted Card Data (Card Number=ExpDate(YYMM)=Security Code)
CDataKSN	Card	Optional	40	String	Card Data Key Serial Number
MskPAN	Card	Optional	30	String	Masked PAN. Format: 4003********6781
Exp	Card	Optional	8	String	Expiration Date. Format: YYMM
CHolder	Card	Optional	80	String	Cardholder Name
AVSAddr	Addr	Optional	50	String	AVS Address
AVSZip	Addr	Optional	20	String	AVS Zip Code
TranType	Tran	Required	40	String	Transaction Type (CREDIT, DEBIT)

Field Name	Attribute	Required	Max Length	Type	Description
EFormat	Card	Optional	2	Integer	Encryption Format: 0 = Default 1 = Format1 2 = Format2 3 = Format3 4 = Format4 5 = Reserved for future use 6 = Reserved for future use

The data output format is XML output message protocol.

The DvcType, DvcApp, DvcMsgVer, and AppVer field can be configured by the following commands:

53 77 53 4B <function ID><data length> <data>

Set DvcType example: 53 77 53 4B 5C 0B 4D 31 33 30 2D 49 44 54 45 43 48

Set DvcApp example: 53 77 53 4B 5D 12 53 65 63 75 72 65 4B 65 79 20 53 6F 66 74 77 61 72 65

Set DvcMsgVer example: 53 77 53 4B 5E 03 31 2E 30

Set AppVer example: 53 77 53 4B 5F 03 31 2E 30

Credit Card Swipe Sample XML:

<DvcMsg Ver="1.1"><Dvc App="SecureKey Software" AppVer="1.0" DvcType="M130-IDTECH" DvcSN="0000000000" Entry="SWIPE"></Dvc><Card CEncode=" 0" ETrk1="9719BCB11786D9F5D26CD2350C6307D82FA980E6E73A02760F2383C2AF9BB8A6A875083B049582C91FCB542A06591DF223034C1A9EAC64A3166406B8516123F5200AC773BAF8ECDD" ETrk2="4623A11A24D344A71137EB2EE5A2E5F4A013E7D286FB9A8A5523316720DF6B47473166171154A07F" CDataKSN="62994901230000000002F" Exp="0809" MskPAN="4266********9999" CHolder="BUSH JR/GEORGE W.MR" EFormat="4"></Card><Tran TranType="CREDIT"></Tran></DvcMsg>
CarriageReturn

Key Value: ED 07 9C 5F 5E 5D F7 E2 03 7B 7F F3 36 F7 10 54
KSN: 62 99 49 01 23 00 00 00 00 2F

Decrypted Data in ASCII:
%B4266841088889999^BUSH JR/GEORGE W.MR^0809101100001100000000046000000?!
;4266841088889999=0809101100000046?0

Decrypted Data in Hex:
2542343236363834313038383838393939395E42555348204A522F47454F52474520572E4D525E30383039313031313030303031313030303030303030303034363030303030303F213B343236363834313038383838393939393D303830393130313130303030303034363F300000000000

Credit Card Manually Keyed Sample XML:

<DvcMsg Ver="1.1"><Dvc App="SecureKey Software" AppVer="1.0" DvcType="M130-IDTECH" DvcSN="0000000000" Entry="MANUAL"></Dvc><Card CEncode="2" ECData="F4EA319F165989392A5A1BA747EF82FF2461DC3CB8B68995F315FCFE54A81CF6" CDataKSN="62994901230000000030" Exp="1206" MskPAN="1234**********6789" EFormat="4"></Card><Addr AVSAddr="10721" AVSZip="91741"></Addr><Tran TranType="CREDIT"></Tran></DvcMsg>
CarriageReturn

Key Value: CA DC 1C 5A D6 5A FF 5D 06 81 A1 E3 37 51 A4 5A
KSN: 62 99 49 01 23 00 00 00 00 30

Decrypted Data in ASCII:
1234567890123456789=1206=123

Decrypted Data in Hex:
313233343536373839303132333435363738393D313230363D31323300000000

Non-Financial Card Swipe Sample XML:

<DvcMsg Ver="1.1"><Dvc App="SecureKey Software" AppVer=”1.0”
DvcType=”M130-IDTECH” DvcSN="0000000000" Entry="SWIPE"></Dvc><Card
CEncode="3" Trk1=”Track1ofGiftCardData"Trk2="Track2ofGiftCardData"
CDataKSN="A08B000C0000002000E6" MskPAN="1212********5588" Exp="1512"
CHolder=" BUSH JR/GEORGE W.MR " EFormat="4"></Card><Addr></Addr><Tran
TranType="OTHER" ></Tran></DvcMsg>
CarriageReturn

Note:
- Manually entered data should always be financial card data.
- The non-encrypted track fields (Trk1, Trk2, Trk3) are only used when the format is a non-financial card.
- “EFormat” is defined by the application

10.0 MSR Settings

10.1 Setting Command

The setting data command is a collection of one or more function setting blocks and its format is as the following:

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

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

<FuncID><Len><FuncData>
The setting command will function with any one, any group or all the setting in one command.

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.

10.2 Get Setting

This command will send current setting to application.
Command: <STX> <R> <ReviewID> <ETX> <LRC 1>
Response: <ACK> <STX> <FuncID> <Len> <FuncData> <ETX> <LRC 2>

<FuncID>, <Len> and <FuncData> definition are same as described above.
Note: ReviewID (value 0x1F) will return all funcID-s.

10.3 Security Management

The MSR reader is intended to be a secure reader. Security features include:

- Can include Device Serial Number
- Can encrypt track 1, track 2 and track 3 data for all bank cards (ETrk1 and ETrk2 will be empty if non bank card is swiped).
- Provides clear text confirmation data including card holder's name and a portion of the PAN as part of the Masked Track Data (for bank cards)
- Optional display expiration date (for bank cards)
- Configurable Security Level

The reader supports five Security Levels. This allows customer to select the security profile needed for the application. The Security Level can be raised by command, but can never be lowered:

- Level 0
  Security Level 0 is a special case. It signifies that all DUKPT keys have been used. In this case the unit is at the end of its useful life. This level is set automatically by the reader when it runs out of DUKPT keys. The life time of DUKPT keys is one millions. Once reach the end of keys' life time, user should inject DUKPT keys again.

- Level 1—not applicable because encryption required
  Reader properties are as configured from factory having the lowest level of default settings. There is no encryption process, no key serial number transmitted with decoded data. The reader has read operation and decoded track data is sent in default format.
  Encrypt type TDES and AES cannot be selected under Level 1.

- Level 2—not applicable because encryption required
  Key Serial Number and/or Initially Loaded Device Key have been injected. The encryption process is not activated and decoded track data is sent in default format.
  Key Serial Number and Initially Loaded Device Key can be set only once after manufacture.

- Level 3
  Both Key Serial Number and Initially Loaded Device Keys are injected and encryption is on. The encryption process is activated. The output of level 3 will be different from level 1 and level 2. Clear data output cannot be selected under Level 3. The output format in this level is more rigidly fixed so many track formatting output options are not supported, see function ID table for limitations.

- Level 4
  When the reader is at Security Level 4, a correctly executed Authentication Sequence is required before the reader sends out data for a card swipe.
  Commands that require security must be sent with a four byte Message Authentication Code (MAC) at the end. Note that data supplied to MAC algorithm should NOT be converted to ASCII-Hex; rather it should be supplied in its raw binary form. Calculating MAC requires knowledge of current DUKPT KSN, this could be retrieved using Get DUKPT KSN and Counter command. The output format in this level is more rigidly fixed so many track formatting output options are not supported, see function ID table for limitations.

10.4 Encryption Management

The Encrypted swipe read supports TDES and AES encryption standards for data encryption. Encryption can be turned on via a command. TDES is the default.

If the reader is in security level 3, for the encrypted fields, the original data is encrypted using the TDES/AES CBC mode with an Initialization Vector starting at all binary zeroes and the Encryption Key associated with the current DUKPT KSN.

10.5 Check Card Format

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

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

10.6 MSR Data Masking

For ABA Card Data (Card type 0)
For cards that need to be encrypted, both encrypted data and clear text data are sent.

Masked Area

The data format of each masked track is ASCII.
The clear data include start and end sentinels, separators, first N, last M digits of the PAN, card holder name (for Track1). Optional expiration date may be revealed.
The rest of the characters should be masked using mask character.

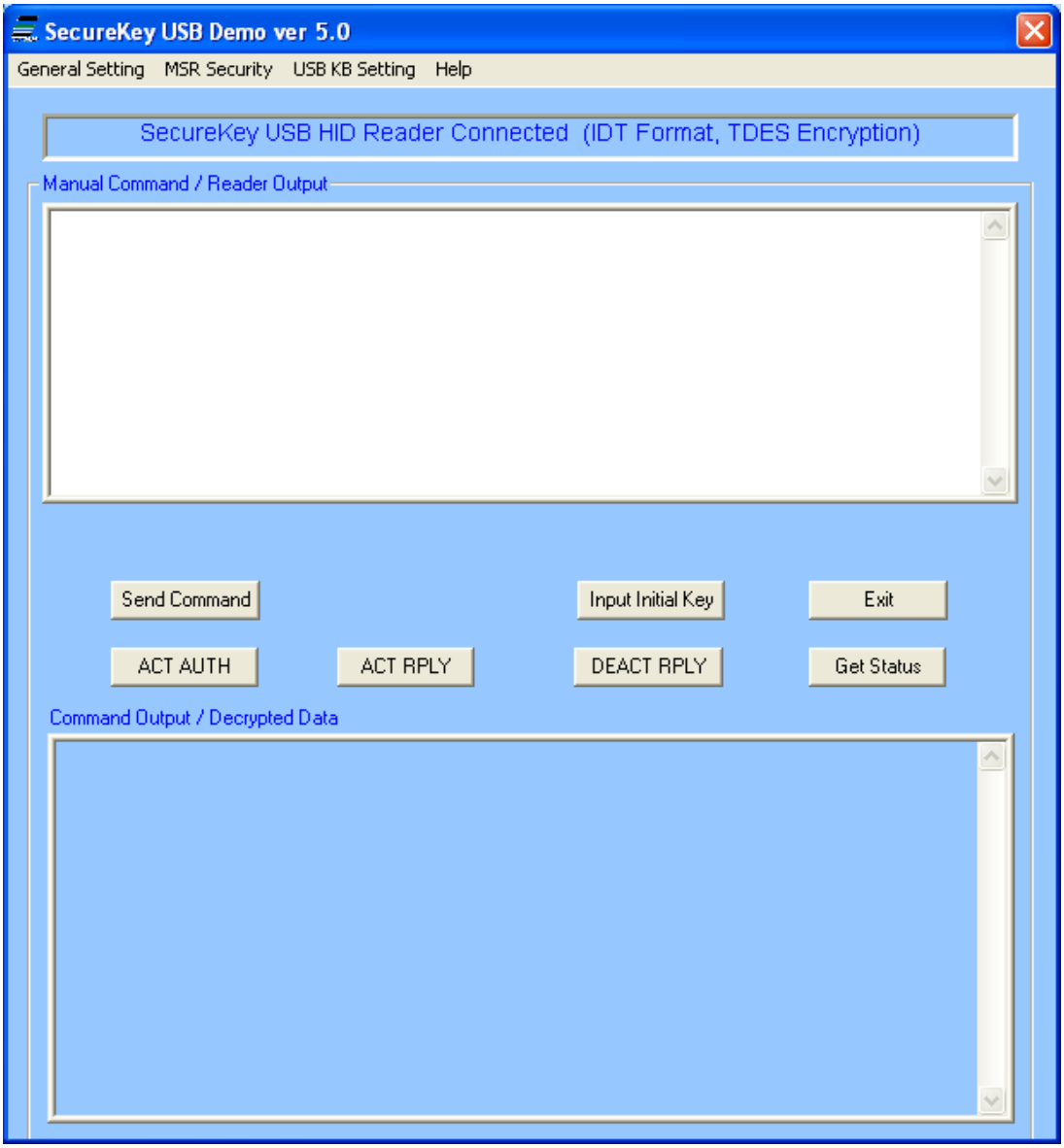
Mask character default value is '*'.

11.0 SecureKey Decryption Demo Software

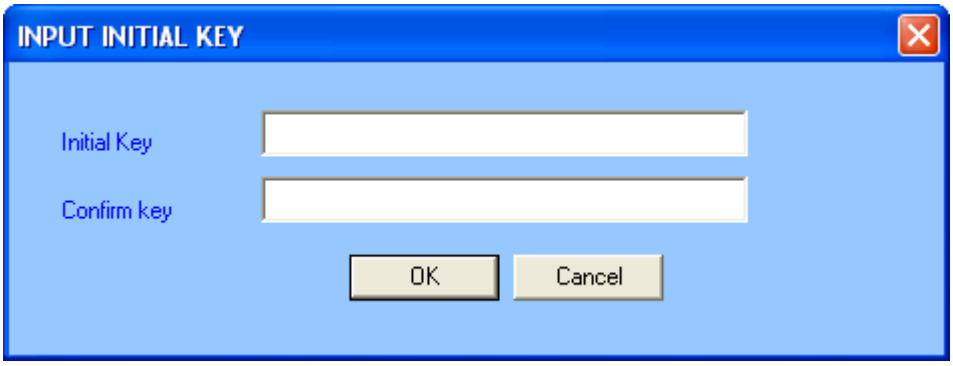
SecureKey demo software is available to demonstrate the MSR data decryption. Please see the below screenshots:

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

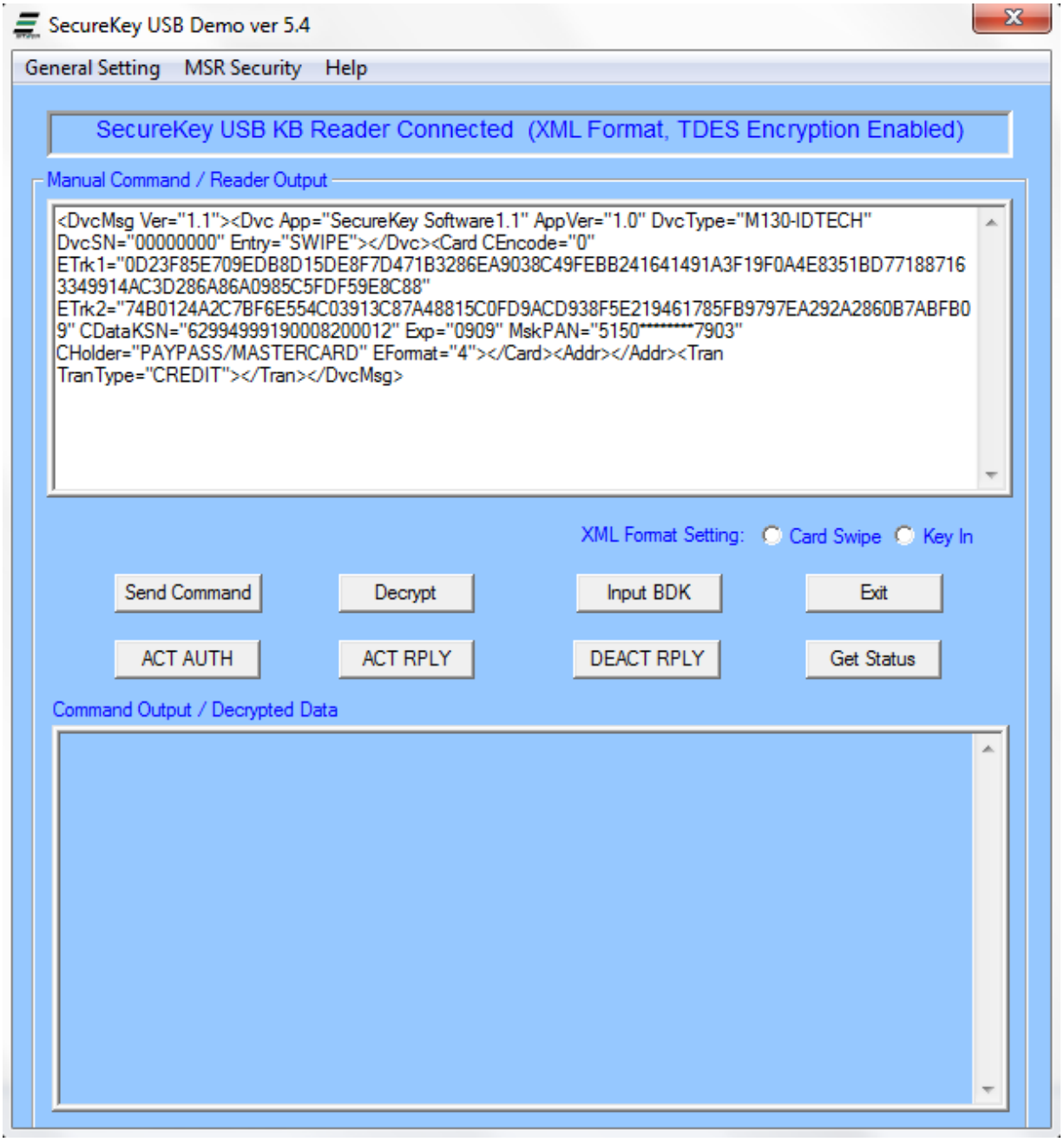
The following demo software screenshots are shown for reference and might not reflect the latest demo software version.



The demo software uses the IDTECH demo key
0123456789ABCDEFFEDCBA9876543210
to decrypt the swiped or entered data by default. To change the decryption key, click on “input initial key”

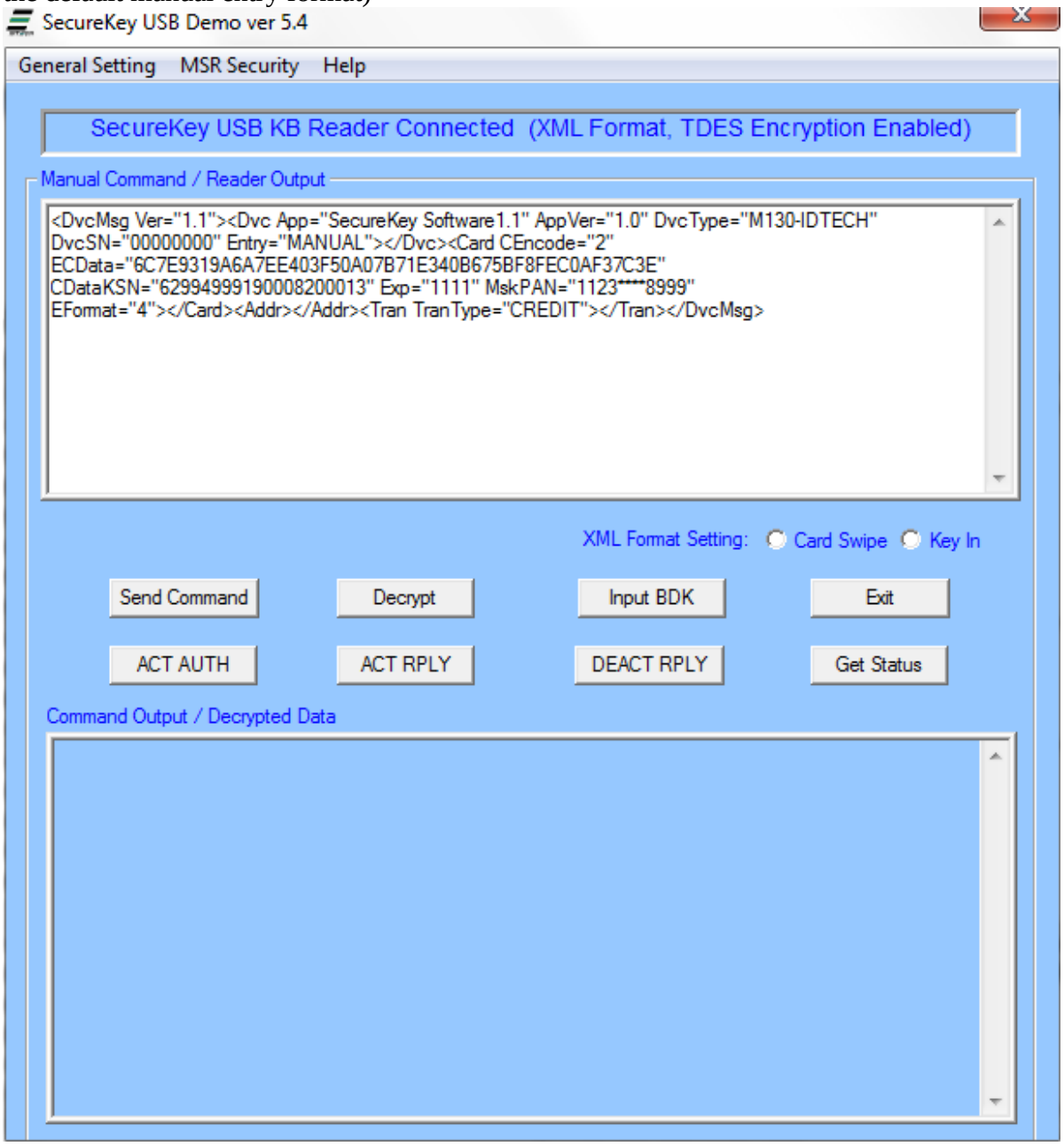


11.1 Card Swipe Data



11.2 Key in data, IDTECH Format

Manually key in the card data on the device, the data will show on the demo as the following (shown is the default manual entry format)



12.Specifications

Mechanical

ITEM	SPECIFICATION
Key switch Information Total/ Pre-Travel Operating Type Operating Force Tactile Feel Force Letter of Keycap Material of Key switch	 2.5 + 0.5 mm/ 1.5 + 0.4 mm Tactile Type 55 + 7g 30 + 14g Traditional North American Silicone Rubber (Rubber Key Pad)
Keyboard Information Enclosure Material Color	 Top & Bottom Case High Impact ABS Black
Cable Information Jacket Material Conductors Color Length PC Connector	 Polyester 0.075 mm Polyester 0.10 mm Upper circuit: 3M467+PET125S Lower circuit: 3M467+PET 100S Acheson ED-725A 5~10 um
Keyboard Membrane Material Spacer Back-up Plate Upper Circuit Lower Circuit Silver	The auxiliary ports are only on the USB keyboard & located horizontal to each other on the rear. USB port plastic color is white.
Interface	USB-KB and USB-HID

Electrical

ITEM	SPECIFICATION
Max Rating	+5.0 VDC ±10%, 60ma Max (excludes ICC)
Type of Circuit	1 Circuit 1 Contact
Insulation Resistance	DC 100V 50 M Ω Min
Bounce	10 ms Max
Operating Life	20,000,000 keystrokes
Industry Requirements	FCC class B and CE

Quality & Reliability

ITEM	SPECIFICATION

MI Requirement	The keyboard meets the FCC class B limits
ESD Immunity	The keyboard passes 0KV to 8 kV minimum without any data loss; passes 8KV to 15 kV minimum that may cause malfunctions. No internal components are destroyed and after reset, the keyboard functions normally.
MTBF	The main operating time between failures will be more than 60,000 hours
Drop	610 mm (24”) height Drop: 4 corner, 4-sidelines, 2-sides front/back
Vibration	Vibration frequency 60 Hz/sec. 3 mm amplitude of an oscillation. X,Y,Z each axis at 2 hours
Operating Temperature	0℃ ~ 40℃
Storage Temperature	-20℃ ~ + 40℃

MagStripe Reader

Number of tracks	Tracks 1 & 2 or Tracks 2 & 3 or Tracks 1, 2 & 3
Encryption	TDES or AES with DUKPT key management
Compatibility	ISO 7810 and 7811-1 through -6
Output data formatting	Standard output format
Operating Life	1,000,000 card swipes
Card speed range	3 to 60 IPS (Inches Per Second)

12.0 Appendix A Setting Configuration Parameters and Values

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

Function ID	Hex	Description	Default Setting	Description
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
TrackSelectID	13	Track Selection	‘0’ (‘0’~’9’)	Any Track 0-any; 1-7—bit 1 tk1, bit 2 tk2; bit 3 tk3. ‘8’—tk1-2; ‘9’ tk2-3
PollingIntervalID	14	Polling Interval	1 (1 ~ 255)	USB HID Polling Interval
TrackSepID	17	Track Separator	0x0D=CR/Enter	CR for RS232, Enter for KB any character supported except 00 which means none.
SendOptionID	19	Send Option	‘1’ (‘0’~’F’) ‘5’ for Port Powered IV	Sentinel and Account number control
DecodingMethodID	1D	Decoding Direction	‘1’ (‘0’~’3’)	Reading Direction 0x30 – Raw Data Decoding in Both Directions. **0x31 – Decode in Both directions.** 0x32 – Moving Stripe Along Head in Direction of Encoding. 0x33 – Moving Stripe Along Head Against Direction of Encoding.
ReviewID	1F	Review All Settings	None	
TerminatorID	21	Terminator	0x0D (any)	CR for RS232, Enter for KB; ‘0’ for CRLF
FmVerID	22	Firmware Version	None	
USBHIDFmtID	23*	USB HID Fmt (HID rdr only)	‘0’ (‘0’, ‘8’)	‘0’ ID TECH Format; ‘8’ HIDKB format
ForeignKBID	24	Foreign KB	'0' ('0' ~0x3A)	Foreign Keyboard

CustSetID	30	Custom Customer Settings	00(00-07)	.0-Level 3/4 Non-CC send as Level 1 .1-Level3: No empty pkt when not enough sampling bits .2- Enhanced Secured Output will have SN after hash
Track1PrefixID	34	Track 1 Prefix	0 (any string)	No prefix for track 1, 6 char max
Track2PrefixID	35	Track 2 Prefix	0 (any string)	No prefix for track 2, 6 char max
Track3PrefixID	36	Track 3 Prefix	0 (any string)	No prefix for track 3, 6 char max
Track1SuffixID	37	Track 1 Suffix	0 (any string)	No suffix for track 1, 6 char max
Track2SuffixID	38	Track 2 Suffix	0 (any string)	No suffix for track 2, 6 char max
Track3SuffixID	39	Track 3 Suffix	0 (any string)	No suffix for track 3, 6 char max
KeyTypeID	3E*	data or pin key	0	0-data key; 1-pin key
PrePANID	49	PAN to not mask	4 (0-6)	# leading PAN digits to display
PostPANID	4A	PAN to not mask	4 (0-4)	# of trailing PAN digits to display
MaskCharID	4B	mask the PAN with this character	‘*’ 20-7E	any printable character
CrypTypeID	4C*	encryption type	‘1’ (‘1’-‘2’)	‘1’ 3DES ‘2’ AES
SerialNumberID	4E*	device serial #	any 8-10 bytes	8-10 digit serial number; Can be set only once
DispExpDateID,	50	mask or display expiration date	'0"0'-'1'	‘0’ mask expiration date; ‘1’ display expiration date
SessionID	54	8 byte hex not stored in EEPROM	None	always init to all ‘FF’
Mod10ID	55	include mod10 check digit	'0' ('0'-'2')	‘0’ don’t include mod10, ‘1’ display mod10, ‘2’ display wrong mod10
KeyManageTypeID	58*	DUKPT	‘1’	‘1’ DUKPT
HashOptID,	5C		'7' (‘0’-‘7’)	Send tk1-2 hash bit 0:1 send tk1 hash; bit 1:1 send tk2 hash; bit2:1 send tk3 hash.
HexCaseID,	5D		'1' (‘0’-‘1’)	‘0’ send in lower case; ‘1’ send in upper case

LRCID	60	track LRC	‘0’ (‘0’~’1’)	‘0’ send without track LRC in output; ‘1’ with track LRC
T17BStartID	61	Track 1 7 Bit Start Char	‘%’ (any)	‘%’ as Track 1 7 Bit Start Sentinel
T16BStartID	62	T16B Start	‘%’ (any)	‘%’ as Track 1 6 Bit Start Sentinel
T15BStartID	63	T15B Start	‘;’ (any)	‘;’ as Track 1 5 Bit Start Sentinel
T27BStartID	64	Track 2 7 Bit Start Char	‘%’ (any)	‘%’ as Track 2 7 Bit Start Sentinel
T25BStartID	65	T25BStart	‘;’ (any)	‘;’ as Track 2 5 Bit Start Sentinel
T37BStartID	66	Track 3 7 Bit Start Char	‘%’ (any)	‘%’ as Track 3 7 Bit Start Sentinel
T36BStartID	67	T36BStart	‘!’ (any)	‘!’ as Track 3 6 Bit Start Sentinel
T35BStartID	68	T35BStart	‘;’ (any)	‘;’ as Track 3 5 Bit Start Sentinel
T1EndID	69	Track 1 End Sentinel	‘?’ (any)	‘?’ as End Sentinel
T2EndID	6A	Track 2 End Sentinel	'?' (any)	‘?’ as End Sentinel
T3EndID	6B	Track 3 End Sentinel	'?' (any)	‘?’ as End Sentinel
T1ERRSTARTID	6C	Track 1 error code	‘%’ (any)	start sentinel if track 1 error report
T2ERRSTARTID	6D	Track 2 error code	‘;’ (any)	start sentinel if track 2 error report
T3ERRSTARTID	6E	Track 3 error code	‘+’ (any)	start sentinel if track 3 error report
SecureLrcID	6F	Secured output format track LRC option	‘1’ (‘0’-‘1’)	‘1’ to send track LRC in secured output data; ‘0’ don’t send track LRC
EquipFwID	77*	feature option setting	any	Factory Reader firmware configuration setting
SyncCheckID	7B	check for track sync bits-can allow poorly encoded cards to be read	‘2’ (‘0’-2’)	check leading & trailing sync bits ‘0’ 13 bits; ‘1’ 13 bits, but allow if valid through track LRC; '2' 9 bits ABA; 13 bits IATA; 16 bits JIS
SecurityLevelID	7E*	Reader’s encryption level	‘1’ or ‘3’ (‘0’-‘4’)	‘1’ no encryption; ‘2’ key loaded; ‘3 encrypted reader; ‘0’ DUKPT exhausted; ‘4’ authentication required
EncryptOptID	84	encryption	0 encrypt card	bit 0 encrypt trk1; bit 1

		options, enhanced only	type 0; (0-1F)	encrypt trk2; bit 3 encrypt trk3; bit 4 encrypt trk3 if card type 0
EncryptStrID	85*	encrypt structure	'0'	‘0’ original; ‘1’ enhanced
MaskOptID	86	clear / mask data options	7	bit 0 send clear/mask trk1 bit 1 send clear/mask trk2 bit 2 send clear/mask trk3
EnFmtID	88		\02\30\34	encryption format defined in xml specification
T3ExpDatePosID	89	expire date position	0x34 ((0x34, 0x36)	track 3 expiration date position offset
AdminLvlID	8E	Admin Level	B, 15, 1F, 29, 33, 3D	B-Admin 1; 15-Admin 2; 1F-Admin 3; 29-Admin 4’ 33-Admin 5; 3D-Admin 6
KeyedOptID	8F*	Keyed Options	0-1	0-original format; 1-enhanced format see 7.7.1 Configuration byte 8F controls Keyed in options page 14
Equip2ID	AE	special settings	00 (any)	if bit4 high send serial number during enumeration
CustSet2ID	AF	sending credit card shifted by lifting card.	**00H** (or 01H)	bit 0=0 allow track shifted CC card; bit0=1 don’t send track shifted Credit Card
PrefixID	D2	Preamble	0 (any 15)	No Preamble, 15 char max
PostfixID	D3	Postamble	0 (any 15)	No Postamble, 15 char max

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

1 PrefixID and PostFixID are ignored on encrypted transaction unless the reader is a keyboard reader, then they are supported so that the host can recognize the reader’s output.

13.0 Appendix B Guide to Encrypting and Decrypting Data

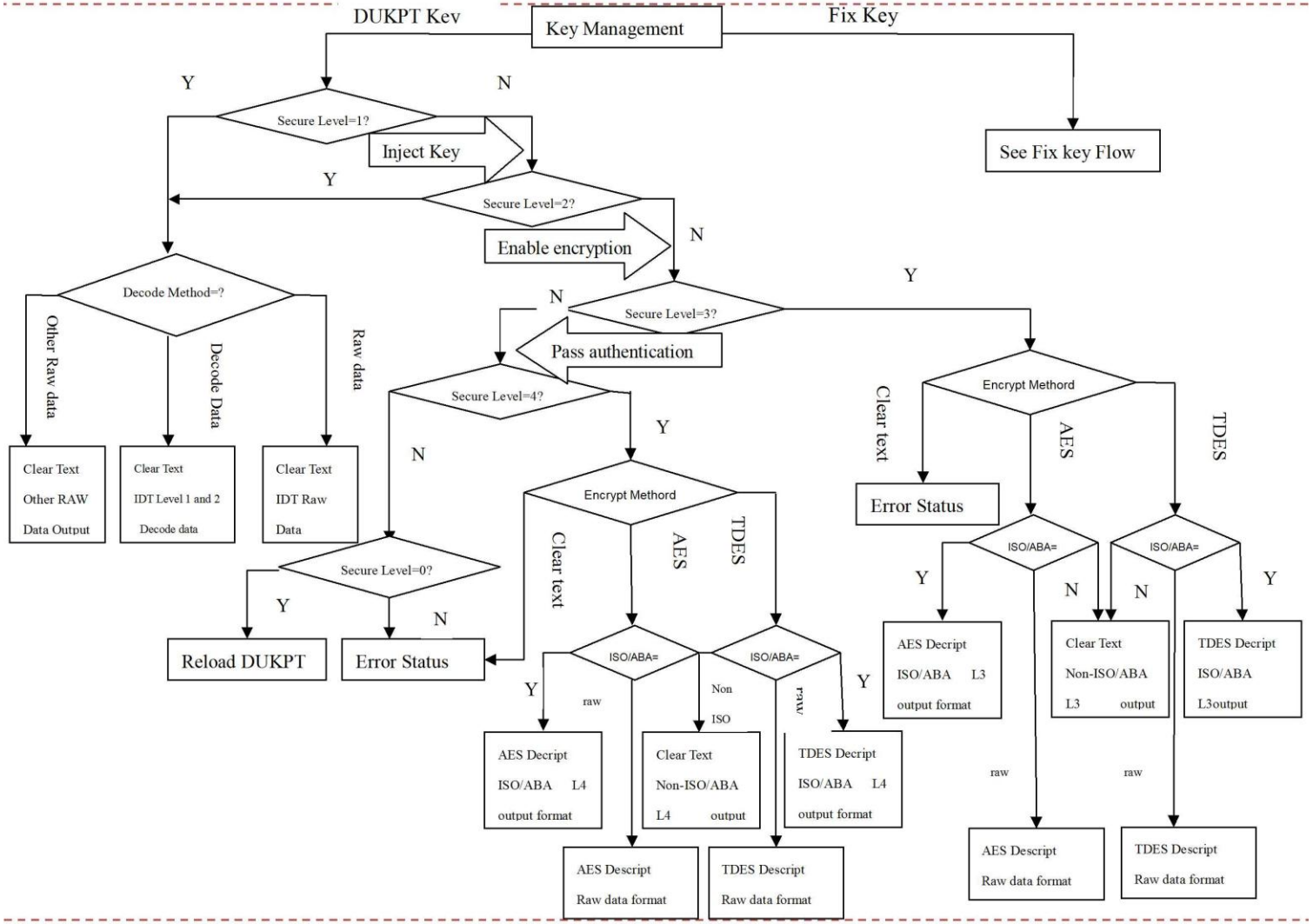
The encryption method used by SecureKey is called Cipher-block Chaining (CBC). With this method, each block of data is XOR'ed with the previous data block before being encrypted. The encryption of each block depends on all the previous blocks. As a result, each encrypted data block would need to be decrypted sequentially.

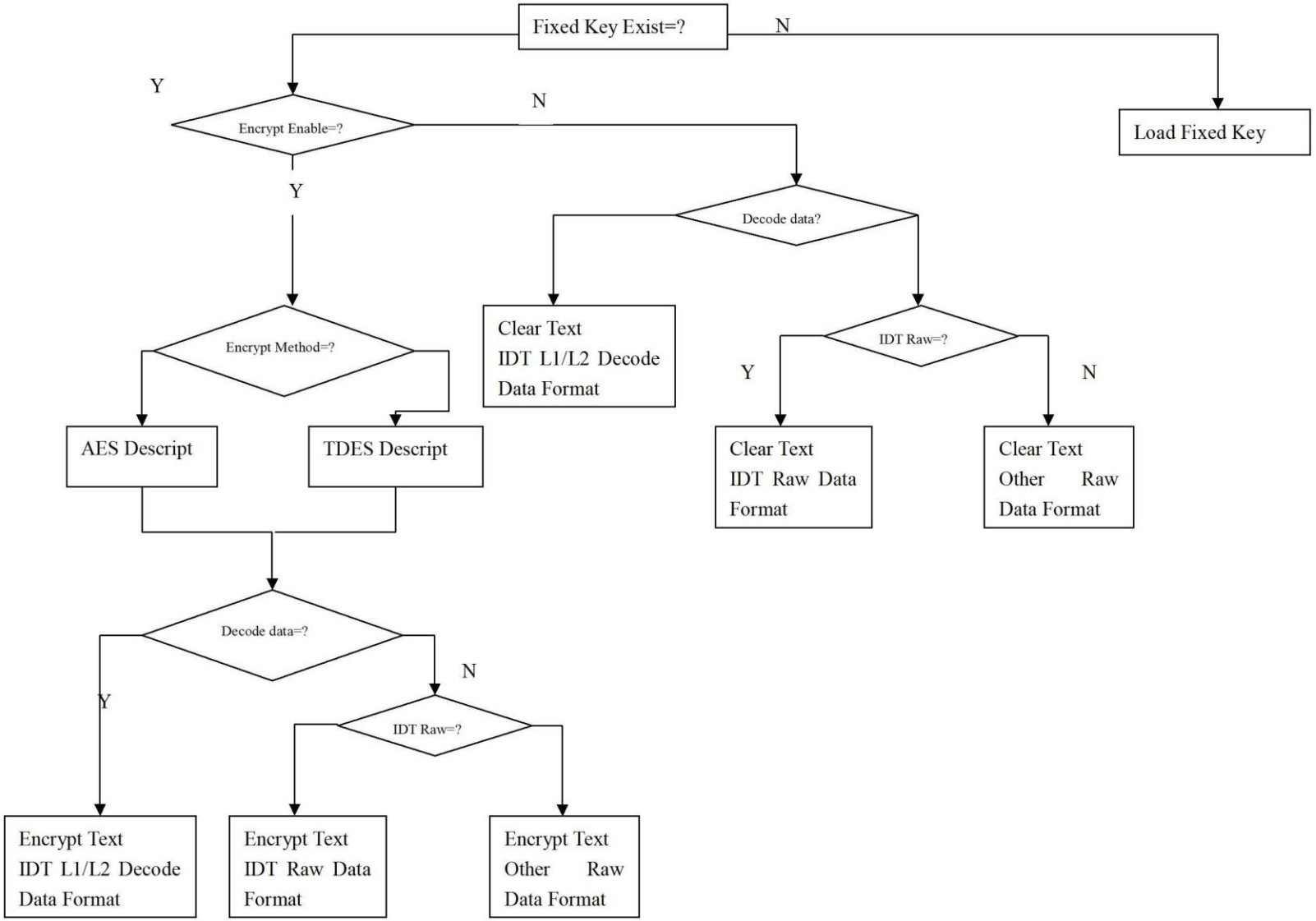
To encrypt the data, first generate an 8-byte random initialization vector which is XOR'ed with the first data block before it is encrypted. Then the data is encrypted with the device key using TDES algorithm. The result is again XOR'ed with the next 8-byte data block before it is encrypted. The process repeats until all the data blocks have been encrypted.

The host can decrypt the cipher text from the beginning of the block when the data is received. However, it must keep track of both the encrypted and clear text data. Or alternatively, the data can be decrypted backward form that last data block to the first, so that the decrypted data can replace the original data as the decryption is in process.

To decrypt the data using reverse method, first decrypt the last 8-byte of data using TDES decryption. Then perform an XOR operation with result and the preceding data block to get the last data block in clear text. Continue to decrypt the next previous block with the same method till it reaches the first block. For the first data block, the XOR operation can be skipped, since it is XOR'ing with 00h bytes.

14.0 Appendix C Key Management Flow Chart




Fixed Key Exist=?
N
Load Fixed Key
Y
Encrypt Enable=?
N
Y
Decode data?
Clear Text
IDT L1/L2 Decode
Data Format
IDT Raw=?
Y
N
Clear Text
IDT Raw Data
Format
Clear Text
Other Raw
Data Format
Encrypt Method=?
AES Descript
TDES Descript
Decode data=?
Y
N
IDT Raw=?
Encrypt Text
IDT L1/L2 Decode
Data Format
Encrypt Text
IDT Raw Data
Format
Encrypt Text
Other Raw
Data Format