unitech

because we care

USER MANUAL

MS246

Magnetic Stripe Reader

CE FC

80096504-001
Rev C 05/02/11

FCC WARNING STATEMENT
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case, the user will be required to correct the interference at his expense.

FCC COMPLIANCE STATEMENT
This device complies with Part 15 of the FCC Rules. Operation of this device is subject to the following conditions: this device may not cause harmful interference and this device must accept any interference received, including interference that may cause undesired operation.

CANADIAN DOC STATEMENT
This digital apparatus does not exceed the Class B limits for radio noise for digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.
Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de las classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par les ministère des Communications du Canada.

CE STANDARDS
An independent laboratory performed testing for compliance to CE requirements. The unit under test was found compliant to Class B.

LIMITED WARRANTY

Unitech warrants to the original purchaser for a period of 24 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. Unitech'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 within the warranty period and with transportation charges and insurance prepaid, and which is, after examination, disclosed to Unitech'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 Unitech any other liabilities in connection with the sales of any product. In no event shall Unitech 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 Unitech. For limited warranty service during the warranty period, please contact Unitech 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, EXPRESSED OR IMPLIED, OTHER THAN THOSE HEREIN STATED. THIS PRODUCT IS SOLD AS IS. IN NO EVENT SHALL UNITECH BE LIABLE FOR CLAIMS BASED UPON BREACH OF EXPRESSED OR IMPLIED WARRANTY OR 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 FABRICATION 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, Unitech is not responsible for damages that might occur because of errors or omissions, including loss of profits 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.

Unitech is a trademark of Unitech Electronics Co., Ltd. USB (Universal Serial Bus) specification is copyright by Compaq Computer Corporation, Intel Corporation, Microsoft Corporation, and NEC Corporation. Windows is registered trademark of Microsoft Corporation.

Unitech America, Inc.
6182 Katella Ave.
Cypress, CA 90630
(714) 891-6400

Table of Contents

1. Introduction

The Unitech MS246 is an intelligent, programmable magnetic stripe reader that provides a wide range of functionality and value in a convenient package size. The entire unit is just 100mm long, about the length of a credit card. It reads up to three tracks of information with a single swipe in either direction, and has a beeper and three-color LED indicator to signal a successful read. The MS246 is programmable so that the data format and intelligent interface output can be programmed & configured to match application and communication requirements.

2. Features and Benefits

- Bi-directional card reading
- Reads up to three tracks of card data
- An LED and a beeper on the reader provide status of the reading operations
- Compatible with USB specification Revision 2.0 (USB interface)
- Compatible with HID specification Version 1.1 (USB interface)
- Uses standard Windows HID driver for communications; no third party device driver is required (USB interface)
- User-friendly configuration software for device configuration

3. Terms and Abbreviations

AAMVA	American Association of Motor Vehicle Administration
ABA	American Banking Association
AES	Advanced Encryption Standard
ASIC	Application Specific Integrated Circuit
BPI	Bits per Inch
CADL	California Drivers License Format (obsolescent)
CE	European Safety and Emission approval authority
COM	serial communication
CTS	Clear-To-Send
CDC	USB to serial driver (Communication Device Class)
DES	Data Encryption Standard
DUKPT	Derived Unique Key Per Transaction
DMV	Department of Motor Vehicle
GND	Signal Ground
HID	Human Interface Device
IPS	Inches per Second
ISO	International Organization for Standardization
JIS	Japanese Industrial Standard
JPOS	Java for Retail Point Of Sale
KB	Keyboard
KSN	Key Serial Number
LED	Light Emitting Diode
LRC	Longitudinal Redundancy Check Character.
MAC	Message Authentication Code
MSR	Magnetic Stripe Reader
OLE	Object Linking and Embedding
OPOS	OLE for Retail Point Of Sale
OTP	One Time Programmable
PAN	Primary account number
PCI	Payment Card Industry
PID	USB Product ID
POS	Point of Sale
PPMSR	Serial Port Power Magstripe Reader
P/N	Part Number
PS/2	IBM Personal System/2 Keyboard Interface
RTS	Request To Send
SPI	Serial Peripheral Interface
T1, T2, T3	Track 1 data, Track 2 data, Track 3 data
TDES	Triple Data Encryption Standard
VID	USB Vendor ID

Note: many unusual words used in this document are defined in the Function ID table in Appendix A on page 59.

4. Applicable Documents

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. Operation

A card may 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 are no errors decoding the card data then the LED will turn green. If there are any errors 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 beeper also provides error indication. 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 clear or encrypted mode.

6. Specification

Power Consumption

- 5VDC +/- 10%.
- Current maximum operating consumption is less than 50mA.
- USB interface – from host interface. No external power adaptor needed.

Swipe speed

- 3 to 65 inches per second.
- Bi-directional.

Indicators

- Tri-color LED:
  - Red indicates a bad read.
  - LED is off while reading and decoding.
  - Green indicates a good read and ready to read.
- Beeper:
  - A beep sound indicates a good read.

Communication Interface

- USB:
  - Complies with USB 2.0 specification.

Card Size

- Supports cards that meet the ISO 7810 and 7811 1-7 standards.

Dimension

- 3.94 in. (length) X 1.38 in. (width) X 1.18 in. (height).

Interface cable and connector

- USB interface:
  - Standard USB interface cable.
  - Series “A” plug.
  - Standard cable length is 6 feet.
  - Pin Out Table:

J1	Color	Signal	P1
1	-	CASE_GND	SHELL
3	GRN	+DATA	3

5	Red	V_IN	1
6	White	-DATA	2
7	BLK	GND	4

LED indicator

- 2mmx5mm, Green/Red dual color under firmware control.

7. Command Process

Command requests and responses are sent to and received from the device. For USB interface devices, the commands are sent to the device using HID class specific request Set_Report (21 09 …). The response to a command is retrieved from the device using HID class specific request Get_Report (A1 01 …). These requests are sent over the default control pipe. For RS232 interface devices, please see the commands listed below.

Function ID Table:
The complete table of Function ID used in command/response are listed in Appendix A.

Setting Command:

The setting data 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 the 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.

Get Setting Command:

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

<FuncID>, <Len> and <FuncData> definition are the same as described above.

Where:

Characters	Hex Value	Description
<STX>	02	Start of Text
<ETX>	03	End of Text
<ACK>	06	Acknowledge
<NAK>	15 for	Negative Acknowledge

	RS232 and USB HID interface; FD for USB KB interface	
<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.

Reader Command Summary

ASCII	HEX	Name	Use
'8'	38	Copyright Report	Requests reader's copyright notice
'9'	39	Version Report	Requests version string
'F"	46	Key Loading	Special command to load encryption keys
'I'	49	Reader Reset	Reset the reader. Software reset does not resend startup string
'M'	4D	OPOS/ JPOS Command	Command to enter OPOS or JPOS mode
'P'	50	Arm/Disarm to Read	Arm to Capture Buffer Mode MSR
'Q'	51	Read Buffered Data	Read Stored MSR Data
'R'	52	Read MSR Options	Read various reader optional settings
'S'	53	Set MSR Options	Set various reader optional functions

Notation used throughout the document:

Bold: boldface font indicates default setting value.
'2': with single quotations, indicates ASCII characters, for example, '2' is 32 in hex.
"Number": is a null terminated character string.
<Len>: with angle brackets indicates a specific character or character string in a command or response.
Hex: is the hex character 53 is '5' in ASCII or 83 in decimal. Sometimes hex characters are represented with an *h* attached to the end, for example, 53h.
\02: is a way to show that the following number is in hex. It is used by the configuration program.

7.1 Get Copyright Information

02 38 03 39

A '31-byte' Copyright Notice will be returned.

Response is as follows:
ACK STX <Copyright String> ETX LRC
Response Example mixed hex and ASCII:
\06\02Copyright (c) 2010, UNITECH \03>

7.2 Version Report Command

02 39 03 38

Response is as follows:
ACK STX<Version String> ETX LRC
Response Example mixed hex and ASCII:
\06\02UNITECH TM3 MS246 RS232 Reader V 3.19\03\LRC

7.3 Key Loading Command

Note: This command is normally only used by a key loading facility.

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.

KSN and Device Key loading commands and responses protocol:
When DUKPT key management is used, it is necessary to load Key Serial Number (KSN) and Initially Loaded Device Key before transaction.

The encryption key is TDES with 128 bit keys or AES encryption with double length keys (128 bit keys including parity).

KSN and Device Key loading commands and responses protocol:
Command:
<STX><'F'><'F'><Command Data (BASE64)><0x0D><0x0A><ETX><LRC>

Response:
<ACK/NAK><STX><'F'><'F'>< Respond Data(BASE64)><0x0D><0x0A><ETX>
<LRC>

STX: 0x02
ETX: 0x03
ACK: 0x06
NAK: 0x15
BASE64: Data encoded with base64 algorithm
LRC: Xor'd all the data before LRC

A successful key loading process includes the following steps:

- Get Key status

Command Data: <FF><13><01><02><LRC>
Response Data: <FF><00><01><04><LRC>

For Example:
Command: \02\46\46\2F\78\4D\42\41\75\38\3D\0D\0A\03\LRC
Response: \06\02\46\46\.....\0D\0A\03\LRC

- Load KSN

Command Data: <FF><0A><11><KSN#><KSN bytes><LRC>
Response Data: <FF><00><06><RESPONSE CODE><LRC>
<KSN#>: TDES: 0x32 DES: 0x0A
<KSN bytes>: 16 bytes ASCII for KSN
<RESPONSE CODE>: 6 bytes data in ASCII format which is converted from the first 3 cipher hex data. These cipher data are generated by encrypting KSN bytes and "00 00 00 00 00 00 00 00".

For Example:
Command:
\02\46\46\2F\77\6F\52\4D\6B\5A\47\52\6B\59\35\4F\44\63\32\4E\54\51\7A\4D\6A\45\77\52\54\43\69\0D\0A\03\5D
Response: \06\02\46\46\.....\0D\0A\03\LRC

- Load Encryption Key

Command Data: <FF><0A><LENGTH><KEY#><KEY bytes><LRC>
Response Data: <FF><00><06><RESPONSE CODE><LRC>
<LENGTH>: TDES: 0x21 DES: 0x11
<KEY#>: TDES: 0x33 DES: 0x0B
<KEY bytes>: TDES: 0x20 DES: 0x10
<RESPONSE CODE>: 6 bytes data in ASCII format which is converted from the first 3 cipher hex data. These cipher data are generated by encrypting KEY bytes and "00 00 00 00 00 00 00 00."

For Example:
Command:
\02\46\46\2F\77\6F\68\4D\7A\5A\42\51\7A\49\35\4D\6B\5A\42\51\54\45\7A\4D\54\56\43\4E\45\51\34\4E\54\68\42\51\6A\4E\42\4D\30\51\33\52\44\55\35\4D\7A\4E\42\6C\51\3D\3D\0D\0A\03\2D
Response: \06\02\46\46\.....\0D\0A\03\LRC

7.4 Reader Reset Command

02 49 03 48

The reader supports a reset reader command. This allows the host to return the reader to its default state.

Response is as follows:

06

7.5 OPOS/JPOS Command

There are three forms of the command:

02 4D 01 30 03 7D	Enter Standard Mode (Exit OPOS Mode)
02 4D 01 31 03 7C	Enter OPOS Mode
02 4D 01 32 03 7F	Enter JPOS Mode

Response is as follows:

17	Reader already in OPOS Mode
15	Command failure (wrong length or wrong parameter)
06	Success

7.6 Arm/Disarm to Read Command

Arm to read:

02 50 01 30 03 LRC

This command enables the MSR to be ready for a card swipe in buffered mode.

Any previously read data will be erased and reader will wait for the next swipe.

As the user swipes a card, the data will be saved, but will not be sent to the host. The reader holds the data until receiving the next “Arm to Read” or “MSR Reset” command.

Disarm to read:

02 50 01 32 03 LRC

This command will disable MSR read and clear any magnetic data in buffered mode. The reader enters to a disarmed state and will ignore MSR data.

Response is as follows:

06

Other possible response statuses:

NAK	'P' command length must be 1.
NAK	'P' command must be 0x30 or 0x32.
NAK	Reader not configured for buffered mode.
NAK	Reader not configured for magstripe read.

NAK for keyboard interface is FD, non-KB mode NAK is 15

7.7 Read Buffered MSR Data Command

02 51 01 <Track Selection Option> 03 LRC

The <Track Select Option> byte is defined as follows:

‘0’ Any Track
‘1’ Track 1
‘2’ Track 2
‘3’ Track 1 and Track 2
‘4’ Track 3
‘5’ Track 1 and Track 3
‘6’ Track 2 and Track 3
‘7’ Track 1, Track 2 and Track 3
‘8’ Track 1 and/ or Track 2
‘9’ Track 2 and/ or Track 3

This command requests card data information for the buffered mode.

The selected MSR data is sent to the host with or without envelope format, according to the operation mode setting.

This command does not erase the data.

Response is as follows:

06 02 <Len_H> <Len_L> <MSR Data> 03 LRC

Other possible response statuses:

18 'Q' command length must be 1
18 Reader not configured for buffered mode
NAK Already armed

NAK for keyboard interface is FD, non-KB mode NAK is 15

7.8 Read MSR Options Command

02 52 1F 03 LRC

<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>.

7.9 Set MSR Options Command

The default value is listed **in bold**.

7.9.1. Beep Volume

The beep volume and frequency can each be adjusted to two different levels, or turned off.

02 53 11 01 <Beep Settings>03 LRC

Beep Settings:
'0' for beep volume off.
'1' for beep volume high, low frequency.
'2' for beep volume high, high frequency.
'3' for beep volume low, high frequency.
'4' for beep volume low, low frequency.

7.9.2. Change to Default Settings

02 53 18 03 LRC

This command does not have any <FuncData>. It returns all non-security settings for all groups to their default values.

7.9.3. MSR Reading Settings

02 53 1A 01<MSR Reading Settings> 03 LRC

MSR Reading Settings:
'0' = MSR reading disabled.
'1' = MSR reading enabled.

7.9.4. Decoding Method Settings

02 53 1D 01<Decoding Method Settings> 03 LRC.

Decoding Method Settings:
'0' = raw data decoding in both directions.
'1' = decoding in both directions.
'2' = moving stripe along head in the direction of encoding.

'3' moving stripe along head against the 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. No checking is done except to verify that the track has or does not have magnetic data.

7.9.5. Terminator Setting

Terminator characters are used to end a string of data in some applications.

02 53 21 01 <Terminator Settings> 03 LRC

<Terminator Settings>
Any one character, 00h is none; default is **CR** (0Dh).

7.9.6. 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.

02 53 D2 <Len><Preamble> 03 LRC

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

7.9.7. 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.

02 53 D3 <Len><Postamble> 03 LRC

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

7.9.8. Track n Prefix Setting

Characters can be added to the beginning of a track data. These can be special characters to identify the specific track to the receiving host, or any other

character string. Up to six ASCII characters can be defined.

02 53 <n><Len><Prefix> 03 LRC

Where:
n is 34h for track 1, 35h for track 2, and 36h for track 3.
Len = the number of bytes of prefix string.
Prefix = {string length}{string}.
NOTE: String length is one byte, maximum six.

7.9.9. Track x Suffix Setting

Characters can be added to the end of track data. These can be special characters to identify the specific track to the receiving host, or any other character string. Up to six ASCII characters can be defined.

02 53 <n><Len><Suffix> 03 LRC

Where:
n is 37h for track 1, 38h for track 2, and 39h for track 3.
Len = the number of bytes of suffix string.
Suffix = {string length}{string}.
NOTE: String length is one byte, maximum six.

7.9.10. 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.

02 53 13 01 <Track_Selection Settings> 03 LRC

<Track_Selection Settings>
'0' = Any Track.
'1' = Require Track 1 Only.
'2' = Require Track 2 Only.
'3' = Require Track 1 & Track 2.
'4' = Require Track 3 Only.
'5' = Require Track 1 & Track 3.
'6' = Require Track 2 & Track 3.
'7' = Require All Three Tracks.
'8' = Any Track 1 & 2.
'9' = Any Track 2 & 3.

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

7.9.11.Track Separator Selection

This option allows the user to select the character to be used to separate data decoded by a multiple-track reader.

02 53 17 01 <Track_Separator> 03 LRC

<Track_Separator> is one ASCII Character.
The default value is C. 0h means no track separator.

7.9.12.Start/End Sentinel and Track 2 Account Number Only

The MS246 can be set to either send, or not send, the Start/End sentinel, and to send either the Track 2 account number only, or all the encoded data on Track 2. (The Track 2 account number setting doesn't affect the output of Track 1 and Track 3.)

02 53 19 01 <SendOption> 03 LRC

<SendOption>
'0' = Don't send start/end sentinel and send all data on Track 2.
'1' = Send start/end sentinel and send all data on Track 2.
'2' = Don't send start/end sentinel and send account number on Track 2.
'3' = Send start/end sentinel and send account number on Track 2.

8. Data Format

The USB version of the reader can be operated in two different modes:
- HID Unitech mode (herein referred to as "***HID*** mode"), Product ID: 2010.
- HID with Keyboard Emulation (herein referred to as "***KB*** mode"), Product ID: 2030.

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 Level 1 and level 2 Standard Mode Data Output Format

USB HID Output Format

Card data is only sent to the host on the Interrupt In pipe using an Input Report. The reader will send only one Input Report per card swipe. If the host requests data from the reader when no data is available, the reader will send a NAK to the host to indicate that it has nothing to send.

8.1.1. USB HID Data Format

Other Mode Reader Data Structure

Offset	Usage Name
0	T1 decode status
1	T2 decode status
2	T3 decode status
3	T1 data length
4	T2 data length
5	T3 data length
6	Card encode type
7-116	T1 data
117-226	T2 data
227-336	T3 data

Notes:

T1, T2 or T3 decode status: 0 for no error, 1 for error

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 was no data on the track or if there was an error decoding the track.

Card Encode Type:

Value	Encode Type	Description
0	ISO/ABA	ISO/ABA encode format.
1	AAMVA	AAMVA encode format.
3	Other	The card has a non-standard format. For example, ISO/ABA track 1 format on track 2.
4	Raw	The card data is sent in Raw encrypted format. All tracks are encrypted and no mask data is sent.

T1, T2 or T3 data: The length of each track data field is fixed at 110 bytes, but the length of valid data in each field is determined by the track data length field that corresponds to the track number. The track data includes all data string starting with the start sentinel and ending with the end sentinel.

Unitech Reader Data Structure

Offset	Usage Name
0	T1 decode status
1	T2 decode status
2	T3 decode status
3	T1 data length
4	T2 data length

5	T3 data length
6	Card encode type
7,8	Total output length
9-512	Output data

In this approach, the reader will keep all of the Unitech data editing and other features like preamble, postamble, etc. The output data is always 512 bytes; the "Total Output Length" field indicates the valid data length in the output data.

8.1.2. 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	20 10 20 20 20 30	HID Unitech Structure HID Other Structure HID Keyboard
BCD Device Release	00 01	
i-Manufacture	01	
i-Product	02	
i-Serial-Number	00	
# 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 Unitech 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 10 02	Report Count (512 + 16)
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 (UNITECH)
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

8.2 Level 1 and level 2 POS Mode Data Output Format

In POS mode use the special envelope to send out card data. The envelope is in the following format:

[Right Shift, Left Shift, Right Ctrl, Left Ctrl,] Read Error, Track x ID; Track x Error; Track x Data Length; Track x Data; Card Track x LEC code; Track x data LRC.

The reader will send out card data in Alt mode if its ASCII code less than H'20'.

Byte NO.	Name
0	Right Shift
1	Left Shift
2	Right Ctrl
3	Left Ctrl
4	Read Error 1
5	Read Error 2
6	Track x ID
7	Track x Error
8	Track x Length 1
9	Track x Length 2
10	Track Data (no extra Track ID for raw data)
	…
10 + Track len -1	Card Track x LRC
10 + Track len	Track x LRC
10 + Track len +1	0x0D
10 + Track len + 2	Track x ID
….	Repeat Track

The data format is independent with MSR setting. There is no track x data if track x sampling data does not exist.

OPOS header:

Only HID KB interface has [Right Shift, Left Shift, Right Ctrl, Left Ctrl] under POS mode.

Read Error:

Read Error 1 byte bits:

MB							LB
0	B6	B5	B4	B3	B2	B1	B0

B0 1: Track 1 sampling data exists (0: Track 1 sampling data does not exist).
B1 1: Track 2 sampling data exists (0: Track 2 sampling data does not exist).
B2 1: Track 3 sampling data exists (0: Track 3 sampling data does not exist).

B3 1: Track 1 decode success (0: Track 1 decode fail).
B4 1: Track 2 decode success (0: Track 2 decode fail).
B5 1: Track 3 decode success (0: Track 3 decode fail).
B6 0: if b0 to b5 are all 1, otherwise 1 (make it printable).

Read Error byte 2:

MB							LB
0	1	B12	B11	B10	B9	B8	B7

B7 1: Track 4 sampling data exists (0: Track 4 sampling data does not exist).
B8 1: Track 4 JIS II decode success (0: Track4 JIS II decode fail).
B9, B10, B11
000: ISO Card (7, 5) or (7, 5, 5) encoding.
001: Old CADL Card (6, 5, 6) encoding (no longer included).
010: AAMVA Card (7, 5, 7) encoding.
011: JIS I Card (8, 5, 8) encoding.
100: JIS II card (8) or ISO+JIS II.
110: OPOS Raw Data Output.
111: JIS I + JIS II.
B12 Reserved for future use
Decode flag will set to 1 (B3, B4 and B5 all set to 1) in OPOS raw data mode.

Track ID
Track ID is a byte of ID, it will be '1', '2' and '3' for track 1, 2 and 3; it is not accurate to use start sentinel to identify track.

Track x Error
Track x error is a byte of flags, it will be in format of: 0 0 1 b4, b3, b2 b1 b0
b0 1: Start sentinel error (0: Not start sentinel error).
b1 1: End sentinel error (0: Not end sentinel error).
b2 1: Parity error (0: Not parity error).
b3 1: LRC error (0: Not LRC error).
b4 1: Other error (0: Not other error).
Track x Error is set to 0x20 in OPOS raw data mode.

Track Length
Assume actual "Track x Data Length" is hex code xy; the Track x data length for OPOS mode output will be hex code 3x, 3y.
Track x data length does not include the byte of "Track x data LRC", it is <30> <30> in case of read error on track x.

Track Data
“Card Track x LRC code” is track x card data.

Track x LRC

"Track x data LRC" is a LRC to check track x data communication; XOR all characters starting from "Track x ID" to "Track x data LRC" should be 0.

8.3 DUKPT Level 3 Data Output Enhanced Format

This mode is used when all tracks must be encrypted, encrypted OPOS support is required, when the tracks must be encrypted separately, when cards other than type 0 (ABA bank cards) must be encrypted, or when track 3 must be encrypted. This format is the standard encryption format, but not yet the default encryption format.

1. Encryption Output Format Setting:

   Command: 53 85 01 <Encryption Format>

   Encryption Format:
   '00h': Original Encryption Format.
   '01h': Enhanced Encryption Format.

2. Encryption Option Setting: (for enhanced encryption format only)

   Command: 53 84 01 <Encryption Option>

   Encryption Option: (**default 08h**)
   bit0: 1 – track 1 force encrypt.
   bit1: 1 – track 2 force encrypt.
   bit2: 1 – track 3 force encrypt.
   bit3: 1 – track 3 force encrypt when card type is 0.

   Note:
   1) When force encrypt is set, this track will always be encrypted, regardless of the card type. No clear/mask text will be sent.
   2) If and only if in enhanced encryption format, each track is encrypted separately. Encrypted data length will round up to 8 or 16 bytes.
   3) When force encrypt is not set, the data will be encrypted in original encryption format, that is, only track 1 and track 2 of type 0 cards (ABA bank cards) will be encrypted.

3. Hash Option Setting:

   Command: 53 5C 01 <Hash Option>

   Hash Option: ('0' – **'7'**)
   Bit0: 1 – track 1 hash will be sent if data is encrypted.
   Bit1: 1 – track 2 hash will be sent if data is encrypted.
   Bit2: 1 – track 3 hash will be sent if data is encrypted.

4. Mask Option Setting: (for enhanced encryption format only)

   Command: 53 86 01 <Mask Option>

   Mask Option: (**Default: 0x07**)
   bit0: 1 – tk1 mask data allowed to send when encrypted.
   bit1: 1 – tk2 mask data allowed to send when encrypted.
   bit2: 1 – tk3 mask data allowed to send when encrypted.

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

Settings for OPOS:

1. Assume reader is under default setting (Encrypt Structure 0).
2. Set to new Encrypt Structure 1:
   53 85 01 31

The OPOS driver/application may also send the following command when changed (Decode/Raw format)
(Set raw or decode data format)
53 1D 01 30 // RAW data format
53 1D 01 31 // Decoded format

Card data is sent out in the following format
<STX><LenL><LenH><Card Data><CheckLRC><CheckSum><ETX>

0	STX
1	Data Length low byte
2	Data Length high byte
3	Card Encode Type[1]
4	Track 1-3 Status[2]
5	Track 1 data length
6	Track 2 data length
7	Track 3 data length
8	Clear/masked data sent status [3]
9	Encrypted/Hash data sent status [4]
10	Track 1 clear/mask data
	Track 2 clear/mask data
	Track 3 clear/mask data
	Track 1 encrypted data
	Track 2 encrypted data
	Track 3 encrypted data
	Session ID (8 bytes) (Security level 4 only)

Track 1 hashed (20 bytes each) (if encrypted and hash track 1 allowed)
Track 2 hashed (20 bytes each) (if encrypted and hash track 2 allowed)
Track 3 hashed (20 bytes each) (if encrypted and hash track 3 allowed)
KSN (10 bytes)
CheckLRC
CheckSum
ETX

Where <STX> = 02h, <ETX> = 03h

Note 1 : Card Encode Type

Card Type will be 8x for enhanced encryption format and 0x for original encryption format.

Value	Encode Type Description
00h / 80h	ISO/ABA format
01h / 81h	AAMVA format
03h / 83h	Other
04h / 84h	Raw, un-decoded format

For Type 04 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. Track indicator '01','02', and '03' will still exist for non-encrypted mode.

Note 2: Track 1-3 status byte

Field 4:
Bit 0: 1— track 1 decoded data present.
Bit 1: 1— track 2 decoded data present.
Bit 2: 1— track 3 decoded data present.
Bit 3: 1— track 1 sampling data present.
Bit 4: 1— track 2 sampling data present.
Bit 5: 1— track 3 sampling data present.
Bit 6, 7 — Reserved for future use.

Note 3: Clear/mask data sent status

Field 8 (clear/mask data sent status) and field 9 (encrypted/hash data sent status) will only be sent out in enhanced encryption format.

Field 8: Clear/masked data sent status byte:
Bit 0: 1 —track 1 clear/mask data present.
Bit 1: 1— track 2 clear/mask data present.
Bit 2: 1— track 3 clear/mask data present.
Bit 3: 0— reserved for future use.
Bit 4: 0— reserved for future use.
Bit 5: 0— reserved for future use.

Note 4: Encrypted/Hash data sent status

Field 9: Encrypted data sent status
Bit 0: 1— track 1 encrypted data present.
Bit 1: 1— track 2 encrypted data present.
Bit 2: 1— track 3 encrypted data present.
Bit 3: 1— track 1 hash data present.
Bit 4: 1— track 2 hash data present.
Bit 5: 1— track 3 hash data present.
Bit 6: 1—session ID present.
Bit 7: 1—KSN present.

8.4 DUKPT Level 3 Data Output Original Format

For ISO cards, both masked clear and encrypted data are sent, no clear data will be sent.
For other cards, only clear data is sent.

A card swipe returns the following data:

Card data is sent out in format of
<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> card data format is shown below.

ISO/ABA Data Output Format:

- card encoding type (0: ISO/ABA, 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, 0 for no track1 data)
- track 2 unencrypted length (1 byte, 0 for no track2 data)

- track 3 unencrypted length (1 byte, 0 for no track3 data)
- track 1 masked (Omitted if in Raw mode)
- track 2 masked (Omitted if in Raw mode)
- track 3 data (Omitted if in Raw mode)
- track 1 encrypted (AES/TDES encrypted data)
- track 2 encrypted (AES/TDES encrypted data)
- track 3 encrypted (Only used in Raw mode)
- track 1 hashed (20 bytes SHA1-Xor)
- track 2 hashed (20 bytes SHA1-Xor)
- DUKPT serial number (10 bytes)

Non ISO/ABA Data Output Format

- card encoding type (1: AAMVA, 3: Others)
- track status (bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling)
- track 1 length (1 byte, 0 for no track1 data)
- track 2 length (1 byte, 0 for no track2 data)
- track 3 length (1 byte, 0 for no track3 data)
- track 1 data
- track 2 data
- track 3 data

8.5 DUKPT Level 4 Data Output Original Format

For the ISO card, both clear and encrypted data are sent. For other cards, only clear data is sent.

A card swipe returns the following data:

Card data is sent out in the following 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, 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, 0 for no track1 data)
- track 2 unencrypted length (1 byte, 0 for no track2 data)
- track 3 unencrypted length (1 byte, 0 for no track3 data)

- if card encoding type is a high bit set:
  - mask and clear sent track status
  - encrypt and hash sent track status

In this mode tracks are encrypted separately rather than as a group

- track 1 masked (Omitted if in Raw mode)
- track 2 masked (Omitted if in Raw mode)
- track 3 data (Omitted if in Raw mode)
- track 1 encrypted (AES/TDES encrypted data)
- track 2 encrypted (AES/TDES encrypted data)
- sessionID encrypted (AES/TDES encrypted data)
- track 1 hashed (20 bytes SHA1-Xor)
- track 2 hashed (20 bytes SHA1-Xor)
- track 3 hashed (optional) (20 bytes SHA1-Xor)
- DUKPT serial number (10 bytes)

Non ISO/ABA Data Output Format:

- card encoding type (1: AAMVA, 3: Others)
- track status (bit 0,1,2:T1,2,3 decode, bit 3,4,5:T1,2,3 sampling)
- track 1 length (1 byte, 0 for no track1 data)
- track 2 length (1 byte, 0 for no track2 data)
- track 3 length (1 byte, 0 for no track3 data)
- track 1 data
- track 2 data
- track 3 data

Note 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 the data field is located.

Notes:
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.

The hashed data may optionally be omitted, and also track 3 may be hashed and included.

Description:

Track 1 and Track 2 unencrypted Length
This one-byte value is the length of the original track data. It indicates the number of bytes in the track masked data field. It should be used to separate track 1's and track 2's data after decrypting the track encrypted data field.

Track 3 unencrypted Length
This one-byte value indicates the number of bytes in track 3's masked data field.

Track 1 and Track 2 masked
Track data masked with the MaskCharID (default is '*'). The first PrePANID (up to 6 for BIN, default is 4) and last PostPANID (up to 4, default is 4) characters can be in the clear (unencrypted). The expiration date is masked by default but can be optionally displayed.

Track 1 and Track 2 encrypted
This field is the encrypted track data, using either TDES-CBC or AES-CBC with initial vector of 0. If the original data is not a multiple of 8 bytes for TDES or a multiple of 16 bytes for AES, the reader right pads the data with 0.

The key management scheme is DUKPT and the key used for encrypting data is called the Data Key. The Data Key is generated by first taking the DUKPT Derived Key exclusive or'ed with 0000000000FF0000 0000000000FF0000 to get the resulting intermediate variant key. The left side of the intermediate variant key is then TDES encrypted with the entire 16-byte variant as the key. After the same steps are preformed for the right side of the key, combine the two key parts to create the Data Key.

How to get Encrypted Data Length
Track 1 and track 2 data are encrypted as a single block. In order to get the number of bytes for the encrypted data field, we need to get track 1 and track 2 to unencrypted length first. The field length is always a multiple of 8 bytes for TDES or a multiple of 16 bytes for AES. This value will be zero if there is no data on both tracks or if there is an error decoding both tracks. Once the encrypted data is decrypted, all padding of 0 needs to be removed. The number of bytes of decoded track 1 data is indicated by track 1's unencrypted length field. The remaining bytes are track 2's data, the length of which is indicated by track 2's unencrypted length filed.

Track 1, 2 and 3 hashed
The MS246 reader uses SHA-1 to generate hashed data for track 1, track 2 and track 3 unencrypted data. It is 20 bytes long for each track. This is provided with

two purposes in mind: One is for the host to ensure data integrity by comparing this field with an SHA-1 hash of the decrypted track data and prevent unexpected noise in data transmission. The other purpose is to enable the host to store a token of card data for future use without keeping the sensitive card holder data. This token may be used for comparison with the stored hash data to determine if it is from the same card.

Some Additional notes: (4/28/2011)

1. "Decode status" bits in "track status" byte is set to 0 for no error (either decode success or no sampling data), or to 1 for error (has sampling data, but failed to decode).
2. Please be aware that track status byte in secure output is different from track status byte in OPOS header (called read error1 and read error2). OPOS header will only be used in OPOS mode security level 1 and level 2, and secure output only used in level 3 or level 4.
3. For USB HID Secure Output, the output format is the same as the secure output structure. No HID header is added, but the total length is the HID standard (537 bytes). Unused bytes will be filled with 0x00. This is applied to secure Level 3 and Level 4 output, whether or not the data is encrypted.
4. Examples for field 8 (clear/mask data sent status) and field 9 (encrypted/hash data sent status):
   These two bytes are omitted in original structure. In the enhanced encrypted structure, these two bytes are used to indicate the presence of each track's clear or masked data, encrypted data and hash data.
   Example :
   field 8 = 0x03 (00000011)
   field 9 = 0xBF (10111111)
   T1: mask data present; encrypted data present; hash present
   T2: mask data present; encrypted data present; hash present
   T3: no Mask data; encrypted data present; hash present
   KSN: present
   Session ID: not present

Additional Settings

Send LRC in secure mode (6F)

```
53 6F 01 31    // to send LRC in secure mode (Default)
53 6F 01 30    // remove LRC from secure mode
```

Display expiration data (50)

```
53 50 01 30    // do not display expiration date (Exp date masked) (Default)
53 50 01 31    // display expiration data
```

Reader Serial Number (4E)

The serial number will be set to the same as S/N as unit's label. The length is 8 to 10 characters. The user can read out the S/N with 52 4E command.

8.6 Decryption Example

Key for all examples is
0123456789ABCDEFFEDCBA9876543210

8.6.1. Security Level 3 Decryption - Original Encryption Format

Decryption of a three-track ABA card with the original encryption format.
The MS246 reader with default settings:

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

027D0100 3F48236B252A343236362A2A2A2A2A2A2A2A393939395E42555348204A
522F47454F52474520572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A
A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B343236362A2A2A2A2A2A2A2A3939
39393D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B333333333333333333337
3637363736303730373037373637363736333333333333333333337363736373630373 0
3730373736373637363333333333333333333337363736373630373037303737363736373637
3633333333333333333333373637363736303730373F32863E9E3DA28E455B28F7736
B77E47A64EDDA3BF03A06E44F31D1818C0BCD7A353FB1AD70EFD30FFC3DA08
A4FBC9372E57E8B40848BAEAA3FE724B3550E2F4B223E6BF264BEAE9E39142B6
48CDB51FB8DAF8EA5B63913D29419B67582FCCCE9B372660F03668CC453216D9
449C6B67EF33418AC88F65E1DB7ED4D10973F99DFC8463FF6DF113B6226C4898A
9D355057ECAF11A5598F02CA3162994901190000000001399F03

STX, length (LSB, MSB), card type, track status, length track 1, length track 2, length track 3
02 7D01 00 3F 48 23 6B

The above broken down and interpreted:
02—STX character.
7D—low byte of total length.
01—high byte of total length.
00—card type byte (interpretation old format ABA card).
3F—3 tracks of data all good.
48—length of track 1.
23—length of track 2.
6B—length of track 3.

Track 1 data masked (length 0x48):
252A343236362A2A2A2A2A2A2A2A393939395E42555348204A522F47454F5247452
0572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2
A2A2A2A2A2A2A2A3F2A

Track 2 data in hex masked (length 0x23):
3B343236362A2A2A2A2A2A2A2A393939393D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2
A2A2A3F2A

Track 3 data unencrypted (length 0x6B):
3B333333333333333333337363736373630373037303737363736373633333333333333
333333373637363736303730373037373637363736333333333333333333333373637363
736303730373037373637363736333333333333333333333736373673630373037373F32

Track 1 & 2 encrypted length 0x48+0x23 rounded up to 8 bytes =0x6B -> 0x70 (112 decimal):
863E9E3DA28E455B28F7736B77E47A64EDDA3BF03A06E44F31D1818C0BCD7A3
5
3FB1AD70EFD30FFC3DA08A4FBC9372E57E8B40848BAEAA3FE724B3550E2F4B2
2
3E6BF264BEAE9E39142B648CDB51FB8DAF8EA5B63913D29419B67582FCCCE9B
3
72660F03668CC453216D9449C6B67EF3

Track 1 hashed:
3418AC88F65E1DB7ED4D10973F99DFC8463FF6DF

Track 2 hashed:
113B6226C4898A9D355057ECAF11A5598F02CA31

KSN:
62994901190000000001

LRC, checksum and ETX:
39 9F 03

Masked Data:
Track 1 data masked in ASCII:
%*4266********9999^BUSH JR/GEORGE
W.MR^**********************************?*
Track 2 data masked in ASCII:
;4266********9999=***************?*

Track 3 data unencrypted in ASCII:
;33333333376767607070776767633333333337676760707077676763333333333767676070707767676333333333376767607070776767633333333337676760707?2

Key Value: F8 2A 7A 0D 7C 67 46 F1 96 18 9A FB 54 2C 65 A3
KSN: 62 99 49 01 19 00 00 00 00 01

Decrypted data in ASCII:
%B4266841088889999^BUSH JR/GEORGE
W.MR^08091011000011000000000046000000?!;4266841088889999=080910110000046?0
;33333333376767607070776767633333333337676760707077676763333333333767676070707767676333333333376767607070776767633333333337676760707?2

Decrypted data in hex:
2542343236363834313038383838393939395E42555348204A522F47454F52474520572E4D525E303830393130313130303030313130303030303030303034363030303030303F213B34323636383431303838383839393939D303830393130313130303030303436F300000000000

8.6.2. Security Level 4 Decryption - Original Encryption Format

028501003F48236B252A343236362A2A2A2A2A2A2A2A393939395E42555348204A522F47454F52474520572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B343236362A2A2A2A2A2A2A2A3939393939D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B3333333333333333333337363736373630373037303737363736373633333333333333333333373637363736303730373037373637363736373633333333333333333333373637363736303730373037373637363736373633333333333333333333373637363736303730373F32ED9DB728814F150D177F769B0441C52B2B1994C83D058F1DDA5DAA6753CF0F61BB7690C7E8A276D3D606513D1F8B79423C70594A0849CBB4C7B5A8DAC2B1A21B11F1C47EF4F12AC07D59A79E9369372D3F906A7F6C6D2B9076BCF05B334441FAEC8B4EFBEB9DD20EBF97B29D910C415FCEA8DA8FEB9775343418AC88F65E1DB7ED4D10973F99DFC8463FF6DF113B6226C4898A9D355057ECAF11A5598F02CA3162994901190000000044B6F03

Masked data:
Track 1: %*4266********9999^BUSH JR/GEORGE
W.MR^********************************?*
Track 2: ;4266********9999=****************?*
Track 3:
;33333333376767607070776767633333333337676760707077676763333333333767676070707767676333333333376767607070776767633333333337676760707?2

Key Value: 8A 92 F6 74 00 BF 25 2E 57 9A A9 01 FF 27 48 41

KSN: 62 99 49 01 19 00 00 00 00 04
Session ID: AA AA AA AA AA AA AA AA

Decrypted data in ASCII:
%B4266841088889999^BUSH JR/GEORGE
W.MR^08091011000011000000000046000000?!;4266841088889999=080910110000046
?0
;333333333767676070707767676333333333376767607070776767633333333337676760707077676763333333333376767607070776767633333333337676760707?2

Decrypted data in Hex:
2542343236363834313038383838393939395E42555348204A522F47454F52474520572E4D525E303830393130313130303030313130303030303030303034363030303030303F213B343236363834313038383838393939393D303830393130313130303030303034363F30AAAAAAAAAAAAAAAA0000000000

8.6.3. Security Level 3 Decryption - Enhanced Encryption Format

Example of decryption of a three-track ABA card with the enhanced encryption format. The MS246 reader 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.

029801<u>80</u>3F48236B03BF252A343236362A2A2A2A2A2A2A2A393939395E42555348204A522F47454F52474520572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B343236362A2A2A2A2A2A2A2A393939393D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2ADA7F2A52BD3F6DD8B96C50FC39C7E6AF22F06ED1F033BE0FB23D6BD33DC5A1F808512F7AE18D47A60CC3F4559B1B093563BE7E07459072ABF8FAAB5338C6CC8815FF87797AE3A7BEAB3B10A3FBC230FBFB941FAC9E82649981AE79F2632156E775A06AEDAFAF6F0A184318C5209E55AD44A9CCF6A78AC240F791B63284E15B4019102BA6C505814B585816CA3C2D2F42A99B1B9773EF1B116E005B7CD8681860D174E6AD316A0ECDBC687115FC89360AEE7E430140A7B791589CCAADB6D6872B78433C3A25DA9DDAE83F12FEFAB530CE405B701131D2FBAAD970248A456000933418AC88F65E1DB7ED4D10973F99DFC8463FF6DF113B6226C4898A9D355057ECAF11A5598F02CA31688861C157C1CE2E0F72CE0F3BB598A614EAABB162994901190000000000206E203

STX, length(LSB, MSB), card type, track status, length track 1, length track 2, length track 3
02 9801 80 3F 48-23-6B 03BF

The above broken down and interpreted:
02—STX character.
98—low byte of total length.
01—high byte of total length.
80—card type byte (interpretation new format ABA card).
3F—3 tracks of data all good.
48—length of track 1.
23—length of track 2.
6B—length of track 3.
03—tracks 1 and 2 have masked/clear data.
BF—bit 7=1—KSN included.
Bit 6=0—no session ID included so not level 4 encryption.
Bit 5=1—track 3 hash data present.
Bit 4=1—track 2 hash data present.
Bit 3-1—track 1 hash data present.
Bit 2=1—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 0x48):
252A343236362A2A2A2A2A2A2A393939395E42555348204A522F47454F5247452
0572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2
A2A2A2A2A2A2A3F2A

Track 1 masked data in ASCII:
%*4266********9999^BUSH JR/GEORGE
W.MR^********************************?*

Track 2 data in hex masked (length 0x23):
3B343236362A2A2A2A2A2A2A393939393D2A2A2A2A2A2A2A2A2A2A2A2A2
A2A2A3F2A

Track 2 masked data in ASCII:
;4266********9999=***************?*

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

Track 1 encrypted length 0x48 rounded up to 8 bytes = 0x48 (72 decimal):
DA7F2A52BD3F6DD8B96C50FC39C7E6AF22F06ED1F033BE0FB23D6BD33DC5A1
F8
08512F7AE18D47A60CC3F4559B1B093563BE7E07459072ABF8FAAB5338C6CC88
15FF87797AE3A7BE

Track 2 encrypted length 0x32 rounded up to 8 bytes =0x38 (56 decimal):

AB3B10A3FBC230FBFB941FAC9E82649981AE79F2632156E775A06AEDAFAF6F0
A
184318C5209E55AD

Track 3 encrypted length 0x6B rounded up to 8 bytes =0x70 (64 decimal):
44A9CCF6A78AC240F791B63284E15B4019102BA6C505814B585816CA3C2D2F42
A99B1B9773EF1B116E005B7CD8681860D174E6AD316A0ECDBC687115FC89360A
EE7E430140A7B791589CCAADB6D6872B78433C3A25DA9DDAE83F12FEFAB530
CE
405B701131D2FBAAD970248A45600093

Track 1 data hashed length 20 bytes:
3418AC88F65E1DB7ED4D10973F99DFC8463FF6DF

Track 2 data hashed length 20 bytes:
113B6226C4898A9D355057ECAF11A5598F02CA31

Track 3 data hashed length 20 bytes:
688861C157C1CE2E0F72CE0F3BB598A614EAABB1

KSN length 10 bytes:
62994901190000000002

LCR, check sum and ETX
06E203

Clear/masked data in ASCII:
Track 1: %*4266********9999^BUSH JR/GEORGE
W.MR^*********************************?*
Track 2: ;4266********9999=****************?*

Key Value: 1A 99 4C 3E 09 D9 AC EF 3E A9 BD 43 81 EF A3 34
KSN: 62 99 49 01 19 00 00 00 00 02

Decrypted Data:
Track 1 decrypted:
%B4266841088889999^BUSH JR/GEORGE
W.MR^080910110000110000000046000000?!
Track 2 decrypted:
;4266841088889999=08091011000046?0
Track 3 decrypted:
;3333333337676760707077676763333333337676760707077676763333333337676760707077676763333333337676760707?2

Track 1 decrypted data in hex including padding zeros (but there are no pad bytes here):

2542343236363834313038383838393939395E42555348204A522F47454F52474520572
E4D525E303830393130313130303030313130303030303030303034363030303030303F
21

Track 2 decrypted data in hex including padding zeros:
3B34323636383431303838383838393939393D303830393130313130303030303034363F300
000000000

Track 3 decrypted data in hex including padding zeros:
3B33333333333333333333373637363736303730373037373637363736336333333333333
33333333736373637363037303730373737363736373633333333333333333333373637363
736303730373037373637363736333333333333333333333736373637363037303730373F32
0000000000

8.6.4. Security Level 4 Decryption – Enhanced Encryption Format

02A001803F48236B03FF252A343236362A2A2A2A2A2A2A2A393939395E42555348
204A522F47454F52474520572E4D525E2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2
A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A3B343236362A2A2A2A2A2A2A2
A393939393D2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A2A3F2A6D7D5B204D3579694
E148F3FB2565544D35825EA89BA30C966D34363151BF592F995EDA86B94A47EBF
DF6434CB3A075DDD18F616E21F1E2038BC3AD5F96C1387177BD89409DA2E92A
684543E007087F8694AEA8D3DB36BA10BC4D4B2771C622FEC8271A6E021AA564
4ED559EC09CABF19F36B422CA2016B48A7241B2DA9584ED4415B4F30637734CF
5031AF475DAF27C188A1A771264011BAA090E91893BC2A52EDD56F8E6E9554BC
0C5207C04E3C21B6DA2A48F2257DC6946DBFBC87F3189E5C8B954BF7303D01E4
43155911E4137AEAD52441567AA1D50924A7597EC9D758AB4F3A8E82BF81A2E3
418AC88F65E1DB7ED4D10973F99DFC8463FF6DF113B6226C4898A9D355057ECA
F11A5598F02CA31688861C157C1CE2E0F72CE0F3BB598A614EAABB16299490119
0000000003D67C03

Clear/masked data:
Track 1: %*4266********9999^BUSH JR/GEORGE
W.MR^********************************?*
Track 2: ;4266********9999=***************?*

Key Value: 89 52 50 33 61 75 51 5C 41 20 CF 45 F4 1A BF 1C
KSN: 62 99 49 01 19 00 00 00 00 03
Session ID: AA AA AA AA AA AA AA AA

Decrypted data in ASCII:
%B4266841088889999^BUSH JR/GEORGE
W.MR^080910110000110000000046000000?!
;4266841088889999=080910110000046?0

;33333333376767607070776767633333333376767607070776767633333333337676760707077676763333333333767607070776767633333333337676760707?2

Decrypted data in hex:
2542343236363834313038383838393939395E42555348204A522F47454F52474520572E4D525E303830393130313130303030313130303030303030303034363030303030303F21
3B343236363834313038383838393939393D303830393130313130303030303034363F3000000000000
3B333333333333333333333736373637363037303730373736373637363733333333333333333333373637363736303730373037373637363736373633333333333333333333373637363736303730373037373637363736373633333333333333333333373637363736303730373F320000000000

8.7 Level 4 Activate Authentication Sequence

The security level changes from 3 to 4 when the device enters authentication mode successfully. Once the security level is changed to level 3 or 4, it cannot go back to a lower level.

Activate Authentication Mode Command
When the reader is in security level 4, it will only transmit the card data when it is in Authenticated Mode.

Authentication Mode Request
When sending the authentication request, the user also needs to specify a time limit for the reader to wait for the activation challenge reply command. The minimum timeout duration required is 120 seconds. If the specified time is less than the minimum, 120 seconds would be used for timeout duration. The maximum time allowed is 3600 seconds (one hour). If the reader times out while waiting for the activation challenge reply, the authentication failed.

Device Response
When authentication mode is requested, the device responds with two challenges: Challenge 1 and challenge 2. The challenges are encrypted using the current DUKPT key exclusive- or'ed with <F0F0 F0F0 F0F0 F0F0 F0F0 F0F0 F0F0 F0F0>.

The decrypted challenge 1 contains 6 bytes of random numbers followed by the last two bytes of KSN. The two bytes of KSN may be compared with the last two bytes of the clear text KSN sent in the message to authenticate the reader. The user should complete the Activate Authentication sequence using the Activation Challenge Reply command.

Command Structure
Host -> Device:

<STX><R><80h><02h><Pre-Authentication Time Limit><ETX><LRC>

Device -> Host:
<ACK><STX><Device Response Data><ETX><LRC> (success)
<NAK> (fail)

Pre-Authentication Time Limit: 2 bytes of time in seconds.
Device Response Data: 26 bytes of data, consists of <Current Key Serial Number> <Challenge 1> <Challenge 2>.

Current Key Serial Number: 10 bytes of data with the Initial Key Serial Number in the leftmost 59 bits and Encryption Counter in the rightmost 21 bits.
Challenge 1: 8 bytes challenge used to activate authentication. Encrypted using the key derived from the current DUKPT key.
Challenge 2: 8 bytes challenge used to deactivate authentication. Encrypted using the key derived from the current DUKPT key.

Activation Challenge Reply Command
This command serves as the second part of an Activate Authentication sequence. The host sends the first 6 bytes of Challenge 1 from the response of Activate Authenticated Mode command, two bytes of Authenticated mode timeout duration, and eight bytes Session ID encrypted with the result of the current DUKPT Key exclusive- or'ed with <3C3C 3C3C 3C3C 3C3C 3C3C 3C3C 3C3C 3C3C>.

The Authenticated mode timeout duration specifies the maximum time in seconds that the reader will remain in Authenticated Mode. A value of zero forces the reader to stay in Authenticated Mode until a card swipe or power down occurs. The minimum timeout duration required is 120 seconds. If the specified time is less than the minimum, 120 seconds will be used for timeout duration. The maximum time allowed is 3600 seconds (one hour).

If Session ID information is included and the command is successful, the Session ID will be changed.

The Activate Authenticated Mode succeeds if the device decrypts Challenge Reply response correctly. If the device cannot decrypt the Challenge Reply command, Activate Authenticated Mode fails and DUKPT KSN advances.

Command Structure
Host -> Device:
<STX><S><82h><08h><Activation Data><ETX><LRC>

Device -> Host:
<ACK> (success)

<NAK> (fail)

Activation Data: 8 or 16 bytes, structured as <Challenge 1 Response> <Session ID>.
Challenge 1 Response: 6 bytes of Challenge 1 random data with 2 bytes of Authenticated Mode timeout duration. It's encrypted using the key derived from the current DUKPT key.
Session ID: Optional 8 bytes Session ID, encrypted using the key derived from the current DUKPT key.

Deactivate Authenticated Mode Command

This command is used to exit Authenticated Mode. The host needs to send the first 7 bytes of Challenge 2 (from the response of Activate Authenticated Mode command) and the Increment Flag (0x00 indicates no increment, 0x01 indicates increment of the KSN) encrypted with the current DUKPT Key exclusive- or'ed with <3C3C 3C3C 3C3C 3C3C 3C3C 3C3C 3C3C 3C3C>.

If the device decrypts Challenge 2 successfully, the device will exit Authenticated Mode. The KSN will increase if the Increment flag is set to 0x01. If the device cannot decrypt Challenge 2 successfully, it will stay in Authenticated Mode until a timeout occurs or when the customer swipes a card.

The KSN is incremented every time the Authenticated Mode is exited by timeout or card swipe action. When the Authenticated Mode is exited by the Deactivate Authenticated Mode command, the KSN will increment when the increment flag is set to 0x01.

Command Structure
Host -> Device:
<STX><S><83h><08h><Deactivation Data><ETX><LRC>

Device -> Host:
<ACK> (success)
<NAK> (fail)

<Deactivation data>: 8 bytes response to Challenge 2. It contains 7 bytes of Challenge 2 with 1 byte of Increment Flag, encrypted by the specified variant of current DUKPT Key.

Get Reader Status Command

Command Structure
Host -> Device:
<STX><R><83h><ETX><LRC>

Device -> Host:

<ACK><STX><83h><02h><Current Reader Status><Pre-conditon><ETX><LRC> (success)
<NAK> (fail)

Current Reader Status: 2 bytes of data with one byte of <Reader State> and one byte of <Pre-Condition>

Reader State – indicates the current state of the reader as follows:

0x00: The reader is waiting for Activate Authentication Mode Command. The command must be sent before the card can be read.

0x01: The authentication request has been sent, the reader is waiting for the Activation Challenge Reply Command.

0x02: The reader is waiting for a card swipe.

Pre-condition – specifies how the reader goes to its current state as follows:

0x00: The reader has no card swipes and has not been authenticated since it was powered up.

0x01: Authentication Mode was activated successfully. The reader processed a valid Activation Challenge Reply command.

0x02: The reader receives a good card swipe.

0x03: The reader receives a bad card swipe or the card is invalid.

0x04: Authentication Activation Failed.

0x05: Authentication Deactivation Failed.

0x06: Authentication Activation Timed Out. The Host fails to send an Activation Challenge Reply command within the time specified in the Activate Authentication Mode command.

0x07: Swipe Timed Out. The user fails to swipe a card within the time specified in the Activation Challenge Reply command.

Appendix A Setting Parameters and Values

The following is a table of default settings 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	u
BeepID	11	Beep Setting	‘2’ (‘0’~’4’)	Beep volume high and frequency high	
ChaDelayID*	12	Character Delay	‘0’ (‘0’~’5’)	2 ms inter-character delay	k
Track SelectID	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	
Polling IntervalID	14	Polling Interval	1 (1 ~ 255)	USB HID Polling Interval	u
DataFmtID	15	Data Output Format	‘0’ (‘0’~’2’)	Unitech Format	-
FmtOptionID	16	UIC, Mag-Tek	H’59’	Refer to MiniMag RS232 User’s Manual	-
TrackSepID	17	Track Separator	CR/Enter 0 for Port Powered IV	CR for RS232, Enter for KB any character supported except 00 which means none.	
Send OptionID	19	Send Option	‘1’ (‘0’~’F’) ‘5’ for Port Powered IV	Sentinel and account number control	
MSRReading ID	1A	MSR Reading	‘1’ (‘0’~’2’)	Enable MSR reading ‘0’ MSR disable; ‘2’ buffer mode	
DTEnable SendID*	1B	DT Enable Send	‘0’(‘0’,’1’,’3’)	Data Editing Control	-
Decoding MethodID	1D	Decoding Direction	‘1’ (‘0’~’3’)	Decoding in both direction; ‘0’ raw data, ‘2’ forward, ‘3’ reverse	
ReviewID	1F	Review All Settings	None		
Terminator ID	21	Terminator	CR/Enter	CR for RS232, enter for KB	

FmVerID	22	Firmware Version			
USBHIDFmt ID	23	USB HID Fmt	‘0’ (‘0’,’1’,’8’)	‘0’: Unitech HID Format ‘1’: Other HID Format ‘8’: Unitech KB Format	u r
ForeignKB ID	24	Foreign KB	'0' ('0' ~ '9')	Foreign Keyboard	k
SecureKeyID *	25	Obsolescent encryption	‘@’ (0x20-0x7F)	No simple encryption	-
ArmtoRead ID*	30				-
ReaderReset ID*	32		None		-
Track1Prefix ID	34	Track 1 Prefix	0	No prefix for track 1, 6 char max	
Track2Prefix ID	35	Track 2 Prefix	0	No prefix for track 2, 6 char max	
Track3Prefix ID	36	Track 3 Prefix	0	No prefix for track 3, 6 char max	
Track1Suffix ID	37	Track 1 Suffix	0	No suffix for track 1, 6 char max	
Track2Suffix ID	38	Track 2 Suffix	0	No suffix for track 2, 6 char max	
Track3Suffix ID	39	Track 3 Suffix	0	No suffix for track 3, 6 char max	
LZ1ID*	3C		0xD		-
LZ2ID*	3D		0xD		-
LZ3ID*	3E		0xD		-
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)	# of 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	r
OutputMode ID	4D	Std, OPOS or JPOS	'0' ('0' ~ '1')	Standard mode	
Serial NumberID	4E	Device serial #	any 8 bytes	8 hex digit serial number	r
DispExpDate ID,	50	Mask or display expiration date	'0"0'-'1'	‘1’ don’t mask expiration date	
CapsCaseID*	51		None		
DataSeqID*	52		None		
StartCharID*	53		None		
SessionID	54	8 byte hex not stored in EEPROM	None	Always init to all ‘FF’	
Mod10ID	55	Include mod10 check digit	'0' '0'-'2'	Don’t include mod10, ‘1’ display mod10, ‘2’ display wrong mod10	
DesKeyID	56	DES Key Value	0	Internal use only	r n
AesKeyID	57	AES Key Value	0	Internal use only	r n
KeyManage TypeID	58	DUKPT	‘1’(‘0’-‘1’)	‘0’ fixed key	
T1GENERIC FMTID*	59		None		
T2GENERIC FMTID*	5A		None		
T3GENERIC FMTID*	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.	
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	T1, 6B Start	'%'	'%' as track 1, 6 Bit Start Sentinel	
T15BStartID	63	T1, 5B Start	';'	';' as track 1, 5 Bit Start Sentinel	
T27BStartID	64	Track 2, 7 Bit Start Char	'%' ';' for Port Powered IV	'%' as track 2, 7 Bit Start Sentinel	
T25BStartID	65	T2, 5BStart	';'	';' as track 2, 5 Bit Start Sentinel	
T37BStartID	66	Track 3, 7 Bit Start Char	'%' '+' for Port Powered IV	'%' as track 3, 7 Bit Start Sentinel	
T36BStartID	67	T3, 6BStart	'!' '+' for Port Powered IV	'!' as track 3, 6 Bit Start Sentinel	
T35BStartID	68	T3, 5BStart	';' '+' for Port Powered IV	';' 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	
T2ERRSTARTID	6D	Track 2 error code	';'	Start sentinel if track 2 error report	
T3ERRSTARTID	6E	Track 3 error code	'+'	Start sentinel if track 3 error report	
T4ERRSTARTID*	6F		None		-
BootloaderID*	70	Boot Loader Mode	None		-
T344EndID*	71		None		
T28BStartID	72	JIS T12 SS/ES	0		
T38BStartID	73	JIS T3 SS/ES	0		
EquipFwID	77	Feature option setting	0-7	Reader firmware configuration	nr
BeepOffComID*	7A	Turn off Beep	'0'		

SyncCheck ID	7B	Check for track sync bits	'0' ('0'-2')	Check leading & trailing sync bits on track data (if poorly encoded card)	
ErrorZoneID *	7C		None		
Security LevelID	7E			'0' key exhausted; '1' non-encrypted; '1' key loaded non encrypted '3' encrypted; '4'	n r
Encrypt OptID	84	Encryption options	8 encrypt trk 3 if card type 0; (0-F)	Bit 0 encrypt trk1; bit 1 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	
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	-
SearchCmdID*	FB	DE Search Cmd	0	No search command	-
SendCmdID*	FC	DE Send Cmd	0	No send command	-

*Unused entries in this table were left for completeness even though unused in the MS246 reader to avoid conflicting definitions between products.

Note not all function ID are present in different hardware versions of the MS246. The last column above has some codes:

'-' feature not currently supported; exists for compatibility.

's' feature not available in the USB version.

'u' feature available only in the USB version.

'k' feature not available in the USB version.

'r' reset all does not affect this value.

'n' not directly settable.

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.

It is currently not possible to mix security with OPOS and JPOS support.

Appendix B Key Code Table in USB Keyboard Interface

For most characters, "Shift On" and "Without Shift" will be reversed 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 the 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 the 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
Delete	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 SendOptionID	Control Code Bit 3: 0	Alt Code 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