MCH100

Magnetic Stripe Card Reader

USB Interface

Programmer's Manual

Document #: PM099-U Revision 2.0

November 11, 2014

NOTICE

The issuer of this manual has made every effort to provide accurate information. The issuer will not be held liable for any technical and editorial omission or errors made herein; nor for incidental consequential damages resulting from the furnishing, performance or use of this material. This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated without the prior written consent of the issuer. The information provided in this manual is subject to change without notice.

AGENCY APPROVED

- Specifications for FCC Class B, CE Class B
- BSMI (Bureau of Standards, Metrology and Inspection, Taiwan)

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/ TV technician for help.

You are cautioned that any change or modifications to the equipment not expressly approve by the party responsible for compliance could void your authority to operate such equipment.

WARRANTY

This product is served under one-year warranty to the original purchaser. Within the warranty period, merchandise found to be defective would be repaired or replaced. This warranty applies to the products only under the normal use of the original purchaser, and in no circumstances covers incidental or consequential damages through consumers' misuse or modification of the products.

PREFACE

This manual provides detailed information relating to the overall operational, electrical, mechanical, environmental and functional aspects of the MCH100. This document should be read and understood prior to initial operation of the product.

For ease of installation and programming use, we have addressed everything from its attractive features to its various configurations.

When designing the MCH100, we selected what we feel are the most useful features and functions. If in some cases you find that your specific needs differ from our existing products, we welcome your comments and suggestions. Custom-designed models are also available.

If further questions do arise, please call for technical support, our FAE will assist you in any way we can.

Table of Contents

1 General Description

The MCH100 can be configured as a secure reader to protect the card holder's privacy. Once the MCH100 is loaded with initial DUKPT key, all the payment card data that can pass the Luhn check (also known as the mod 10 check) will be sent out in encrypted form, and in addition the administration commands for changing the status or settings of the reader can be set to be protected and then have to be authenticated prior to execution. For non-payment card, which are unable to pass Luhn check, the card data won't be encrypted no matter if the initial DUKPT key is loaded or not.

1.1 Features

The MCH100 provides the following features:

1	Power through the USB port, no external power supply required
2	HID Keyboard, HID MSR or Virtual COM interfaces
3	DUKPT (Derived Unique Key Per Transaction) Key management and Triple-DES (TDES) encryption
4	Read magnetic stripe cards that conform to ISO standards
5	Read both High-coercivity and Low-coercivity cards
6	Bi-directional card swipe and read capability
7	Triple track allow reading ISO, AAMVA, CA DMV and Trade show cards
8	Provide control signals for LED and Buzzer to indicate the status of reader (Optional)

1.2 Data Security and Key Management

The MCH100 security arrangement involves a cryptography system for supporting end-to-end encryption.

- Card Data Encryption: It uses the symmetric-key encryption, Triple DES (TDES) with the Derived Unique Key Per Transaction (DUKPT) key management, to protect the card data.
- Authentication for the administration command: The administration commands can be set to be protected. Once protected, all of the administration commands, including the command used to disable the protection, must be authenticated prior to execution. A challenge-Response mechanism is involved in the process.
- Credit Card Number Hashing: For some applications, there is a need to use a credit card number for identification. However, legal requirements mean that actual card numbers cannot be stored. MCH100 use HMAC-SHA256 on the credit card number to generate a cryptographic hash that is practically impossible to reserve for the above-mentioned need.

1.3 Product Life Cycle

The reader will go through several phases in relation to key management. The phase number will be increased automatically according to the conditions on key loading operation, but doesn't have to move sequentially one increment at a time.

Phase	Key Loading Key	DUKPT Key	Security	Remark
Phase 0	Empty	Initial DUKPT key can be loaded or reset to empty for MFG testing purpose.	Card data can be encrypted or unencrypted according to the existence of DUKPT key.	Phase 0 can be seen only in the factory.
Phase 1	factory default*	Initial DUKPT key has **not** been loaded.	No authentication is required for initial DUKPT key loading; Card data is **not** encrypted.	The initial DUKPT key loading needs to be performed in clear text because the key loading key has not been updated yet.
Phase 2	factory default*	Initial DUKPT key has been loaded.	No authentication is required for initial DUKPT key loading; Card data is encrypted**.	The initial DUKPT key updating needs to be performed in clear text because the key loading key has not been updated yet.
Phase 3	updated (different than the factory default)	Initial DUKPT key has **not** been loaded	No authentication is required for initial DUKPT key loading; Card data is **not** encrypted.	The initial DUKPT key loading can be performed in clear text or in ANSI TR-31 format.
Phase 4	updated (different than the factory default)	Initial DUKPT key has been loaded only via clear text format (not via ANSI TR-31 format).	No authentication is required for initial DUKPT key loading; Card data is encrypted**.	The initial DUKPT key loading can be performed in clear text or in ANSI TR-31 format.

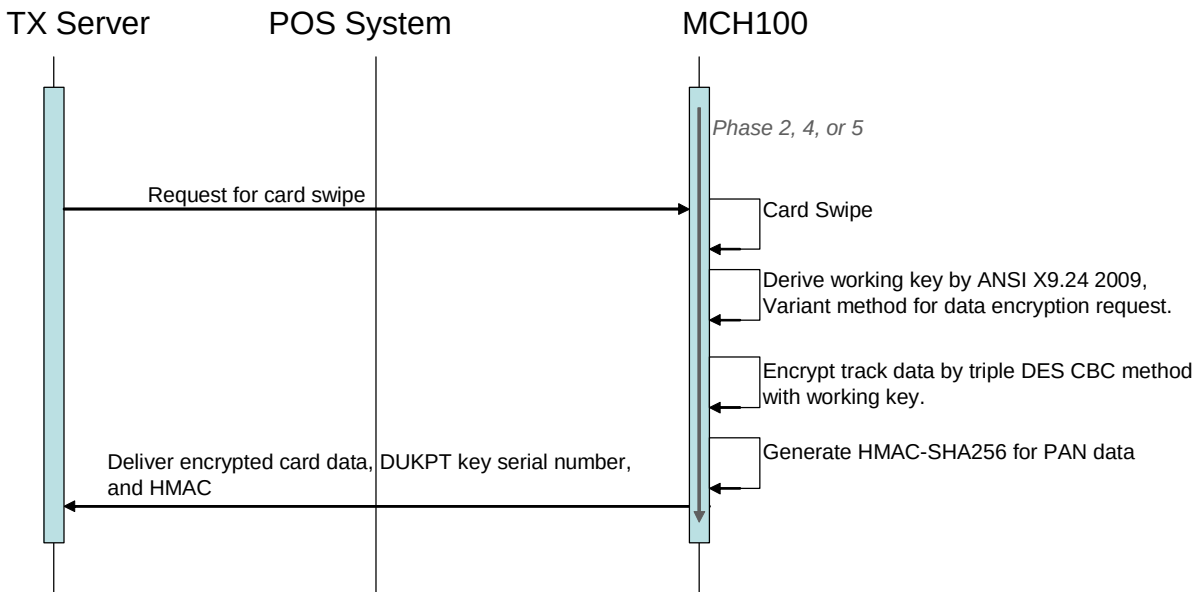
Phase 5	updated (different than the factory default)	Initial DUKPT key has been loaded via ANSI TR-31 format.	Authentication is needed for initial DUKPT key loading; Card data is encrypted**.	The initial DUKPT key loading needs to be performed in ANSI TR-31 format.
Phase 6 (Terminated)	factory default	Key generation reaches to the end	No more card reading operation will be performed.	The reader reached the end of its lifetime.
	updated (different than the factory default)			

* Before the key loading key is loaded, the initial DUKPT key loading is not allowed to be performed in ANSI TR-31 format.

** Only the payment card data that can pass the Luhn check (also known as the mod 10 check) will be encrypted. For non-payment cards, which are unable to pass Luhn check, the card data won't be encrypted.

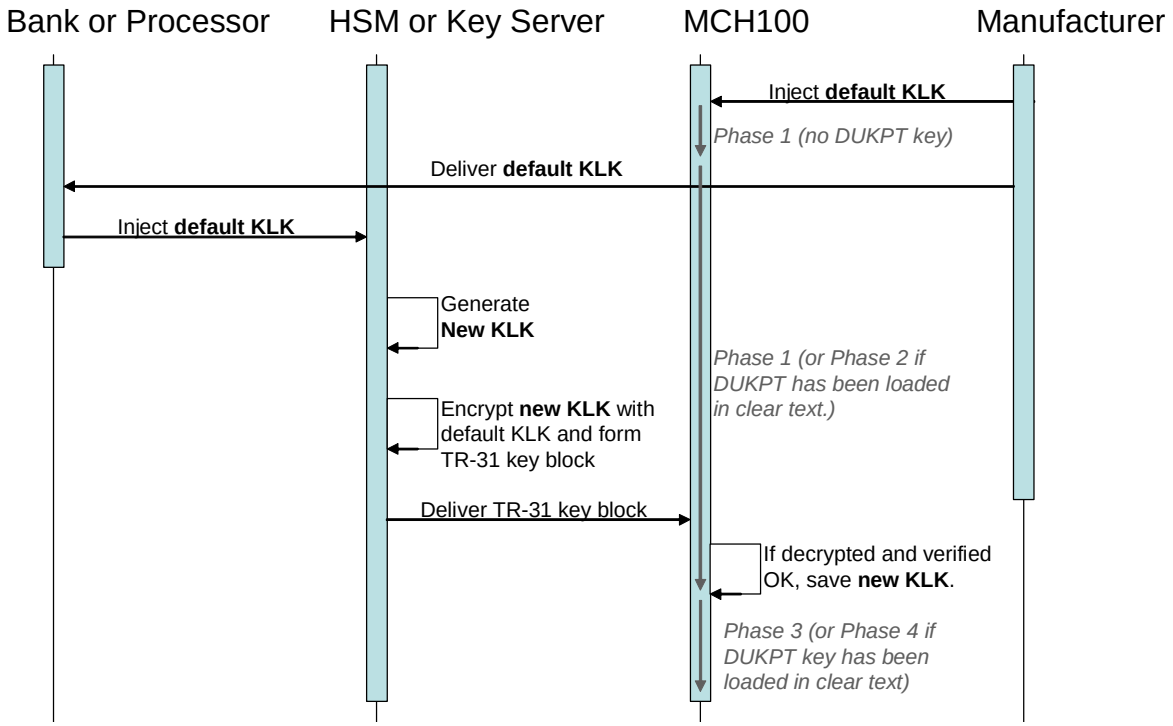
1.4 Transaction Flow

Once loaded with the initial DUKPT key, MCH100 outputs the payment card data in encrypted form for each transaction.

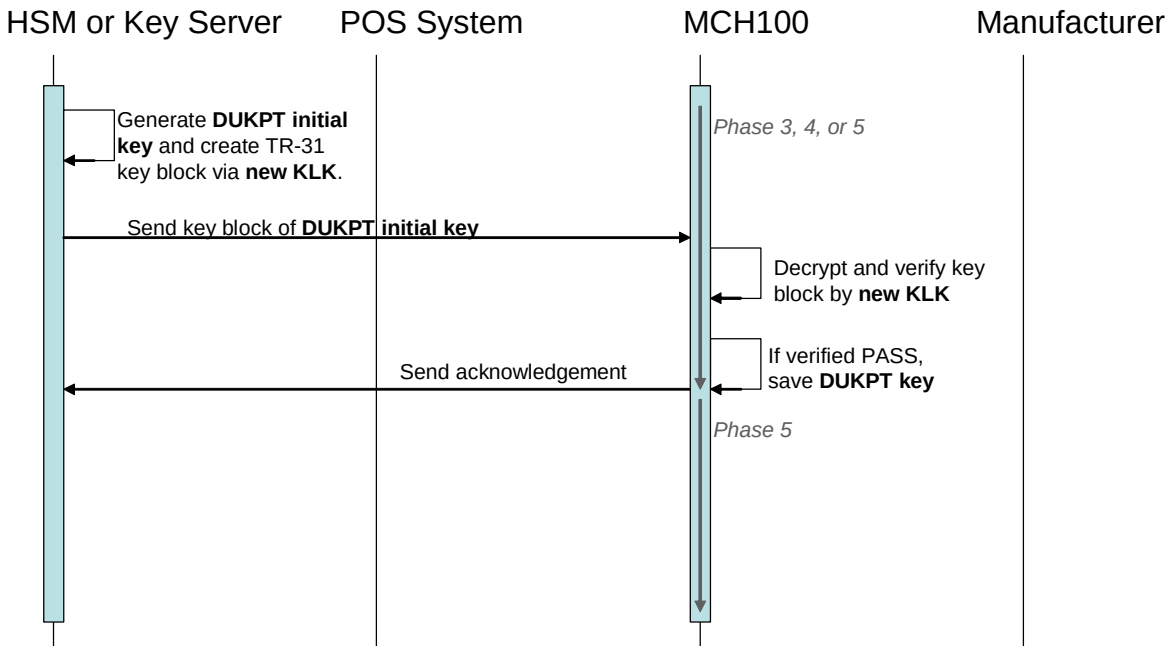


1.5 Operation Flow of MCH100 Remote Key Update

1.5.1 Preparation for remote key update



1.5.2 Remote key update



2 General Description

This section shows the dimensions and setup for the MCH100.

2.1 Dimensions of MCH100

(See Sec 5.2, USB Connector Termination Assignment, for pin assignment.)

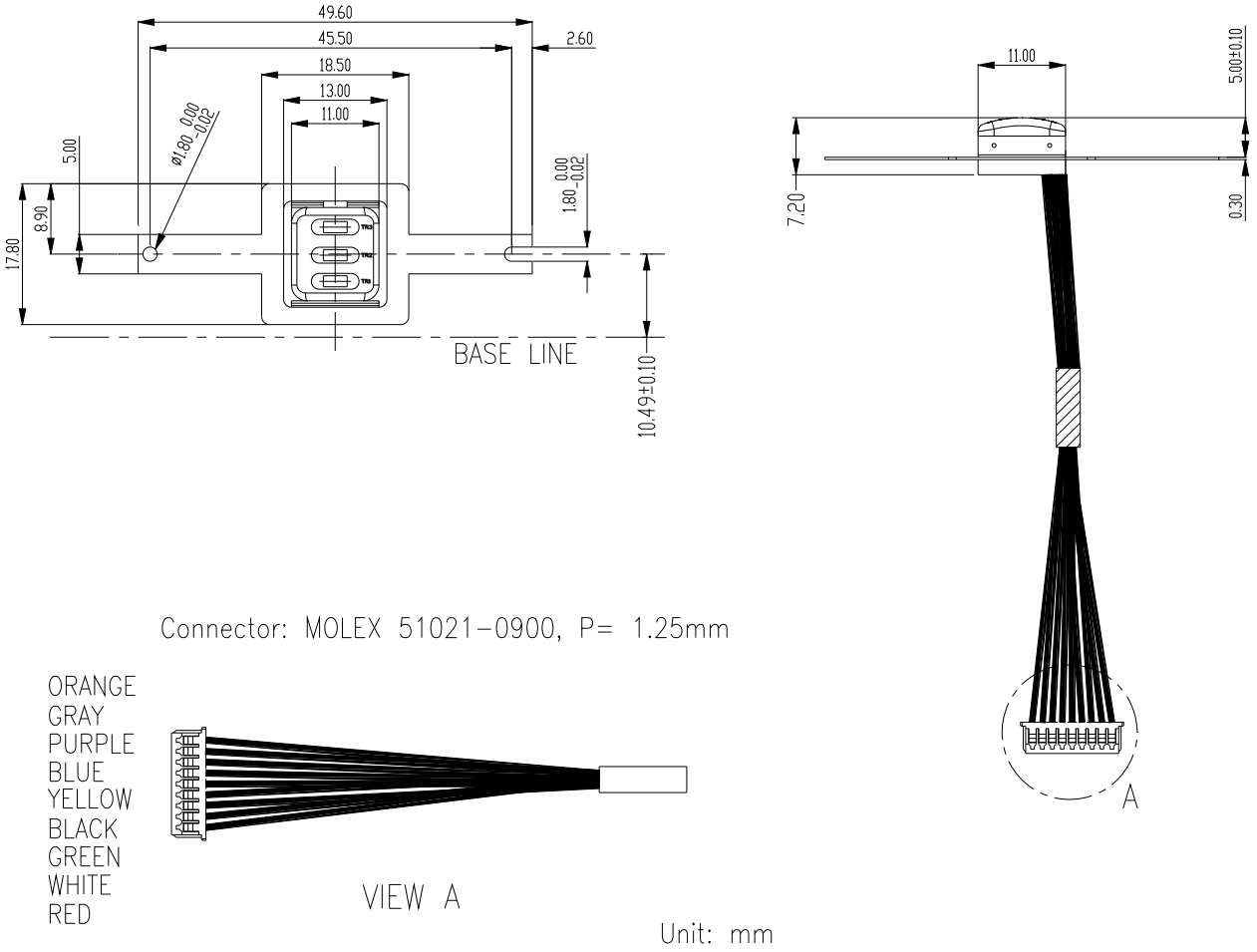
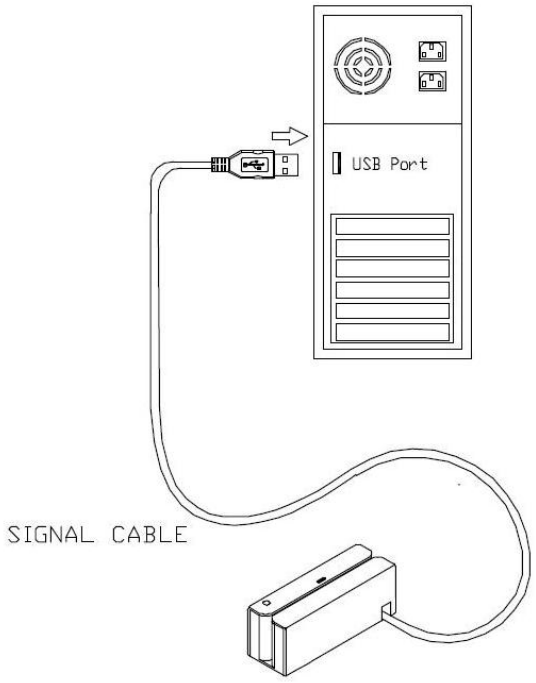


Figure 1 Dimensions of MCH100

2.2 Installation

1) Insert USB connector to a free USB port on the PC system.
2) The LED of MCH100 will turn green indicating that the device is ready for use.



Suppose that MCH100 is integrated into a housing equipped with a LED and a USB extension cable connected to the pigtail cable of MCH100.

Figure 2 Installing MCH100

3 Technical Specifications

3.1 Magnetic Card Specifications

Recording Method

Two-frequency coherent phase (F2F)

Card Type

ISO 7811

CA old DMV

AAMVA

Tradeshow card

Read high or low coercivity magnetic stripes (300-4000oe)

Thickness

0.76mm ± 0.08mm

Card Format

Track 1 & 3: 210 bpi

Track 2: 75⁄210 bpi

Card Operation Speed

Test Card	Speed (IPS)
ISO standard card	5-55
*Jitter	5-50
**Low Amplitude	5-50

Notes

*Jitter card: Reliable reading of magnetic stripes encoded with bit cell length variations within ±15% of normal as defined by ISO 7811.

**Low amplitude: Reliable reading of magnetic stripes encoded at 60% or more of the encoding amplitude as defined by ISO 7811.

3.2 Mechanical Specifications

Dimension

Length: 49.6 mm

Width: 17.8 mm

Height: 7.2 mm

Weight

Approx. 5g

Cable Length

135 mm

Connector

MOLEX 51021-0600, P=1.25mm

Magnetic Head Life

Min. 1M swipes

3.3 Electrical Specifications

Power Required
+5VDC, +/-5%

Power Consumption
50mA Max.

Communication
Compatible with USB specification Revision 2.0

Ripple
50mVp-p Max

Dielectric Strength
250VDC for 1 minute

Insulation Resistance
10MΩ min. at 250VDC

3.4 Environmental Specifications

Temperature
Operating: -10℃ to 55℃

Humidity
Operating: 5% to 95% relative humidity

4 Reader Operation

4.1 Mode

The MCH100 supports three different modes of operation. The factory default is in *Virtual COM* mode.

- Keyboard Emulation mode (KB)
- Uniform defined HID Device mode (HID MSR)
- Virtual COM Port mode (Virtual COM)

4.2 LED and Buzzer Control Signals (Optional)

MCH100 provides control signals for connecting to external LED and buzzer to indicate the status of reader. The LED indicator will be either off, amber, red and green in the normal mode. When the device is not powered, the LED will be off. The LED will turn green and buzzer beeps one only if the device is attached and enumerated.

When a card is being swiped, the LED will turn off awhile or until the swipe is accomplished. If there is no error occurred, the LED will turn green and buzzer beeps once. If the LED turns amber and buzzer beeps twice, there is probability some data unrecognizable or it is not a triple track card. If no data is recognized, the LED will turn red and buzzer beeps three times. When the LED becomes green from red, the device will be ready to read the next card.

When all DUKPT keys have been used, the LED will turn red to indicate MCH100 is not useful.

4.3 Card Reading

To exhibit the card reading capabilities, any text editor program that accepts keyboard input can be used such as Microsoft Notepad and Word.
Note that reader working in the HID MSR or Virtual COM is not applicable in this case.

5 Communication Specifications

This section describes the information for connecting to the reader.

5.1 Identification Information

Vendor ID: 6352h

Product ID: 101Bh(HID Keyboard)／101Ch(HID MSR)／101Ah(Virtual COM)

5.2 USB Connector Termination Assignment

Contact Number	Signal Name	Typical Wiring Assignment
1	USB VBUS	Red
2	USB D-	White
3	USB D+	Green
4	GND	Black
5	Reserved for MFG Test	Yellow
6	Buzzer Output	Blue
7	LED-B Output	Purple
8	LED-R Output	Gray
9	Shield	Orange

5.3 Data Output Format

5.3.1 HID Keyboard & Virtual COM

Clear Text output

Output Sequence	Length	Description
<Preamble>		Cleartext Data Field (available when reading a non-payment card that cannot pass the Luhn check, also known as the mod 10 check.)
<TK1 Prefix><SS> <TK1 Cleartext Data> <ES><TK1 Suffix>		
<TK2 Prefix><SS> <TK2 Cleartext Data> <ES><TK2 Suffix>		
<TK3 Prefix><SS> <TK3 Cleartext Data> <ES><TK3 Suffix>		

<Postamble>		

Encrypted Output

Output Sequence	Length	Description
<'|'><Card Decode Type>	2	00:ISO/ABA 01:AAMVA 02:CADL 03:Blank 04:Other 05:Unknown
<'|'><TK1 Encrypted Data>		Encrypted Data Field
<'|'><TK2 Encrypted Data>		
<'|'><TK3 Encrypted Data>		
<'|'><DUKPT KSN>	20	DUKPT Serial Number/Counter
<'|'><Session ID>	16	Encrypted Current Session ID
<'|'><Serial Number>	32	MCH100 Serial Number
<'|'><Encrypted mode>	2	00: TDES CBC/PIN 01: RFU 10: TDES CBC/DATA 11: RFU
<'|'> HMAC(DATA)	32	HMAC-SHA256 of card data
<'CR'>	0 or 1	Carriage Return. Only applies to HID Keyboard.

5.3.2 HID MSR

Offset	Usage Name	Description
0	Track 1 decode status	00h→decode error, 01h→decode ok
1	Track 2 decode status	00h→decode error, 01h→decode ok
2	Track 3 decode status	00h→decode error, 01h→decode ok
3	TK1 encrypted data length	Track 1 encrypted data length
4	TK2 encrypted data length	Track 1 encrypted data length
5	TK3 encrypted data length	Track 1 encrypted data length
6	Card Decode Type	00:ISO/ABA 01:AAMVA 02:CADL 03:Blank 04:Other 05:Unknown
7	Encrypted mode	00: TDES CBC/PIN 01: RFU 10: TDES CBC/DATA 11: RFU
8-167	TK1 encrypted data	Original TK1 data encrypted by Triple DES using DUKPT key management
168-327	TK2 encrypted data	Original TK2 data encrypted by Triple DES using DUKPT key management

Offset	Usage Name	Description
328-487	TK3 encrypted data	Original TK3 data encrypted by Triple DES using DUKPT key management
488-497	DUKPT serial number/counter	DUKPT serial number and counter
498-513	Serial Number	Serial number for device
514	TK1 cleartext data length	TK1 cleartext data length
515	TK2 cleartext data length	TK2 cleartext data length
516	TK3 cleartext data length	TK3 cleartext data length
517-676	TK1 cleartext data	SS + TK1 Cleartext Data + ES
677-836	TK2 cleartext data	SS + TK2 Cleartext Data + ES
837-996	TK3 cleartext data	SS + TK3 Cleartext Data + ES
997-1012	Encrypted Session ID	Session ID encrypted by Triple DES using DUKPT key management
1013	TK1 absolute data length	Original TK1 data length
1014	TK2 absolute data length	Original TK2 data length
1015	TK3 absolute data length	Original TK3 data length
1016~1048	HMAC data	HMAC-SHA256 of card data

5.4 Device Descriptor

Field	Value		
	HID Keyboard	HID MSR	Virtual COM
Length	12	12	12
Descriptor Type	01	01	01
USB	0200	0200	0200
Device Class	00	00	02
Device Sub Class	00	00	00
Device Protocol	00	00	00
Max Packet Size	08	08	40
Vendor	6352	6352	6352
Product	101B	101C	101A
Device	0103	0103	0002
Manufacturer	01	01	01
Product	02	02	02
Serial Number	00	00	00
Num Configurations	01	01	01

5.5 Report Descriptor, HID MSR Mode Setting

Field	Value	Description
	06 00 FF	Usage Page (MSR)
	09 01	Usage (Decoding Reader)
	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 40	Usage (Tk1 Encrypted Data Length)
	09 41	Usage (Tk2 Encrypted Data Length)
	09 42	Usage (Tk3 Encrypted Data Length)
	09 38	Usage (Card Encode Type)
	09 52	Usage (Encrypt Mode)
	95 08	Report Count
	81 02	Input (Data, Var, Abs, Bit Field)
	09 45	Usage (Tk1 Encrypted Data)
	95 A0	Report Count (160)
	82 02 01	Input (Data, Var, Abs, Buff)
	09 46	Usage (Tk2 Encrypted Data)
	95 A0	Report Count (160)
	82 02 01	Input (Data, Var, Abs, Buff)
	09 47	Usage (Tk3 Encrypted Data)
	95 A0	Report Count (160)
	82 02 01	Input (Data, Var, Abs, Buff)
	09 3A	Usage (DUKPT Serial Number & Counter)
	95 0A	Report Count (10)
	82 02 01	Input (Data, Var, Abs, Buff)
	09 50	Usage (Serial Number)
	95 0A	Report Count (16)
	82 02 01	Input (Data, Var, Abs, Buff)
	09 28	Usage (Tk1 Cleartext Data Length)
	09 29	Usage (Tk2 Cleartext Data Length)
	09 2A	Usage (Tk3 Cleartext Data Length)

Field	Value	Description
	95 03	Report Count (3)
	81 02	Input (Data, Var, Abs, Bit Field)
	09 30	Usage (Tk1 Cleartext Data)
	95 A0	Report Count (160)
	82 02 01	Input (Data, Var, Abs, Buff)
	09 31	Usage (Tk2 Cleartext Data)
	95 A0	Report Count (160)
	82 02 01	Input (Data, Var, Abs, Buff)
	09 32	Usage (Tk3 Cleartext Data)
	95 A0	Report Count (160)
	82 02 01	Input (Data, Var, Abs, Buff)
	09 51	Usage (Encrypted Session ID)
	95 10	Report Count (16)
	82 02 01	Input (Data, Var, Abs, Buff)
	09 4A	Usage (Tk1 Absolute Data Length)
	09 4B	Usage (Tk2 Absolute Data Length)
	09 4C	Usage (Tk3 Absolute Data Length)
	95 03	Report Count (3)
	81 02	Input (Data, Var, Abs, Bit Field)
	09 52	Usage (HMAC-SHA256)
	95 20	Report Count (16)
	82 02 01	Input (Data, Var, Abs, Buff)
	09 20	Usage (Command Message)
	96 50 03	Report Count
	B2 02 01	Feature (Data, Var, Abs, Buff)
	C0	End Collection

5.6 Card Encode Type

0 ISO/ABA: ISO/ABA encode format

1 AAMVA: AAMVA encode format

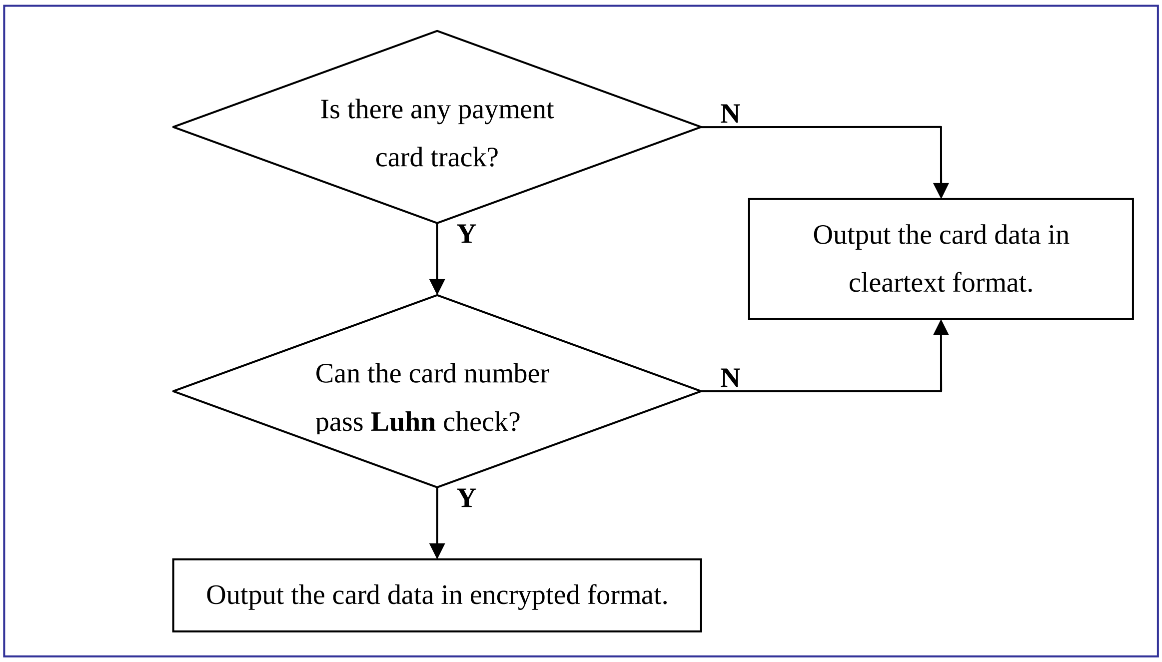
2 CADL: California Driver License

3 Blank: The card is blank

4 Other: The card has a non-standard format. For example, ISO/ABA track 1 format on track 2.

6 Track Encryption Rules

This section describes how MCH100 determines if the card data is sent in cleartext or encrypted format.



EXAMPLE: (a payment card track exists) & (card number passes the Luhn check)

Encrypted:

|00|033A4A6F4B13971164C7DB2413E57DC51979F73207A1AAE764686EAE174322B0D50ADCDFD7C1BED27
6F155139E65C76B3ED53939262901C062283FC8FC560805|7A616C88699EEABD89DE6EF52E3F042422ED12
010E24F047F1D6053B7826CF87DDD45F5C05A3974F|ADA9EE86C2AD7B848A7E3F95808BDF61D6780B0FF8F
1B67833A2B598A784C24CE9DBE54F3476C31D46E05B355CD480123F1215702B1D71529234226540ECC9471
A28C6DCEA8EDEA6E044302F6AD9DE62F643CCEF3A31605BCBC75422C2A13CC6C18A998CA088A7DFEF921
DBD791ABB23|55494330303031000002|54E755672E52C69C|30303030303030303030303030303030|10|C
74B737FC4169674A859808E6350DA1343DFF7E52AC3687CDC20A9D9B7208C1A|

EXAMPLE: (no payment card track exists)

Cleartext:

%11111111111111111111111111111111111111111111111111111111111111111111111111111?
;2222222222222222222222222222222222222?
;33333333333333333333333333333333333333333333333333333333333333333333333333333333333333333
3333333333333333?

EXAMPLE: (a payment card track exists), but (the card number fails the Luhn check)

Cleartext:

%B8086232911967^VERIFONE INC/DQ TESTCARD   ^991201076350226304?
;8086232911967=991201076350226304?

7 Commands and Responses

7.1 Command Format

7.1.1 HID Keyboard and HID MSR

Protocol 1

C2	XX	XX	Command	Data

C2: HEADER

XX XX: Length, including Command and Data

Protocol 2

C2	XX	XX	STX	Command	Data	ETX	LRC

C2: HEADER

XX XX: Length, including STX, Command, Data, ETX and LRC

STX: 02h

ETX: 03h

LRC: Perform XOR operation on all bytes starting from Command to ETX.

This protocol supports commands “90” and “76”.

Protocol 3

C2	XX	XX	SI	Command	Data	SO	LRC

C2: HEADER

XX XX: Length, including SI, Command, Data, SO and LRC

SI: 0Fh

SO: 0Eh

LRC: Perform XOR operation on all bytes starting from Command to SO.

This protocol supports commands “02”, “05” and “06”.

7.1.2 Virtual COM

Protocol 4

Command	Data

Protocol 5

STX	Command	Data	ETX	LRC

STX: 02h

ETX: 03h

LRC: Perform XOR operation on all bytes starting from Command to ETX.

This protocol supports commands “90” and “76”.

Protocol 6

SI	Command	Data	SO	LRC

SI: 0Fh

SO: 0Eh

LRC: Perform XOR operation on all bytes starting from Command to SO.

This protocol supports commands “02”, “05”, “06”.

7.2 Response Format

7.2.1 HID Keyboard and HID MSR

C2	XX	XX	Response

C2: HEADER

XX XX: Length

Response: VALUE or RETURN CODE

RETURN CODE	Description
06h	ACK
15h	NAK

7.2.2 Virtual COM

Response

Response: VALUE or RETURN CODE

RETURN CODE	Description
06h	ACK
15h	NAK

7.3 Command List

Following are the commands and responses available for the device.

General Commands/Responses	
COMMAND	Description
39h	Get Firmware Version
53h	Load Serial Number
73h	Get Serial Number
7Fh	Device Reset
A6h	Get Administration Commands Protection Status
5Ah 36h 34h	Query Key Check Value (KCV)
5Ah 36h 35h	Key Check Value Response
44h 30h 35h	Get Key Management Phases
DUKPT Operation Commands/Responses	
COMMAND	Description
30h 32h	Change Key Loading Key
39h 30h	Load Initial Key Request
39h 31h	Load Initial Key Response
30h 35h	Load Serial Number
30h 36h	Get Serial Number
37h 36h	PIN Entry Test Request
37h 31h	Encrypted PIN Block Response
93h	Get DUKPT Serial Number/Counter and Encrypted Random Number
Administration Commands	
COMMAND	Description
A5h	Set Administration Commands Protection Status
62h	Set Device Interface
96h	Set Session ID
45h	Set Properties in the Device
52h	Get Properties from the Device
44h 30h	Set Properties in Default for Current Interface
44h 41h	Set Properties in Default for All Interface
Note The new setting will not take effect until the device is reset.	

7.4 General Commands/Responses

7.4.1 39h - Get Firmware version

This command is used to get firmware version.

EXAMPLE

Host request	Reader response
C2 00 01 39	
	C2 00 08 32 31 45 30 31 36 31 41

7.4.2 53h - Load Serial Number

This command is used to set device serial number, 16 bytes max.

EXAMPLE

Host request	Reader response
C2 00 0A 53 30 31 32 33 34 35 36 37 38	
	C2 00 01 06

7.4.3 73h - Get Serial Number

This command is used to get device serial number.

EXAMPLE

Host request	Reader response
C2 00 01 73	
	C2 00 09 30 31 32 33 34 35 36 37 38

7.4.4 7Fh - Device Reset

This command is used to reset device.

EXAMPLE

Host request	Reader response
C2 00 01 7F	
	C2 00 01 06

7.4.5 A6h - Get Administration Commands Protection Status

This command is used to query whether the administration commands are protected or not.

Response Parameters:

‘00h’: Means Administration Commands are not protected (default)

‘01h’: Means Administration Commands are protected

EXAMPLE

Host request	Reader response
C2 00 01 A6	
	C2 00 01 00

7.4.6 5Ah 36h 34h - Query Key Check Value (KCV)

Format: **<STX>Z64[KeyID]<ETX>[LRC]**

Message length: Fixed 7 bytes.

Usage: This message will export the KCV of specified master key.

KCV is calculated as following:

1. Use [KeyID] specified key as encryption key.
2. Use "0000000000000000" (8 bytes zero) as data.
3. Use TDES algorithm to encrypt the data.
4. Take leftmost 3 bytes as KCV, output KCV as message Z65 (i.e. 5Ah 36h 35h - Key Check Value Response).

Note:

- The [Key ID] field’s format is an ASCII characteristic. On MCH100, it is always ‘F’.

Example: TDES key "0123456789ABCDEF FEDCBA9876543210" will have KCV as "08D7B4".

Message element:

Field	Length	Value and description
<STX>	1	<02>
Z64	3	Message ID
[KeyID]	1	Key position, always ‘F’ on MCH100. (i.e. ‘F’ is the ID of key loading keys for MCH100).
<ETX>	1	<03>
[LRC]	1	Checksum

Message flow:

HOST	Direction	MCH100 Reader
Message Z64 (5Ah 36h 34h) request frame	→	
	←	<ACK> /<NAK>/<EOT>
	←	Processing request. If format error, send <EOT> and end. Message Z65 (5Ah 36h 35h), the echo of request frame.

Verify echo frame. If verified ok, send <ACK>. If packet LRC error, send <NAK>. If host wants to cancel key loading procedure, send <EOT>.	→	

7.4.7 5Ah 36h 35h - Key Check Value Response

Format: **<STX>Z65[KeyID][KCV]<ETX>[LRC]**

Message length: Variable. 13 bytes for KCV, or 8 bytes for error code.

Usage: This message is the response of Z64 (command 5Ah 36h 34h). If [KeyID] specified in Z64 is pointing to a valid master key, the KCV will be sent. Otherwise a question mark '?' will be sent.

Message element:

Field	Length	Value and description
<STX>	1	<02>
Z65	3	Message ID ; Key Check Value Response
[KeyID]	1	Key position, always 'F' on MCH100. (i.e. 'F' is the ID of key loading keys for MCH100).
[KCV]	6 or 1	Success: 6 characters KCV. Fail: '?'.
<ETX>	1	<03>
[LRC]	1	Checksum

7.4.8 44h 30h 35h – Get Key Management Phases

Format: **<STX>D05<ETX>[LRC]**

Message length: Fixed 6 bytes.

Usage: This command is used to get key management phases.

Request frame (HOST to MCH100 Reader)

Field	Length	Value and description
<STX>	1	<02>
D05	3	Message ID
<ETX>	1	<03>
[LRC]	1	Checksum

Response frame (MCH100 Reader to HOST)

Field	Length	Value and description
<STX>	1	<02>
[Key Flag 1]	1	This flag is used to keep track of whether MCH100 is still in phase 0. <00>: MCH100 is running in any phase higher than phase 0. <FF>: MCH100 is running in phase 0.
[Key Flag 2]	1	This flag is used to keep track of whether the KLK (key loading key) has been loaded with a value different than the factory default. <00>: The KLK has been loaded and is different than the factory default. <FF>: The KLK is empty or factory default.
[Key Flag 3]	1	This flag is used to keep track of whether the DUKPT key has been loaded. <00>: The initial DUKPT key has been loaded via ANSI TR-31 format. <FE>: The initial DUKPT key has been loaded only via clear text format. <FF>: The initial DUKPT key has not been loaded yet.
[Key Flag 4]	1	This flag is used to keep track of whether the DUKPT Key generation reaches to the end. <00>: Key generation reaches to the end (i.e. The reader reached the end of its lifetime.) <FF>: Key generation has not reached to the end.
<ETX>	1	<03>
[LRC]	1	Checksum

With the values of the above three flags (Key Flag 1 to Key Flag 4), several phases in relation to key management are defined as follows:

	Key Flag 1	Key Flag 2	Key Flag 3	Key Flag 4
Phase 0	<FF>	<FF>	<FF> or <FE>	<FF>
Phase 1	<00>	<FF>	<FE>	<FF>
Phase 2	<00>	<FF>	<FE>	<FF>
Phase 3	<00>	<00>	<FE>	<FF>
Phase 4	<00>	<00>	<FE>	<FF>
Phase 5	<00>	<00>	<00>	<FF>
Phase 6	<00>	<FF> or <00>	<FF> or <00>	<99>

Note: For more explanations about Phase 0 to Phase 6, please refer to Sec 1.3 – Product Life Cycle.

7.5 DUKPT Operation Commands/Responses

7.5.1 30h 32h - Change Key Loading Key

Format: **<SI>02[Key ID] [Key bundle (ANSI TR-31 format)]<SO>[LRC]**

Message length: Variable (38 to 94 bytes).

Usage: Change Key Load Key in MCH100.

This command is used to load or update “Key Loading Key” into MCH100. “Key Loading Key” is used as a key block protection key (KBPK) to derive necessary encrypting keys for ANSI TR-31 key bundle. After receiving a brand new MCH100 from the supplier, the user has to replace the factory default “Key Loading Key” with a new one via a secure computer in a secure environment, and keep the new “Key Loading Key” in a secure place to protect it from unauthorised access. Before changing the default “Key Loading Key” to a new one, the reader won’t be allowed to inject the Initial DUKPT Key into the reader to have encrypted output. Please contact UIC sales to obtain the factory default “Key Loading Key”.

Note:

- The [Key ID] field’s format is an ASCII characteristic. On MCH100, it is always ‘F’.
- The MCH100 reader requires key loading key to be TDES.

Request frame (HOST to MCH100 Reader)

Field	Length	Value and description
<SI>	1	<0F>
02	2	Message ID
[Key ID]	1	Key position, always ‘F’ on MCH100.
[Key bundle]	Var.	ANSI TR-31 key block data.
<SO>	1	<0E>
[LRC]	1	Checksum

Response frame – Error message (MCH100 Reader to HOST)

Field	Length	Value and description
<SI>	1	<0F>
02	2	Message ID
?	1	
[Err msg]	1	‘2’: Not allowed to be the factory default key ‘3’: Internal fail: fail to allocate memory ‘4’: Internal fail: fail to read key structure ‘7’: Fail to decrypt key value.

Field	Length	Value and description
		‘A’: TR-31 format error. ‘C’: Fail to verify MAC value. ‘D’: KLK does not exist / The selected key (KLK) is not with usage “K0” ‘E’: Incompatible key usage.
<SO>	1	<0E>
[LRC]	1	Checksum

Message flow:

HOST	Direction	MCH100 Reader
Message 02 (request frame)	→	
	←	<ACK> /<NAK>/<EOT>
	←	Processing request. If format error, send <EOT> and end. Message 02 (echo of request frame).
Verify echo frame. If verify ok, send <ACK>. If packet LRC error, send <NAK>. If host want to cancel key loading procedure, send <EOT>.	→	
	←	Save key value and send <EOT>

Example:

Encrypted (ANSI TR-31 2005 Key Variant Binding Method)

Key condition:	Load a double length key encryption key to key position ‘F’
Key encrypting key (i.e. key loading key loaded in MCH100 with Key ID ‘F’):	1919191919191919 5B5B5B5B5B5B5B5B
Master Key (i.e. key loading key) to be loaded:	AA55AA55AA55AA55 3434343434343434
Key Block Header (KBH):	A0072K0TD00N0000 (ASCII)
TDES CBC encrypted key value:	7D2D21FC9ECD3EEC BB0A2615BD8F0560 5722120BDFF2CCAC
Left 4 bytes of MAC value:	319C3198
The Key ID you want to load:	‘F’
The resulting 02 (30h 32h) message:	<SI>02FA0072K0TD00N00007D2D21FC9ECD3EECBB0A2615BD8F056 05722120BDFF2CCAC319C3918 <SO>[LRC]

Encrypted (ANSI TR-31 2010 Key Derivation Binding Method)

Key condition:	Load a double length key encryption key to key position ‘F’
Key block protection key (KBPK) (i.e. key loading key loaded in MCH100 with Key ID	1919191919191919 5B5B5B5B5B5B5B5B

'F'):	
Master key (i.e. key loading key) to be loaded:	AA55AA55AA55AA55 3434343434343434
Padded key data:	0080 AA55AA55AA55AA55 3434343434343434 1C2965473CE2
Key Block Header (KBH):	B0080P0TE00N0000 (ASCII)
Derived Key block encryption key (KBEK):	DB7F2A99D5647A7D D3EDFE3DA7CF5B21
Derived Key block MAC key (KBMK):	87EE6C0795954446 A34A0BB5F305BCE1 (See **Appendix C** for details of deriving process)
CMAC of (KBH + Padded key data), using KBMK:	EA391E5834C1AA0C (See **Appendix C** for details of CMAC algorithm)
Use CMAC as IV to do TDES CBC encryption on padded key data, using KBEK:	
Encrypted key data:	3C4F5024C59C182F 7165BC870FCB7F63 456AAE07DB736C32
The resulting 02 message:	<SI>02FB0080P0TE00N0000 3C4F5024C59C182F 7165BC870FCB7F63 456AAE07DB736C32 EA391E5834C1AA0C<SO>[LRC]

7.5.2 39h 30h - Load Initial Key Request

Format: <STX> 90[TR-31 Key Block]<ETX>[LRC]

Message length: 93 or 109 bytes for TR-31 format.

Usage: Load DUKPT initial key and serial number key, encrypted in ANSI TR-31 or Clear Text mode, to MCH100 Reader.

Note:

VISA required key serial number format are as follows:

4'F' characters, a 6-digit keyset identifier, 5-digit device ID, followed by a '0',

i.e. "FF FF kk kk kk dd dd d0 00 00"

ANSI TR-31

Field	Length	Value and description
<STX>	1	<02>
90	2	Message ID
[TR-31 Key Block]	88 or 104	TR-31 key block with optional header block that contains KSN. See **Appendix C** for details.
<ETX>	1	<03>
[LRC]	1	Checksum

Clear Text

Field	Length	Value and description
<STX>	1	<02>

Field	Length	Value and description
90	2	Message ID
[IPEK]	16 or 32	Initial PIN encryption key. (i.e. load DUKPT initial key) 32-characters Initial key will make MCH100 act in TDES DUKPT mode. Format: hexadecimal string.
[KSN]	20	Key serial number used in generating consequent keys. Format: hexadecimal string.
<ETX>	1	<03>
[LRC]	1	Checksum

Message flow:

HOST	Direction	MCH100 Reader
Message 90	→	
	←	<ACK> (Good LRC) <NAK> (Bad LRC) (<EOT> after 3 NAKs)
	←	Message 91
<ACK>/<NAK>/<EOT>	→	

Example:

TR-31 Key Block

Key Block Protecting Key (i.e. key loading key loaded in MCH100 with Key ID 'F'):	AA55AA55AA55AA55 3434343434343434
IPEK key to be loaded:	ABCDEF0123456789 FEDCBA9876543210
KSN:	FFFF9876543210E00000
Key Block Header:	B0104B1TX00N0100 KS18FFFF9876543210E00000
Padded IPEK:	0080 ABCDEF0123456789 FEDCBA9876543210 30111D18CC4C
Derived KBEK:	3C50E1B7962F2171DC8643F1D923ABF7
Derived KBMK:	46FBEEB64EAE26A650952DA4F6DD8325
CMAC of (KBH + Padded key data), using KBMK:	93C3D5EBC6C407E4
Use CMAC as IV to do TDES CBC encryption on padded key data, using KBEK:	
Encrypted key data:	EC86E6E3B24544F97C629FB0E0586A0285D35BA78E9B13FB
Result:	<STX>90B0104B1TX00N0100KS18FFFF9876543210E00000EC86E6E3B24544F97C629FB0E0586A0285D35BA78E9B13FB93C3D5EBC6C407E4<ETX>[LRC]

7.5.3 39h 31h - Load Initial Key Response

Format: <STX>91[Status]<ETX>[LRC]

Message length: Variable (max 7 bytes.)

Usage: Confirmation of the initial key loading.

Message element:

Field	Length	Value and description
<STX>	1	<02>
91	2	Message ID
[Status]	1..2	'0' if successful '1' + [Error Code] if process failed.
<ETX>	1	<03>
[LRC]	1	Checksum

Message flow: Please refer to command 39h 30h.

Error codes:

Code	Meaning
'3'	Internal fail: fail to allocate memory
'4'	Internal fail: fail to read key structure
'7'	Fail to decrypt key value.
'A'	TR-31 format error.
'C'	Fail to verify MAC value

7.5.4 30h 35h - Load Serial Number

Format: **<SI>05[string]<SO>[LRC]**

Message length: Variable, maximum length is 21 bytes.

Usage: Load the device with the serial number given in the message frame. Device will send the whole message frame back to host as a confirmation of good reception. Host should then send an <ACK> to confirm or <EOT> to cancel this serial number loading process if the LRC is good but serial number echoed is incorrect. Follow the standard <NAK> process if an invalid LRC is detected.

Message element:

Field	Length	Value and description
<SI>	1	<0F>
05	2	Message ID

[string]	0..16	Alphanumeric string (0~9, A~Z, a~z)
<SO>	1	<0E>
[LRC]	1	Checksum

Message flow:

HOST	Direction	Device
Message 05	→	
	←	<ACK> (Good LRC) <NAK> (Bad LRC) (<EOT> after 3 NAKs)
	←	Message 05 (echo frame) or <EOT> indicate error.
<ACK> (Good echo) <NAK> (Bad LRC) (<EOT> after 3 NAKs)	→	
	←	(Stores serial number) <EOT>

7.5.5 30h 36h - Get Serial Number

Format: **<SI>06<SO>[LRC] <SI>06[string]<SO>[LRC]**

Message length: Fixed 5 bytes for requesting message, variable for response message (max 21 bytes.)

Usage: This message is used to get serial number of the device. Device will send the serial number previously loaded or string of 16 ‘0’s as the serial number.

Message element:

Request frame (Host to Device)

Field	Length	Value and description
<SI>	1	<0F>
06	2	Message ID
<SO>	1	<0E>
[LRC]	1	Checksum

Response frame (Device to HOST)

Field	Length	Value and description
<SI>	1	<0F>
06	2	Message ID
[string]	0..16	String for serial number
<SO>	1	<0E>

[LRC]	1	Checksum

Message flow:

HOST	Direction	Reader
Message 06 (request)	→	
	←	<ACK> (Good LRC) <NAK> (Bad LRC) (<EOT> after 3 NAKs)
	←	Message 06 (response frame) or <EOT> if read error
<ACK> (Good echo) <NAK> (Bad LRC) (<EOT> after 3 NAKs)	→	
	←	<EOT>

7.5.6 37h 36h - PIN Entry Test Request

Format: **<STX>76[account]<FS>[DC Ind][amount]<ETX>[LRC]**

Message length: Variable 19 to 34 bytes.

Usage: This command is designed to do DUKPT key iteration test. The reader will return 71 (37h 31h) assuming a PIN of '1234' and pack the data in ANSI X9.8 PIN block format. This command can be used to verify the key being loaded properly or not.

Message element:

Field	Length	Value and description
<STX>	1	<02>
76	2	Message ID
[Account]	8..19	Primary account number
<FS>	1	<1C>, field separator
[DC Ind]	1	D/C: Debit/Credit Indicator
[Amount]	4..8	Amount of goods
<ETX>	1	<03>
[LRC]	1	Checksum

Message flow:

HOST	Direction	Reader
Message 76	→	
	←	<ACK> (Good LRC) <NAK> (Bad LRC) (<EOT> after 3 NAKs)
	←	Message 71 or <EOT>

<ACK> (Good LRC) <NAK> (Bad LRC) (<EOT> after 3 NAKs)	→	

NOTE

- Command (37h 36h) can be used to do DUKPT one million testing.
- When all DUKPT keys have been used, the LED will turn red to indicate MCH100 is not useful. When MCH100 is at above state, the execution of key injection can relive MCH100.

7.5.7 37h 31h - Encrypted PIN Block Response

Format: **<STX>71<fkey flag>[Key Serial#][PIN][LRC] (PIN block frame)**

<STX>71[error code]<ETX>[LRC] (Error code frame)

Message length: Variable 32 to 42 bytes.

Usage: The response to command (37h 36h). The encrypted PIN block will be sent out for HOST to verify if the key is loaded properly or not.

Message element:

Field	Length	Value and description
<STX>	1	<02>
71	2	Message ID
[fkey flag]	1	Always '0' (This field is kept to retain old model compatibility.)
[Key Serial#]	10..20	Key Serial number used in encrypting PIN. Included only when PIN is entered. Format: hexadecimal string.
[PIN]	16	Encrypted PIN block Format: hexadecimal string.
<ETX>	1	<03>
[LRC]	1	Checksum

Error codes:

Code	Meaning
'0'	Null Account input field.
'2'	Account number shorter than 8 digits.
'3'	Account number longer than 19 digits.
'4'	Account number have character other than '0'-'9'.
'5'	[D/C ind] field not exist or format error.
'6'	Timeout value error.
'8'	Amount string format error.
'A'	No DUKPT key injected.
'B'	Flash read/write error.
'C'	Memory buffer allocation error.

‘F’	DUKPT operation limit (1 million) reached, program stop.

7.5.8 93h - Get DUKPT Serial Number/Counter and Encrypted Random Number

This command is used to get DUKPT serial number, counter and encrypted random number.

Response Parameters:

First 10 bytes, DUKPT serial number and counter

Last 8 bytes, Encrypted random number

EXAMPLE

Host request	Reader response
C2 00 01 93	
	C2 00 12
	55 49 43 30 30 30 31 00 00 04 (DUKPT serial number and counter)
	E3 7A 26 F4 5E 36 11 E6 (Encrypted random number)

7.6 Administration Commands

The administration commands can be protected or not. The default state of the administration commands is not protected. Please refer to **Appendix A** for more details.

7.6.1 A5h - Set Administration Commands Protection Status

This command is used to set the administration commands are protected or not.

Data Field:

‘00h’: Sets Administration Commands are not protected

‘01h’: Sets Administration Commands are protected

EXAMPLE

Host request	Reader response
C2 00 02 A5 01	
	C2 00 01 06

7.6.2 62h - Set Device Interface

This command is used to set the interface type of MCH100.

Data Field:

‘00h’: HID Keyboard

‘01h’: HID MSR

‘02h’: Virtual COM

EXAMPLE

Host request	Reader response
C2 00 02 62 01	
	C2 00 01 06

7.6.3 96h - Set Session ID

This command is used to load 8 bytes Session ID to MCH100.

EXAMPLE

Host request	Reader response
C2 00 09 96 31 32 33 34 35 36 37 38	
	C2 00 01 06

7.6.4 45h - Set Properties in the Device

This command is used to change the properties in non-volatile memory.

(See next section for device properties description).

Parameters:

AddrM: 1 byte, MS nibble of write address

AddrL: 1 byte, LS nibble of write address

LenM: 1 byte, MS nibble of write data length

LenL: 1 byte, LS nibble of write data length

Data: Max 512 bytes.

EXAMPLE

Host request	Reader response
C2 02 01 45 AddrM AddrL LenM LenL memory value (max 512 bytes)	
	C2 00 01 06

7.6.5 52h - Get Properties in the Device

This command is used to get the properties in non-volatile memory.

(See next section for Device Properties description).

Parameters:

AddrM: 1 byte, MS nibble of read address

AddrL: 1 byte, LS nibble of read address

LenM: 1 byte, MS nibble of read data length

LenL: 1 byte, LS nibble of read data length. (Max 512 bytes)

EXAMPLE

Host request	Reader response

C2 00 01 52 00 00 00 08	
	C2 00 08 00 01 08 87 88 39 00 00

7.6.6 44h 30h- Set Properties in Default for Current Interface

This command is used to set the device properties in default for current interface.

(See next section for Device Properties description).

EXAMPLE

Host request	Reader response
C2 00 02 44 30	
	C2 00 01 06

7.6.7 44h 41h - Set Properties in Default for All Interface

This command is used to set the device properties in default for all interface.

(See next section for Device Properties description).

EXAMPLE

Host request	Reader response
C2 00 02 44 41	
	C2 00 01 06

8 Memory Map of the Device Properties

This section provides the memory map of the device properties.

Bytes 1 ~ 150: HID Keyboard interface

Bytes 151 ~ 300: HID MSR interface

Bytes 301 ~ 450: Virtual COM interface

Bytes 451 ~ 511: Common

8.1 Summary

BYTE	DESCRIPTION	DEFAULT(hex)
0	Reader Mode	02
HID KEYBOARD		
1	Polling Interval	01
2	Max Packet Size	08
3	MSR Basic Editing	8F
4	MSR Advanced Editing(1)	A8
5	MSR Advanced Editing(2)	39
6	Keyboard language	00
7~18	Track1 prefix	
19~30	Track2 prefix	
31~42	Track3 prefix	
43~54	Track1 suffix	
55~66	Track2 suffix	
67~78	Track3 suffix	
79~96	Preamble	
97~114	Postamble	
115~116	Read error indicator*	
117~118	TK1 SS for ISO	
119~120	TK1 SS for AAMVA	
121~122	TK1 SS for DMV	
123~124	TK1 SS for Tradeshow	
125~126	Reserved	

BYTE	DESCRIPTION	DEFAULT(hex)
127~128	TK2 SS for ISO	
129~130	TK2 SS for AAMVA	
131~132	TK2 SS for DMV	
133~134	TK2 SS for Tradeshow	
135~136	TK3 SS for ISO	
137~138	TK3 SS for AAMVA	
139~140	TK3 SS for DMV	
141~142	TK3 SS for Tradeshow	
143~144	ES for all track	
145~150	Reserved	
HID MSR		
151	Polling Interval	01
152	Max Packet Size	08
153	MSR Basic Editing	0F
154	MSR Advanced Editing(1)	A0
155	MSR Advanced Editing(2)	39
156	Read error indicator*	
157	TK1 SS for ISO	
158	TK1 SS for AAMVA	
159	TK1 SS for DMV	
160	TK1 SS for Tradeshow	
161	Reserved	
162	TK2 SS for IOS	
163	TK2 SS for AAMVA	
164	TK2 SS for DMV	
165	TK2 SS for Tradeshow	
166	TK3 SS for ISO	
167	TK3 SS for AAMVA	
168	TK3 SS for DMV	
169	TK3 SS for Tradeshow	
170	ES for all track	

BYTE	DESCRIPTION	DEFAULT(hex)
171~300	Reserved	
Virtual COM		
301	Polling Interval	01
302	Max Packet Size	08
303	MSR Basic Editing	8F
304	MSR Advanced Editing(1)	A8
305	MSR Advanced Editing(2)	39
306~311	Track1 prefix	
312~317	Track2 prefix	
318~323	Track3 prefix	
324~329	Track1 suffix	
330~335	Track2 suffix	
336~341	Track3 suffix	
342~350	Preamble	
351~359	Postamble	
360	Read error indicator*	
361	TK1 SS for ISO	
362	TK1 SS for AAMVA	
363	TK1 SS for DMV	
364	TK1 SS for Tradeshow	
365	Reserved	
366	TK2 SS for ISO	
367	TK2 SS for AAMVA	
368	TK2 SS for DMV	
369	TK2 SS for Tradeshow	
370	TK3 SS for ISO	
371	TK3 SS for AAMVA	
372	TK3 SS for DMV	
373	TK3 SS for Tradeshow	
374	ES for all track	

BYTE	DESCRIPTION	DEFAULT(hex)
375~450	Reserved	
Common Properties		
451~474	Reserved	
475	Reserved	01
476	Reserved	04
477	Reserved	04
478	Reserved	30
479	Reserved	
480~495	Reader Serial Number	
496	Reserved	
497	Reserved	10
498~499	Reserved	
500~503	Check Sum	
504~508	Reserved	
509~511	Check Data	'213'

** The "Error Indicator"-related features are Not implemented yet!*

8.2 Data Description

8.2.1 Reader Mode

Byte 0

Value	Set Reader Mode
00h	HID Keyboard
01h	HID MSR
02h	Virtual COM
Note Any value other than 00h, 01h or 02h will reset all MEMORY to default.	

8.2.2 HID Keyboard

Byte 1

Interval for polling, this value must be in the range from 0 to 255(milliseconds).

Byte 2

Maximum packet size (read-only)

Byte 3

	7	6	5	4	3	2	1	0	Meaning	Default
Enable Track								0/1	Tk1 1:enable 0:disable	1
							0/1		Tk2 1:enable 0:disable	1
						0/1			Tk3 1:enable 0:disable	1
RFU					0					0
RFU				0						0
RFU			0							0
Send SS/ES		0/1							1:no send 0:send	0
Caps Lock	0/1								1:On 0:Off	1

Byte 4

	7	6	5	4	3	2	1	0	Meaning	Default
Required Track								0/1	Tk1 1:enable 0:disable	1
							0/1		Tk2 1:enable 0:disable	1
						0/1			Tk3 1:enable 0:disable	1
Default CR				0/1	0/1				00: No CR 01: Enter 10: (Number) Enter	01
RFU			0/1							00
		0/1								
Beep	0/1								Buzzer 1:enable 0:disable	1

Byte 5

	7	6	5	4	3	2	1	0	Meaning	Default
Track Output Order: First output								0/1	00:no send 01:TK1 10:TK2 11:TK3	01
							0/1			
Track Output Order: Second output						0/1			00:no send 01:TK1 10:TK2 11:TK3	10
					0/1					
Track Output Order: Third output				0/1					00:no send 01:TK1 10:TK2 11:TK3	11
			0/1							

	7	6	5	4	3	2	1	0	Meaning	Default
Error Indicator		0/1							0:no send 1:send	0
RFU	0									0

Byte 6

Value	Keyboard Country
00h	US
01h	German
02h	French
03h	UK English
04h	Spanish
05h	Italy
06h	Dutch
07h	Portuguese
08h	Swedish
09h	Danish

Bytes 7~18 (2*6) MXA 6 char 00 is DISABLE default 00

Tk1 prefix

Bytes 19~30 (2*6) MXA 6 char 00 is DISABLE default 00

Tk2 prefix

Bytes 31~42 (2*6) MXA 6 char 00 is DISABLE default 00

Tk3 prefix

Bytes 43~54 (2*6) MXA 6 char 00 is DISABLE default 00

Tk1 suffix

Bytes 55~66 (2*6) MXA 6 char 00 is DISABLE default 00

Tk2 suffix

Bytes 67~78 (2*6) MXA 6 char 00 is DISABLE default 00

Tk3 suffix

Bytes 79~96 (2*9) MXA 6 char 00 is DISABLE default 00

Preamble

Bytes 97~114 (2*9) MXA 9 char 00 is DISABLE default 00

Postamble

Bytes 115~116(2*1) default 00

Send ERROR code

Bytes 117~118(2*1) default 00
Chang TK1 SS for ISO

Bytes 119~120(2*1) default 00
Chang TK1 SS for AAMVA

Bytes 121~122(2*1) default 00
Chang TK1 SS for DMV

Bytes 123~124(2*1) default 00
Chang TK1 SS for Tradeshow

Bytes 127~128(2*1) 00
Chang TK2 SS for ISO

Bytes 129~130(2*1) 00
Chang TK2 SS for AAMVA

Bytes 131~132(2*1)
Chang TK2 SS for DMV

Bytes 133~134(2*1)
Chang TK2 SS for Tradeshow

Bytes 135~136(2*1)
Chang TK3 SS for ISO

Bytes 137~138(2*1)
Chang TK3 SS for AAMVA

Bytes 139~140(2*1)
Chang TK3 SS for DMV

Bytes 141~142(2*1)
Chang TK3 SS for Tradeshow

Bytes 143~144(2*1)
Chang all ES for reader

8.2.3 HID MSR

Byte 151
Interval for polling, this value must be in the range from 0 to 255(milliseconds).

Byte 152
Specify the maximum packet size (bytes), 1~64.

Byte 153

	7	6	5	4	3	2	1	0	Meaning	Default
Enable Track								0/1	Tk1 1:enable 0:disable	1
							0/1		Tk2 1:enable 0:disable	1
						0/1			Tk3 1:enable 0:disable	1
RFU					0/1					1
RFU				0						0
RFU			0							0
Send SS/ES		0/1							1:no send 0:send	0
RFU	0									0

Byte 154

	7	6	5	4	3	2	1	0	Meaning	Default
Required Track								0/1	Tk1 1:enable 0:disable	0
							0/1		Tk2 1:enable 0:disable	0
						0/1			Tk3 1:enable 0:disable	0
RFU					0					0
RFU				0						0
RFU			0/1							01
		0/1								
Beep	0/1								Buzzer 1:enable 0:disable	1

Byte 155

	7	6	5	4	3	2	1	0	Meaning	Default
Track Output Order: First output								0/1	00:no send 01:TK1 10:TK2 11:TK3	01
							0/1			
Track Output Order: Second output						0/1			00:no send 01:TK1 10:TK2 11:TK3	10
					0/1					
Track Output Order: Third output				0/1					00:no send 01:TK1 10:TK2 11:TK3	11
			0/1							
Error indicator		0/1							0:no send 1:send	0
RFU	0									0

Byte 156

Replace the default Error indicator (‘E’, 45h) with specified character.

Note: 00h means default value is used.

Bytes 157 default 00

Chang TK1 SS for ISO

Bytes 158 default 00

Chang TK1 SS for AAMVA

Bytes 159 default 00

Chang TK1 SS for DMV

Bytes 160 default 00

Chang TK1 SS for Tradeshow

Bytes 162 default 00

Chang TK2 SS for ISO

Bytes 163 default 00

Chang TK2 SS for AAMVA

Bytes 164 default 00

Chang TK2 SS for DMV

Bytes 165 default 00

Chang TK2 SS for Tradeshow

Bytes 166 default 00

Chang TK3 SS for ISO

Bytes 167 default 00

Chang TK3 SS for AAMVA

Bytes 168 default 00

Chang TK3 SS for DMV

Bytes 169 default 00

Chang TK3 SS for Tradeshow

Bytes 170 default 00

Chang all ES for reader

8.2.4 Virtual COM

Byte 301

Interval for polling, this value must be in the range from 0 to 255(milliseconds).

Byte 302

Maximum packet size (read-only).

Byte 303

	7	6	5	4	3	2	1	0	Meaning	Default
Enable Track								0/1	Tk1 1:enable 0:disable	1
							0/1		Tk2 1:enable 0:disable	1
						0/1			Tk3 1:enable 0:disable	1
RFU					0					0
RFU				0						0
RFU			0							0
Send SS/ES		0/1							1:no send 0:send	0
RFU	0									0

Byte 304

	7	6	5	4	3	2	1	0	Meaning	Default
Required Track								0/1	Tk1 1:enable 0:disable	0
							0/1		Tk2 1:enable 0:disable	0
						0/1			Tk3 1:enable 0:disable	0
RFU					0					0
RFU				0						0
RFU			0/1							01
		0/1								
Beep	0/1								Buzzer 1:enable 0:disable	1

Byte 305

	7	6	5	4	3	2	1	0	Meaning	Default
Track Output Order: First output								0/1	00:no send 01:TK1 10:TK2 11:TK3	01
							0/1			
Track Output Order: Second output						0/1			00:no send 01:TK1 10:TK2 11:TK3	10
					0/1					

Track Output Order: Third output				0/1					00:no send 01:TK1 10:TK2 11:TK3	11
			0/1							
Error indicator		0/1							0:no send 1:send	0
RFU	0									0

Bytes 306~311

Set TK1 prefix, 6 chars max. Note: 00h means disable.

Bytes 312~317

Set TK2 prefix, 6 chars max. Note: 00h means disable.

Bytes 318~323

Set TK3 prefix, 6 chars max. Note: 00h means disable.

Bytes 324~329

Set TK1 suffix, 6 chars max. Note: 00h means disable.

Bytes 330~335

Set TK2 suffix, 6 chars max. Note: 00h means disable.

Bytes 336~341

Set TK3 suffix, 6 chars max. Note: 00h means disable.

Bytes 342~350

Set Preamble, 9 chars max. Note: 00h means disable.

Bytes 351~359

Set Postamble, 9 chars max. Note: 00h means disable.

Byte 360

Replace the default Error indicator (‘E’, 45h) with specified character.

Note: 00h means default value is used.

Bytes 361 default 00

Chang TK1 SS for ISO

Bytes 362 default 00

Chang TK1 SS for AAMVA

Bytes 363 default 00

Chang TK1 SS for DMV

Bytes 364 default 00

Chang TK1 SS for Tradeshow

Bytes 366 default 00

Chang TK2 SS for ISO

Bytes 367 default 00

Chang TK2 SS for AAMVA

Bytes 368 default 00

Chang TK2 SS for DMV

Bytes 369 default 00

Chang TK2 SS for Tradeshow

Bytes 370 default 00

Chang TK3 SS for ISO

Bytes 371 default 00

Chang TK3 SS for AAMVA

Bytes 372 default 00

Chang TK3 SS for DMV

Bytes 373 default 00

Chang TK3 SS for Tradeshow

Bytes 374 default 00

Chang all ES for reader

8.2.5 Common Properties

Bytes 480~495

The reader serial number, up to 16 characters.

Bytes 500~503

It is computed automatically from the device for the purpose of detecting accidental errors.
It could not be changed by the application program.

Bytes 509~511

It is used to identify MCH100.
It could not be changed by the application program.

APPENDIX A. Guide on Administration Commands

Operation

The application program can use command (A6h) to query and use command (A5h) to enable or disable the encryption of administration command parameters. The administration commands must be authenticated as the following steps if they are protected.

(1) The application program needs to send command (93h) to the reader first.
(2) The reader responds with key serial number, counter and encrypted random number.
(3) The application program uses the current DUKPT key to decrypt random number.
(4) The application program XOR the current DUKPT key and clear text random number to make a new key
(5) The application program uses the new key to encrypt transmitting data. The transmitting data consists of clear text random number and command parameters.
(6) The application program sends the administration command with encrypted data.

Example:

The host wants to send command (96h) [Set Session ID = “3132333435363738”] to the reader.
DUKPT Initial Key is “554E49464F524D5F44454641554C5421”.

	The host sends command (93h) “C2000193” to the reader	→
←	The reader replies with key serial number counter and encrypted random number. “55494330303031000004 E37A26F45E3611E6”.	
	“55494330303031000004” is the Serial number/counter. “E37A26F45E3611E6” is the encrypted random number. The host uses the initial key and serial number/counter to find out the current key ”DFD0A84FD0E3CA06964748FE8339A296”.	
	The host uses the current key to decrypt the encrypted random number. The host finds out the clear text random number is “6580D888115B37FE”.	
	The host XOR the current key and clear text random number to make a new key. ”DFD0A84FD0E3CA06964748FE8339A296” (The current key) XOR “6580D888115B37FE6580D888115B37FE” (The extended clear text random number) is “BA5070C7C1B8FDF8F3C7907692629568” (The new key)	
	The host uses the new key to encrypt transmitting data. Transmitting data = ”clear text random number + command parameters”. “6580D888115B37FE 3132333435363738”	
	“69A97590611D6EE5177B312015F4F615” (Encrypted Transmitting Data)	
	The host sends the command with encrypted transmitting data to the reader. “C200119669A97590611D6EE5177B312015F4F615”	→
←	The reader replies “C2000106”.	

APPENDIX B. DATA Encryption

Example of Decrypting Track Data TDES (CBC)

DUKPT Initial Key is “554E49464F524D5F44454641554C5421”.

The swiped card data is:

|00|033A4A6F4B13971164C7DB2413E57DC51979F73207A1AAE764686EAE174322B0D50ADCDFD7C1BED276F155139E65C76B3ED53939262901C062283FC8FC560805|7A616C88699EEABD89DE6EF52E3F042422ED12010E24F047F1D6053B7826CF87DDD45F5C05A3974F|ADA9EE86C2AD7B848A7E3F95808BDF61D6780B0FF8F1B67833A2B598A784C24CE9DBE54F3476C31D46E05B355CD480123F1215702B1D71529234226540ECC9471A28C6DCEA8EDEA6E044302F6AD9DE62F643CCEF3A31605BCBC75422C2A13CC6C18A998CA088A7DFEF921DBD791ABB23|55494330303031000002|54E755672E52C69C|30303030303030303030303030303030|10|C74B737FC4169674A859808E6350DA1343DFF7E52AC3687CDC20A9D9B7208C1A|

(1) Track 1 Encrypted data is

“033A4A6F4B13971164C7DB2413E57DC51979F73207A1AAE764686EAE174322B0D50ADCDFD7C1BED276F155139E65C76B3ED53939262901C062283FC8FC560805”

Track2 Encrypted data is

“7A616C88699EEABD89DE6EF52E3F042422ED12010E24F047F1D6053B7826CF87DDD45F5C05A3974F”

Track3 Encrypted data is

“ADA9EE86C2AD7B848A7E3F95808BDF61D6780B0FF8F1B67833A2B598A784C24CE9DBE54F3476C31D46E05B355CD480123F1215702B1D71529234226540ECC9471A28C6DCEA8EDEA6E044302F6AD9DE62F643CCEF3A31605BCBC75422C2A13CC6C18A998CA088A7DFEF921DBD791ABB23”

(2) DUKPT Serial Number/Counter is

“55494330303031000002”

(3) The host uses the initial key and serial number/counter to find out the current key, so the current key is “1ECCDC3E051E854DDC3D693CD08FC004”.

(4) The host uses the new key to decrypt Track1 Encrypted Data.

“254238303836323332393131393637 5E56455249464F4E4520494E432F4451205445535443415244202 05E39393132303130373633353032323633303 43FFFFF”

(5) The decrypted data is hexadecimal string. Represent it in ASCII string.

“%B8086232911967^VERIFONE INC/DQ TESTCARD ^991201076350226304?”

(6) The host uses the new key to decrypt Track2 Encrypted Data.

“3B383038363233323931313936373D393931323031303736333530323236333034 3FFFFFFFFFFFF”

(7) The decrypted data is hexadecimal string. Represent it in ASCII string.

“;8086232911967=9912010763502263 04?”

(8) The host uses the new key to decrypt Track3 Encrypted Data.

“3B303138303836323332393131393637 3D393939303031383039303030313030383031303939383633303430303939383132333435363738393031323334353637383930313233343536373839303132333435363738393031323334353637383930313233343536373839303132333435363FFFFFFFFFFFFFF”

(9) The decrypted data is hexadecimal string. Represent it in ASCII string.

“;018086232911967=99900180900010080109986304009981234567890123456789012345678901234567890123456789012345678901234567890123456?”

APPENDIX C. Symmetric Key Management

The symmetric key (TDES) in MCH100 reader is used to encrypt MSR track data.

MCH100 can store and use one key loading key (16 bytes) and one set of double length (16 bytes) DUKPT key.
To load or update symmetric keys, host should encrypt and authenticate key data according to ANSI TR-31 standard, then send to MCH100 via command 02 (30h 32h) or 90 (39h 30h).

MCH100 support versions 2010 and 2005 of ANSI TR-31 Key Block. The following explanation take version 2010 as an example.

Symmetric key management schemes supported by MCH100

Key loading key:

Following table shows the available key ID and usage of key loading key on MCH100:

Key ID	Length	Usage	Algorithm	Mode	Remark
F	16	K0	T	D	Key Block Protect Key (Ref. ANSI TR-31)

The “usage”, “algorithm”, and “mode” are defined in ANSI TR-31 specification as key attributes. Refer to next section – “Detail for composing ANSI TR-31 key blocks”.

Derived Unique Key Per Transaction (DUKPT):

Following table shows the available key ID and usage of DUKPT keys on MCH100:

Set ID	Length	Usage	Algorithm	Mode	Remark
0	16	B1	T	X	Derive keys for MSR track encryption.

MCH100 implements ANSI X9.24 (ver. 2009) DUKPT algorithm and is able to use the derived key to encrypt MSR track data. Each successful card swipe, in which the payment card data pass the Luhn check (also known as mod 10 check), causes MCH100 derive new key along with unique serial number to encrypt data. For non-payment card, which are unable to pass Luhn check, the card data won’t be encrypted.
According to ANSI X9.24 specification, a key set can provide about 1 million (2^{20}) unique keys before stopping operation. Reaching operation limit will cause MCH100 to stop DUKPT related operation.

Note:
MCH100 encrypts MSR data in DUKPT method and uses **CBC mode** to encrypt each track.

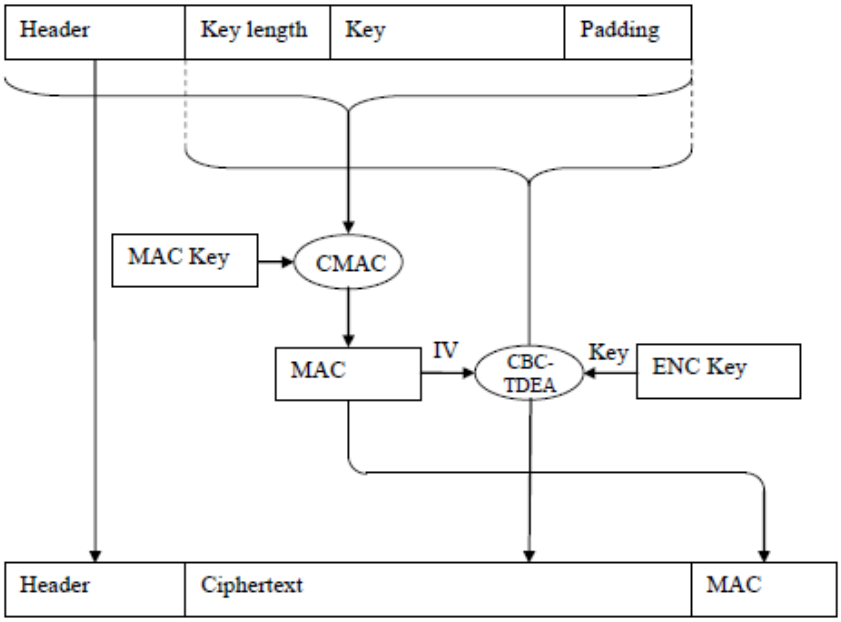
Detail for composing ANSI TR-31 key blocks

ANSI TR-31 key block contains three components:

Component	Description
Key block header (KBH)	Contains attribute information about the key and the key block.

Confidential data	Encrypted key value to be exchanged.
Message authenticate code (MAC)	The authenticate code covered whole clear text data (KBH + Key data) with NIST SP 800-38B CMAC algorithm.

The following graph (from TR-31-2010 chapter 5.3.2.1.) shows the general flow of data binding and encrypting:



Message components of the KBH:

Field	Length	Value and description for attributes supported by MCH100
Version ID	1	'A': TR-31-2005 Key Variant Binding Method 'B': TR-31-2010 Key Derivation Binding Method 'C': TR-31-2010 Key Variant Binding Method
Key block length	4	ASCII numeric digits providing key block length after encoding. i.e. "0112" means the whole key block contains 112 bytes.
Key usage	2	Provides information about the intended function of the protected key. "K0", indicates that this key is used for key transportation. "B1", indicates that this key is used for DUKPT initial key.
Algorithm	1	The approved algorithm for which the protected key may be used. 'T': TDES algorithm (double or triple length key)
Mode of use	1	Defines the operation the protected key can perform. 'D': Decryption 'X': Key derivation (DUKPT)
Key version num	2	Two-digit ASCII character version number. i.e. "00" to "99".
Exportability	1	Defines whether the protected key may be transferred outside the cryptographic domain. Always 'N' on MCH100.

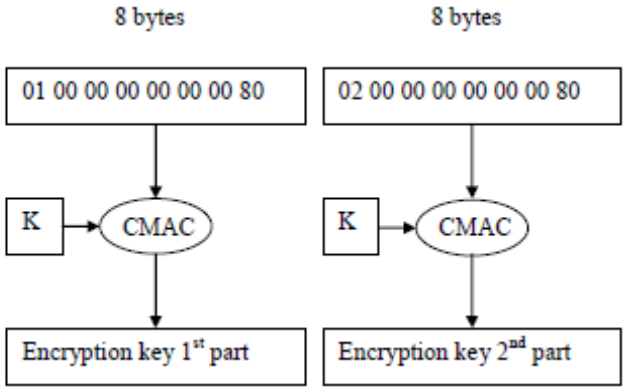
Field	Length	Value and description for attributes supported by MCH100
Number of Optional Blocks	2	ASCII numeric digits defines the number of Optional Blocks included in the key block. “00”: No optional block (for key loading key). “01”: One optional block (for DUKPT initial key serial number).
Reserved	2	Always “00” on MCH100.
Opt. block ID	2	(Optional) Identifier of optional block. “KS”: for DUKPT key serial number.
Opt. block len	2	(Optional) Hexadecimal string defines length of optional block. “18”: 24 (0x18) bytes for DUKPT key serial number. (incl. ID and len field).
Opt. block data	20	(Optional) Hexadecimal string of DUKPT key serial number, always 20 bytes. i.e. “FFFF9876543210E00000”.

Derive "MAC key" and "ENC key" from KBPK:

MCH100 uses the master key in slot 'F' as KBPK in TR-31 algorithm to derive two keys to be used in MAC calculation and data encryption. Refer to following figure (from TR-31-2010 chapter 5.3.2.1.)

Derive double length (16 bytes) ENC key

The "K" means KBPK (i.e. Key loading key in MCH100).



Derive double length (16 bytes) MAC key

The "K" means KBPK (i.e. Key loading key in MCH100).