Trans Infotech Vietnam Ltd.

TRANS INFOTECH POS SWITCH SYSTEM

ISO Message Specification Document

Version 1.0

Revision History

Date	Version	Description	Author
21 January 2011	1.0	Message Specification Document 1.0	Ho Minh Hiep

Table of Contents

Message Specification Document

1. INTRODUCTION

1.1 Purpose

This document specifies the message structure and data elements, and their values, required for an effective interface for transaction messages between card accepting POS (Point Of Service) and TI-PSS.

1.2 Scope

This message specification document is only used for TI-PSS. This document is built based on International Organization For Standardization's International Standard ISO 8583 - Bank Card Originated Messages - Interchange Message Specifications - Content For Financial Transactions.

1.3 Definitions, Acronyms, and Abbreviations

The following table provides the definitions of all terms, acronyms, and abbreviations used in this document.

Abbreviations	Description
TI-PSS	Trans Infotech POS Switch System

1.4 References

This document is built based on the requirement and background details in the following documents:

Document name	File Name	Notes

1.5 Overview

This document includes the message format of all transactions that POS should send to TI-PSS.

2. MESSAGE SPECIFICATION

2.1 Overview

TI-PSS uses an implementation of the International Organization For Standardization's International Standard ISO 8583 - Bank Card Organization Message - Interchange Message Specifications - Content For Financial.

ISO 8583 uses a concept called Bit map", where each data element is assigned a position indicator in a control field, or bit map. The presence of a data element in a specific message is indicated by a one (1) in the assigned position; The absence of a data element is indicated by a zero (0) in the assigned position.

2.2 Message Structure

The structure of a terminal / host message is:

	Message Length	TPDU	Application data variable to Max.
Size	2	5	240

- **Message Length** - It is the length of data (including TPDU)
- **TPDU** - Transport Protocol Data Unit

2.2.1 Transport Protocol Data Unit (TPDU)

The TPDU contains addressing information related to both the transaction destination and the transaction origination device. The TPDU is a 5-byte header that precedes the application data:

+ Request Message TPDU

TPDU	DESTINATION ADDRESS	ORIGINATION ADDRESS
1	2	2

- TPDU: Identifier TPDU
- DESTINATION ADDRESS: Network International Identifier
- ORIGINATION ADDRESS: Identifier the individual terminal or process originating the transaction.

+ Response Message TPDU

TPDU	DESTINATION ADDRESS	ORIGINATION ADDRESS
1	2	2

- TPDU: Identifier TPDU - Same value as in the request message
- DESTINATION ADDRESS: Network International Identifier
- ORIGINATION ADDRESS: Identifier the individual terminal or process originating the transaction.

2.3 Message Length

2 bytes BCD, as indicated in the message structure above, the maximum data content of a message is 240 bytes.

2.4 Application Data Structure

Each application message consists of three components in the following sequence.

- MESSAGE TYPE - 2 bytes.
- BIT MAP - 8 bytes
- A variable number of Data Element

2.4.1 Bit map

The second component is one (10) Bit Map of 64 bits (8 bytes) numbered from the left starting with '1'

Each bit in the bit map signifies the presence-on (1) or absence-off (0) in the message of the message the Data Element associated with that particular bit.

Bit Values 0,1,0*******0,1	Data Element
1,2,3******..63,64 Bits	

2.4.2 Data element

Data Element characteristics - name, formats, attributes, conditional code values.

The following rules apply to the data elements within a message

- All data elements begin on a byte boundary.
- Fixed length n type fields with an odd length are right- justified to a byte boundary, and zero-filled on the left.
- All lengths for variable length fields are represented in Binary Coded Decimal, right-justified to a byte boundary, and zero-filled on the left.
- The length indicator for a variable length field is a count of the number of data elements to follow. It does not include the length of the length indicator.
- Variable length n fields with an odd length are left justified within the field, and zero-filled.

2.4.3 Response Code

00 - Approve or completed successfully

01 - Refer to card issuer

02 - Refer to card issuer

03 - Invalid Merchant

04 - Pickup card

05 - Do not honor

12 - Invalid Transaction

13 – Invalid Amount

14 – Invalid Account Number

25 – Original Not Found

41 – Pickup card (lost card)

43 – Pickup card (stolen card)

51 - Insufficient funds

52 – No Checking Account

53 – No Saving Account

54 – Expired Card

55 – Incorrect PIN

75 - Allowable number of PIN-entry tries exceeded

82 - Incorrect CVV

83 - Unable to verify PIN

96 - System malfunction

2.5 Transaction Data Format

The following table shows the fields from the ISO 8583 specification implemented in TI-PSS. This section will describe the use of the following table and define each field.

Bit	Data Element Name	Attribute		Request	Response	Comments
	Message Type Id	n	4			
	Bit Map	b	64			
02	Primary Acct. Num.	n	..19			
03	Processing Code	n	6			
04	Amount, Trans.	n	12			
07	Transmission Date & Time	n	10			MMDDhhmmss
11	Systems Trace No	n	6			
12	Time, Local Trans.	n	6			
13	Date, Local Trans.	n	4			
14	Date, Expiration	n	4			
22	POS Entry Mode	n	3			
24	NII	n	3			
25	POS Condition Code	n	2			
35	Track 2 Data	z	..37			
37	Retrieval Ref. No.	an	12			
38	Auth. Id. Response	an	6			
39	Response Code	an	2			
41	Terminal Id	ans	8			
42	Card Acq. Id	ans	15			
43	Card Acq. Name	ans	40			

45	Track 1 Data	ans ..76			
48	Add. Data - Private	ans ...999			
52	PIN Data	b 64			
53	Security Control Info	b 128			
54	Additional Amounts	an ...120			
55	ICC Sys Related Data	b ...255			
60	Private Use	ans ...999			
61	Private Use	ans ...999			
62	Private Use	ans ...999			
63	Private Use	ans ...999			
64	Message Auth. Code	b 64			

The first two columns, **Bit, Data Element Name** show the data element assignment to a bit position, refer to Table 2 ISO 8583. The following sections will define the use of each field.

The "**Attribute**" column lists the format and size of the data element. The size of the field is the number of data elements contained in the field. Variable length fields are shown with preceding "." characters indicating the number of variable length digits. (...999 defines a field that's maximum length is 999 data elements.) The following table defines each attribute.

Attribue Abbreviation	Meaning	Size
a	Alphabetic characters (a-z, A-Z)	Each data element represents 1 byte
n	Numeric digits (0-9)	Each data element represents 1 nibble (2 data elements = 1 byte)
s	Special Characters	Each data element represents 1 byte

an	Alphabetic and numeric characters (0-9, a-z, A-Z)	Each data element represents 1 byte
as	Alphabetic and special characters	Each data element represents 1 byte
ns	Numeric and special characters	Each data element represents 1 byte
ans	Alphabetic, numeric and special characters	Each data element represents 1 byte
MM	Month	
DD	Day	
YY	Year	
hh	Hour	
mm	Minute	
ss	Second	
LL,LLL	Length of variable field that follows	
VAR	Variable length field	
3	Fixed length of three characters	
..17	Variable length up to maximum 17 characters. All variable length fields will in addition contain two or three positions at the beginning of the field to identify the number of positions following to the end of that field.	

x	"C" for credit, "D" for debit and must always be associated with a numeric amount data element, i.e., x + n16 in amount, net settlement means prefix "C" or "D" and 16 digits of amount, net settlement.	
b	Binary data	Each data element represents 1 bit. (8 data elements = 1 byte)
z	Track 2 data, as read from the magnetic strip.	Each data element represents 1 nibble (2 data elements = 1 byte)

The "Request" and "Response" columns show the contents of the terminal request and response messages comprising a transaction. These contents can be one of the following:

Code	Meaning
M	Mandatory
O	Optional
C xx	Conditional field, where xx is:
01	The primary account number is included when the transaction is entered manually via the keyboard.
02	The expiration date field will be included if the card number was entered manually, and the card processing options are set to accept a date, expiration to be entered.
03	For on-line transactions when the account number is read from the magnetic stripe reader track I and/or track II will be included.
04	Terminal only stores the primary account number and expiration date from a track read. Any transactions processed other than an on-line transaction will include the primary account number and expiration date.
05	The first two digits of the POS entry mode will be set to ‘02’ if the card is read by the card reader, and ‘01’ if the card number is entered via the keyboard. The last digit will indicate the PIN entry capability of the terminal. It will have a value of ‘1’ if there is PIN entry capability, and ‘2’ if there is no PIN entry capability. This information should be treated as additional transaction information, and not used to determine which field to use for the card number.
06	Some check guarantee services use primary account numbers for data. If account number is entered manually the bit 2 will be included in the request. If the account number is read via the magnetic card reader then either track I and/or track II will be included.
07	Transaction performed from a terminal with ICC capabilities performing an EMV compliant credit or debit transaction.

2.5.1 Logon (before every transaction)

This transaction is called before every financial or authorization transaction (sale, reversal, void, transaction inquiry) to get the dynamic working key for the specific transaction. The encrypted working key for the transaction will be returned in F53.

Bit	Data Element Name	Attribute		Request	Response	Comments
	Message Type Id	n	4	0800	0810	
	Bit Map	b	64	M	M	
02	Primary Acct Num.	n	..19	M	M	
03	Processing Code	n	6	950000	950000	
11	Systems Trace No	n	6	M	M	
39	Response Code	an	2		M	
53	Encrypted Working Key	b	128		M	
62	OnePay Tranx Id	ans	…999	M		OnePay Tranx Id

2.5.2 Sale

Bit	Data Element Name	Attribute		Request	Response	Comments
	Message Type Id	n	4	0200	0210	
	Bit Map	b	64	M	M	
02	Primary Acct Num.	n	..19	M	M	
03	Processing Code	n	6	00a00x	00a00x	
04	Amount, Trans.	N	12	M	O	Amount is verified when included in response
11	Systems Trace No	n	6	M	M	
12	Time, Local Trans.	n	6	O	M	
13	Date, Local Trans.	n	4	O	M	
14	Date, Expiration	n	4	C06		
22	POS Entry Mode	n	3	C05		
25	POS Condition Code	n	2	00		
35	Track 2 Data	z	..37	C03		
37	Retrieval Ref. No.	an	12	O	M	
38	Auth. Id. Response	an	6		O	
39	Response Code	an	2		M	
41	Terminal Id	ans	8	M	M	

42	Card Acq. Id	ans 15	M		
52	PIN Data	b 64	O		
62	OnePay Tranx Id	ans ...999	M		OnePay Tranx Id
63	MAC	ans ...999	M		

2.5.3 Reversal

The Reversal message is sent if the terminal sent a transaction request into the network, and did not receive a valid response before the transaction time-out period expired. The reversal is sent persistently until a valid response to the reversal is received from the host. Reversals will only be sent for on-line financial transaction messages.

Bit	Data Element Name	Attribute	Request	Response	Comments
	Message Type Id	n 4	0400	0410	
	Bit Map	b 64	M	M	
02	Primary Acct Num.	n ..19	C06		
03	Processing Code	n 6	M	M	Same as original processing code
04	Amount, Trans.	n 12	M	O	
11	Systems Trace No	n 6	M	M	
12	Time, Local Trans.	n 6	O	O	
13	Date, Local Trans.	n 4	O	O	
22	POS Entry Mode	n 3	C05		
25	POS Condition Code	n 2	M		
37	Retrieval Ref No.	an 12	O	M	
38	Auth. Id. Response	an 6		O	
39	Response Code	an 2		M	Host should always send ‘00’ response code
41	Terminal Id	ans 8	M	M	
42	Card Acq. Id	ans 15	M		
62	OnePay Tranx Id	ans ...999	M		OnePay Tranx Id
63	MAC	ans ...999	M		

2.5.4 Void

Eximbank CTL’s host does not support Refund transaction. So the void transaction is

used instead.

The Void transaction is used to inform the host that a transaction previously performed at the terminal has been canceled.

Bit	Data Element Name	Attribute	Request	Response	Comments
	Message Type Id	n 4	0200	0210	
	Bit Map	b 64	M	M	
02	Primary Acct Num.	n ..19	C06		
03	Processing Code	n 6	02a00x	02a00x	
04	Amount, Trans.	n 12	M	O	
11	Systems Trace No	n 6	M	M	
12	Time, Local Trans.	n 6	M	M	Request contains original transaction time
13	Date, Local Trans.	n 4	M	M	Request contains original transaction date
14	Date, Expiration	n 4	C06		
22	POS Entry Mode	n 3	C05		
25	POS Condition Code	n 2	00		
37	Retrieval Ref No.	an 12	M	M	Request contains original retrieval reference no.
38	Auth. Id. Response	an 6		O	
39	Response Code	an 2		M	
41	Terminal Id	ans 8	M	M	
42	Card Acq. Id	ans 15	M		
62	OnePay Tranx Id	ans ...999	M		OnePay Tranx Id
63	MAC	ans ...999	M		

2.5.5 Transaction Inquiry

This is the transaction that is used to return the transaction history of the specific card number. If OnePay Transaction Id is provided in F62, TI-PSS will only return data of one transaction. Otherwise, TI-PSS will return the newest ten transactions. In case, no transaction data found, F60 will not be available in the response. The following is transaction data format:

- **F60: Transaction1#Transaction2**
- **Transaction pattern:**
  - *transaction type = amount = trace no = ref no = transaction date (yyyymmddhhmmss) = transaction status*
- **Example:**
  - *One Transaction:*

SALE=00005000000=123456=161206312602=20110121150420=APPROVED#

  - *Many Transactions:*

SALE=00005000000=123456=161206312602=20110121150420=REVERSED#

SALE=00004000000=678910=171206312602=20110121150420=APPROVED#

VOID=00004000000=678911=171206312602=20110121150420=APPROVED#

Bit	Data Element Name	Attribute	Request	Response	Comments
	Message Type Id	n 4	0100	0110	
	Bit Map	b 64	M	M	
02	Primary Acct Num.	n ..19	C06		
03	Processing Code	n 6	95a00x	95a00x	
11	Systems Trace No	n 6	M	M	
12	Time, Local Trans.	n 6	O	M	
13	Date, Local Trans.	n 4	O	M	
22	POS Entry Mode	n 3	M		
25	POS Condition Code	n 2	M		
37	Retrieval Ref No.	an 12		M	
38	Auth. Id. Response	an 6	O		
39	Response Code	an 2	O	M	If original response code is not present, assume ‘00’
41	Terminal Id	ans 8	M	M	
42	Card Acq. Id	ans 15	M		
60	Original Tranx Data	ans ...999		O	
62	OnePay Tranx Id	ans ...999	M		OnePay Tranx Id
63	MAC	ans ...999	M		

2.6 Transaction Flow And Security

- ***Transaction Security***: OnePay and TI-PSS will use the same Master Key (3DES) to encrypt clear working key and decrypt the encrypted working key returned by

TI-PSS. And for every transaction, OnePay has to send message Logon firstly to get the working key for the main transaction. The clear working key then is used to encrypt the PIN Block (if F52 available) and calculate the MAC value and set the value in F63 in the request message.

- ***Transaction Flow***:
  - For every main transaction (Sale, Reversal, Void, Transaction Inquiry), OnePay needs to send the Logon message to TI-PSS to get the working key
  - TI-PSS will calculate the dynamic working key based on the information the OnePay provides such as Card number, Trace no and OnePay Transaction Id. After calculating the clear working key. TI-PSS will use the Master Key to encrypt the clear working key and return the encrypted working key in F53 and send the response to OnePay
  - OnePay has to use the Master Key to decrypt the encrypted working key in F53 to get the clear working key.
  - After getting the clear working key, OnePay uses it to encrypt the PIN Block in F52 (if available) before sending the main request message to TI-PSS
  - For the MAC value, OnePay combines clear working key, card number, trace no and OnePay transaction id (MAC = clear working key + card number + trace no + OnePay transaction id). Then OnePay uses the Master Key to encrypt the MAC, hash the encrypted MAC and finally set the hashed value in F63
  - The request message with encrypted data in F52, F63 will be sent to TI-PSS
  - TI-PSS will calculate the hashed MAC for the transaction and compare with the hashed MAC in F63 in the request message to authorize the transaction.
  - TI-PSS will also decrypt the PIN Block using the clear working key (with OnePay) and encrypt the PIN Block again using the clear working key between TI-PSS and CTL before sending the request message to CTL.
  - TI-PSS will send the response to OnePay after receiving the response from CTL.