



# **POS Interface Specifications**

## **ISO 8583 (1987 version)**

Prepared by:

Nigeria Inter – Bank Settlement System (NIBSS)

Version: 1.16

August 07, 2018





## TABLE OF CONTENTS

<b>POS INTERFACE SPECIFICATIONS .....</b>	<b>1</b>
<b>ISO 8583 (1987 VERSION) .....</b>	<b>1</b>
<b><i>DOCUMENT CONTROL</i> .....</b>	<b>3</b>
<b>1. INTRODUCTION.....</b>	<b>4</b>
<b>2. EXTERNAL MESSAGE TYPES.....</b>	<b>5</b>
<b>2.1 PROTOCOL .....</b>	<b>5</b>
<b>2.2 BITMAP.....</b>	<b>5</b>
<b>2. 3 SUPPORTED MESSAGE TYPE.....</b>	<b>5</b>
<b>3. EXTERNAL MESSAGE TYPE LAYOUTS.....</b>	<b>6</b>
<b>3.1 AUTHORIZATION REQUEST/REPEAT (0100).....</b>	<b>6</b>
<b>3.2 AUTHORIZATION REQUEST RESPONSE (0110) .....</b>	<b>7</b>
<b>3.3 FINANCIAL REQUEST/REPEAT (0200).....</b>	<b>11</b>
<b>3.4 FINANCIAL REQUEST RESPONSE (0210) .....</b>	<b>12</b>
<b>3.5 REVERSAL ADVICE (REPEAT) (0420/0421) .....</b>	<b>15</b>
<b>3.6 REVERSAL ADVICE RESPONSE (0430) .....</b>	<b>16</b>
<b>3.7 NETWORK MANAGEMENT (REPEAT) (0800).....</b>	<b>17</b>
<b>3.8 NETWORK MANAGEMENT (0810).....</b>	<b>17</b>
<b>4. DATA ELEMENT DEFINITION .....</b>	<b>19</b>
<b>5. KEY MANAGEMENT .....</b>	<b>62</b>





## Document Control

S/N	Document Section	Changes	Version
1.	Section 3.7	DE63 was added	1.7
2.	Section 4	<ol style="list-style-type: none"> <li>EMV and CA public key download parameters .deleted from DE62</li> <li>Description for DE63 was added to add EMV AID and CA public key Download.</li> </ol>	1.7
3.	Section 4	<p>Report Generation from POS Terminal added as a transaction type in Data Element 3.</p> <p>Report Generation field descriptions added to DE63.</p>	1.8
4.	Section 3.3	DE62 added to 0200 message to carry Key Serial Number (KSN) for transactions based on Derived Unique Key Per Transaction (DUKPT)	1.9
5	Section 4	BDK Request added as a transaction type	1.9
6.	Section 5	DUKPT implementation	1.9
7.	Section 2 and 4	Field #124 – Near Field Communication Data added	1.9
8.	Section 4	Purchase with additional data added	1.10
9.	Section 5	<ol style="list-style-type: none"> <li>Initial PIN Encryption Key (IPEK) was added for both Track2 and EMV.</li> <li>BDK was adjusted to remove the functionality for downloading it online</li> </ol>	1.11
10.	Section 4	Processing code for IPEK (Track2 Data and EMV) added	1.11
11.	Section 4	Addition of Dynamic Currency Conversion (DCC) Inclusion of Form Data in ICC Data (DE55)	1.12
12	Section 3	<ol style="list-style-type: none"> <li>Inclusion of Message type layout for 220/221 and 230</li> <li>Inclusion of DE26 “POS PIN capture code” in the message type for <b>0210</b></li> <li>The MTI for Sales completion was changed from 0200 to 0220</li> <li>Include Message type for 0120/0130</li> </ol>	1.13
14	Section 4	1. Inclusion of DE 102 and 103 in 0200 message type	1.14
15	Section 4	1. Inclusion of mCash Receipt Printing Spec.	1.15
16	Section 4	1. Clarification on the value of X +n	1.16





## 1. Introduction

This specification document covers the interface specifications that must be supported by POS Terminals or other Payment Channels to integrate with Central Terminal Management System (CTMS). It contains definitions for all messages and the data elements (or fields) transmitted between the POS Terminals or other Payment Channels and CTMS.

### Acronyms and Abbreviations

NCS	Nigeria Central Switch
ATM	Automated Teller Machine.
POS	Point of Sale Machine
CMS	Card Management System
CTMS	Central Terminal Management System



## 2. External Message types

### 2.1 Protocol

The interface to CTMS will be over TCP/IP. The application data will be prefixed by a 2-byte length header field (Binary) indicating the length of the application data to follow.

### 2.2 Bitmap

CTMS supports ASCII ISO bitmap representations. ASCII ISO bitmap representation is either 16 or 32 byte representation of the bitmap in Hex.

### 2.3 Supported Message Type

Message type codes are used to identify the general function of messages, and one Message type code is required in each message. CTMS supports the message types shown in the following table for both inbound and outbound messages. The message types in the table are divided according to the ISO standard message classes.

Message Class	Type	Description
Authorization	0100	Authorization Request
	0110	Authorization Response
Financial Transaction	0200	Financial Transaction Request
	0210	Financial Transaction Response
Reversal	0420	Reversal Advice
	0421	Reversal Advice Repeat
	0430	Reversal Advice Response
Network Management	0800	Network Management Request
	0810	Network Management Request Response





### 3. External Message Type Layouts

CTMS uses the following codes to denote whether a data element should be present in its external message.

*Conditional:* The element is mandatory under certain conditions.

*Echo:* In response messages, this code indicates that the response message sender must include the same value it received in the data element in the associated request message. In other words, the responder must *echo back* the data element if it is present in the request message.

*Mandatory:* The element is required in the message.

*Optional:* The element is not always required in the message.

#### 3.1 Authorization Request/Repeat (0100)

Bit Data	Element Name	Presence Indicator
2	Primary account number	Mandatory
3	Processing code	Mandatory
4	Amount, transaction	Mandatory
7	Transmission date and time	Mandatory
11	Systems trace audit number	Mandatory
12	Time, local transaction	Mandatory
13	Date, local transaction	Mandatory
14	Date, expiration	Mandatory
18	Merchant's type	Mandatory
22	POS entry mode	Mandatory
23	Card sequence number	Conditional
25	POS condition code	Mandatory
26	POS PIN capture code	Conditional
28	Amount, transaction fee	Mandatory
32	Acquiring institution id code	Mandatory
35	Track 2 data	Conditional
37	Retrieval reference number	Mandatory
40	Service restriction code	Optional
41	Card acceptor terminal id	Mandatory





42	Card acceptor id code	Mandatory
43	Card acceptor name/location	Mandatory
49	Currency code, transaction	Mandatory
52	PIN data	Conditional
53	Security related control information	Conditional
54	Additional amounts	Conditional
55	Integrated Circuit Card System Related Data	Conditional
56	Message reason code	Optional
59	Transport (echo) data	Optional
60	Payment Information	Conditional
62	Private Field, Management Data 1	Conditional
102	Account identification 1	Optional
103	Account identification 2	Optional
123	POS data code	Mandatory
124	Near Field Communication Data	Conditional
128	Secondary Message Hash Value	Mandatory

### 3.2 Authorization Request Response (0110)

Bit Data	Element Name	Presence Indicator
2	Primary account number	Mandatory
3	Processing code	Mandatory
4	Amount, transaction	Mandatory
7	Transmission Date and Time	Conditional
11	Systems trace audit number	Conditional
12	Time, local transaction	Mandatory
13	Date, local transaction	Conditional
14	Date, expiration	Conditional
15	Date, Settlement	Conditional
18	Merchant's type	Mandatory
22	POS entry mode	Mandatory
23	Card sequence number	Conditional
25	POS condition code	Mandatory
28	Amount, transaction fee	Conditional
30	Amount, transaction processing fee	Conditional
32	Acquiring institution id code	Mandatory
33	Forwarding institution id code	Conditional
35	Track 2 data	Conditional
37	Retrieval reference number	Mandatory
38	Authorization id response	Conditional





39	Response code	Mandatory
40	Service restriction code	Conditional
41	Card acceptor terminal id	Optional
42	Card acceptor id code	Conditional
43	Card acceptor name/location	Conditional
49	Currency code, transaction	Mandatory
54	Additional amounts	Conditional
55	Integrated Circuit Card System Related Data	Conditional
59	Transport (echo) data	Conditional
60	Payment Information	Conditional
102	Account identification 1	Optional
103	Account identification 2	Optional
123	POS data code	Mandatory
124	Near Field Communication Data	Conditional
128	Secondary Message Hash Value	Mandatory

### 3.3 Authorization Advice/Repeat (0120/0121)

Bit Data	Element Name	Presence Indicator
2	Primary account number	Conditional
3	Processing code	Mandatory
4	Amount, transaction	Mandatory
5	Amount, settlement	Conditional
7	Transmission date and time	Mandatory
9	Conversion rate, settlement	Conditional
11	Systems trace audit number	Mandatory
12	Time, local transaction	Mandatory
13	Date, local transaction	Mandatory
14	Date, expiration	Conditional
15	Date, settlement	Conditional
16	Date, conversion	Conditional
18	Merchant's type	Conditional
22	POS entry mode	Mandatory
23	Card sequence number	Conditional
25	POS condition code	Mandatory
28	Amount, transaction fee	Optional
29	Amount, settlement fee	Conditional
30	Amount, transaction processing fee	Optional
31	Amount, settle processing fee	Conditional







32	Acquiring institution id code	Conditional
33	Forwarding institution id code	Optional
35	Track 2 data	Conditional
37	Retrieval reference number	Optional
40	Service restriction code	Optional
41	Card acceptor terminal id	Mandatory
42	Card acceptor id code	Mandatory
43	Card acceptor name/location	Mandatory
45	Track 1 data	Optional
49	Currency code, transaction	Mandatory
50	Currency code, settlement	Conditional
54	Additional amounts	Conditional
55	Integrated Circuit Card System Related Data	Conditional
56	Message reason code	Optional
58	Authorizing agent id cod	Conditional
59	Transport (echo) data	Optional
67	Extended payment code	Conditional
90	Original data elements	Conditional
95	Replacement amounts	Conditional
98	Payee	Conditional
100	Receiving institution id code	Conditional
102	Account identification 1	Conditional
103	Account identification 2	Conditional
123	POS data code	Mandatory
124	Near Field Communication Data	Conditional
128	Secondary Message Hash Value	Mandatory

### 3.4 Authorization Advice Response (0130)

Bit Data	Element Name	Presence Indicator
2	Primary account number	Conditional
3	Processing code	Optional
4	Amount, transaction	Optional
5	Amount, settlement	Conditional
7	Transmission date and time	Mandatory
9	Conversion rate, settlement	Conditional
11	Systems trace audit number	Mandatory
12	Time, local transaction	Mandatory





13	Date, local transaction	Mandatory
14	Date, expiration	Optional
15	Date, settlement	Conditional
16	Date, conversion	Conditional
18	Merchant's type	Conditional
22	POS entry mode	Mandatory
23	Card sequence number	Optional
25	POS condition code	Mandatory
28	Amount, transaction fee	Optional
29	Amount, settlement fee	Conditional
30	Amount, transaction processing fee	Optional
31	Amount, settle processing fee	Conditional
32	Acquiring institution id code	Optional
33	Forwarding institution id code	Conditional
35	Track 2 data	Conditional
37	Retrieval reference number	Optional
38	Authorization id response	Conditional
39	Response code	Mandatory
40	Service restriction code	Conditional
41	Card acceptor terminal id	Mandatory
42	Card acceptor id code	Mandatory
43	Card acceptor name/location	Mandatory
44	Additional response data	Optional
48	Additional data	Conditional
49	Currency code, transaction	Mandatory
50	Currency code, settlement	Conditional
54	Additional amounts	Optional
55	Integrated Circuit Card System Related Data	Conditional
58	Authorizing agent id code	Conditional
59	Transport (echo) data	Conditional
90	Original data elements	Conditional
102	Account identification 1	Optional
103	Account identification 2	Optional
123	POS data code	Mandatory
124	Near Field Communication Data	Conditional
128	Secondary Message Hash Value	Mandatory





### 3.5 Financial Request/Repeat (0200)

Bit Data	Element Name	Presence Indicator
2	Primary account number	Mandatory
3	Processing code	Mandatory
4	Amount, transaction	Mandatory
7	Transmission date and time	Mandatory
11	Systems trace audit number	Mandatory
12	Time, local transaction	Mandatory
13	Date, local transaction	Mandatory
14	Date, expiration	Mandatory
18	Merchant's type	Mandatory
22	POS entry mode	Mandatory
23	Card sequence number	Conditional
25	POS condition code	Mandatory
26	POS PIN capture code	Conditional
28	Amount, transaction fee	Mandatory
32	Acquiring institution id code	Mandatory
35	Track 2 data	Conditional
37	Retrieval reference number	Mandatory
40	Service restriction code	Optional
41	Card acceptor terminal id	Mandatory
42	Card acceptor id code	Mandatory
43	Card acceptor name/location	Mandatory
49	Currency code, transaction	Mandatory
52	PIN data	Conditional
53	Security related control information	Conditional
54	Additional amounts	Conditional
55	Integrated Circuit Card System Related Data	Conditional
56	Message reason code	Optional
59	Transport (echo) data	Optional
60	Payment Information	Conditional
62	Private Field, Management Data 1	Conditional
102	Account identification 1	Optional
103	Account identification 2	Optional
123	POS data code	Mandatory
123	POS data code	Mandatory
124	Near Field Communication Data	Conditional
128	Secondary Message Hash Value	Mandatory





### 3.6 Financial Request Response (0210)

Bit Data	Element Name	Presence Indicator
2	Primary account number	Mandatory
3	Processing code	Mandatory
4	Amount, transaction	Mandatory
7	Transmission date and time	Conditional
11	Systems trace audit number	Conditional
12	Time, local transaction	Mandatory
13	Date, local transaction	Conditional
14	Date, expiration	Conditional
15	Date, Settlement	Conditional
18	Merchant's type	Mandatory
22	POS entry mode	Mandatory
23	Card sequence number	Conditional
25	POS condition code	Mandatory
26	POS PIN capture code	Conditional
28	Amount, transaction fee	Conditional
30	Amount, transaction processing fee	Conditional
32	Acquiring institution id code	Mandatory
33	Forwarding institution id code	Conditional
35	Track 2 data	Conditional
37	Retrieval reference number	Mandatory
38	Authorization id response	Conditional
39	Response code	Mandatory
40	Service restriction code	Conditional
41	Card acceptor terminal id	Optional
42	Card acceptor id code	Conditional
43	Card acceptor name/location	Conditional
49	Currency code, transaction	Mandatory
54	Additional amounts	Conditional
55	Integrated Circuit Card System Related Data	Conditional
56	Message reason code	Optional
59	Transport (echo) data	Conditional
60	Payment Information	Conditional
102	Account identification 1	Optional
103	Account identification 2	Optional
123	POS data code	Mandatory
124	Near Field Communication Data	Conditional
128	Secondary Message Hash Value	Mandatory





### 3.7 Financial Advice/Repeat (Repeat) (0220/0221)

Bit Data	Element Name	Presence Indicator
2	Primary account number	Conditional
3	Processing code	Mandatory
4	Amount, transaction	Mandatory
5	Amount, settlement	Conditional
7	Transmission date and time	Mandatory
9	Conversion rate, settlement	Conditional
11	Systems trace audit number	Mandatory
12	Time, local transaction	Mandatory
13	Date, local transaction	Mandatory
14	Date, expiration	Conditional
15	Date, settlement	Conditional
16	Date, conversion	Conditional
18	Merchant's type	Conditional
22	POS entry mode	Mandatory
23	Card sequence number	Conditional
25	POS condition code	Mandatory
26	POS PIN capture code	Conditional
28	Amount, transaction fee	Optional
29	Amount, settlement fee	Conditional
30	Amount, transaction processing fee	Optional
31	Amount, settle processing fee	Conditional
32	Acquiring institution id code	Conditional
33	Forwarding institution id code	Optional
35	Track 2 data	Conditional
37	Retrieval reference number	Optional
38	Authorization id response	Conditional
40	Service restriction code	Optional
41	Card acceptor terminal id	Mandatory
42	Card acceptor id code	Mandatory
43	Card acceptor name/location	Mandatory
45	Track 1 data	Optional
49	Currency code, transaction	Mandatory
50	Currency code, settlement	Conditional
54	Additional amounts	Conditional
55	Integrated Circuit Card System Related Data	Conditional
56	Message reason code	Optional





58	Authorizing agent id code	Conditional
59	Transport (echo) data	Optional
67	Extended payment code	Conditional
90	Original data elements	Conditional
95	Replacement amounts	Conditional
98	Payee	Conditional
100	Receiving Institution ID Code	Optional
102	Account identification 1	Conditional
103	Account identification 2	Conditional
123	POS data code	Mandatory
124	Near Field Communication Data	Conditional
128	Secondary Message Hash Value	Mandatory

### 3.8 Financial Advice Response (0230)

Bit Data	Element Name	Presence Indicator
2	Primary account number	Mandatory
3	Processing code	Mandatory
4	Amount, transaction	Mandatory
7	Transmission date and time	Conditional
9	Conversion rate, settlement	Conditional
11	Systems trace audit number	Conditional
12	Time, local transaction	Mandatory
13	Date, local transaction	Conditional
14	Date, expiration	Conditional
15	Date, Settlement	Conditional
16	Date, conversion	Conditional
18	Merchant's type	Mandatory
22	POS entry mode	Mandatory
23	Card sequence number	Conditional
25	POS condition code	Mandatory
26	POS PIN capture code	Conditional
28	Amount, transaction fee	Conditional
29	Amount, settlement fee	Conditional
30	Amount, transaction processing fee	Conditional
31	Amount, settle processing fee	Conditional
32	Acquiring institution id code	Mandatory
33	Forwarding institution id code	Conditional
35	Track 2 data	Conditional
37	Retrieval reference number	Mandatory





38	Authorization id response	Conditional
39	Response code	Mandatory
40	Service restriction code	Conditional
41	Card acceptor terminal id	Optional
42	Card acceptor id code	Conditional
43	Card acceptor name/location	Conditional
44	Additional response data	Optional
48	Additional data	Conditional
49	Currency code, transaction	Mandatory
50	Currency code, settlement	Conditional
54	Additional amounts	Conditional
55	Integrated Circuit Card System Related Data	Conditional
56	Message reason code	Optional
59	Transport (echo) data	Conditional
60	Payment Information	Conditional
102	Account identification 1	Optional
103	Account identification 2	Optional
123	POS data code	Mandatory
124	Near Field Communication Data	Conditional
128	Secondary Message Hash Value	Mandatory

### 3.9 Reversal Advice (Repeat) (0420/0421)

Bit Data	Element Name	Presence Indicator
2	Primary account number	Mandatory
3	Processing code	Mandatory
4	Amount, transaction	Mandatory
7	Transmission date and time	Mandatory
11	Systems trace audit number	Mandatory
12	Time, local transaction	Mandatory
13	Date, local transaction	Mandatory
14	Date, expiration	Mandatory
18	Merchant's type	Mandatory
22	POS entry mode	Mandatory
23	Card sequence number	Conditional
25	POS condition code	Mandatory
26	POS PIN capture code	Conditional
28	Amount, transaction fee	Conditional
30	Amount, transaction processing fee	Conditional
32	Acquiring institution id code	Mandatory





35	Track 2 data	Conditional
37	Retrieval reference number	Mandatory
40	Service restriction code	Optional
41	Card acceptor terminal id	Mandatory
42	Card acceptor id code	Mandatory
43	Card acceptor name/location	Mandatory
49	Currency code, transaction	Mandatory
52	PIN data	Conditional
54	Additional amounts	Conditional
56	Message reason code	Mandatory
59	Transport (echo) data	Optional
60	Payment Information	Conditional
90	Original data elements	Mandatory
95	Replacement Amounts	Mandatory
123	POS data code	Mandatory
124	Near Field Communication Data	Conditional
128	Secondary Message Hash Value	Mandatory

### 3.10 Reversal Advice Response (0430)

Bit Data	Element Name	Presence Indicator
2	Primary account number	Mandatory
3	Processing code	Mandatory
4	Amount, transaction	Mandatory
7	Amount, settlement	Conditional
11	Systems trace audit number	Conditional
12	Time, local transaction	Mandatory
13	Date, local transaction	Conditional
14	Date, expiration	Conditional
15	Date, Settlement	Conditional
18	Merchant's type	Mandatory
22	POS entry mode	Mandatory
23	Card sequence number	Optional
25	POS condition code	Mandatory
28	Amount, transaction fee	Conditional
30	Amount, transaction processing fee	Conditional
32	Acquiring institution id code	Mandatory
33	Forwarding institution id code	Conditional
35	Track 2 data	Conditional
37	Retrieval reference number	Mandatory







38	Authorization id response	Conditional
39	Response code	Mandatory
40	Service restriction code	Conditional
41	Card acceptor terminal id	Optional
42	Card acceptor id code	Conditional
43	Card acceptor name/location	Conditional
49	Currency code, transaction	Mandatory
54	Additional amounts	Conditional
59	Transport (echo) data	Conditional
90	Original data elements	Mandatory
95	Replacement amounts	Mandatory
102	Account identification 1	Optional
103	Account identification 2	Optional
123	POS data code	Mandatory
124	Near Field Communication Data	Conditional
128	Secondary Message Hash Value	Mandatory

### 3.11 Network Management (Repeat) (0800)

Bit Data	Element Name	Presence Indicator
3	Processing code	Mandatory
7	Transmission date and time	Mandatory
11	Systems trace audit number	Mandatory
12	Time, local transaction	Mandatory
13	Date, local transaction	Mandatory
41	Card acceptor terminal id	Mandatory
62	Private, management data 1	Conditional
63	Private, management data 2	Conditional
64	Primary Message Hash Value	Conditional

### 3.12 Network Management (0810)

Bit Data	Element Name	Presence Indicator
7	Transmission date and time	Mandatory
11	Systems trace audit number	Mandatory
12	Time, local transaction	Mandatory
13	Date, local transaction	Mandatory
39	Response code	Mandatory
41	Card acceptor terminal id	Mandatory
53	Security related control information	Conditional





62	Private, management data 1	Conditional
63	Private, management data 2	Conditional
64	Primary Message Hash Value	Conditional





## 4. DATA ELEMENT DEFINITION

The following ISO Data Elements are supported by the Interface.

### Field #2 – Primary Account Number

Field No	Format	Attr
2	LLVAR	n..19

A number identifying the cardholder and the card issuer. Typically, this number is embossed on the front of the card and encoded on Track 2 of the magnetic stripe.

### Field #3 - Processing Code

Field No	Format	Attr
3		an 6

The customer transaction type and the account types, if any, affected by the transaction. This is a fixed length field consisting of 3 data elements:

- Transaction type (positions 1 - 2)
- Account type affected for debits and inquiries and the "from" account for transfers (positions 3 - 4)
- Account type affected for credits and the "to" account for transfers (positions 5 - 6)

#### *Transaction Type*

Code	Description	Message Type Identifier (MTI)
00	Purchase	0200
01	Cash Advance	0200
20	Refund/Return	0200
21	Deposit	0200
09	Purchase with Cash back	0200
31	Balance Inquiry	0100





30	Link Account Inquiry	0100
38	Mini – Statement	0100
40	Fund Transfer	0200
48	Bill Payments	0200
4A	Prepaid	0200
4B	Biller List Download	0800
4C	Product List Download	0800
4D	Biller Subscription Information Download	0800
4E	Payment Validation	0800
4F	Purchase with Additional Data	0200
60	POS Pre – Authorization	0100
61	POS Pre – Authorization Completion	0220
90	PIN Change	0100
9A	Terminal Master Key	0800
9B	Terminal Session Key	0800
9G	Terminal PIN Key	0800
9I	Initial PIN Encryption Key Download – Track2 Data	0800
9J	Initial PIN Encryption Key Download – EMV	0800
9C	Terminal Parameter Download	0800
9D	Call – home	0800
9E	CA Public Key Download	0800
9F	EMV Application AID Download	0800
9H	Daily Transaction Report Download	0800
9K	Dynamic Currency Conversion	0800

*Account Type Codes*

Code	Description
00	Default – unspecified
10	Savings





20	Current
30	Credit
40	Universal Account
50	Investment Account

#### Field #4 - Amount, Transaction

Field No	Format	Attr
4		n 12

This field contains the transaction amount in the transaction currency. This amount is expressed in lowest denominations.

#### Field #5 - Amount, Settlement

Field No	Format	Attr
5		n 12

The funds to be transferred between the acquirer and card issuer equal to the amount, transaction as expressed in the settlement currency.

#### Field #7 - Transmission Date and Time

Field No	Format	Attr
7	MMDDhhmmss	n 10

The date and time, expressed in Coordinated Universal Time (UTC), when this message is sent by the message initiator.

#### Field #9 - Conversion Rate, Settlement

Field No	Format	Attr
9		n 8





This field contains the factor used in conversion from the transaction currency amount to the local currency amount. The left most digit indicates the number of decimal places from the right.

### Field #11 - System Trace Audit Number

Field No	Format	Attr
11		n 6

A number assigned by a transaction originator to assist in identifying a transaction uniquely. The systems trace audit number remains unchanged for all messages within a transaction.

### Field #12 - Time, Local Transaction

Field No	Format	Attr
12	Hhmmss	n 6

The local time at which the transaction takes place at the card acceptor location in authorization and financial messages.

For all other transactions, this field indicates the local time set by the initiator of the first message of the transaction.

### Field #13 - Date, Local Transaction

Field No	Format	Attr
13	MMDD	n 4

The local date at which the transaction takes place at the card acceptor location in authorization and financial messages.





For all other transactions, this field indicates the local date set by the initiator of the first message of the transaction.

#### Field #14 - Date, Expiration

Field No	Format	Attr
14	YYMM	n 4

The year and month after which the card expires.

#### Field #15 - Date, Settlement

Field No	Format	Attr
13	MMDD	n 4

The month and day for which financial totals are reconciled between the acquirer and the issuer.

#### Field #16- Date, Conversion

Field No	Format	Attr
13	MMDD	n 4

The month and day on which the currency for the transaction was converted.

#### Field #18 –Merchant Type

Field No	Format	Attr
18		n 4

The classification of the merchant's type of business product or service. Codes to be developed within each country.





### Field #22 –POS Entry Mode

Field No	Format	Attr
22		N3

A series of codes that identify the actual method used to capture the account number and expiry date when a terminal is used, and the PIN capture capability of the terminal.

This is a fixed length field consisting of 2 data elements:

- PAN entry mode (positions 1 - 2)
  - 00 – Unknown
  - 01 – Manual (i.e keypad)
  - 02 – Magnetic Stripe (possibly constructed manually, CVV may be checked)
  - 03 – Barcode
  - 04 – OCR
  - 05 – ICC (CVV may be checked)
  - 07 – Auto - entry via contactless ICC
  - 90 – Magnetic strip as read from track 2
  - 91 – Auto - entry via contactless magnetic stripe
  - 95 – ICC (CVV may not be checked)
- PIN entry capability (position 3)
  - 0 – Unknown
  - 1 – Terminal can accept PIN
  - 2 – Terminal cannot accept PIN

### Field #23 – Card Sequence number

Field No	Format	Attr
23		n3







A number distinguishing between separate cards with the same primary account number or primary account number extended.

**Field #25 –POS Condition Code**

Field No	Format	Attr
25		n2

A code that describes the condition under which the transaction takes place at the Point-Of-Service.

- 00 Normal presentment
- 01 Customer not present
- 02 Unattended terminal - card can be retained
- 03 Merchant suspicious
- 04 Electronic Cash Register interface
- 05 Customer present, card not present
- 06 Pre-authorized request
- 07 Telephone device required
- 08 Mail/telephone order
- 09 POS security alert
- 10 Customer identity verified
- 11 Suspected fraud
- 12 Security reasons





- 13 Representation of item
  - 14 Public utility terminal
  - 15 Customer's terminal
  - 16 Administrative terminal
  - 17 Returned item
  - 18 No check in envelope – return
  - 19 Deposit out of balance – return
  - 20 Payment out of balance – return
  - 21 Manual reversal
  - 22 Terminal error – counted
  - 23 Terminal error - not counted
  - 24 Deposit out of balance – apply
  - 25 Payment out of balance – apply
  - 26 Withdrawal error – reversed
  - 27 Unattended terminal - card cannot be retained
- Additional codes can be defined for private use.

**Field #26 – POS PIN Capture Code**

Field No	Format	Attr
26		n2

The maximum number of PIN characters that can be accepted by the Point-of-Service device.





Valid values are "04" to "12" ("00" to "03" are reserved by ISO) and if the POS device does not accept PINs or it is unknown whether the device does, this value should be set to "12".

**Field #28 - Amount, Transaction Fee**

Field No	Format	Attr
28		x + n 8

A fee charged, by the acquirer to the issuer, for transaction activity, in the currency of the amount, transaction.

**Field #29 - Amount, Settlement Fee**

Field No	Format	Attr
29		x + n 8

A fee charged, by the acquirer to the issuer, for transaction activity, in the currency of the amount, settlement. X can have a value of either "C" or "D".

**Field #30 - Amount, Transaction Processing Fee**

Field No	Format	Attr
30		x + n 8

A fee charged by the network for the handling and routing of messages, in the currency of amount, transaction. This field is usually inserted by the network into the applicable messages. X can have a value of either "C" or "D".

**Field #31 - Amount, Settlement Processing Fee**

Field No	Format	Attr
31		x + n 8





A fee charged by the network for the handling and routing of messages, in the currency of amount, settlement. This field is usually inserted by the network into the applicable messages.

### Field #32 - Acquiring Institution Identification Code

Field No	Format	Attr
32	LLVAR	an.. 11

A code identifying the financial institution acting as the acquirer of this customer transaction. The acquirer is the member or system user that signed the merchant, installed the ATM or dispensed cash. This field usually contains the BIN (see PAN) of the acquirer, but could be any other number assigned to it by the relevant authorities. When a processing center operates for multiple acquirers, this is the code for the individual member or system user, not a code for the processing center.

### Field #33 - Forwarding Institution Identification Code

Field No	Format	Attr
33	LLVAR	n.. 11

A code identifying the institution that forwards the transaction in an interchange system en route to the card issuer. For example, assume that an acquirer routes a transaction via a third-party EFT switch to the card issuer. In the request from the acquirer to the EFT switch, this field contains the code of the acquirer. When the request is forwarded by the EFT switch to the card issuer, this field contains the code assigned to the EFT switch.

### Field #35 – Track 2 Data

Field No	Format	Attr
35	LLVAR	z..37





The information encoded on Track 2 of the magnetic stripe as defined in ISO 7813, including field separators but excluding the begin sentinel, end sentinel and longitudinal redundancy check characters. The field separator (FS) can be either a "=" or a "D" character. The layout of this field is as follows:

Field	Length
-------	--------

Primary account number up to 19 digits

Field separator 1 digit

Expiry date (YYMM) 4 digits (or a field separator if not present)

Service restriction code 3 digits (or a field separator if not present)

Discretionary data balance of available digits

The *primary account number*, *expiry date* and *service restriction code* fields are described in further detail under fields 2, 14 and 40 in this document.

### Field #37 – Retrieval Reference Number

Field No	Format	Attr
37		an 12

A reference number supplied by the system retaining the original source information and used to assist in locating that information or a copy thereof.

### Field #38 – Authorization code

Field No	Format	Attr
38		n 6

A code assigned by the authorizing institution indicating approval.





### Field #39 - Response Code

Field No	Format	Attr
39		an 2

A code that defines the disposition of a transaction.

- 00 Approved or completed successfully
- 01 Refer to card issuer
- 02 Refer to card issuer, special condition
- 03 Invalid merchant
- 04 Pick-up card
- 05 Do not honor
- 06 Error
- 07 Pick-up card, special condition
- 08 Honor with identification
- 09 Request in progress
- 10 Approved, partial
- 11 Approved, VIP
- 12 Invalid transaction
- 13 Invalid amount
- 14 Invalid card number
- 15 No such issuer
- 16 Approved, update track 3





- 17 Customer cancellation
- 18 Customer dispute
- 19 Re-enter transaction
- 20 Invalid response
- 21 No action taken
- 22 Suspected malfunction
- 23 Unacceptable transaction fee
- 24 File update not supported
- 25 Unable to locate record
- 26 Duplicate record
- 27 File update edit error
- 28 File update file locked
- 29 File update failed
- 30 Format error
- 31 Bank not supported
- 32 Completed partially
- 33 Expired card, pick-up
- 34 Suspected fraud, pick-up
- 35 Contact acquirer, pick-up
- 36 Restricted card, pick-up
- 37 Call acquirer security, pick-up





- 38 PIN tries exceeded, pick-up
- 39 No credit account
- 40 Function not supported
- 41 Lost card
- 42 No universal account
- 43 Stolen card
- 44 No investment account
- 51 Not sufficient funds
- 52 No check account
- 53 No savings account
- 54 Expired card
- 55 Incorrect PIN
- 56 No card record
- 57 Transaction not permitted to cardholder
- 58 Transaction not permitted on terminal
- 59 Suspected fraud
- 60 Contact acquirer
- 61 Exceeds withdrawal limit
- 62 Restricted card
- 63 Security violation
- 64 Original amount incorrect







- 65 Exceeds withdrawal frequency
- 66 Call acquirer security
- 67 Hard capture
- 68 Response received too late
- 75 PIN tries exceeded
- 77 Intervene, bank approval required
- 78 Intervene, bank approval required for partial amount
- 90 Cut-off in progress
- 91 Issuer or switch inoperative
- 92 Routing error
- 93 Violation of law
- 94 Duplicate transaction
- 95 Reconcile error
- 96 System malfunction
- 98 Exceeds cash limit

**Field #40 - Service Restriction Code**

Field No	Format	Attr
40		N3

An identification of geographic/service availability. Contains:

- The area of usage and whether the card has additional read facilities

- 1 International card





- 2 International card - integrated circuit facilities
- 5 National use only
- 6 National use only - integrated circuit facilities
- 9 Test card - online authorization mandatory
  - The authorization processing requirements for this card
- 0 Normal authorization
- 2 Online authorization mandatory
- 4 Online authorization mandatory
  - The range of services available and PIN requirements
- 0 PIN required
- 1 No restrictions - normal cardholder verification
- 2 Goods and services only
- 3 PIN required, ATM only
- 5 PIN required, goods and services only at POS, cash at ATM
- 6 PIN required if PIN pad present
- 7 PIN required if PIN pad present, goods and services only at POS, cash at ATM

**Field #41 - Card Acceptor Terminal Identification**

Field No	Format	Attr
41		ans 8

A unique code identifying a terminal at the card acceptor location.

**Field #42 - Card Acceptor Identification Code**

Field No	Format	Attr
----------	--------	------





42		ans 15
----	--	--------

A code identifying the card acceptor (typically a merchant).

### Field #43 - Card Acceptor Name / Location

Field No	Format	Attr
43		ans 40

The name and location of the card acceptor (such as a merchant or an ATM). This is a fixed length field consisting of 4 data elements:

- The *location information* (positions 1 - 23), exclusive of city, state and country
- The *city* (positions 24 - 36) in which the Point-of-Service is located
- The *state* (positions 37 - 38) in which the Point-of-Service is located
- The *country* (positions 39 - 40) in which the Point-of-Service is located

### Field #44 - Additional Response Data

Field No	Format	Attr
48	LLVAR	ans..25

Used to provide other supplemental data (such as a telephone number for referrals) that may be required in response to an authorization or other type of transaction request.

After a **PIN Change** request has been processed, this field contains the PIN offset (or PVV) in a 0610 message to the Source Node, as well as in a 0620 message to the Sink Node. If set in a 0610 message from the Sink Node, this field again indicates the PIN offset (or PVV).

For **Visa Cash** load transactions, this field is used to carry signature information. In load responses, it contains the *Visa Cash Service Identifier* ("SV:") followed by the load response signature (S2). This is a fixed length field consisting of 2 data elements:





- The *Visa cash service identifier* (positions 1 - 3), a constant value of "SV:"
- The *load authorization signature* (positions 4 - 19) for this load operation

In load settlement advices, it contains the *Visa Cash Service Identifier* ("SV:") followed by the load completion signature (S3). This is a fixed length field consisting of 2 data elements:

- The *Visa cash service identifier* (positions 1 - 3), a constant value of "SV:"
- The *load completion signature* (positions 4 - 19) for this load operation

#### Field #45 - Track 1 Data

Field No	Format	Attr
48	LLVAR	ans..76

The information encoded on Track 1 of the magnetic stripe as defined in ISO 7813, including field separators but excluding the begin sentinel, end sentinel and longitudinal redundancy check characters.

Note that two structures are defined by ISO 7813, namely Structure A and Structure B. Structure A is reserved for proprietary use by card issuers, while Structure B is defined as follows:

Field	Length
Format Code	B (ASCII 66)
Primary account number	up to 19 digits
Field separator	1 character (ASCII 61 or 94)
Country Code	3 digits (or a field separator if not present)
Name	2 to 26 characters (this field is further described below)
Field separator	1 character (ASCII 61 or 94)
Expiry date (YYMM)	4 digits (or a field separator if not present)
Service restriction code	3 digits (or a field separator if not present)
Discretionary data	balance of available digits





The *primary account number, expiry date and service restriction code* fields are described in further detail under fields 2, 14 and 40 in this document.

The structure of the **Name** field is defined in the following table. Sub-fields are separated by means of a space character (ASCII 32). The minimum encoded data allowed is a single character followed by the surname separator.

Field	Notes
Surname	
Surname separator	ASCII 47
First Name or Initial	
Space	When required
Middle Name or Initial	
Period	When followed by Title; ASCII 46
Title	When used

The space character (ASCII 32) is required to separate the sub-fields of the **Name** field other than the surname. The separator terminating the surname should be encoded following the last sub-field of the **Name** field. If only the surname is encoded, it will follow the surname separator.

#### Field #48 - Additional Data

Field No	Format	Attr
48	LLVAR	ans...999

Used to provide linked account or mini-statement information for a linked account inquiry or a mini-statement inquiry.

#### Mini – statement Information

The format for field 48 when mini-statement data is to be sent downstream is as follows:





1. A mini-statement heading line, containing tags to identify the format of the mini-statement data lines that follows, e.g.

DATE\_TIME|SEQ\_NR|TRAN\_TYPE|TRAN\_AMOUNT~

The different fields of the mini-statement heading line are separated by bar characters ("|") and the line is terminated by a tilde character ("~").

2. One or more mini-statement data lines, each similar to the identifying string above in structure, but containing the actual transaction data to be printed per line, e.g.

19971201123123|001234|01|000000005000~

Below is a list of tags supported.

Field	Tag name	Format
Sequence number	SEQ_NR	<a href="#">n6</a>
Date and time	DATE_TIME	<a href="#">n14, CCYYMMDDhhmmss</a>
Terminal ID	TERM_ID	<a href="#">n8</a>
Transaction type	TRAN_TYPE	<a href="#">n2</a>
From account	FROM_ACC	<a href="#">n2</a>
To account	TO_ACC	<a href="#">n2</a>
Transaction amount	TRAN_AMOUNT	<a href="#">n12</a>
Account ID 1	ACC_ID1	<a href="#">ans28</a>
Account ID 2	ACC_ID2	<a href="#">ans28</a>
Authorization ID	AUTH_ID	<a href="#">n6</a>
Currency code	CURR_CODE	<a href="#">n3</a> (Currency code of the Transaction Amount field)





Surcharge                    SURCHARGE    [n8](#)

### Linked Account Inquiry

In the case of a linked account inquiry, this field contains information relating to the accounts linked to the card that initiated the transaction. The information for up to 20 accounts can be returned. Note that when "00" is specified as an account type in the original request, a list of all accounts linked to the card is retrieved, and not only the linked accounts of the default account type. The format of the information associated with each account is as follows:

Field	Length	Description
Account ID	28	The identifier uniquely identifying the account, left justified, space-filled.
Account type	2	The ISO 8583 account type of the account.
Currency code	3	The ISO numeric currency code of the account.
Ledger balance	13	The ledger balance of the account. The first character contains the sign. A "D" indicates a debit (negative) balance and a "C" indicates a credit (positive) balance.

### Field #49 - Currency Code, Transaction

Field No	Format	Attr
49		n 3





The local currency of the acquirer or source location of the transaction. This is the currency code used for the following amount fields:

- amount, transaction
- amount, transaction fee
- amount, transaction processing fee

#### Field #50 - Currency Code, Settlement

Field No	Format	Attr
50		n 3

A code identifying the currency of settlement. If this field is not present for a transaction, it is assumed that this field is the same as the currency code, transaction field. This is the currency code used for the following amount fields:

- amount, settlement
- amount, settlement fee
- amount, settlement processing fee
- amount, net settlement

#### Field #52 – PIN Data

Field No	Format	Attr
52		Hex16

The PIN data field contains the PIN (a number assigned to a cardholder intended to uniquely identify that cardholder) of the cardholder formatted into a 64-bit block and encrypted with a DES key.

#### Field #53 – Security Related Control Information

Field No	Format	Attr
53		Hex96

Identifies security management information used in the current transaction or specifies security management information to be used in future transactions.







In **PIN change** transactions, the first byte indicates the PIN to change:

- binary 0 – insecure PIN (e.g. telephone PIN)
- binary 1 – secure PIN (e.g. ATM PIN)

The following 8 bytes of this field contains the new PIN formatted into a 64-bit block and encrypted with a DES key.

In **key change** transactions, this field contains the encrypted key in the first 8-24 bytes (8 for single, 16 for double, 24 for triple length), followed by a 3-byte key check value (i.e. the first 3 bytes of a clear value of all zeroes encrypted with the key).

#### Field #54 – Additional Amounts

Field No	Format	Attr
54	LLVAR	an...120

Information on up to 6 amounts and related account data for which specific data elements have not been defined. Each amount is a fixed length field consisting of 5 data elements:

- [Account type](#) (positions 1 - 2)
- [Amount type](#) (positions 3 - 4)
- Currency code (positions 5 - 7)
- Amount sign (position 8) - "C" or "D"
- Amount (position 9 - 20)

When this field is sent by the entity that performed currency conversion this field should contain amounts in the transaction and settlement currencies if they differ.

In a response message from the NCS, this field will always contain the approved amounts and cash amounts, if applicable.





### Field #55 – Integrated Circuit Card System Related Data

Field No	Format	Attr
55	LLLVAR	ANS..510

This data element contains EMV data. This EMV data in this data element is structured in the following manner:

<2-or-4-character Tag><2-character length field><variable length data>

The 2-byte or 4-byte tag is an EMV tag (in hexadecimal format) that uniquely identifies the data content of the P-55 fields, and the 2-digit length field defines the length of the variable-length data that follows it. The length specifies the number of hexadecimal values represented in the data part, the actual string is twice as long as the length specifies. The format of the length field is binary converted to a hexadecimal string, e.g., 0x1F would be represented as "1F". A tag identifying the type of data, followed immediately by a two-digit length (LL) identifying the length of the data, followed immediately by the data itself.

The variable length data for a tag cannot exceed the maximum specified length specified for the data. When the variable length data is longer than the defined maximum length for the tag value, it is truncated. The following table describes each of the EMV tags that can be carried in the P-55 data element, the maximum length for each tag value, the transaction data elements (TDEs) to which each tag is mapped, and flags indicating whether the tag data is required (Y), optional (N), or not applicable (N/A) for requests and responses.





EMV Tag	Description	Max Length	TDE	Required	
				Request	Response
9F26	Authorization Request	H8	EMV Request	Y	N/A
9F27	Cryptogram Information Data	H1	EMV Request	Y	N/A
9F10	Issuer Application Discretionary data	32	EMV	Y	N/A
9F37	Unpredictable Number	H4	EMV Request	Y	N/A
9F36	Application Transaction Counter	H2	EMV Request	Y	N/A
95	Terminal Verification Result	H5	EMV Request	Y	N/A
9A	Transaction Date	H3	EMV Request	Y	N/A
9C	Transaction Type	H1	EMV Request	Y	N/A
9F02	Transaction Amount	H6	EMV Request	Y	N/A
5F2A	Transaction Currency Code	H2	EMV Request	Y	N/A
82	Application Interchange Profile	H2	EMV Request	Y	N/A
9F1A	Terminal Country Code	H2	EMV Request	Y	N/A
9F34	Cardholder Verification Method Results	H4	EMV Discretionary Data	N	N/A
9F33	Terminal Capabilities	H3	EMV Discretionary	N	N/A





			Data		
9F35	Terminal Type	H1	EMV Request	N	N/A
9F1E	Interface Device Serial Number	H8	EMV Discretionary Data	N	N/A
84	Dedicated File Name	H16	EMV Discretionary Data	N	N/A
9F09	Application Version Number	H2	EMV Discretionary Data	N	N/A
9F03	Amount, other	H6	EMV Request	N	N/A
5F34	Application PAN Sequence Number	H1	EMV Status	N	N
91	Issuer Authentication Data	H32	EMV Response	N/A	N
71	Issuer Script	H128	EMV Script	N/A	N
72	Issuer Script	H128	EMV Script	N/A	N
9F6E	Form Factor Indicator (FFI)	H4	EMV Request	N	N

**Field #56 – Message Reason Code**

Field No	Format	Attr
56	LLVAR	n..4

A code that provides the receiver of a request, advice or notification message with the reason, or purpose of that message.

For original authorizations and financial transactions, it identifies why the type of message was sent (e.g. why an advice versus a request); for other messages, it states why this action was taken.





- 1003 Card issuer unavailable
- 1006 Under floor limit
- 1376 PIN verification failure
- 1377 Change dispensed
- 1378 IOU receipt printed
- 1510 Over floor limit
- 1800 Negative card
- 4000 Customer cancellation
- 4001 Unspecified, no action taken
- 4004 Completed partially
- 4021 Timeout waiting for response

For *place hold on card* transactions, in *Issuer File Update Advice (0322)* or *Administration (0600/0620)* messages, it states why a card should be put on the hotcard list:

- 3000 Lost card
- 3001 Stolen card
- 3002 Undelivered card
- 3003 Counterfeit card
- 3700 Lost PIN

If a *hold response code* has not been specified in these transactions, the *message reason code* field will be used to determine which *hold response code* to use for the transaction.





A *message reason code* of "3001-Stolen card" will result in a *hold response code* of "43-Stolen card", otherwise "41-Lost card" will be used.

In the case of a *message to bank* transaction, the *message reason code* specifies the type of message the cardholder wants to forward to the issuer. Note that in this case, the *message reason code* field is treated as a free-format field that the user can use for any user specific code.

*Message reason codes* are defined in the *ISO 8583 (1993)* specification, and this specification has been used as basis for the codes defined here.

### Field #58 – Authorizing Agent Code

Field No	Format	Attr
59	LLVAR	n...11

A code identifying the authorizing agent institution.

### Field #59 – Echo Data

Field No	Format	Attr
59	LLVAR	ans...255

Contains data from the originator of the message that shall be returned unaltered in the response message





### Field #60 – Payment Information

Field No	Format	Attr
60	LLVAR	ans...999

This data element contains information relating to bills payments and token (recharge cards, tickets etc) purchases. This data element carries tagged data items. The tags defined for this data element are as listed in the table below:

Transaction Type	Tag	Description	Length	Presence Indicator	Request/Response
Payment for Bills	*41	Biller Identification Code	015	Mandatory	Request
	45	Product Identification Code		Conditional	
	**50	Customer Subscription Information		Mandatory	
	**50	Customer Subscription Information		Optional	Response
Purchase of Token (Recharge Card, ticket etc)	*41	Biller Identification Code	015	Mandatory	Request
	45	Product Identification Code		Conditional	
	**50	Customer Subscription Information (or products)		Optional	
	***51	Token (e.g. PIN or Voucher)		Conditional	Response
	**50	Customer Subscription Information		Optional	

### Field #62 – Private Field, Management Data 1

Field No	Format	Attr
62	LLVAR	ans...999





This data element carries tagged data items. The tags defined for this data element are listed in the table below. Tagged data items are structured in the following manner: a tag identifying the type of data, followed immediately by a three-digit length (LLL) identifying the length of the data, followed immediately by the data itself.

Tag + LLL + data.

Transaction Type	Tag	Description	Length	Request/Response
Terminal Parameter Download	01	POS/Payment Channel Serial Number		Request
	02	CTMS Date and Time	014	Response
	03	Card Acceptor Identification Code	015	
	04	Timeout (maximum time interval to wait for response – in seconds)	002	
	05	Currency Code	003	
	06	Country Code	003	
	07	Call home time (maximum time interval idleness for which a call – home must be done – in hours)	002	
	52	Merchant Name and Location	040	
	08	Merchant Category Code	004	
Call – Home	01	POS/Payment Channel Serial Number		Request
	09	POS/Payment Channel Application Version	003	
	10	POS Terminal/Payment Channel Model	020	
	11	Call – Home Merchant Information/Complaint/Comm		







		ents		
	12	Communications Service Provider		
Billers List Download	01	POS/Payment Channel Serial Number		Request
	*41	Biller Identification Code	015	Response
	42	Biller Name		
Billers Subscription Information Download	01	POS/Payment Channel Serial Number		Request
	*41	Biller Identification Code	015	
	43	Required Information Name		Response
	44	Default Value		
Product List Download	01	POS/Payment Channel Serial Number		Request
	*41	Biller Identification Code	015	
	45	Product Identification Code		Response
	46	Product Name		
	47	Product Amount	012	
Payment Validation	01	POS/Payment Channel Serial Number		Request
	*41	Biller Identification Code	015	
	***48	Payment Code		Response
	***49	Payment Validated Information		
Base Derivation Key (BDK) Request	01	POS/Payment Channel Serial Number		Request
	57	Key Serial Number	020	
Dynamic Currency Conversion	01	POS/Payment Channel Serial Number		Request
	58	Cardholder Preferred Currency	003	
	59	Local Country Currency	003	
	60	DCC Identification Code	015	Response
	58	Cardholder Preferred Currency	003	
	60	DCC Identification Code	015	
	61	Rate		





Note:

\*Tag 41: Biller Identification Code is in the format below:

1<sup>st</sup> position – transaction type the biller is setup for:

4 – Token (e.g. Recharge Card) Sales

5 – Bill Payments

2<sup>nd</sup> – 4<sup>th</sup> position – VAS Provider Code

5<sup>th</sup> – 8<sup>th</sup> position – Merchant Category Code

9<sup>th</sup> – 15<sup>th</sup> position – Unique Number identifying the Biller

\*\*Tag 50: Customer Subscription Information, if more than one, it should be separated by '|'|  
e.g. name=Halima Eze Ajayi|customerid=00001||prod1=3||prod2=4

From the example, name and customerid are values downloaded during Biller Subscription Information Download request and the values the customer entered are after the equals signs. prod1 and prod2 are products while values 3 and 4 after the equals signs are the quantities.

\*\*\*Tag 48: Payment Code and \*\*\*Tag 49: Payment Validated Information can be used interchangeably. Format is same as tag 50.

Note: For receipt printing of mCash Transactions on POS, send the Customer Information in the format of Tag 50 as above. For example:

SellerCode=0731170253|Phone=07069302232|RefNo=10012344546567|Amount=1000.23

\*\*\*\*51: Token, if more than one, should be separated by comma ','

### Field #63 – Private Field, Management Data 2

Field No	Format	Attr
63	LLLLVAR	ans...9999

This data element carries tagged data items. The tags defined for this data element are listed in the table below. Tagged data items are structured in the following manner: a tag identifying the type of data, followed immediately by a three-digit length (LLL) identifying the length of the data, followed immediately by the data itself. Each block of data is separated by "~".





Tag + LLL + data.

Transaction Type	Tag	Description	Length	Request/Response
EMV Application AID Download	01	POS/Payment Channel Serial Number		Request
	13	AID Index		Response
	14	Application Internal Reference Number		
	15	Application Identification Number (EMV AID)		
	16	Match	001	
	17	EMV Application Name		
	18	EMV Application Version		
	19	EMV Application Selection Priority		
	20	EMV DDOL		
	21	EMV TDOL		
	22	EMV TFL Domestic		
	23	EMV TFL International		
	24	EMV Offline Threshold Domestic		
	25	EMV Max Target Domestic		
	26	EMV Max Target International		
	27	EMV Target Percentage Domestic		
	28	EMV Target Percentage International		
	CA Public Key Download	01	POS/Payment Channel Serial Number	
32		Certificate Authority (CA) Key Index		Response





	33	CA Key Internal Reference Number		
	34	CA Key Name		
	35	EMV RID		
	36	Hash Algorithm		
	37	EMV CA PK Modulus		
	38	EMV CA PK Exponent		
	39	EMV CA PK Hash		
	40	Public Key Algorithm		
Daily Transaction Report Download	01	POS/Payment Channel Serial Number		Request
	53	Transaction Date and Time		Response
	54	Response Code		
	55	Amount		
	56	Transaction Type		

#### Field #64 – Primary Message Hash Value

Field No	Format	Attr
64	AN	64

This data element carries the hash value for the messages subject to no secondary data elements (DE65 through DE128) are included in the message. The algorithm is SHA-256. If the message contains secondary data elements, data element DE128 is used to carry the hash value. If the hash value is carried in data element DE128, data element DE64 is not included in the message.

#### Field #67 – Extended Payment Code

Field No	Format	Attr
67		n 2

The number of months that the cardholder prefers to pay for this item if permitted by the card issuer.





### Field #90 – Original Data Elements

Field No	Format	Attr
90		n 42

The data elements contained in the original message intended for transaction matching (e.g. to identify a transaction for correction or reversal). It is a fixed length field consisting of 5 data elements:

- Original message type (positions 1 - 4) - the message type identifier of the original message of the transaction being reversed.
- Original systems trace audit number (positions 5 - 10) – the system trace audit number of the original message.
- Original transmission date and time (positions 11 - 20) – the transmission date and time of the original message
- Original acquirer institution ID code (position 21 - 31) – the acquirer institution ID code of the original message (right justified with leading zeroes).
- Original forwarding institution ID code (position 32 - 42) – the forwarding institution ID code of the original message (right justified with leading zeroes).

### Field #95 – Replacement Amounts

Field No	Format	Attr
95		n 42

The corrected amounts of a transaction in a partial or full reversal (or the final amounts for the transaction). It is a fixed length field consisting of 4 data elements:

- Actual amount, transaction (positions 1 - 12) - the corrected, actual amount of the customer’s transaction, in the currency of the transaction.





- Actual amount, settlement (positions 13 - 24) - the corrected, actual amount of the customer's transaction, in the settlement currency.
- Actual amount, transaction fee (positions 25 - 33) - the corrected, actual amount of the fee (in format x + n8) for this customer transaction, in the currency of the transaction.
- Actual amount, settlement fee (positions 34 - 42) - the corrected, actual amount of the fee (in format x + n8) for this customer transaction, in the settlement currency.

#### Field #98 – Payee

Field No	Format	Attr
98		ans25

A code or ID identifying the payee (recipient) of a payment transaction. This field is used in a payment transaction when the payee is an Institution defined payee. Customer defined payees do not have a payee ID.

When using this field with the NCS Payments Engine, however, it contains the ID of the payee as maintained in the payee list for a cardholder. Because the Payments Engine assigns an ID to both institution and customer defined payees, this field can be used to refer to either type of payee.

#### Field #100 – Receiving Institution ID Code

Field No	Format	Attr
100	LLVAR	n...11

A code identifying the financial institution that should receive a request or advice. This identification code is used when it is not possible to route a message using the account





number field in the message, e.g. in a check verification message. When this field is included in a request or advice, it takes precedence over all account number fields for routing.

### Field #102 – Account Identification 1

Field No	Format	Attr
102	LLVAR	n..28

A series of digits and/or characters used to identify a specific account held by the cardholder at the card issuer and if present, shall remain unchanged for the life of the transaction. This field usually contains the description of the ["from" account](#).

### Field #103 – Account Identification 2

Field No	Format	Attr
103	LLVAR	n..28

A series of digits and/or characters used to identify a specific account held by the cardholder at the card issuer and if present, shall remain unchanged for the life of the transaction. This field usually contains the description of the ["to" account](#).

When used in payment transactions, this field specifies the bank account number of the payee.

### Field #123 – POS Data Code

Field No	Format	Attr
123	LLLVAR	an15

The field is used to identify terminal capability, terminal environment and presentation security data. It is used to indicate specific conditions that were present at the time a





transaction took place at the Point-of-Service. This field consists of the following sub-fields:

- The card data input capability (position 1) of the terminal.  
Possible values are:
  - 0 – Unknown
  - 1 – Manual, no terminal
  - 2 – Magnetic Stripe
  - 3 – Barcode
  - 4 – OCR
  - 5 – Magnetic Stripe, Key Entry and ICC
  - 6 – Key Entry
  - 7 – Magnetic Stripe and Key Entry
  - 8 – Magnetic Stripe and ICC
  - 9 – ICC
  - A – Contactless ICC
  - B – Contactless Magnetic Strip
- The cardholder authentication capability (position 2) of the terminal.  
Possible values are:
  - 0 – No electronic authentication
  - 1 – PIN
  - 2 – Electronic signature analysis
  - 3 – Biometric
  - 4 – Biographic
  - 5 – Electronic authentication inoperative
  - 6 – others
- The card capture capability (position 3) of the terminal.







Possible values are:

0 – None

1 - Capture

- The operating environment (position 4) of the terminal.

Possible values are:

0 – No terminal use

1 – On premise of card acceptor, attended

2 – On premise of card acceptor, unattended

3 – Off premise of card acceptor, attended

4 – Off premise of card acceptor, unattended

5 – On premise of cardholder, unattended

- Indicates whether the cardholder is present (position 5).

Possible values are:

0 – Cardholder present

1 – Cardholder not present, unspecified

2 – Cardholder not present, mail order

3 – Cardholder not present, telephone

4 – Cardholder not present, standing authorization/recurring transaction

5 – Cardholder not present, electronic order

- Indicates whether the card is present (position 6)

Possible values are:

0 – Card not present

1 – Card present

- The actual card data input mode (position 7) of the transaction

Possible values are:

0 – Unknown





- 1 – Manual, no terminal
- 2 – Magnetic Stripe
- 3 – Barcode
- 4 – OCR
- 5 – ICC
- 6 – Key Entry
- 7 – Contactless, ICC
- 8 – Contactless, magnetic stripe
- The actual cardholder authentication method (position 8) of the transaction.  
Possible values are:
  - 0 – no electronic authentication
  - 1 – PIN
  - 2 – Electronic signature analysis
  - 3 – Biometric
  - 4 – Biographic
  - 5 – Manual
  - 6 – Others
- The cardholder authentication entity (position 9) of the transaction  
Possible values are:
  - 0 – not authenticated
  - 1 – ICC
  - 2 – Terminal
  - 3 – Authorizing agent
  - 4 – Merchant
  - 5 – Others
- The card data output capability (position 10) of the terminal.





Possible values are:

- 0 – Unknown
- 1 – None
- 2 – Magnetic Stripe write
- 3 – ICC

- The terminal output capability (position 11) of the terminal.

Possible values are:

- 0 – Unknown
- 1 – None
- 2 – Printing
- 3 – Display
- 4 – Printing and display

- The PIN capture capability (position 12) of the terminal.

- 0 – No PIN capture capability
- 1 – Device PIN capture capability unknown
- 4 – Four characters
- 5 – Five characters
- 6 – Six characters
- 7 – Seven characters
- 8 – Eight characters
- 9 – Nine characters
- A – Ten characters
- B – Eleven characters
- C – Twelve characters

- The terminal operator (position 13).

- Possible values are:





- 0 – Customer operated
- 1 – Card acceptor operated
- Terminal Type (position 14 and 15)
  - 00 – Administrative Terminal
  - 01 – POS
  - 02 – ATM
  - 03 – Home Terminal
  - 90 – E – commerce – no encryption (no authentication)
  - 91 – E – commerce – FET/3D Secure Encryption: cardholder certificate not used (non authentication)
  - 92 – E – commerce – FET/3D Secure Encryption: cardholder certificate used (authentication)
  - 93 – E – commerce – FET/3D Secure Encryption: Chip Cryptography used: cardholder certificate not used
  - 94 – E – commerce – FET/3D Secure Encryption: cardholder certificate used
  - 95 – E – commerce – FET/3D Secure Encryption: channel encryption (SSL): cardholder certificate not used (non – authentication)
  - 96 – E – commerce – FET/3D Secure Encryption: Chip cryptography used: cardholder certificate not used
  - 21 – Smart Phone
  - 16 – Vending
  - 15 – Public Utility
  - 13 – Franchise Teller
  - 09 – Coupon Machine
  - 07 – Fuel Machine





### Field #124 – Near Field Communication Data

Field No	Format	Attr
124	LLLLVAR	ans...9999

This data element carries NFC Data. This would be transmitted to the processing system as received from POS Terminal.

### Field #128 – Secondary Message Hash Value

Field No	Format	Attr
128	AN	64

This data element carries the message hash value for the message, subject to at least one other secondary data element (DE65 through DE128) being included in the message. The algorithm is SHA-256.

If the message does not contain at least one other secondary data element, the hash value is placed in data element DE64.





## 5. Key Management

This section discusses how keys are managed between POS Terminals or other Payment Channels. The system has support for Master Key Session and Derived Unique Key Per Transaction (DUKPT).

For Master Key session, the following are the keys to be exchanged:

- 1. Clear Terminal Master Key (CTMK):** This key is transmitted in clear form and injected into the POS Terminal or other Payment Channels. This can be generated for a group of POS Terminals. A group could be a logical grouping by Payment Terminal Service Provider (PTSP) or Merchant Acquirers.
- 2. Encrypted Terminal Master Key (TMK):** This key is transmitted in encrypted form to the POS Terminal or other Payment Channels. This is not injected into terminal manually. This is requested for online by the POS Terminal when it is being setup or if it is suspected that the key has been compromised. TMK is encrypted with CTMK.
- 3. Encrypted Terminal PIN Key (TPK):** This key is usually transmitted in encrypted form to the POS Terminal or other Payment Channels. This is not injected into the terminal manually. POS terminal requests online for this key at predefined time from the CTMS. TPK is encrypted with the TMK. At transaction, this key is used to encrypt the PIN block if it is sent in the message.
- 4. Encrypted Terminal Session Key (TSK):** This key is usually transmitted in encrypted form to the POS Terminal or other Payment Channels. This is not injected into terminal manually. POS Terminal requests online for this key at predefined time from the CTMS. TSK is encrypted with TMK.





At transaction, this key is used for seeding the algorithm for generating hash value in DE64 or DE128.

For DUKPT, the following are the keys to be exchanged:

1. **Clear Terminal Master Key (CTMK):** This key is transmitted in clear form and injected into the POS Terminal or other Payment Channels. This can be generated for a group of POS Terminals. A group could be a logical grouping by Payment Terminal Service Provider (PTSP) or Merchant Acquirers.
2. **Encrypted Terminal Master Key (TMK):** This key is transmitted in encrypted form to the POS Terminal or other Payment Channels. This is not injected into terminal manually. This is requested for online by the POS Terminal when it is being setup or if it is suspected that the key has been compromised. TMK is encrypted with CTMK.
3. **Base Derivation Key (BDK):** This key is NOT transmitted to the POS Terminal. In clear form it is injected into the POS Terminal or other Payment Channels in two components manually. This can be generated for a group of POS Terminals.
4. **Encrypted Terminal Session Key (TSK):** This key is usually transmitted in encrypted form to the POS Terminal or other Payment Channels. This is not injected into terminal manually. POS Terminal requests online for this key at predefined time from the CTMS. TSK is encrypted with TMK. At transaction, this key is used for seeding the algorithm for generating hash value in DE64 or DE128.
5. **Encrypted Initial PIN Encryption Key (IPEK) for Track 2 Data:** This key is usually transmitted in encrypted form to the POS Terminal or other





Payment Channels. This is not injected into terminal manually. POS Terminal requests online for this key at predefined time from the CTMS. IPEK is encrypted with TMK.

- 6. Encrypted Initial PIN Encryption Key (IPEK) for EMV:** This key is usually transmitted in encrypted form to the POS Terminal or other Payment Channels. This is not injected into terminal manually. POS Terminal requests online for this key at predefined time from the CTMS. IPEK is encrypted with TMK.

**NOTE:**

- All Data Elements (Fields) received from the POS for all transaction types should be forwarded to NCS.

