



TranzWare Online

TranzWare ISO8583 Terminal Protocol (TITP)

May 4, 2012

Table of Contents

| | |
|---|-----------|
| 1. Overview | 8 |
| 2. Terminal-to-Host Communication | 9 |
| 3. Message Format..... | 10 |
| 4. Message Type Identifier (MTI) | 12 |
| 5. List of Fields | 13 |
| 6. Fields Usage in Different Messages | 15 |
| 7. Fields Definition | 16 |
| 7.1 P-0 PRIMARY BITMAP | 16 |
| 7.2 P-1 SECONDARY BITMAP | 17 |
| 7.3 P-2 PAN | 18 |
| 7.4 P-3 PROCESSING CODE | 19 |
| 7.5 P-4 TRANSACTION AMOUNT | 22 |
| 7.6 P-11 SYSTEM TRACE AUDIT NUMBER | 23 |
| 7.7 P-12 LOCAL (TERMINAL) TRANSACTION TIME | 24 |
| 7.8 P-13 LOCAL (TERMINAL) TRANSACTION DATE | 25 |
| 7.9 P-14 DATE, EXPIRATION | 26 |
| 7.10 P-22 POS ENTRY MODE | 27 |
| 7.11 P-23 CARD SEQUENCE NUMBER | 28 |
| 7.12 P-25 POS CONDITION CODE | 29 |
| 7.13 P-35 TRACK 2 | 30 |
| 7.14 P-37 RETRIEVAL REFERENCE NUMBER | 31 |
| 7.15 P-38 AUTHORIZATION IDENTIFICATION RESPONSE | 32 |
| 7.16 P-39 RESPONSE CODE | 33 |
| 7.17 P-41 CARD ACCEPTOR TERMINAL ID | 35 |
| 7.18 P-42 CARD ACCEPTOR ID CODE | 36 |
| 7.19 P-45 TRACK 1 | 37 |
| 7.20 P-48 WORKING KEYS | 38 |
| 7.21 P-49 TRANSACTION CURRENCY CODE | 39 |
| 7.22 P-52 PIN | 40 |
| 7.23 P-54 EXTRA AMOUNTS | 41 |
| 7.24 P-55 ICC SYSTEM RELATED DATA | 42 |
| 7.25 P-57 ADDITIONAL DATA | 44 |
| 7.26 P-59 DETAIL ADDENDA | 50 |
| 7.26.1 Additional Data on VISA Fleet Cards | 51 |
| 7.27 P-60 PRIVATE USE | 53 |
| 7.27.1 Batch Number | 54 |
| 7.27.2 Original Message Data | 55 |
| 7.27.3 Original Amount | 56 |
| 7.27.4 Cashback Amount | 57 |
| 7.28 P-62 PRIVATE USE | 58 |
| 7.28.1 Invoice Number | 59 |
| 7.28.2 Working Keys | 60 |
| 7.28.3 Working EWK | 61 |
| 7.29 P-63 PRIVATE USE | 62 |
| 7.29.1 Extra Data in Request | 62 |
| 7.29.1.1 CVV2 | 62 |
| 7.29.1.2 DUK/PT Key Serial Number | 63 |
| 7.29.1.3 DUKPT Key Serial Number 2 | 63 |
| 7.29.1.4 DUKPT Key Serial Number 3 | 64 |
| 7.29.1.5 Additional Data | 64 |
| 7.29.1.6 Reserved for Future Use | 65 |

| | | |
|------------|---|-----------|
| 7.29.2 | Data in Response to Terminal | 66 |
| 7.29.2.1 | Balance Inquiry | 66 |
| 7.29.2.2 | Extra Information | 66 |
| 7.29.3 | Reconciliation Request Totals | 68 |
| 7.30 | P-64 MAC | 69 |
| 8. | Message Exchange Algorithm | 70 |
| 8.1 | FINANCIAL ONLINE TRANSACTIONS | 70 |
| 8.2 | TOTALS RECONCILIATION | 71 |
| 9. | Traffic Encryption | 72 |
| 10. | Recommendations on Chip Card Transactions Processing | 73 |
| 10.1 | RECOMMENDATIONS ON PROCESSING OF CONTACTLESS CARD TRANSACTIONS..... | 74 |

1. Overview

The document describes the TITP protocol designed for communication between the POS terminals (other similar devices) and systems with host supporting TranzWare Online (hereinafter - **TWO**) and TranzAxis. The protocol is based on ISO8583.

The part initiating request to TWO is referred to as *terminal, device, POS* and *POS terminal*. The service receiving requests from the terminal and responding is referred to as *server, host, driver* or *TWO*.

2. Terminal-to-Host Communication

When performing the financial transactions and administrative operations, the terminal exchanges messages with host. The connection is established/broken on the terminal initiative. The host connects to terminal either directly or via the network hub. In the first case, the terminal holds a connection during a transaction, in the latter case, the connection can be held permanently.

The exchange protocol includes one or several pairs of messages: terminal request and host response. The messages are transferred as packets incorporating message body and framing. The format of message body is based on ISO 8583. The frames allow to separate packets. TWO host supports several framing methods described in the document **Frame.doc**.

3. Message Format

A message consists of the elements of various format and length. The table below provides the message element formats:

| Legend | Description |
|--------|---|
| A | English characters (a-z, A-Z). Each character is 1-byte. |
| n | Digits (0-9). Each character is 1-nibble in the BCD encoding. |
| an | Alphabetic characters and digits (0-9, a-z, A-Z). Each character is 1-byte. |
| ans | Alphabetic characters, digits and special characters (all ASCII characters within the range from 20h to 7Eh). Each character is 1 byte. |
| b | Binary data. Each character is 1-byte. |
| z | Track 2 data read from the magnetic stripe. Each character is 1-nibble. |
| MM | Month |
| DD | Day |
| YY | Year |
| hh | Hour |
| mm | Minutes |
| ss | Seconds |

The element length can be either fixed or variable. In the latter case, the element length is of one or two bytes (if the element max length exceeds 99) in BCD encoding.

The field length is shown as follows:

n5 – figure including 5 decimal digits

ans..16 – string including not more than sixteen characters

Message Structure

| Description | Terminal Name (see below) | Header (see below) | Message Type Identifier (MTI) | Bit Map | Data Elements |
|-------------|------------------------------|-----------------------|----------------------------------|---------|---------------|
| Format | ans8 | b5 | n4 | b8 | ... |

Terminal Name

It contains the terminal unique name and transferred only if the message is encrypted, see p. 9 Traffic Encryption.

Header

The Header length is 5 bytes, its contents are neither analyzed nor used by the host. In the host response, the first byte from the request remains unchanged, whereas the 2nd and 3rd bytes are swapped with the 4th and 5th.

4. Message Type Identifier (MTI)

Format: n4

The *Message Type Identifier* (message type) parameter is a set of 4 digits, where the first pair of digits stands for the message class and the second one - for the message transfer mode.

The message type is mandatory for all the messages.

The table below lists all the available types of messages:

| Transaction Type Identifier | Description |
|-----------------------------|--|
| 0100 | Authorization Request |
| 0110 | Authorization Request Response |
| 0200 | Financial Transaction Request |
| 0210 | Financial Transaction Request Response |
| 0220 | Financial Transaction Advice |
| 0230 | Financial Transaction Advice Response |
| 0320 | Batch Upload Request |
| 0330 | Batch Upload Response |
| 0400 | Reversal Advice |
| 0410 | Reversal Advice Response |
| 0500 | Settlement Request |
| 0510 | Settlement Response |
| 0800 | Network Management Request |
| 0810 | Network Management Request Response |

5. List of Fields

| Field | Format | Description | Respective Field of the TWO Transactions Log |
|-------|----------|---------------------------------------|--|
| P-0 | b8 | Primary Bitmap | |
| P-1 | b8 | Secondary Bitmap | |
| P-2 | n ..19 | Primary Account Number | PAN |
| P-3 | n6 | Processing Code | |
| P-3.1 | n2 | Transaction Code | TRANCODE |
| P-3.2 | n2 | Debit Account Type | FROMACCTTYPE |
| P-3.3 | n2 | To Account Type | TOACCTTYPE |
| P-4 | n12 | Transaction Amount | AMOUNT |
| P-11 | n6 | System Trace Audit Number | |
| P-12 | n6 | Local (Terminal) Transaction Time | ORIGTIME |
| P-13 | n4 | Local (Terminal) Transaction Date | ORIGTIME |
| P-14 | n4 | Date, Expiration | |
| P-22 | n3 | POS Entry Mode | POSENTRYMODE |
| P-23 | n3 | Card Sequence Number | CARDMEMBER |
| P-25 | n2 | POS Condition Code | POSCONDITION |
| P-35 | z ..37 | Track 2 Data | TRACK2 |
| P-37 | ans12 | Retrieval Reference Number | TRANNUMBER |
| P-38 | ans6 | Authorization Identification Response | APPROVALCODE |
| P-39 | n2 | Response Code | RESPCODE |
| P-41 | ans8 | Card Acceptor Terminal Identification | TERMNAME |
| P-42 | ans15 | Card Acceptor Identification Code | |
| P-45 | ans ..76 | Track 1 Data | TRACK1 |
| P-48 | b34 | Working Keys | |
| P-49 | an3 | Transaction Currency Code | CURRENCY |
| P-52 | b8 | Personal Identification Number | PIN |
| P-54 | an ..120 | Additional Amounts | |
| P-55 | b ..255 | ICC System Related Data | ICC_APPPROFILE ICC_TVR ICC_TRANDATE ICC_TRANSTYPE ICC_CURRENCY ICC_AMOUNT |

| Field | Format | Description | Respective Field of the TWO Transactions Log |
|-------|------------|-----------------|---|
| | | | ICC_CBAMOUNT ICC_ISSUERDATA ICC_TERMCOUNTRY ICC_TERMSN ICC_CRYPTOGRAM ICC_CRYPTINFORMDATA ICC_TERMCAPS ICC_APPTRANCOUNT ICC_RANDOM ICC_TERRMTRANCOUNT ICC_ISSUERSSCRIPT1 ICC_ISSUERSSCRIPT2 ICC_IAD ICC_CARDMEMBER ICC_ISSUERSSCRIPTRESULTS |
| P-57 | ans ..999 | Additional Data | |
| P-59 | ans ..4000 | Detail Addenda | DETAILADDENDA |
| P-60 | ans ..999 | Private Use | |
| P-62 | ans ..999 | Private Use | |
| P-63 | ans ..999 | Private Use | |
| P-64 | b8 | MAC | |

6. Fields Usage in Different Messages

- M – mandatory
C – conditionally
O – optionally
ME – mandatory echo
CE – conditional echo
OE – optional echo

| Field | 100 | 110 | 200 | 210 | 220 | 230 | 320 | 330 | 400 | 410 | 500 | 510 | 800 | 810 |
|-------|-----|----------|-----|----------|-----|---------|-----|-----|-----|-----|-----|-----|-----|----------|
| P-2 | C | CE | C | CE | C | | | | C | CE | | | | |
| P-3 | M | ME | M | ME | M | ME | M | ME | M | ME | M | ME | M | ME |
| P-4 | M | ME | C | CE C | C | CE | C | CE | | | | | | |
| P-11 | M | ME | M | ME | M | ME | M | ME | M | ME | M | ME | M | ME |
| P-12 | C | CE, M | C | CE, M | C | | M | ME | C | CE | | M | O | OE, M |
| P-13 | C | CE,M | C | CE, M | C | | M | ME | C | CE | | M | O | OE, M |
| P-14 | C | C | C | | C | | M | ME | | - | | | | |
| P-22 | M | | M | | M | | M | ME | | - | | | | |
| P-23 | C | CE | C | CE | C | CE | | | | | | | | |
| P-25 | M | | M | | M | | M | ME | | - | | | | |
| P-35 | C | | C | | C | | | | C | - | | | | |
| P-37 | | M | C | CE M | C | CE M | C | | | C | | C | | |
| P-38 | | C | C | C | C | C | C | | | | | | | |
| P-39 | | M | C | M | M | M | | M | C | M | | M | | M |
| P-41 | M | ME | M | ME | M | ME | M | ME | M | ME | M | ME | M | ME |
| P-42 | O | | O | | O | | O | | | | | | | |
| P-48 | | C | | C | | C | | | | C | | | | |
| P-49 | C | CE | C | CE | C | CE | | | O | OE | | | | |
| P-52 | C | CE | C | CE | | | | | | | | | | |
| P-54 | C | | C | | C | | | | C | CE | | | | |
| P-55 | C | C | C | C | C | C | | | C | C | | | | |
| P-57 | C | C | C | C | C | C | | | | | | | | |
| P-60 | C | | C | | C | | M | | | | M | | | |
| P-62 | C | | C | | C | | | | C | CE | | | | C |
| P-63 | C | C | C | C | C | C | | | | | C | | | |
| P-64 | C | C | C | C | C | C | C | C | C | C | C | C | | |

7. Fields Definition

7.1 P-0 Primary Bitmap

Format: b8

Bitmap consists of 64 bits, each of them indicating the presence (bit=1) or absence (bit=0) of message elements described below.

Primary Bitmap is present in all the messages.

7.2 P-1 Secondary Bitmap

Format: b8

The second bitmap.

It is never used.

7.3 P-2 PAN

Format: n ..19

Card number.

If PAN contains odd number of characters, the field is right-padded with “F”, e.g. 1234567F.

7.4 P-3 Processing Code

Format: n6

The first two digits stand for the transaction code (Processing Code).

| Processing Code | MTI | Transaction |
|-----------------|---------------|--|
| 00 | 0100 | Pre-Purchase |
| | 0200 | Purchase if P-37 is absent Pre-Purchase Complete if P-37 is present |
| | 0220 | Offline Purchase if P-37 is absent Pre-Purchase Complete if P-37 is present |
| 01 | 0200, 0220 | Cash Advance |
| 02 | 0200 | Void |
| | 0220 | Offline Void if P4=0 Adjust purchase or adjust cash advance, if P4>0 |
| 03 | 0200, 0220 | Void if P4=0 Adjust Purchase or Adjust Cash Advance if P4>0 |
| 09 | 0200 | Purchase with Cashback |
| 11 | 0200, 0220 | Quasi Cash |
| 17 | 0200, 0220 | Cash Advance |
| 20 | 0200, 0220 | Merchandize Return |
| 21 | 0200, 0220 | Deposit |
| 22 | 0200 | Void |

| Processing Code | MTI | Transaction |
|--------------------------------|---------------|--|
| | 0220 | Offline Void if P4=0 Adjust Merchandize Return /Deposit if P4>0 |
| 30 | 0100 | In protocol v.1 - Card Verification In protocol v.2 and later versions - Pre-Purchase |
| 31 | 0100, 0200 | Balance Inquiry |
| 33 | 0200, 0220 | Void if P4=0 Adjust Merchandize Return /Deposit if P4>0 |
| 34 | 0200 | Statement Request |
| 38 | 0100, 0200 | Card Verification |
| 40 | 200, 220 | Transfer |
| 50 | 0200, 0220 | Payment |
| 53 | 0200, 0220 | Prepaid |
| 61 | 0200 | P2P Card Transfer |
| 62 | 0200, 0220 | P2P Cash Transfer |
| 63 | 0200 | P2P Transfer Calc Fee |
| 70 | 200 | PIN Change |
| As in the original transaction | 0320 | Batch Upload |
| As in the original transaction | 0400 | Previous Transaction Reversal |
| 92 | 0500 | Settlement Request |
| 97 | 0500 | Cutover Request (a terminal proceeds to the next business day) |
| 96 | 0500 | Settlement after Upload |

| Processing Code | MTI | Transaction |
|-----------------|------|--|
| 92 | 0800 | New Working Keys Inquiry from the Host |
| 95 | 0800 | New Working Key for traffic encryption inquiry |
| 99 | 0800 | Echo test (request for connection check) |

The third and the fourth digits of the P-3 stand for the account type:

- 00 – default account
- 10 – savings account
- 20 – current (checking) account
- 30 – credit account

For the Transfer transaction, the 5th digit stands for the type of transfer destination account (To Account):

- 0 – default account
- 1 – savings account
- 2 – current (checking) account
- 3 – credit account

The 6th digit of the P-3 in the host response to the terminal can be equal to 4, thus enforcing the terminal to perform initialization.

7.5 P-4 Transaction Amount

Format: n12

Includes the transaction amount with the acquiring fee (if the terminal calculates the acquiring fee) in the transaction minor currency units (field P-49).

For the adjustment transactions, it contains the transaction adjusted amount.

For the partial reversal and partial void transactions, it contains reversal amount.

In the host response to the balance request, it contains the available balance.

7.6 P-11 System Trace Audit Number

Format: n6

The message number assigned by the terminal increases with each message. In the reversal, this field value matches the one of the original transaction. In the host response, the field value matches the one of the respective request.

7.7 P-12 Local (Terminal) Transaction Time

Format: n6 (HHMMSS)

Includes the terminal local time.

7.8 P-13 Local (Terminal) Transaction Date

Format: n4 (MMDD)

Includes the local date of terminal initiated a transaction.

7.9 P-14 Date, Expiration

Format: n4 (YYMM)

Card expiration date. The field is used in case Track I and Track II data are absent.

7.10 P-22 POS Entry Mode

Format: n3

The first two digits indicate the card data entry mode:

- 01 – Manual
- 02 – Magnetic stripe
- 05 - ICC read
- 07 – ContactlessEMV
- 09 – Magnetic stripe
- 80 – EMV Fallback transaction
- 90 – Magnetic stripe
- 91 – ContactlessMSD

The third digit indicates the PIN entry facility at the current terminal:

- 1 – PIN can be entered
- 2 – PIN cannot be entered.

7.11 P 23 Card Sequence Number

Format: n3

Includes the card member number (MBR).

7.12 P-25 POS Condition Code

Format: n2

Includes a code indicating the transaction conditions:

- 00 – normal
- 03 - merchant suspicious
- 05 - card not present
- 08 - mail/phone order

7.13 P-35Track 2

Format: z ..37

Includes the information from the second track of the card magnetic stripe (originator), to the exclusion of the start and end sentinels and LRC. It is allowed to use '=' or 'D' as a separator.

If Track2 includes odd number of characters, the field is right-padded with "F", e.g. 12345678901234=041210111234F.

7.14 P-37 Retrieval Reference Number

Format: ans12

Includes the transaction identifier assigned by host. The value in the void request must match the one in the source transaction.

7.15 P-38 Authorization Identification Response

Format: ans6

Includes the response identification code (approval code) assigned by the authorization institution to the approved transaction.

Request:

It is present for the *Pre-Purchase Complete* transactions and indicates approval code of the original *Pre-purchase* transaction; it is also recommended for the approved transaction of the type 220 (Financial Transaction Advice).

Response:

It is present for any approved transactions.

7.16 P-39 Response Code

Format: ans2

Includes the authorizer response code.

The table provides a list of the available codes transferred to the terminal.

| Code | Description |
|------|--|
| 00 | Approved |
| 01 | Contact card issuer |
| 03 | Format error |
| 05 | External decline |
| 12 | Invalid transaction |
| 13 | Merchant limit exceeded |
| 14 | Invalid track 2 |
| 30 | Invalid format |
| 41 | Lost card |
| 43 | Stolen card |
| 51 | Insufficient funds |
| 54 | Expired card |
| 55 | Invalid PIN, PIN tries exceeded |
| 58 | Invalid processing code |
| 62 | Invalid MAC |
| 78 | Original request not found |
| 81 | Wrong format of customer information field (Invalid format of the payment information field) |
| 82 | Prepaid Code not found (Prepaid-code to the defined amount is not found) |
| 89 | Invalid terminal id. |
| 91 | Destination not available |
| 94 | Duplicate transmission |
| 96 | System error |

The field can be present in the offline-request in order to transfer the transactions declined offline to host.

Response code transmitted to terminal in case the card must be captured is specified on host. It can contain the void reason in the reversals and Transaction Void requests (VOID). The table provides a list of available values:

| Code | Description |
|------|--|
| 01 | Timeout. The terminal generates such reversal if it does not receive the response to the previous request. |
| 08 | Reversal at the request of customer. |
| 10 | Reversal initiated by the terminal in case of terminal technical fault. |

| Code | Description |
|------|--|
| 20 | Reversal performed due to the high risk of fraud operation (Fraud Alert). |
| 21 | Reversal initiated by the terminal in case the received response contains invalid MAC. |

7.17 P-41 Card Acceptor Terminal ID

Format: ans ..8

Includes the terminal unique name.

7.18 P-42 Card Acceptor ID Code

Format: ans15

Includes the terminal unique code.

7.19 P-45 Track 1

Format: ans ..76

Includes the information from the first track of the card magnetic stripe (originator), to the exclusion of the start and end sentinels and LRC.

7.20 P-48 Working Keys

Format: b34

It is used to transfer the working keys to the terminal. The field may be present in the response to the request sent from the terminal in case MAC verification was not successful.

| Subfield | Format | Size (byte) | Value |
|----------|--------|-------------|------------------------------------|
| Length | B2 | 2 | '0x00 0x32' |
| MAC | b16 | 16 | Cryptogram of new working MAC key. |
| PIN | b16 | 16 | Cryptogram of new working PIN key. |

Single-length working keys (8 bytes) are right-padded with binary zeros up to 16 bytes.

E.g.:

For the single-length key (hex): b5 cb 01 f2 35 0d aa 0b,

b5 cb 01 f2 35 0d aa 0b 00 00 00 00 00 00 00 00 will be transmitted to the terminal.

If PIN keys are not used, the PIN subfield transfers ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff (hex) to the terminal.

7.21 P-49 Transaction Currency Code

Format: an3

Includes ISO numeric code of the transaction currency. If the field is empty, code from the host settings is applied.

7.22 P-52 PIN

Format: b 8

Includes PIN-block cryptogram.

PIN-block format: ANSI X9.8 (ISO Format 0).

7.23 P-54 Extra Amounts

Format: an ..120

Includes the acquiring fee amount in the transaction currency (P-49).

Negative fee ("-" precedes the amount) stands for the acquiring bonus.

If it is present in the original transaction, it is mandatory for the partial reversal and partial void transactions and it must contain the amount of the fee being returned. E.g.:

For the original transaction to the amount of 100.00 USD with the fee 1.00 USD (1% of the amount), the terminal should send the following data:

F4='000000010100' (transaction amount with the fee)

F49=840 (transaction currency is USD)

F54='000000000100' (fee amount)

If the transaction actual amount is 80.00 USD, the terminal should send a partial void containing the following data:

F4='000000002020' (reversal amount with the fee)

F49=840 (transaction currency is USD)

F54='000000000020' (amount of the fee being returned)

7.24 P-55 ICC System Related Data

Format: b ..255

The data related to EMV transactions are packed in compliance with BER-TLV standard. Transaction EMV tags requirements are provided in the documentation **EMV2000**).

| Message Type | Tag | Length, bytes | Value |
|--------------|------|---------------|---------------------------------|
| REQUEST | 9F26 | 8 | Application Cryptogram |
| | 9F27 | 1 | Cryptogram Info Data |
| | 9F10 | ..32 | Issuer Application Data |
| | 9F37 | 4 | Unpredictable Number |
| | 9F36 | 2 | ATC |
| | 95 | 5 | TVR |
| | 9A | 3 | Transaction Date |
| | 9C | 1 | Transaction Type |
| | 9F02 | 6 | Transaction Amount |
| | 5F2A | 2 | Transaction Currency Code |
| | 5F34 | 1 | Application Sequence Number |
| | 82 | 2 | Application Interchange Profile |
| | 9F1A | 2 | Terminal Country Code |
| | 9F03 | 6 | Amount Other |
| | 9F33 | 3 | Terminal Capabilities |
| | 4F | 5..16 | Application ID |
| | 9F08 | 2 | Application Version Number |
| | 9F34 | 3 | CVM Results |
| | 9F35 | 1 | Terminal Type |
| | 9F1E | 8 | IFD Serial Number |
| | 9F53 | 1 | Transaction Category Code |

| Message Type | Tag | Length, bytes | Value |
|--------------|------|---------------|--|
| | 84 | 5..16 | Dedicated File Name |
| | 9F09 | 2 | Terminal Application Version Number |
| | 9F41 | 2..4 | Transaction Sequence Counter |
| | 9F5B | ..20 | Issuer Script Results Transmitted in the reversals only. |
| | 8A | 2 | ISO Authorization Response Code Transmitted in the Offline transactions only. |
| RESPONSE | 91 | 8..16 | Issuer Authentication Data |
| | 71 | ..127 | Issuer Script Template 1 |
| | 72 | ..127 | Issuer Script Template 2 |
| | 8A | 2 | ISO Authorization Response Code |

7.25 P-57 Additional Data

Format: ans ..999

It is used by the terminal and host to transfer the transaction additional data. For the protocol v.3, it is not transferred in the host responses.

The field can include one or several subfields. Each subfield has own identifier of length and subfield type, thus enabling to extend a list of subfields without violating the field parsing rules.

Subfield format:

Subfield Length n3 - length of the subfield including the Subfield ID ('LLL' – ASCII) length

Subfield ID n2 - subfield identifier (ASCII)

Subfield body ans..999 - subfield contents

| Subfield ID | Format | Size | Description |
|-------------|----------|-----------------|--|
| 10 | ANS..30 | Up to 30 bytes | To Account – destination account, in payment transaction – vendor account, in Prepaid – Prepaid-provider account, in Transfer transaction – transfer destination account |
| 12 | ANS..900 | Up to 900 bytes | Personal Payment Information – payment details entered by the cardholder (e.g.: phone number). It may include several '/'-separated fields (e.g.: '12345/6789/111') |
| 15 | ANS..100 | Up to 100 bytes | Prepaid code to be printed on an invoice. It is posted in the response to the Prepaid transaction. Format: Code1[/Code2]. |
| 21 | ans..250 | Up to 250 bytes | From Account Description – description of the source account. If present, it is posted in response to a transaction. |
| 22 | ans..250 | Up to 250 bytes | To Account Description – description of the destination account. If present, it is posted in response to a transaction. |
| 23 | ans..30 | Up to 30 bytes | From Account – source account number. If present, it is posted in response to a transaction. |
| 24 | ans..30 | Up to 30 bytes | To Account – destination account number. If present, it is posted in response to a transaction. |
| 30 | a1 + n12 | 13 bytes | Acquiring fee amount in the transaction currency. If present, it is posted in response to a transaction. The first character is D or C: <ul style="list-style-type: none"> D – fee amount to be debited |

| Subfield ID | Format | Size | Description |
|-------------|----------|-----------------|---|
| | | | <ul style="list-style-type: none"> C – fee amount to be credited (bonus) |
| 31 | a1 + n12 | 13 bytes | <p>Issuer fee amount in the account currency.</p> <p>If present, it is transferred in the response to transaction.</p> <p>The first char is D or C:</p> <ul style="list-style-type: none"> D – fee amount is debited from the account C – fee amount is credited to the account (e.g., bonus) |
| 32 | n3 | 3 bytes | <p>ISO numeric code of the account currency. It is transferred in the response if the issuer fee is present.</p> |
| 34 | ans..300 | Up to 300 bytes | <p>Statements records – posted in response to the Statement transaction, contains the card history. The field includes several records of the fixed size (each string is a separate operation).</p> <p>The record format: an20: mmddkkk000000000000s where dd – day, mm – month, kkk – operation code (see TWO dictionary), 000 – amount (indicated in the minor currency units, left-padded with spaces), s – character (+,-).</p> <p>E.g.: '0707022 121200-0707022 1200-0707022 12100-‘.</p> |
| 50 | ans..50 | Up to 50 bytes | <p>Cardholder address.</p> <p>It is indicated in the Pre-purchase, Purchase and Card Verification transactions if it is necessary to verify an address.</p> <p>The field contains the following sub-fields separated by character with the 0x1D code:</p> <ol style="list-style-type: none"> 1) PostalCode – cardholder postal code; 2) Address – cardholder address in Latin upper-case chars. Numeric data must be transferred as digits, e.g.: "Thirty-One Park Place" must be transferred as "31 Park Place". |
| 51 | a1 | 1 byte | <p>Result of the cardholder address verification.</p> <p>It is specified in the response to the transaction which processing involves verification of the address transferred in P57.50.</p> |

| Subfield ID | Format | Size | Description |
|-------------|-----------|-----------------|--|
| | | | See the available values in the “Result of the cardholder address verification” table. |
| 58 | n12 | 12 bytes | Transaction amount in the minimum units of the dynamic conversion currency. It is specified in the request together with the Subfield ID 59 if the terminal supports the Dynamic Currency Conversion (DCC). |
| 59 | n3 | 3 bytes | ISO code of the dynamic conversion currency. It is specified in the request together with the Subfield ID 58 if the terminal supports Dynamic Currency Conversion (DCC). |
| 61 | n1 | 1 byte | <p>Sender type:</p> <ul style="list-style-type: none"> • ‘1’ – unknown • ‘2’ – on-us • ‘3’ – resident • ‘4’ – foreign <p>It is indicated in the <i>P2P Cash Transfer</i> and <i>P2P Transfer Calc Fee</i> transactions.</p> |
| 62 | n..19 | Up to 19 bytes | <p>Card PAN of the transfer recipient. The field is mandatory for the following transactions:</p> <ul style="list-style-type: none"> • P2P Card Transfer • P2P Cash Transfer • P2P Transfer Calc Fee |
| 63 | a1 + n12 | 13 bytes | <p>Acquiring fee amount in the transaction currency (field p-49) is transmitted in response to the <i>P2P Transfer Calc Fee</i> transaction.</p> <p>The first character is D or C:</p> <ul style="list-style-type: none"> • D – fee amount to be debited • C – fee amount to be credited (e.g.: bonus) |
| 64 | ans...250 | Up to 250 bytes | <p>Data on a person who sent the funds to payment system card via P2P Cash Transfer transaction</p> <p>It is indicated in the transaction request.</p> <p>The field contains the following sub-fields separated by the character with the code 0x1D:</p> <ol style="list-style-type: none"> 1) <reserved> – bank field; 2) SenderName – sender name in Latin upper-case chars; 3) ResidentCityInLatin – sender city in Latin upper-case |

| Subfield ID | Format | Size | Description |
|-------------|--------|----------------|---|
| | | | chars; 4) ResidentCountry – sender country code; 5) SenderPostalCode – sender postal code 6) Address – sender address 7) RecipientName 0 recipient name in Latin chars 8) IdentificationType – type of identity document 1 – passport 2 – driving license 3 – social insurance number 4 – TPN 9) IdentityNumber – document number |
| 70 | ans16 | 16 bytes | New PIN. It is used in the PIN Change transaction, contains PIN block with the new PIN entered by the customer. It is posted as ASCII Hex. E.g.: the 0123456789ABCDEF block will be posted as hex 30 13 32 33 34 35 36 37 38 39 41 42 43 44 45 46. |
| 71 | ans16 | 16 bytes | New PIN Confirmation. It is used in the PIN Change transaction, contains PIN block with repeated PIN entered by customer. It is posted as ASCII Hex. E.g.: the 0123456789ABCDEF block will be posted as hex 30 13 32 33 34 35 36 37 38 39 41 42 43 44 45 46. |
| 75 | ans11 | Up to 11 bytes | Agent Unique Account Result. For details, refer to specifications V.I.P. System BASE I Technical Specifications, Volume 1 and V.I.P. System SMS POS Technical Specifications, Volume 1, section "FIELD 126.18 - AGENT UNIQUE ACCOUNT RESULT". |
| 80 | ans4 | 4 bytes | Transit Program. Consists of 2 subfields: 1. Transit Transaction Type Indicator Available values: <ul style="list-style-type: none"> • 01 Prefunded • 02 Real-time Authorized • 03 Post-Authorized Aggregated • 04 Authorized Aggregated Split Clearing • 05 Other |

| Subfield ID | Format | Size | Description |
|-------------|--------|------|---|
| | | | <ul style="list-style-type: none"> • 06-99 Reserved for Future Use <p>2. Transportation Mode Indicator</p> <p>Available values:</p> <ul style="list-style-type: none"> • 00 Unknown • 01 Urban Bus • 02 Interurban Bus • 03 Light Train Mass Transit (Underground Metro, LTR) • 04 Train • 05 Commuter Train • 06 Water Borne Vehicle • 07 Toll • 08 Parking • 09 Taxi • 10 High Speed Train • 11 Rural Bus • 12 Express Commuter Train • 13 Para Transit • 14 Self Drive Vehicle • 15 Coach • 16 Locomotive • 17 Powered Motor Vehicle • 18 Trailer • 19 Regional Train • 20 Inter City • 21 Funicular Train • 22 Cable Car • 23-99 Reserved for Future Use <p>For details, refer to <i>MasterCard Customer Interface Specification</i> / section "DE 48-Additional Data-Private Use, Subelement 64-Transit Program".</p> |

Result of the cardholder address verification

| Value | Result of the postal code verification | Address Verification Result |
|----------|--|--|
| A | Match | Mismatch |
| B | Not verified due to incompatible formats | Match |
| C | Not verified due to incompatible formats | Not verified due to incompatible formats |
| D | For VISA only: match | For VISA only: match |
| F | For addresses in the UK only: match | For addresses in the UK only: match |
| G | Address cannot be verified as it is the international transaction (the issue is outside the USA) | |
| I | Address cannot be verified as it is the international transaction | |
| M | Match | Match |
| N | Mismatch | Mismatch |
| P | Match | Not verified due to incompatible formats |
| R | Service is unavailable | |
| S | Service is not supported by the acquirer | |
| U | No data for address verification/service is not supported by the issuer | |
| W | Match (for addresses in the USA, the 9 digit postal code matches) | Mismatch |
| X | Match (for addresses in the USA, the 9 digit postal code matches) | Match |
| Y | For addresses in the USA only: the 5 digit postal code matches | Match |
| Z | For addresses in the USA only: the 5 digit postal code matches | Match |

7.26 P-59 Detail Addenda

Format: ans..4000

It is used by the terminal to transfer the information on the extra programs, services and other peculiarities concerned the financial transaction. The field is used in clearing.

For the transactions by *American Express* cards, it corresponds to the *AEGNS Industry Specific Detail Addenda (9240/9340)* messages. See the field format description in specification *American Express/Addenda Messages*.

For the air ticket purchase transactions by VISA cards, the field transfers the ticket number in the tag VISA AVIATICKET. In this case, the format of data transfer is as follows: tag name «VISA AVIATICKET», the symbol «=», field value (air ticket number).

7.26.1 Additional Data on VISA Fleet Cards

The field transfers the additional data for the transactions by the VISA Fleet cards performed at the "fuel merchants" terminals.

The terminals with the following MCCs are of the "fuel merchants" class:

| MCC | Description |
|------------|--|
| 4468 | Marinas, Marine Service, and Supplies |
| 5499 | Miscellaneous Food Stores—Convenience Stores and Specialty Markets |
| 5541 | Service Stations (with or without ancillary services) |
| 5542 | Automated Fuel Dispensers |
| 5983 | Fuel Dealers—Fuel Oil, Wood, Coal, and Liquefied Petroleum |

Format of data being transferred

The data are transferred as a structure in the UAMP format. The structure consists of the subfields separated by the symbol 0x10(hex). The subfields format is 'parameter=value', where 'parameter' is a parameter notation (see below), 'value' – parameter value. If the value contains the symbol '=', it is replaced by [SP]3D, where [SP] is special symbol 0x13, '3D' – ASCII code of the symbol '=', that is, in hex format, the value is as follows 0x13 0x33 0x44. The symbols with the following codes are also forbidden: 0x0a, 0x10, 0x1d, 0x1c, 0x07, 0x13. To transfer these symbols, the special symbol [SP] is used, e.g., [SP]0A, [SP]10, [SP]1D, etc. For details on the UAMP format, refer to UAMP.doc.

Currently, the following data can be transferred:

| Parameter | Notation | Format |
|----------------------|-----------------|---------------|
| Purchasing Card Data | PCD | ans..17 |
| Type of Purchase | 01 | an1 |
| Service Type | 02 | an1 |
| Fuel Type | 03 | an2 |
| Unit of Measure | 04 | an1 |
| Quantity | 05 | n12 |
| Unit Cost | 06 | n12 |
| Gross Fuel Price | 07 | n12 |
| Net Fuel Price | 08 | n12 |
| Gross Non-Fuel Price | 09 | n12 |

| Parameter | Notation | Format |
|---|----------|--------|
| Net Non-Fuel Price | 0A | n12 |
| Odometer Reading | 0B | n7 |
| VAT/Tax Rate | 0E | n4 |
| Miscellaneous Fuel Tax Exemption Status | 0F | an1 |
| Miscellaneous Fuel Tax | 10 | n12 |
| Miscellaneous Non-Fuel Tax Exemption Status | 11 | an1 |
| Miscellaneous Non-Fuel Tax | 12 | n12 |
| Local Tax Included | 13 | an1 |
| Local Tax | 14 | n12 |
| National Tax Included | 15 | an1 |
| National Tax | 16 | n12 |
| Other Tax | 17 | n12 |
| Merchant VAT Registration/Single Business Reference Number | 18 | an20 |
| Customer VAT Registration Number | 19 | an13 |
| Message Identifier | 1B | an15 |
| Additional Data Indicator | 1C | an1 |
| Summary Commodity Code | 1E | n4 |
| Non-Fuel Product Code 1 | 1F01 | an2 |
| Non-Fuel Product Code 2 | 1F02 | an2 |
| Non-Fuel Product Code 3 | 1F03 | an2 |
| Non-Fuel Product Code 4 | 1F04 | an2 |
| Non-Fuel Product Code 5 | 1F05 | an2 |
| Non-Fuel Product Code 6 | 1F06 | an2 |
| Non-Fuel Product Code 7 | 1F07 | an2 |
| Non-Fuel Product Code 8 | 1F08 | an2 |

For details on parameters, refer to the specifications *V.I.P. System BASE I Technical Specifications, Volume 1* and *V.I.P. System SMS POS Technical Specifications, Volume 1*:

- See the details on the Purchasing Card Data parameter in section "FIELD 48, USAGE 36 – PURCHASING CARD DATA"
- See the details on other parameters in section "FIELD 104, USAGE 2 – TRANSACTION-SPECIFIC DATA, Dataset ID 5C, Commercial Card Data".

7.27 P-60 Private Use

Format: ans..999

It is used by the terminal to transfer transaction extra details.

7.27.1 Batch Number

Format: ans6

Batch number is sent to the host on closing the batch (message type 0500).

7.27.2 Original Message Data

Format: an 22

The original transaction data are used on unloading the transactions batch (message type 0320) .

| Field | Format | Size, bytes | Value |
|-------------------------------------|--------|-------------|-----------------------------------|
| Original Message Type | an 4 | 4 | Original transaction message type |
| Original Systems Trace Audit Number | an 6 | 6 | Original transaction P-11 value |
| Reserved | an 12 | 12 | Reserved for future use |

7.27.3 Original Amount

Format: an 12

For the Adjustment transaction, it includes the original amount of the transaction being adjusted, at that, considering the acquiring fee.

For the Reversal and Void transactions, it includes the amount of the original transaction.

7.27.4 Cashback Amount

Format: an 12

It is used in the *Purchase with Cashback* transaction and includes cashback amount.

7.28 P-62 Private Use

Format: ans..999

It is used by the terminal in order to transfer transaction extra data.

7.28.1 Invoice Number

Format: an 12

Includes invoice number in the messages 0100, 0200, 0220, and 0320.

7.28.2 Working Keys

It is used to update the working keys. The field is transferred in the message 0810 – in response to the new working keys request (Processing Code 92). All the keys must have the same length – 8 or 16 bytes.

If one of the keys is not used, the field of that key transfers 'ff ff ff ff ff ff ff ff ff ff ff ff' (hex) to the terminal.

| Field | Format | Size, bytes | Description |
|--------------|--------|-------------|--|
| Extra length | n 4 | 2 | '0x00 0x16' or '0x00 0x32' - BCD length |
| PWK | B | 8 or 16 | Working PIN key encrypted by the terminal master key |
| MWK | B | 8 or 16 | Working MAC key encrypted by the terminal master key |

7.28.3 Working EWK

Format: b 8 or b 16

It is used to update the working key of traffic encryption (EWK). The field is transferred in the message 0810, in response to the EWK request (Processing Code 95). It contains the EWK encrypted by the appropriate terminal master key. It can be of single or double length.

7.29 P-63 Private Use

Format: ans..999

7.29.1 Extra Data in Request

It is used by the terminal to transfer transaction extra data.

On receiving a request from the terminal, it contains one or several subfields.

Field format:

| Field | Format | Size, bytes | Value |
|--------------|--------|-------------|--|
| Length | n4 | 2 | '0LLL' – BCD length of the data. |
| Subfield (1) | | var | First subfield. |
| Subfield (2) | | var | Second subfield. |
| : | : | : | Extra data can be transferred in any order. Each subfield contains own identifier and length. Unknown elements can be skipped. |
| : | : | : | |
| : | : | : | |
| Subfield (N) | | var | N subfield. |

Available subfields:

- CVV2
- DUK/PT Key Serial Number
- DUK/PT Key Serial Number 2
- Additional Data

7.29.1.1 CVV2

| Field | Format | Size, bytes | Value |
|--------------|--------|-------------|----------------------------------|
| Extra length | n 4 | 2 | '0LLL' – BCD length of the data. |
| Field ID | ans 2 | 2 | '16' - CVV2 data |

| Field | Format | Size, bytes | Value |
|-------|--------|-------------|---|
| Value | an 6 | 6 | <p>6 characters of the CVV2 data</p> <p>Position 1</p> <p>0 - CVV2 value is not transferred 1 - CVV2 value is present 2 - CVV2 value is present but illegible 9 – cardholder states that CVV2 is not present.</p> <p>Position 2</p> <p>0 – return only the response code. 1 – return the response code and CVV2 verification code.</p> <p>Position 3-6</p> <p>CVV2 value (left-padded with spaces) If position 1 = 0, 2 or 9, the positions 3-6 should be space-padded.</p> |

7.29.1.2 DUK/PT Key Serial Number

| Field | Format | Size, bytes | Value |
|--------------|--------|-------------|--|
| Extra length | N4 | 2 | '0LLL' - BCD length of the data |
| Field ID | ans 2 | 2 | '33' - DUKPT data |
| Value | ans 20 | 20 | <p>Includes <i>Key Serial Number</i> for the DUKPT encryption. <i>Key Set Id</i> is transmitted in the decimal encoding.</p> <p>The value is right aligned. If necessary, it is left-padded with '0xFF' binary characters.</p> |

7.29.1.3 DUKPT Key Serial Number 2

| Field | Format | Size, bytes | Value |
|--------------|--------|-------------|---|
| Extra length | N4 | 2 | '0LLL' - BCD length of the following data |
| Field ID | ans 2 | 2 | '34' - DUK/PT data |

| Field | Format | Size, bytes | Value |
|-------|--------|-------------|--|
| Value | ans 20 | 20 | Includes <i>Key Serial Number</i> for DUK/PT encryption. <i>Key Set Id</i> is transferred in <i>Key Serial Number</i> in the decimal encoding. The value is right aligned. If necessary, it is left-padded with '0xFF' binary characters. It can be used in <i>PIN Change</i> transaction if the terminal encrypts new PIN block by another key. |

7.29.1.4 DUKPT Key Serial Number 3

| Field | Format | Size (bytes) | Value |
|--------------|--------|--------------|---|
| Extra length | N4 | 2 | '0LLL' - BCD length of the following data |
| Field ID | ans 2 | 2 | '35' - DUKPT data |
| Value | ans 20 | 20 | Includes <i>Key Serial Number</i> for DUKPT encryption. <i>Key Set Id</i> is transferred in <i>Key Serial Number</i> in the decimal encoding. The value is right aligned. If necessary, it is left-padded with '0xFF' binary characters. It can be used in <i>PIN Change</i> transaction if the terminal encrypts new PIN block with the re-entered PIN by another key. |

7.29.1.5 Additional Data

| Field | Format | Size, bytes | Value |
|-------------------|--------|-------------|---|
| Additional length | N4 | 2 | '0LLL' - BCD length of the following data |
| Field ID | ans 2 | 2 | '29' |

| Field | Format | Size, bytes | Value |
|-------|---------|-------------|--------------------------|
| Value | ans ..x | x | Additional textual data. |

7.29.1.6 Reserved for Future Use

Currently, this subfield is not used.

| Field | Format | Size, bytes | Value |
|--------------|---------|-------------|---|
| Extra Length | N4 | 2 | '0LLL' - BCD length of the following data |
| Field ID | ans 2 | 2 | '89' |
| Value | ans ..x | x | Data of variable length |

7.29.2 Data in Response to Terminal

7.29.2.1 Balance Inquiry

In response to the Balance Inquiry transaction, it contains the available balance:

Format:

1. Currency character code - 3 chars (e.g.: "UAH", "USD", "EUR", "RUR", etc.)
2. Space
3. Char ("-" or "+")
4. Amount with a decimal point and fraction (e.g.: "14.00")

Total: "UAH -14.00"

7.29.2.2 Extra Information

In other cases, it can contain extra information which can be printed on an invoice.

The extra information is transferred in the subfields described below. These fields do not duplicate each other, therefore both of them can be present in the response.

7.29.2.2.1 Alternate Host Response

| Field | Format | Size, bytes | Description |
|-------------------|--------|-------------|--|
| Additional length | N4 | 2 | '0LLL' - BCD length of the data |
| Field ID | ans 2 | 2 | '22' |
| Value | ans 40 | 40 | Additional textual data to be printed on an invoice. The field is of fixed length. |

7.29.2.2.2 Additional Host Print Data

| Field | Format | Size, bytes | Description |
|-------------------|---------|-------------|--|
| Additional length | N4 | 2 | '0LLL' - BCD length of the data |
| Field ID | ans 2 | 2 | '29' |
| Value | ans ..x | x | Additional textual data to be printed on a receipt. The field is of variable length. |

7.29.2.2.3 Reserved for Future Use

Currently, this subfield is not used.

| Field | Format | Size, bytes | Value |
|--------------|---------|----------------|---|
| Extra Length | N4 | 2 | '0LLL' - BCD length of the following data |
| Field ID | ans 2 | 2 | '89' |
| Value | ans ..x | x | Data of variable length |

7.29.3 Reconciliation Request Totals

Format: an 60

Totals are sent to the host for reconciliation in the message 0500 (Processing Code = 92).

| Field | Format |
|---|--------|
| Number of debit operations on credit cards | an 3 |
| Amount of debit operations on credit cards | an 12 |
| Number of credit operations on credit cards | an 3 |
| Amount of credit operations on credit cards | an 12 |
| Number of debit operations on debit cards | an 3 |
| Amount of debit operations on debit cards | an 12 |
| Number of credit operations on debit cards | an 3 |
| Amount of credit operations on debit cards | an 12 |

Reversed/voided transactions are not included into totals. The adjustment transactions impact the amount of totals but do not impact the number of transactions.

7.30 P-64 MAC

Format: b8

Includes Message Authentication Code. MAC can be indicated in all the messages to the exclusion of 0800.

The whole message, except for the Header fields is used to calculate MAC.

MAC in the request from terminal is calculated with the enabled bit 64 in Primary Bitmap.

MAC in the message to terminal is calculated with the disabled bit 64 in Primary Bitmap.

8. Message Exchange Algorithm

8.1 Financial Online Transactions

Once the messages 0100 or 0200 are sent, the terminal is waiting for the response 0110 or 0210 from the host. If the response hasn't been received within the definite time period or it has been received in the invalid format, the terminal should reverse the transaction.

Once a financial advice 0220 or reversal 0400 has been sent, the terminal is waiting for the response 0230 or 0410. If a correctly formatted response hasn't been received within the definite time period, the terminal should resend the message 0220 or 0400.

8.2 Totals Reconciliation

On closing a batch, the terminal sends a message 0500 with P-3=920000 and the totals in P-63 to the host. The host reconciles the totals. If the totals match, the host posts to the terminal 0510 with P-39=00. In case no match is found, the host posts 0510 with P39=95. On receiving such response, the terminal may unload all the batch transactions to the host for further reconciliation in the messages 0320.

The message 0320 allows to unload the batch. Once all the batch transactions have been unloaded, the terminal sends 0500 with P-3=960000.

9. Traffic Encryption

The traffic encryption feature is optional, if it is enabled, the messages are sent encrypted. But note that only the Data Elements are encrypted (see section 3 Messages Format), the Header, MTI and Bit Map are transferred in clear text.

The encryption is based on the 3DES algorithm in the Cipher Block Chaining (CBC) mode with the zero initialization vector.

If the traffic is encrypted, the terminal name in clear text must be specified at the beginning of the message. The terminal name is used to determine the traffic encryption working key (EWK).

There is provided the facility to dynamically change the EWK. To obtain a new EWK, terminal sends the request with the message type 0800 and Processing Code 95. The request can be transferred encrypted (by the current EWK) or in clear text (e.g., it the first request for EWK). If the request is sent unencrypted, do not specify the terminal name at the beginning of the request. New EWK is transferred to terminal in the field 62.

If the traffic encryption option is enabled, the terminal can send some message in clear text (without the terminal name at the beginning). In this case, the response to terminal will be also transferred unencrypted, e.g. the non-financial message of terminal can be sent in clear text

10. Recommendations on Chip Card Transactions Processing

The recommendations are based on EMVCo “Recommendations for EMV Processing for Industry-Specific Transaction Types” v.1.1, Dec.2008. There are the following types of transactions initiated by chip cards:

1. **EMV transaction executed by the complete scheme.** It is a debit financial transaction (purchase of goods/services or disbursement of cash) that is executed regarding all mandatory functions described in the EMV specifications. Approved Transactions of such type must result in generation of TC cryptogram. If the card decides to authorize the request online, the terminal transmits the ARQC cryptogram and all the data used by card to calculate the cryptogram in the field 55 of the authorization request. The terminal must also specify that the card entry mode is chip in the field 22. For the on-us transactions, the host controls the ATC increment in each new transaction by the particular card.
2. **EMV transaction executed by the simplified scheme** (“Non-EMV Transaction using EMV functionality” in the EMVCo recommendations). It is non-financial transactions, e.g., informational and technical requests, deposit, adjustment, pre-authorization completion transactions. The terminal is able to execute such transaction by the complete scheme, in this case, the request is created according to the requirements described in p.1. To execute the transaction by the simplified scheme following the EMVCo recommendations, the terminal selects the application, initiates the transaction by card, reads the payment application data sufficient for authorization request creation, and completes by the AAC cryptogram request. In the authorization requests, the field 55 is absent, but the terminal specifies the chip entry mode in the field 22.
3. **Fallback to magnetic stripe.** It is a Fallback request if the field 55 is absent and the card entry mode 80 (EMV Fallback transaction) is specified in the field 22.

The notifications on transactions completed offline without the host connection establishing must be sent as requests with MTI 0220. In this case, they will be processed by host as electronic Slip.

The terminal must not transfer the chip fields from the original request in the requests for adjustment and preauthorization completion. It is recommended to use the simplified scheme to execute the adjustment or preauthorization completion transaction if the transaction is executed by the chip card as original transaction.

In the reversal requests, the terminal can transfer the chip fields from the original request, except for the following fields: Terminal Verification Results, Issuer Application Data and Issuer Script

Results. If the terminal does not transfer the original chip fields in the reversal, the host uses the chip data from the original request.

10.1 Recommendations on Processing of Contactless Card Transactions

A set of fields in the message authorizing the contactless chip card transactions is identical to that presented in the message authorizing the EMV transactions; the same applies to the contactless magstripe card transactions. Therefore, for the proper processing of transactions by the contactless cards, the terminal should explicitly define the contactless entry mode in the field 22.

To ensure the proper unloading of information on the cardholder verification procedure to clearing file, the tag 9F34 "CVM Results" must be transferred in the requests for PayPass – MagStripe transactions. The values of this tag are created according to the EMV specifications.

Samples of CVM Results values for the PayPass – MagStripe transactions:

| Method | Value | Description |
|------------|--------|--|
| Online PIN | 020000 | Fail CV if unsuccessful - Online Encrypted PIN - Always - Result unknown |
| Signature | 1E0000 | Fail CV if unsuccessful - Signature (paper) - Always - Result unknown |
| No CVM | 1F0002 | Fail CV if unsuccessful - No CVM - Always - Result successful |