mPOS Communication Interface

Operation

St. Andrews, The Belfry,
Colonial Way,
Watford,
Hertfordshire
WD2 4YW
United Kingdom

Tel: +44 (0) 1923 - 236 050
Fax: +44 (0) 1923 - 236 630

SPIRE PAYMENTS

St. Andrews, The Belfry,
Colonial Way,
Watford,
Hertfordshire
WD2 4YW
United Kingdom

Tel: +44 (0) 1923 - 236 050
Fax: +44 (0) 1923 - 236 630

Title:	mPOS Communication Interface
Reference:	mPOS API.doc
Version:	1.0.14A
Date:	1st Mar 2018
Status:	Final
Authors:	Adrian Hyland, Lucian Lupu
Approved by:	Bob Parry
Circulation:	Under NDA only

TABLE OF CONTENTS

MPOS COMMUNICATION INTERFACE 1

1 OVERVIEW 2

1.1 Scope 2
1.2 Amendment History 2
1.3 Document References 3

2 INTRODUCTION 4

3 COMMUNICATION PROTOCOL 5

3.1 Communication Message Format 5
3.2 Transmission Protocol 5

4 MESSAGE EXCHANGES 7

5 MESSAGE EXCHANGES – STAND-BY MODE 8

5.1 Transaction Mode Initialisation 8
5.2 File Download 9
5.3 TR-31 Key Block Download 10
5.4 Get Key Information 10
5.5 Restart 11
5.6 Get Information 11
5.7 Transaction Record Management 11

6 MESSAGE EXCHANGES – TRANSACTION MODE 12

6.1 Start Transaction 12
6.2 ICC Transaction 12
6.3 Contactless Transaction 15
6.4 Swiped Transaction 16
6.5 Logon Transaction 17
6.6 Status Report 18
6.7 Transaction Record Storage 19

7 MESSAGE CONTENT 20

7.1 General Message Format 20
7.2 Common Message Fields 22
7.3 Generic parse error response 24

8 MESSAGE CONTENT – STAND-BY MODE 25

8.1 Transaction Mode Initialisation (12) 25
8.2 File Download (62) 27
8.3 Load TR-31 Key Block (63) 30
8.4 Get Key Information (64) 31
8.5 RKL_CERT_EXCHANGE (65) 32

8.6 RKL_KEY_LOAD (66) 33
8.7 Restart (14) 34
8.8 Get Information (15) 35
8.9 Control (16) 37
8.10 Get Record Count (31) 38
8.11 Fetch Record (32) 39
8.12 Delete Records (33) 40
8.13 PIN entry (20) 40
8.14 Display Text (21) 43

9 MESSAGE CONTENT – TRANSACTION MODE 44

9.1 Start Process (41 - ICC or Swipe) 44
9.2 Get Transaction and Application Data (42 - ICC Only) 45
9.3 Update Transaction and Application Data (57 – ICC only) 48
9.4 Get Cashback Amount (50 - ICC Only) 49
9.5 Get DCC Amount (51 - ICC or Swipe) 50
9.6 Referral Performed (45 - ICC or Swipe or Contactless) 52
9.7 Go Online (46 - ICC & Contactless) 53
9.8 Complete Transaction (47 - ICC & Contactless) 55
9.9 Terminate Transaction (48 - ICC or Swipe or Contactless or Logon) 57
9.10 Signature Verified (54 - ICC or Swipe or Contactless) 58
9.11 Process Swiped Card (52 - Swipe Only) 59
9.12 Get Swiped Transaction Data (53 - Swipe Only) 61
9.13 Logon Transaction (55 - Logon Only) 63
9.14 Supplementary (ICC or Contactless) 64
9.15 Supplementary MAC Generation (ICC or Swipe or Contactless) 66
9.16 Supplementary MAC Verification (ICC or Swipe or Contactless) 67
9.17 Status Report (49 - ICC or Swipe or Contactless) 68
9.18 Stand-By (13) 70
9.19 Add Record (30) 71
9.20 Card Details (56) 72

10 APPENDIX A – EXAMPLE ICC TRANSACTION 73

10.1 Transaction Flow 73
10.2 Starting a Transaction 74
10.3 Initialising a Transaction 74
10.4 Processing a Transaction 78
10.5 Completing a Transaction 83

11 APPENDIX B – CONFIGURATION FILE FORMAT 85

11.1 ICC Applications File 85
11.2 CA Public Keys File 86
11.3 Logon Transaction File 88
11.4 Currency File 89
11.5 Terminal Configuration File 90
11.6 Contactless Configuration File 93
11.7 Logo Configuration File 94

12 APPENDIX C - DATA ELEMENT CODES 96

12.1 Transaction Type 96
12.2 Terminal Country Code 96
12.3 Terminal Currency Code 96
12.4 Transaction and Merchant Category Codes 97

12.5 Regions Codes **99**

13 APPENDIX D - ASCII CONTROL CHARACTERS **100**

1 Overview

1.1 Scope

This document describes:

The message exchanges, the message content and the communication protocol that are used between a Spire mPOS and an EPOS system.

This version applies to SPm2 mPOS API release versions 4.00.xx only.

1.2 Amendment History

Version	Date	Amendments
Version 1.0.14A	1st Mar 2018	Special customer release only. Definition of message types 65 and 66 for certificate and KEK loading.
Version 1.0.14	26th Jan 2018	Reserved message types 65 & 66 for future use Changes to type 15 and type 62 messages for config file versioning
Version 1.0.13	17th Nov 2017	Integrated the PINPad mode Expanded the message 16-Control with flags field References to reset button use and to the separate contactless configuration document
Version 1.0.12 (TR31 Draft 2)	28th September 2017	Added 'Load TR-31 Key Block' message Added 'Get Key Information' message
Version 1.0.11	18th July2017	Clarification added to the Regions table New 16-Control message Clarification of messages only supported by SPm2 or SPm20.
Version 1.0.10	22 Feb 2017	Added TML_LanguagePreference terminal configuration, TML_Regions, TML_AllowManualUSBSelection Updated Timeout-2 description Added Regions table and
Version 1.0.9	13th June 2016 29th June	Added contactless Mastercard MSD mode capabilities Added Mastercard additional tags Added ICC update transaction data message - 57 (29/06) – Added the TML_AdjustSN, TML_BTAdjustSN and COM_BTNCFirst to the terminal configuration.

Version 1.0.8	29th April 2016	Requesting Cardholder Mobile Number for ICC and Swipe Transactions Requesting Track 1 Data for Swipe Transactions Added Changes for Displaying Logo using logob.cfg file
Version 1.0.7	4th April 2016	Added changes for PIN Verification only functionality: Encrypted PAN and PIN verification status on 56, Incorrect PIN Entry status message PIN Blocked status message Low Battery status message
Version 1.0.6	1st Feb 2016	Added status messages AB and AC Added gratuities amount field in to the 41-Start message Added Process type 'Balance Inquiry' in 41 - Start message
Version 1.0.5	16 October 2015	Added transaction storage enhancements
Version 1.0.4	15 May 2015	Minor corrections and added MK update
Version 1.0.3	01 April 2015	Go Online and Completion messages apply to contactless also
Version 1.0.2	06 January 2015	Corrected FS and US message fields to Conditional instead of Mandatory or Optional where appropriate.
Version 1.0.1	11 December 2014	Added MK/SK & Contactless support
Version 1.0.0	15 September 2014	Moved to SPm20 platform Change PED to mPOS throughout Changed Level 2 mode to Transaction Mode Removed Level 1 mode and RS232 references Added applicable application version number. Clarification for mag swipe second KSN when using a single BDK
PosMate API Version 3.3.12	2 December 2013	Base document

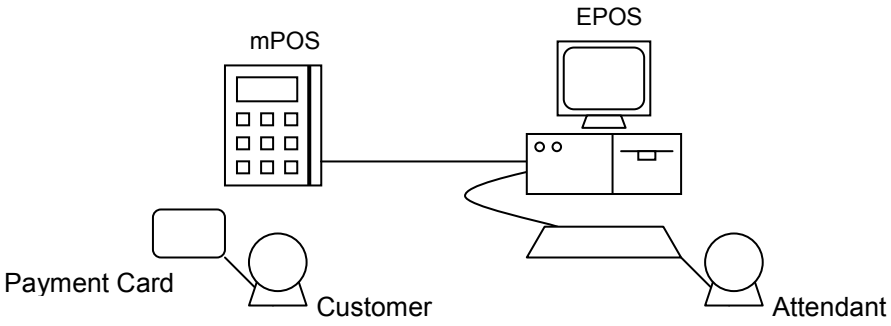
1.3 Document References

Document Name	Document Reference

2 Introduction

The Spire mPOS is a device that is capable of performing secure ICC, Contactless and swiped card transactions on behalf of an EPOS system. The mPOS interfaces to an EPOS system using a Bluetooth serial connection.

The diagram below shows the typical environment that the mPOS is expected to be used in.



The EPOS system is used by the Attendant and is responsible for determining the transaction details and for determining how the transaction is performed – either by using a magnetic swipe card or an ICC/Contactless card.

If the payment card is swiped then the encrypted and masked card track 2 details can be obtained from the mPOS. The EPOS is responsible for processing the transaction using the card details obtained from the card reader, performing authorisation and settlement, receipt printing etc.

If an ICC card is inserted into the mPOS then the mPOS shall process the transaction according to the EMV Transaction specifications. During the transaction, the mPOS shall communicate with the EPOS system in order to obtain transaction details and, if necessary, to go online to get authorisation. If a PIN is required then the mPOS will prompt the cardholder for their PIN. Once the transaction is complete, the EPOS system will capture any appropriate transaction data and go on to print a receipt.

This document goes on to describe the message exchanges, the message content and the communication protocol that are used in order to carry out a transaction using the mPOS.

WARNING: Spire mPOS devices are secure devices that continually verify their integrity. If the integrity check detects a possible attack, the device will clear or disable all stored keys and become inoperable.

On some Spire mPOS devices, there is a reset button. Using this button may abruptly cut the power to the processor, such that the device does not shut down cleanly. This can lead to corruption of stored files and so an integrity failure.

For this reason, the reset button should only be used when the device fails to respond to any other key presses and will not shut down using the standard power off options.

3 Communication Protocol

The mPOS shall be connected to the EPOS device using Bluetooth.

Once paired, the EPOS device initiates the connection to the mPOS. Some EPOS devices can struggle with establishing the security level required for the connection and can fail an initial connection attempt. For this reason it is highly recommended that an automatic connection retry is employed to ensure the user has no problems with mPOS connections.

The communication protocol that is used between the mPOS and the EPOS system is based on the protocol that is used in APACS to transmit application messages.

3.1 Communication Message Format

Messages are communicated to and from the mPOS using the format as shown:

STX	MESSAGE	ETX	LRC

Where:

- STX indicates the start of the communication message
- MESSAGE is the actual message content
- ETX indicates the end of the communication message
- LRC is the longitudinal redundancy check character. It is calculated by performing an XOR of every character in the communication message excluding the STX character but including the ETX character.

3.2 Transmission Protocol

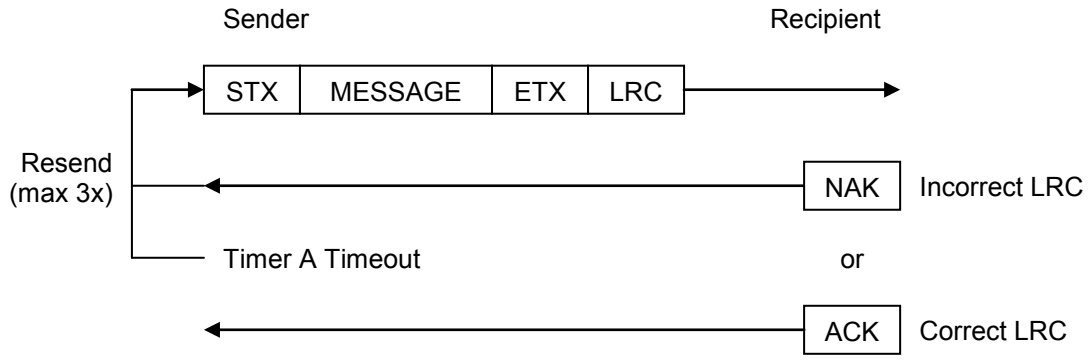
The recipient of each communication message must respond with either an ACK character if the LRC is valid or a NAK character if the LRC is not valid. If the recipient responds with a NAK then the sender must send the communication message again.

Only two timers are used: Timer A and Timer B. Timer C will not be used since the communication channel is expected to be always available.

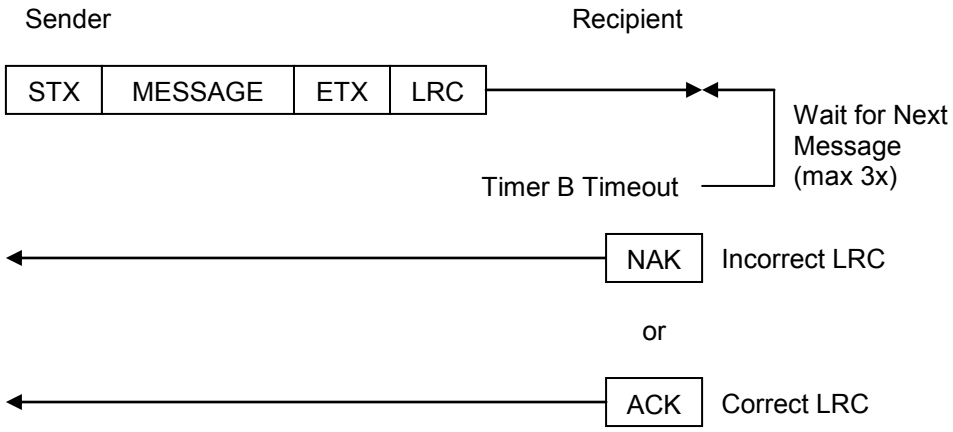
Timer A is used to wait for a valid reply to a message (i.e. an ACK, NAK or an STX). It is started after a communication message has been sent. If after 3 seconds, a valid reply has not been received, the communication message is sent again. Up to 3 attempts may be made to transmit a message

Timer B is used to wait for the receipt of a character. It is started whenever a character in a communication message is received. If after 0.5 seconds, a character has not been received then the communication message is discarded and the recipient waits for another communication message to arrive.

The diagram below illustrates the transmission of a message:



The diagram below illustrates the receipt of a message:



4 Message Exchanges

Message exchanges are used between the mPOS and the EPOS system in order to perform a particular action.

These occur during:

- Stand-by Mode – used to set up the mPOS and manage its configuration
- Transaction Mode – used to perform card transactions using the mPOS

A message exchange consists of a number of request and response messages. Each request and response in a message exchange will be of the same type (identified by the message identifier) but will be distinguished from each other by using a sequence number.

A message exchange may be initiated either by the mPOS or the EPOS system depending on the action that is being performed:

- Message exchanges used during Initialisation mode will be initiated by the EPOS system.
- Message exchanges used during Transaction mode will be initiated by the mPOS.

This document describes the message exchanges that occur in Stand-by mode and in Transaction mode.

5 Message Exchanges – Stand-by Mode

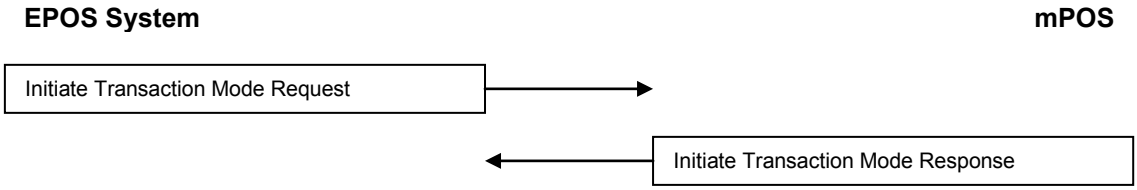
When the mPOS is first powered up, it automatically starts off in 'stand-by' mode. Whilst in this mode, the EPOS can choose to

- Put the mPOS into Transaction mode by sending a *Transaction Mode Initialisation* request
- Manage the mPOS configuration by sending a *File Download* request
- Restart the mPOS by sending a *Restart* request
- Get information about the mPOS by sending a *Get Information* request
- Manage records held in the mPOS transaction store

These message exchanges are described below

5.1 Transaction Mode Initialisation

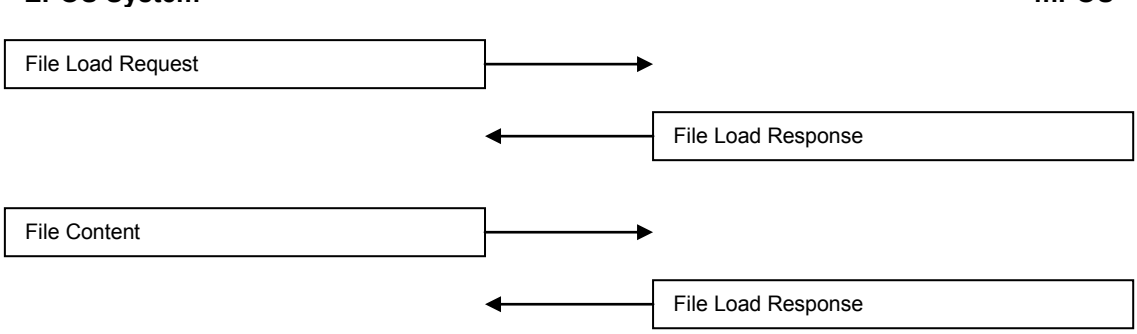
Description:
The diagram below illustrates the message exchanges that are used to put the mPOS into Transaction mode.



The message exchanges that can occur when the mPOS is in Transaction mode are described in the section 'Message Exchanges – Transaction Mode'

5.2 File Download

Description:
The diagram below illustrates the message exchanges that normally occur during file download. These exchanges may only occur whilst the mPOS is in stand-by mode.



The *File Content* is sent as a series of 1 kilobyte blocks (the last block may be less than 1K depending of the size of the file content). The first block should have a prefix consisting of an **STX** byte followed by a four byte value (most significant byte first) that gives the total length of the file content. Each block that is sent should also have a 32-bit CRC suffix that is used the check the data integrity. The mPOS will acknowledge the receipt of each block with either:

- An **ACK** byte if the block was successfully received
- A **NAK** byte if the block has a data error (bad LRC)
- An **EOT** byte if the mPOS could not accept the data block (the block could not be written to the file)

If the EPOS does not receive an **ACK** from the mPOS for a data block then it should abort the file load and wait for the mPOS to respond with the final *File Load Response*.

The *Final Load Response* is used by the mPOS to indicate whether the file was successfully downloaded or not.

Any number of file downloads may be performed whilst the mPOS is in stand-by mode

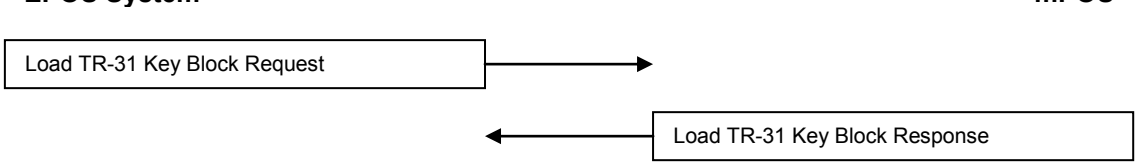
WARNING
This mechanism can be used to upgrade the main application on the mPOS by sending an update package. If an invalid application is written to the device and the device is restarted then it may become inoperable.

Only genuine application packages provided by Spire Payments and approved for use on your mPOS devices should be loaded to the mPOS.

Before loading a new boot file, use the Get Information (15) command to retrieve the current application version. If the returned version begins with a “t” then it is a test version and only another test version can be loaded and run. If the returned version begins with a number then it is a production version and only another production version should be loaded and run. If any other condition is found then there is an error and you should proceed with caution.

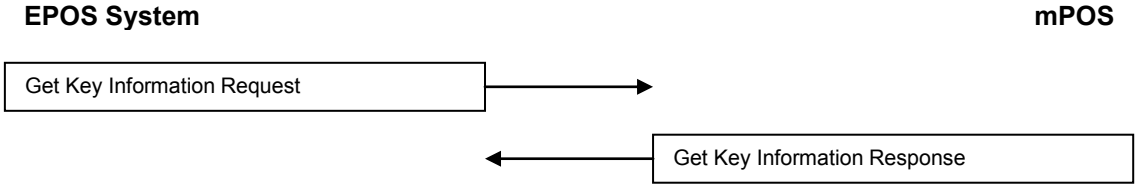
5.3 TR-31 Key Block Download

Description:
The diagram below illustrates the message exchanges that normally occur during a TR-31 key block download. These exchanges may only occur whilst the mPOS is in stand-by mode.



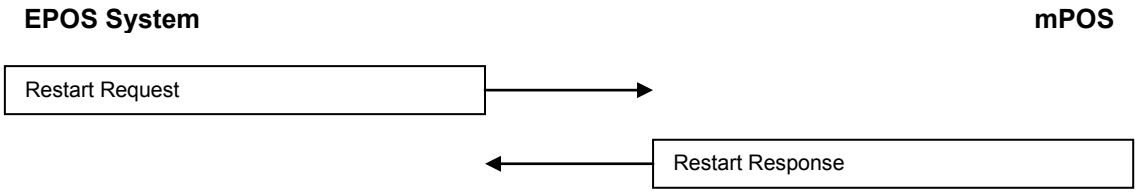
5.4 Get Key Information

Description:
The diagram below illustrates the message exchanges that normally occur to retrieve information about the keys that have been loaded on the mPOS. These exchanges may only occur whilst the mPOS is in stand-by mode.



5.5 Restart

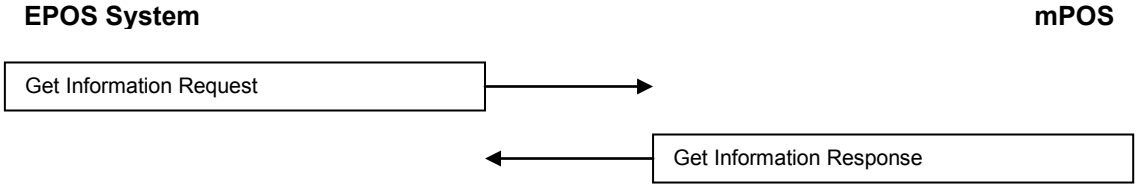
Description:
The diagram below illustrates the message exchanges that can be used by the EPOS to restart the mPOS.



The EPOS would normally use the Restart message after updating the configuration on the mPOS

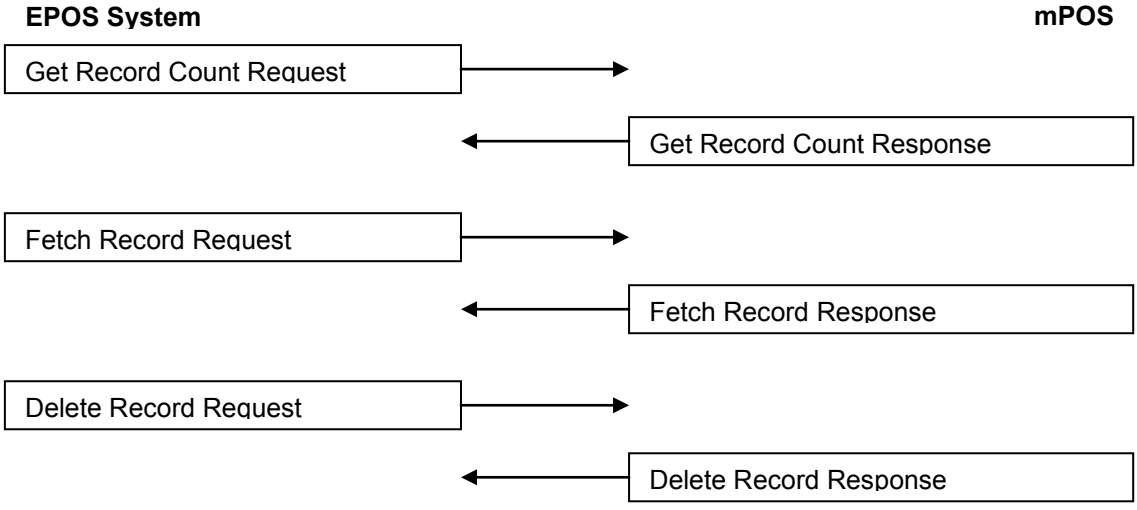
5.6 Get Information

Description:
The diagram below illustrates the message exchanges that can be used by the EPOS to get information about the mPOS.



5.7 Transaction Record Management

Description
This set of messages can be used by the EPOS to manage any transaction records that have been stored on the mPOS



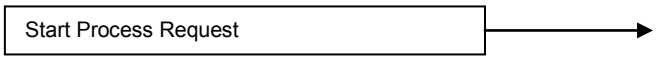
6 Message Exchanges – Transaction Mode

Once the mPOS has been initialised in Transaction mode, the EPOS system shall continue with the following series of message exchanges. The mPOS will continue to remain in this mode until a *Stand-by* message is exchanged. Note that the *Stand-by* message should only be sent by the EPOS at the start (or end) of a transaction.

6.1 Start Transaction

Description:
The diagram below shows the message exchange that the EPOS system uses to start a transaction. Note that there is no response message to this request.

EPOS System



The message exchange is used to start a card transaction process (using either an ICC, a contactless or swipe card) or a logon transaction process

If an ICC card transaction is started then the mPOS will continue with the series of message exchanges described in 'Message Exchanges – ICC Transaction'

If a contactless card transaction is started then the PosMate will continue with the series of message exchanges described in 'Message Exchanges – Contactless Transaction'

If a swipe card transaction is started then the mPOS will continue with the series of message exchanges described in 'Message Exchanges – Swiped Transaction'

If a logon transaction is started then the mPOS will continue with the series of message exchanges described in 'Message Exchanges – Logon Transaction'

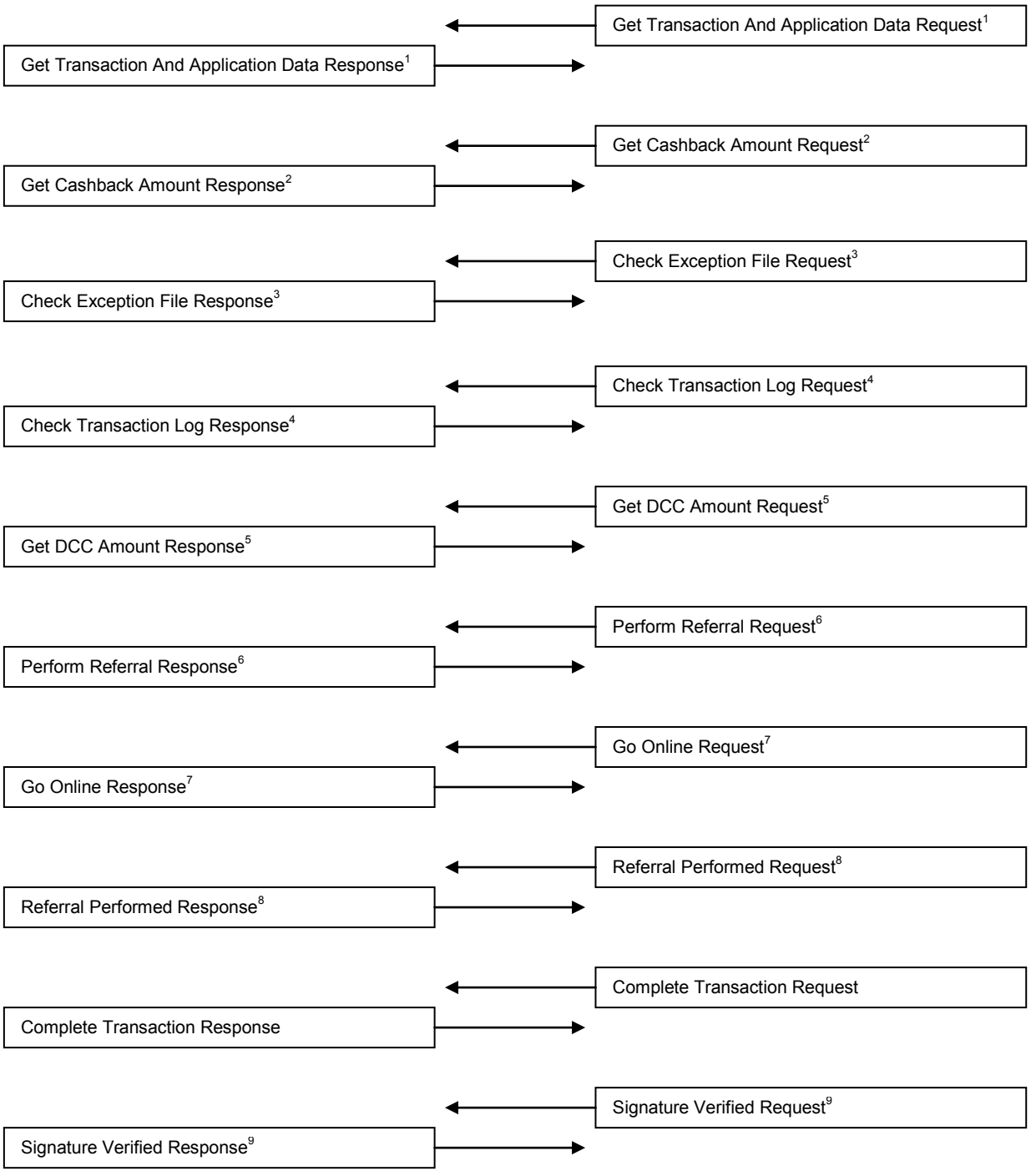
If there was card entry error (too many attempts at inserting or swiping a card) then the transaction will be terminated using a *Terminate Transaction* message exchange

6.2 ICC Transaction

Description:
The diagram below illustrates the message exchanges that may occur during the processing of an ICC transaction.

The *Terminate Transaction* message exchange is not shown but may occur at any point during the transaction.

Once this series of message exchanges is complete, the EPOS system should go back to sending a *Start Process* message exchange.

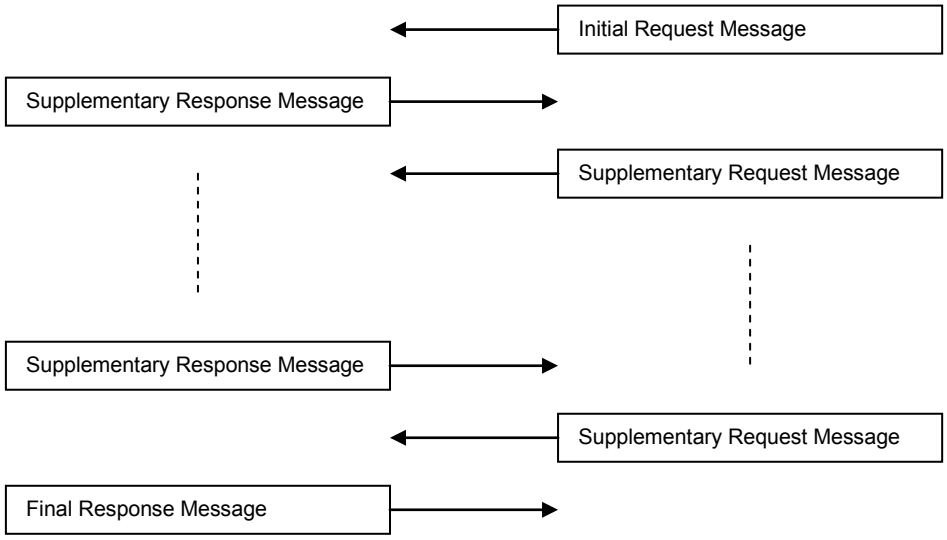


Notes:

1. There may be more than one *Get Transaction And Application Data* messages. These indicate that the chosen card application could not be used for the transaction and an alternative card application has been selected.
2. The *Get Cashback Amount* message is only used if the *Additional Terminal Capabilities* indicate that cashback is supported and if providing a cashback amount will not cause the transaction to be declined offline

3. The *Check Exception File* message exchange is only used if the *Constraint Checks* sent in the *Get Transaction And Application Data* message indicate that an exception file (hot card list) is supported
4. The *Check Transaction Log* message exchange is only used if the *Constraint Checks* sent in the *Get Transaction And Application Data* message indicate that a transaction log is supported and a floor limit has been provided
5. The *Get DCC Amount* message exchange is only used if the *Constraint Checks* sent in the *Get Transaction And Application Data* message indicate that DCC is supported
6. The *Perform Referral* message exchange is only used if the card has indicated that a voice referral is required.
7. The *Go Online* message exchange is only used if the transaction needs to be authorised online.
8. The *Referral Performed* message exchange is only used if the response from the online authorisation indicates that a voice referral is required.
9. The *Signature Verified* message exchange is only used if the transaction has been approved and the *Attendant Action* sent in the *Complete Transaction* response indicate that signature verification is required

During any of the above message exchanges, supplementary messages may be used to obtain additional data about the transaction. They may also be used to generate and/or verify MAC's that are required for online messages. The supplementary message identifiers must be the same as the initial request (as they're part of the same message exchange) but will be distinguished by using different sequence numbers. This is illustrated in the diagram below:

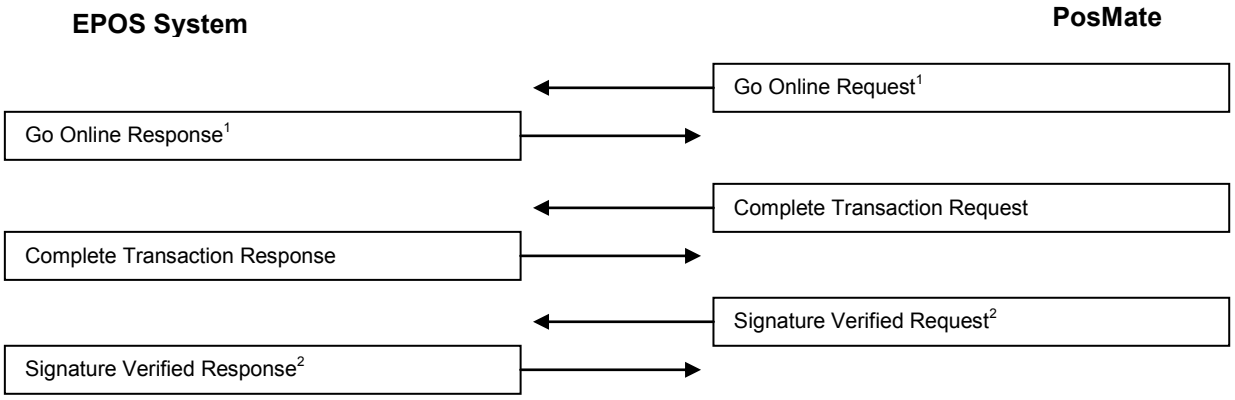


6.3 Contactless Transaction

Description:
The diagram below illustrates the message exchanges that may occur during the processing of a contactless transaction.

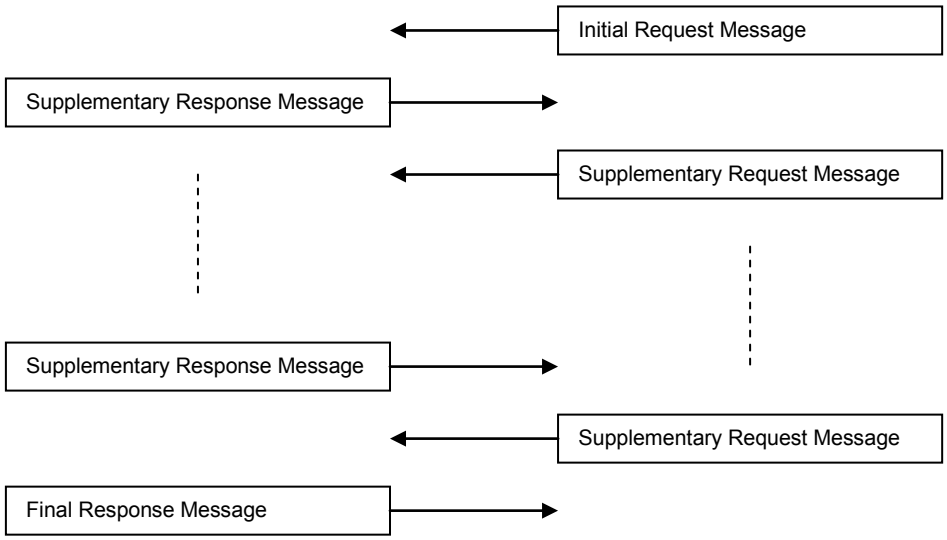
The *Terminate Transaction* message exchange is not shown but may occur at any point during the transaction.

Once this series of message exchanges is complete, the EPOS system should go back to sending a *Start Process* message exchange.



Notes:
1. The *Go Online* message exchange is only used if the transaction needs to be authorised online.
2. The *Signature Verified* message exchange is only used if the transaction has been approved and the *Attendant Action* sent in the *Contactless Complete Transaction* response indicate that signature verification is required

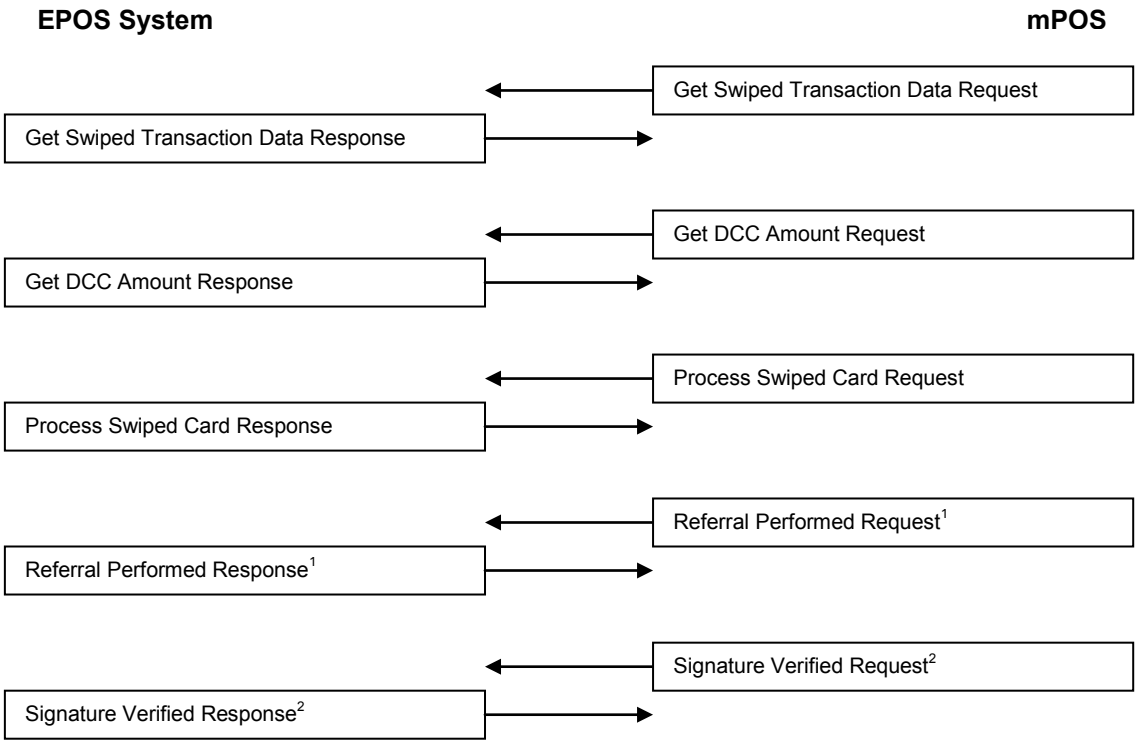
During any of the above message exchanges, supplementary messages may be used to obtain additional data about the transaction. They may also be used to generate and/or verify MAC's that are required for online messages. The supplementary message identifiers must be the same as the initial request (as they're part of the same message exchange) but will be distinguished by using different sequence numbers. This is illustrated in the diagram below:



6.4 Swiped Transaction

Description:
The diagram below illustrates the message exchanges that may occur during the processing of a swiped card transaction.

Once this series of message exchanges is complete, the EPOS system should go back to sending a *Start Process* message exchange.

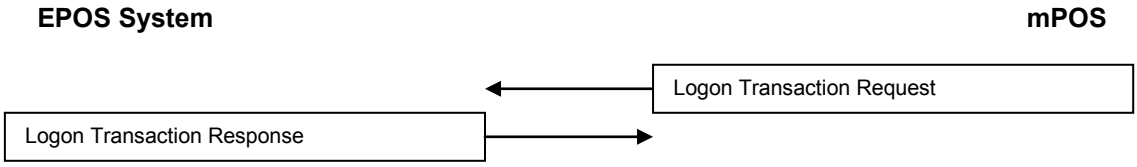


Notes:
1. The *Referral Performed* message exchange is only used if the *Transaction Result* in the *Process Swiped Card* response indicates that a voice referral is required.
2. The *Signature Verified* message exchange is only used if the *Transaction Result* in the *Process Swiped Card* response indicates that:
   - A signature check is required or
   - A voice referral is required and the referral was approved

6.5 Logon Transaction

Description:
The diagram below illustrates the message exchanges that may occur during the processing of a logon transaction.

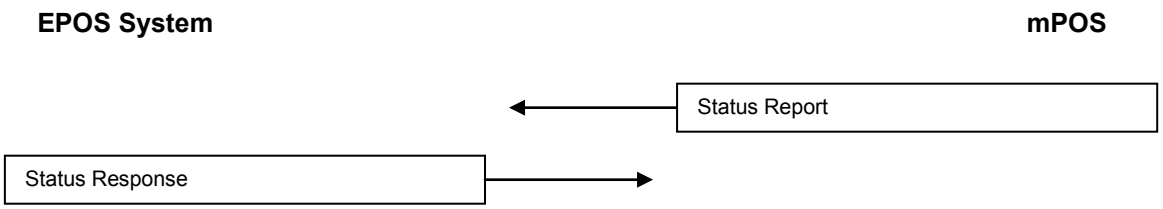
Once this series of message exchanges is complete, the EPOS system should go back to sending a *Start Process* message exchange.



6.6 Status Report

The *Status Report* messages are sent by the mPOS to the EPOS to inform it of certain events that may occur during a transaction. For example, a *Status Report* message will be sent whenever the cardholder inserts or swipes their payment card at the beginning of the transaction.

Description:
The diagram below illustrates the status messages exchanges that may occur during the processing of an ICC transaction:

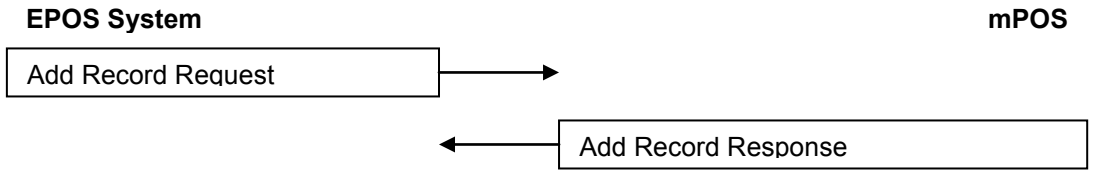


Notes:
The mPOS will report several status messages during a transaction being processed. The EPOS may use this message to acknowledge the current status of the transaction; it also may elect to cancel the transaction (using the response message) if it wishes to do so.

6.7 Transaction Record Storage

At the end of a transaction, the *Add Record* message can be used by the EPOS to store a record in the transaction store

Description:
The diagram below illustrates the status messages exchanges that may occur during the processing of an ICC transaction:



7 Message Content

This section describes the fields that are present in the various messages.

7.1 General Message Format

The request and response messages used in a message exchange shall have the format as shown in the following tables

General Request Content:

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Data	Mandatory or Optional	Fixed or Variable	Numeric or Alpha or Hex or Base64 or DateTime	-
: :	: :	: :	: :	: :
Data	Mandatory or Optional	Fixed or Variable	Numeric or Alpha or Hex or Base64 or DateTime	-

General Response Content:

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Data	Mandatory or Optional	Fixed or Variable	Numeric or Alpha or Hex or Base64 or DateTime	-
: :	: :	: :	: :	: :
Data	Mandatory or Optional	Fixed or Variable	Numeric or Alpha or Hex or Base64 or DateTime	-

General Notes:

- In general, optional and variable length fields are terminated with a FS character.
- The presence of an FS or US character is conditional i.e. it is mandatory if there are any data fields present after the FS but otherwise it is optional.
- Optional data fields that have a variable length and are not present should be marked with a Field Separator (FS) character unless there are no other data fields following it.
- Fields that have a *Boolean* range should only contain ASCII characters ‘0’ and ‘1’. The Field length must be 1.
- Fields that have a *Numeric* range should only contain ASCII characters in the range ‘0’ – ‘9’
- Fields that have a *Alpha* range should only contain ASCII characters in the range 0x20 – 0x7E
- Fields that have a *Hex* range should only contain ASCII characters in the range ‘0’ – ‘9’ and ‘A’ – ‘F’. Also the field length must be even.
- Fields that have a *Base64* range are used for the base-64 encoding of binary data. They should only contain ASCII characters in the range ‘0’ – ‘9’, ‘a’ – ‘z’, ‘A’ –‘Z’, ‘+’, ‘/’ and ‘=’. Also the field length must be a multiple of 4 characters.

- Fields that have a *DateTime* range should only contain ASCII numeric characters and should be in the format: YYMMDDhhmmss
- The *Message Identifier* value of the response message should have the same value of the *Message Identifier* of the request message
- The *Sequence Number* value of the response message should have the same value of the *Sequence Number* of the request message

The general fields are described in the following section

7.2 Common Message Fields

This section describes the message fields that are common to all request and response messages.

Message Identifiers
The *Message Identifier* field identifies a particular message exchange. The value of the *Message Identifier* field should be the same for all requests and responses in a message exchange.

The following table provides the list of identifiers for each message.

Message	Identifier	Comments
Stand-by message group		
Transaction Mode Initialisation	12	
Restart	14	
Get Information	15	
Control	16	
PIN entry	20	PINPad mode only
Display Text	21	PINPad mode only
Load File	62	
Load TR-31 Block	63	
Get Key Information	64	
RKL_CERT_EXCHANGE	65	
RKL_KEY_LOAD	66	
Get Record Count	31	
Fetch Record	32	
Delete Records	33	
Transaction message group		
Stand-by	13	
Add Record	30	
Start Process	41	ICC or Swipe or Contactless
Get Transaction And Application Data	42	ICC Only
Check Exception File	43	*Deprecated*
Check Transaction Log	44	*Deprecated*
Referral Performed	45	ICC or Swipe or Contactless
Go Online	46	ICC or Contactless
Complete Transaction	47	ICC or Contactless
Terminate Transaction	48	ICC or Swipe or Contactless
Status Message	49	ICC or Swipe or Contactless
Get Cashback Amount	50	ICC Only
Get DCC Amount	51	ICC or Swipe
Process Swiped Card	52	Swipe Only
Get Swiped Transaction Data	53	Swipe Only
Signature Verified	54	ICC or Swipe
Logon Transaction	55	Logon Only
Card Details	56	ICC or Swipe
Update Transaction Data	57	ICC only

Sequence Number
The sequence number is used to identify any repeated request or response messages. Messages may need to be repeated if a timeout occurs (if an ACK was sent too late for example). The sequence number in a response should always be the same as the sequence number in the request.

The EPOS system and mPOS should each keep track of the message identifier and sequence number of the last request that was successfully received. If a request is received with the same message identifier and sequence number as the last then it should be ignored (as it is a request that should have already been processed).

At the start of any message exchange, the value of the sequence number should always be equal to 1. It will be incremented for any requests that are subsequently sent in the same message exchange (i.e. any requests with the same message identifier) and will wrap round to 1 after reaching the value of 9.

Response
The response field is only present in response messages. It is used to indicate whether the request was successfully processed or not or whether supplementary data is required.

This field may have one of the following values:

Response Value	Description
0	Request successfully processed
1	Failed to process request
2	Require supplementary information
3	Abort operation
4	Require supplementary MAC generation
5	Require supplementary MAC verification

7.3 Generic parse error response

In the unfortunate event that the mPOS is unable to parse a message from EPOS, it will send an error message with the following format:

Response Content:

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1

Notes:
- The *Message Identifier* field will contain the original message identifier, in the event it was parsed correctly.
- The *Sequence Number* field will contain the original sequence number, in the event it was parsed correctly.
- The *Response* field will have a value of 1 as described above.

8 Message Content – Stand-by Mode

This section describes the content of the messages that are used in stand-by mode.

8.1 Transaction Mode Initialisation (12)

Description:
This message is used to initialise the mPOS for Transaction operation. The EPOS system uses this message to provide the mPOS with information about the terminal and merchant.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Terminal Serial Number	Mandatory	Fixed	Alpha	8
Terminal Type	Mandatory	Fixed	Numeric	2
Terminal Country Code	Mandatory	Fixed	Numeric	3
Terminal Capabilities	Mandatory	Fixed	Hex	6
Terminal Additional Capabilities	Mandatory	Fixed	Hex	10
Terminal Currency Code	Mandatory	Fixed	Numeric	3
Terminal Currency Exponent	Mandatory	Fixed	Numeric	1
Merchant Category Code	Mandatory	Fixed	Numeric	4
Merchant Name And Location	Mandatory	Variable	Alpha	32
FS	Conditional	FS	FS	1
Transaction Category Code	Optional	Fixed	Alpha	1
FS	Conditional	FS	FS	1
TimeOut1	Optional	Variable	Numeric	4
FS	Conditional	FS	FS	1
TimeOut2	Optional	Variable	Numeric	4
FS	Conditional	FS	FS	1
TimeOut3	Optional	Variable	Numeric	4
FS	Conditional	FS	FS	1
Operator PIN	Optional	Fixed	Numeric	4
FS	Conditional	FS	FS	1
Merchant Language	Optional	Fixed	Alpha	2
FS	Conditional	FS	FS	1
Encrypted Data Key	Optional	Fixed	Hex	16, 24 or 32
FS	Conditional	FS	FS	1
Encrypted MAC Key	Optional	Fixed	Hex	16, 24 or 32
FS	Conditional	FS	FS	1
Encrypted PIN Key	Optional	Fixed	Hex	16, 24 or 32

Notes:

- The *Terminal Serial Number* is the serial number given to the terminal by the manufacturer. This should be the same as the value supplied to the EPOS in the Terminal Information Response message and is not the Terminal Identifier, which depends on the card acquirer.
- The value of the *Terminal Type* field should correspond to those given in EMV 4.0 Book 4 Annex A.1.
- The value of the *Terminal Country Code* field should correspond to those given in ISO3166
- The value of the *Terminal Capabilities* field should correspond to those given in EMV 4.0 Book 4 Annex A.2.
- The value of the *Terminal Additional Capabilities* field should correspond to those given in EMV 4.0 Book 4 Annex A.3.

- The value of the *Terminal Currency Code* field should correspond to those given in ISO 4217.
- The value of the *Merchant Category Code* field should correspond to those given in ISO 8583: 1993 (Card Acceptor Business Code)
- The *Transaction Category Code* field is optional – if no value is provided then the application will derive its value from the *Merchant Category Code* value
- Timeout1, 2 and 3 are used as follows:
  - Timeout 1 – by the 'Insert Card' prompt; (Default value is 3 minutes)
  - Timeout 2 – by non-interactive generic prompts only; (Default value is 3 seconds)
  - Timeout 3 – by all other prompts; (Default value is 3 minutes)
- The *Operator PIN* field is optional. If provided it is stored and used to protect the voice referral and signature verification processes.
- The *Merchant Language* field is optional. If provided, prompts will be displayed in chosen language. The field should follow ISO 639-1 formatting.
- The *Encrypted Data Key* is only present if the Data Encryption Key for Master/Session Key is to be updated. The field is the new data encryption session key encrypted under the master data encryption key.
- The *Encrypted MAC Key* is only present if the Data MAC Key for Master/Session Key is to be updated. The field is the new MAC session key encrypted under the master MAC key.

The *Encrypted PIN Key* is only present if the PIN Encryption Key for Master/Session Key is to be updated. The field is the new PIN encryption session key encrypted under the master PIN encryption key.

Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Reader Capabilities	Optional	Fixed	Hex	2
FS	Conditional	FS	FS	1
Secure Mode	Optional	Fixed	Numeric	1
Secure Mode PIN	Optional	Fixed	Numeric	1

Notes:

- The *Reader Capabilities* field provides information on the card reader capabilities of the mPOS (e.g. indicates if the mPOS can read track 2 data from magnetic cards). It may have one of the following values:
  - '01' – A chip card reader is available
  - '03' – A chip card reader and magnetic card reader (track 2) are available

  This field is optional – if the field is not present then the EPOS should assume that the mPOS has only a chip card reader available.
- The *Secure Mode* field indicates how sensitive information (such as the card PAN or track 2 data) is secured by the mPOS. Currently three values are supported:
  - '1' – The data is encrypted using a DUKPT key.
  - '2' – The data is encrypted using DUKPT key – mode 2 (XML format)
  - '3' – The data is encrypted using Master Key/Session Key
- The *Secure Mode PIN field* indicates how the PIN is secured by the mPOS if different to the other secure data.

8.2 File Download (62)

Description:
This message is used to initiate a file download onto the mPOS. Once the EPOS has received a response message that indicates that the mPOS is ready to download, the EPOS should proceed to sending the file content. The way that the content is sent is described below. Once the file has been downloaded, another response message will be sent to the EPOS to indicate whether the file was received ok.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
File Name	Mandatory	Variable	Alpha	32
FS	Mandatory	FS	FS	1
File Size	Mandatory	Variable	Numeric	8
FS	Conditional	FS	FS	1
Baud Rate	Optional	Fixed	Numeric	1
File Version	Optional	Variable	ASCII	2-64

Notes:

- The *File Name* field provides the name of the file. It must include the drive letter e.g. f:\iccapp.cfg
- The *File Size* field provides the size of the file. This allows the mPOS to check that there is sufficient room to hold the file – if there is not enough space then the mPOS can abort the download by returning an appropriate error in the response
- The *Baud Rate* field indicates what baud rate the mPOS should change to in order to receive the subsequent file content data blocks. It may have one of the following values:
  - '0' – default baud
  - '1' – 9600 baud
  - '2' – 19200 baud
  - '3' – 57600 baud
  - '4' – 115200 baud

  If no value is provided (or if a zero value is given) then the baud rate will not be changed (i.e. the default baud rate 19200 will be used)
- The *File Version* is an option field that can be stored with the file name and returned in the Get Information (15) message, info. sub type 0001.
  If specified, this field replaces the Baud Rate field, which will default to a value of '0'.
  The *File Version* must be a minimum of 2 characters long. A single character will be taken as the *Baud Rate*.

Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Result	Mandatory	Fixed	Numeric	1

Notes:

- The *Result* field may have one of the following values:
  - '0' – Ready to receive file data content
  - '1' – Not enough drive space
  - '2' – File received OK
  - '3' – Unable to save file (during communication)
  - '4' – Unable to rename / move file
  - '5' – No data received / timeout
  - '6' – Bad CRC on file

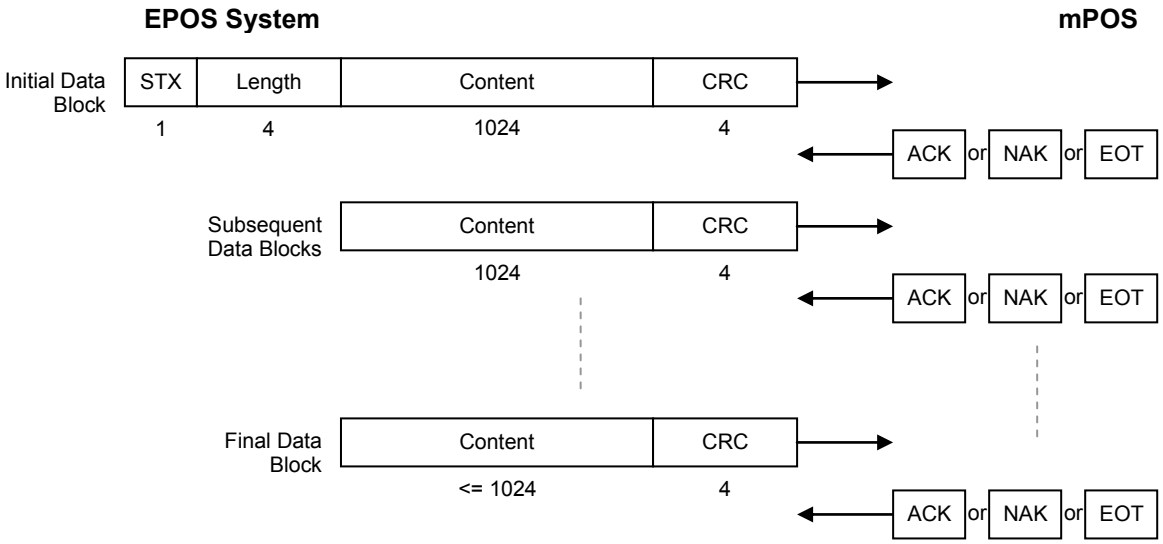
  The values '0' and '1' are only used in the response prior to the file content being received. If the EPOS receives a 'Not enough drive space' (1) error in the first response then the EPOS should abort the download.
  The values '2' – '6' are only used in the response that is sent after the file content has been received. A value other than 'File received OK' (2) indicates that the file was not successfully downloaded
- If there was an error during the download then the file will not be created on the mPOS. In this case, if a file was being replaced (i.e. a file existed with the same file name) then the original file will remain in place – there should be no file corruption.

Downloading the File Content:
The *File Content* must be sent as a series of 1 kilobyte blocks after the mPOS has sent a response indicating that it is ready to receive the file data (the last block may be less than 1K depending of the size of the file content). The first block should have a prefix consisting of an **`STX`** byte followed by a four byte binary value (most significant byte first) that gives the total length of the file content. Each block that is sent should also have a 32-bit CRC suffix that is used the check the data integrity. The mPOS will acknowledge the receipt of each block with either:

- An **`ACK`** byte if the block was successfully received
- A **`NAK`** byte if the block has a data error (bad LRC)
- An **`EOT`** byte if the mPOS could not accept the data block (the block could not be written to the file)

If the EPOS does not receive an **`ACK`** from the mPOS for a data block then it should abort the file load and wait for the mPOS to respond with the final *File Load Response*.

The process is illustrated in the diagram below



Notes:

- The **`Length`** value given in the initial data block should be formatted as a binary value (most significant byte first)
- The **`Content`** is sent in binary
- If the file content is less than 1024 bytes then just an initial data block will be sent (consisting of the **`STX`**, **`Length`**, **`Content`** and **`CRC`** bytes)
- If the file length is not a multiple of 1024 bytes then the final data block will have a content length that is less than 1024 bytes (it will be equal to: **`Length`** mod 1024)
- The **`CRC`** is calculated over the **`Content`** of the data block. I.e. the **`CRC`** of the initial data block will **not** include the **`STX`** and **`Length`** bytes

8.3 Load TR-31 Key Block (63)

Description:
This message is used to load a key, encrypted and formatted according to TR-31, onto the mPOS.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Key Block	Mandatory	Variable	Alpha	256
FS	Conditional	FS	FS	1
Key Block Protection Key KCV	Optional	Fixed	Hex	6

Notes:
- The *Key Block* field must be generated according to TR-31
- At least one Key Block Protection key must have been loaded onto the mPOS in order to load a TR-31 key block. These keys are loaded onto the mPOS at production time using a PKLD.
- The *Key Block Protection Key KCV* field is used to identify the key that is used to authenticate and decrypt the key that is held in the *Key Block* value. This field is required if the mPOS has more than one Key Block Protection key loaded onto it. If the mPOS has only one Key Block Protection key then this key will be used by default if the *Key Block Protection Key KCV* field is not present.

Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Result	Mandatory	Fixed	Numeric	1
KCV	Conditional	Fixed	Hex	6

Notes:
- The *Result* field shall have one of the following values:
  - '0' – The key was successfully loaded onto the mPOS
  - '1' – There is no Key Block Protection key loaded on the mPOS
  - '2' – The required Key Block Protection key could not be found on the mPOS
  - '3' – There was a failure loading the key block
- If the key is successfully loaded then the KCV of the loaded key will be returned in the *KCV* field – no *KCV* field will be present if there was a failure loading the key. For a DUKPT key, the KCV will be generated using its first transaction MAC key.

8.4 Get Key Information (64)

Description:
This message is used to retrieve information of each Master or TR31 Key Block Protection key that has been loaded on the mPOS.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1

Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Key Information 1	Conditional	Fixed	Alpha	12
: : : :	: : : :	: : : :	: : : :	: : : :
Key Information n	Conditional	Fixed	Alpha	12

Notes:

- There will be one *Key Information* field for each Master key or TR31 Key Block Protection key that has been loaded on the mPOS. The *Key Information* field will consist of the following values:

Byte Offset	Description
0 – 1	Key Usage
2	Mode Of Use
3 – 5	Key ID
6 – 11	Key Check Value

The *Key Usage* and *Mode Of Use* values shall correspond to the following keys:

Key Usage	Mode Of Use	Description
K1	D	TR31 Key Block Protection Key
D0	1	Master Key (for data encryption session key)
M3	N	Master Key (for MAC session key)
P0	N	Master Key (for PIN encryption session key)

8.5 RKL_CERT_EXCHANGE (65)

IMPLEMENTATION NOTE: it is expected that the KDH will send the KDH certificate along with its full trust chain for the mPOS to verify against a pre-stored root of trust. However, due to internal memory limitations, the depth of the KDH certificate chain, including the end-point KDH certificate must NOT exceed 10 levels.

1.1.1 Description:

This message is used to load a certificate that can then be used to verify and securely load an RKL key.

1.1.2 Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Last Certificate	Mandatory	Fixed	Alpha	1
Certificate No.	Mandatory	Fixed	Numeric	2
Certificate Length	Mandatory	Fixed	Numeric	4
Certificate	Mandatory	Variable	Hex	4096

1.1.3 Notes:

- The *Last Certificate* field must is N for all messages until the final certificate where it is Y to initiate validation. A value of A means abort certificate load.
- The *Certificate Number* is a sequential number of the certificate in the chain.
- The *Certificate Length* field is length the certificate field.
- The *Certificate* field is the certificate encoded as hex.

1.1.4 Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Result	Mandatory	Fixed	Numeric	1
KRD Certificate Length	Conditional	Fixed	Numeric	4
KRD Certificate	Conditional	Variable	Hex	4096

1.1.5 Notes:

- The *Result* field shall have one of the following values:
  - '0' – The certificate chain was successfully validate by the mPOS
  - '1' – The certificate just sent was successfully received by the mPOS
  - '2' – The certificate just sent was not successfully received by the mPOS, resend
  - '3' – There was a failure validating the certificate chain
- If the certificate chain is successfully loaded and validated then the *KRD Certificate* field will contain the mPOS KRD certificate and its length is defined in *KRD Certificate Length*. In all other cases, these fields will be missing.

8.6 RKL_KEY_LOAD (66)

1.1.6 Description:

This message is used to load a TR31 key, encrypted by the mPOS public asymmetric key and verified using the asymmetric public key loaded using the 65 messages.

1.1.7 Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
TR31 length	Mandatory	Fixed	Numeric	4
Asymmetric Key Blob	Mandatory	Variable	Hex	1200

1.1.8 Notes:

- The *TR31 Length* field defines the bytes length (usually "0256") of the enciphered TR31 block.
- The *Asymmetric Key Blob* field contains the new TR31 key, encrypted using the key owner's KRD public key, of length *TR31 length*, plus the signature as signed by the mPOS KDH private key. The field is encoded as hex.

1.1.9 Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Result	Mandatory	Fixed	Numeric	1

1.1.10 Notes:

- The *Result* field shall have one of the following values:
  - '0' – The key was successfully validate and loaded onto the mPOS
  - '3' – There was a failure validating or processing the blob

8.7 Restart (14)

Description:
This message is used to restart the mPOS. This would normally be used after updating the mPOS.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1

Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1

Notes:
- The mPOS will restart itself once it has successfully sent the response.

8.8 Get Information (15)

Description:
This message is used to get information about the mPOS.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Info. Sub Type	Optional	Fixed	Numeric	4
US	Optional	Fixed	US	1
Info data	Optional	Variable	ASCII	64

Notes:
The info. Sub Type is an optional field. If missing then the response will be the default response, with not Info. Sub Type in the response.

Info Data is an optional field, not valid for info. Sub Type 0000, that can be used to qualify the Info. Sub Type request e.g. For an Info Sub type of 0001 (File versions), a single file name can be set in Info Data to return just that specific file version.

Valid Info. Sub Type:
0000 – Default message response
0001 – File Version request

Response Content (mPOS):
Default/ Info. Sub Type=0000

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Info. Sub Type	Conditional	Fixed	Numeric	4
Serial Number	Mandatory	Fixed	Numeric	8
Version Number	Mandatory	Variable	Alpha	16

Notes:
This is the default response when the request Info. Sub Type was not present or was set to 0000.

The Info. Sub Type in the response will be the same as the info. Sub Type in the request i.e. if it was missing from the request then it will be missing in the response. If it was 0000 in the request then it will be 0000 in the response.

Response Content (mPOS):
Info. Sub Type=0001

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Info. Sub Type	Mandatory	Fixed	0001	4
Repeating group				
File Name	Optional	Variable	ASCII	128
Unit Separator	Optional	Fixed	FS	1
File Version	Optional	Variable	ASCII	64
Field Separator	Optional	Fixed	FS	1

Notes:
This is the file version response when the request Info. Sub Type was set to 0001.

If the Info data was missing from the request then the versions of all standard .cfg files are returned in a repeating array of - File name <US> File version <FS>.

If the Info data was present in the request then only the file name and version for a file on the mPOS device matching the file name sent in the info data request field will be returned

8.9 Control (16)

Description:
This message is used to set volatile device configuration (not preserved in the configuration files). It is intended to be sent to the mPOS device as soon as the serial link service (Bluetooth socket) has been established. Due to the volatile nature of the information within (not backed up in the configuration files for making it available at the next start / reboot) this message could also be sent before initialising transaction mode (via message 12).
This message is currently only used by SPm2 devices.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Auto connect frequency	Optional	Variable	Numeric	3
FS	Conditional	FS	FS	1
Auto connect duration	Optional	Variable	Numeric	4
FS	Conditional	FS	FS	1
Auto connect profile	Optional	Fixed	Numeric	1
FS	Conditional	FS	FS	1
Flags	Optional	Variable	Hex	4

Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1

Notes:

- For SPm2 platform, the auto-connect facility runs on the main thread and only during the idle stage (ready/idle screen displayed). Auto-connect is designed to help establishing the Bluetooth link with the iOS mobile platforms and is recommended to be disabled for the Android clients.
- The auto-connect frequency value is in seconds. A zero value disables the auto-call and the value is capped at maximum 255. If missing, a default value of 7 is used.
- The auto-connect duration value is in milliseconds. The value is capped at maximum 7000. If missing, a default value of 2000 is used.
- The Auto connect profile field selects the Bluetooth profile. The following values may be used for this field:
  - '0' – IAP
  - '1' – SPP

  If missing the default SPP profile shall be used. Only SPm20 currently uses this parameter.
- The flags field represents an array of maximum 16 bits: two bytes passed as four ASCII-Hex digits. Their description, in LSB-0 (right to left, 0 to n) order, is:
  - bit0: the status LED is not active (bit set). When reset, the LED flashes every 5 seconds as to indicate the capability to perform contactless transactions (for the blinking to be active, the terminal must also be USB charging, initialised via Msg-12 and not actually transacting). Default value for bit0 is OFF.
  - bit1: the backlight is active and would not timeout (bit set). When reset, the backlight turns OFF instantly (if was forced ON before) and reverts to being subject to the predefined timer (5 seconds, value not editable) for subsequent interactions. Default value for bit1 is OFF.

The flags are bitwise 'or' cumulative in the value to be passed, e.g. passing a flags value of "0B" equaling "0000 1011" would indicate flags b3 (RFU), b1 (backlight) and b0 (status LED) were set.

8.10 Get Record Count (31)

Description:
This message is used to get the number of record that are currently held in the mPOS.offline transaction store.
This message is only supported by the SPm20 terminals.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1

Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Record Count	Mandatory	Fixed	Numeric	4

-

8.11 Fetch Record (32)

Description:
This message is used to fetch a record that is currently held in the mPOS.offline transaction store.
This message is only supported by the SPm20 terminals.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Record Number	Optional	Fixed	Numeric	4

Notes:

- If the *Record Number* field is not given then the next available record in the offline transaction store shall be returned

Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
MAC	Mandatory	Fixed	Hex	16
KSN	Mandatory	Fixed	Hex	20
Time Stamp	Mandatory	Fixed	DateTime	12
Record Content	Mandatory	Variable	Base64	1968

Notes:

- The *Time Stamp* field shall provide the date and time of the transaction when the record was stored on the terminal
- The *MAC* field shall be calculated over the concatenation of the *Time Stamp* and *Record Content* field values
- The *KSN* field shall identify the DUKPT key that was used to generate the *MAC* field value

8.12 Delete Records (33)

Description:
This message is used to delete records from the mPOS.offline transaction store. This message is typically used once the record(s) have successfully been fetched.
This message is only supported by the SPm20 terminals.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Record Count	Optional	Fixed	Numeric	4

Notes:

- If the *Record Count* is not given then the next available record in the offline transaction store shall be deleted

Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1

8.13 PIN entry (20)

The purpose of this command is to request an encrypted PIN block for online processing (Online PIN Request). The command shall display a prompt message (up to 3 lines) and enable the numeric keypad for PIN entry (only asterisks are shown when numeric keys are pressed).

Important: currently, this command is only available via the USB link. mPOS will discard such requests if received over Bluetooth.

The calling host must specify the encryption key details, such as key index, hierarchy (MK/SK, Fixed, DUKPT), Session Key data and its encryption mode for MK/SK. Additionally the calling entity must specify a maximum number of PIN digits, whether the Enter key must be pressed after that maximum is reached and a timeout for the operation. The request structure is listed in the table below:

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Key Index Data	Optional	Variable	Numeric	2
FS	Mandatory	FS	FS	1
Encrypted Data Key	Optional	Variable	Hex	32 or 48
FS	Mandatory	FS	FS	1
Data Key Mode	Optional	Fixed	Numeric	1
FS	Mandatory	FS	FS	1
PAN	Mandatory	Variable	ASCII or Hex	19 or 48
FS	Mandatory	FS	FS	1
Clear PAN Length	Mandatory	Variable	Numeric	2
FS	Mandatory	FS	FS	1
PIN Block Format	Optional	Fixed	Numeric	1
FS	Mandatory	FS	FS	1
Key Index PIN	Optional	Variable	Numeric	2
FS	Mandatory	FS	FS	1

Key Type PIN	Mandatory	Fixed	Numeric	1
Encrypted PIN Key	Optional	Variable	Hex	32 or 48
FS	Mandatory	FS	FS	1
PIN Key Mode	Optional	Fixed	Numeric	1
FS	Mandatory	FS	FS	1
Bypass allowed	Mandatory	Fixed	Numeric	1
Max. PIN Digits	Mandatory	Variable	Numeric	2
FS	Mandatory	FS	FS	1
Keypad Timeout	Mandatory	Variable	Numeric	2
FS	Mandatory	FS	FS	1
Display Line 1	optional	Variable	UTF-8	64
FS	Mandatory	FS	FS	1
Display Line 2	optional	Variable	UTF-8	64
FS	Mandatory	FS	FS	1
Display Line 4	optional	Variable	UTF-8	64

Notes

- Key Index Data identifies the key to be used for decrypting the data session key. This is provided for future enhancements only; the Spm2/20 products will only support (be loaded with) one Data MasterKey.
- The Encrypted Data Key is only present if the Data Encryption Key for Master/Session Key is to be updated. The field is the new data encryption session key encrypted under the master data encryption key at Key Index Data. This key used for extracting the PAN. The key is updated/extracted accordingly to the Data Key Mode.
- Data Key Mode is an optional field that specifies the DES block mode used for decoding the Encrypted Data Key. It overwrites (if present) the terminal configuration TML_SecurityModeSessionData element with a corresponding value. If not present, the data session key is extracted accordingly to existing TML_SecurityModeSessionData. The possible values are:
  - 0 = CBC encrypted (TML_SecurityModeSessionData = 3 or missing)
  - 1 = ECB encrypted (TML_SecurityModeSessionData = 5)

- PAN could be either in clear or encrypted with the above session data key. If in clear, the value should be presented in ASCII. If encrypted, the value should be the hexadecimal representation. Example:
  - 4444333322221111 (max 19 ASCII chars) or
  - AF7560D598D58248098A71B70EA79CD160D7DB568B64D3EF (max 48 hex / 24 bytes padded

data).

The CBC mode is always used for encrypting the PAN value. Although the PAN field has been defined as mandatory, there are cases when the value will not be used.

- Clear PAN Length has a non-zero value as an indication that the PAN value was encrypted (after decryption it helps with removing the padding added at encryption stage). A zero length value indicates the PAN value is in clear (actual ASCII length being already available from the message parsing layer).
- The PIN Block Format instructs how to the construct the PIN block accordingly to the ISO-9564 options. The supported values for this field are:
  - 0 = use Format 0
  - 1 = use Format 1
  - 3 = use Format 3

By default (missing value for field) the mPOS products will use the Format 0. Format 2 is not supported.

- The Key Index PIN could identify two separate things depending on the encryption scheme used:
  - if using MK/SK: it points to the MK to be used for decrypting the Encrypted PIN Key.
  - if using DUKPT: it points to the key to be used for encrypting the PIN block.

Subject to the value being translated to the mPOS type specific key slots, the possible values are:
- 0 = Use the Data key in the *exceptional* case the acquirer uses a single key. **DUKPT only!**
- 1 = use the PIN key (MK or DUKPT) loaded for the first acquirer
- 2 = use the PIN key (MK or DUKPT) loaded for the second acquirer
- 3 = use the PIN key (MK or DUKPT) loaded for the third acquirer, etc

This field is provided for future enhancements only; the Spm2/20 products will only support (be loaded with) one PIN Master Key and maximum one DUKPT PIN key.

Unlike the standard transaction processing of the mPOS API, there will be no implicit fallback to the DUKPT Data Key in the event the DUKPT PIN key was not loaded; use a value of '0' in this case.

- The Key Type PIN identifies a particular encryption mode for the PIN block The supported values are in the range:
  - 0 - Master/Session uses the passed/updated PIN session key.
  - 1 - DUKPT using the factory loaded DUKPT key.
- The Encrypted PIN Key is only present if the PIN Encryption Key for Master/Session Key is to be updated. The field is the new PIN encryption session key encrypted under the master PIN encryption key at Key Index PIN. The key is updated/extracted accordingly to the PIN Key Mode.
- PIN Key Mode is an optional field that specifies the DES block mode used for decoding the Encrypted PIN Key. It overwrites (if present) the terminal configuration element TML_SecurityModeSessionPIN with a corresponding value. If not present, the PIN session key is extracted accordingly to the existing TML_SecurityModeSessionPIN. The possible values are:
  - 0 = CBC encrypted (TML_SecurityModeSessionPIN = 3 or missing)
  - 1 = ECB encrypted (TML_SecurityModeSessionPIN = 5)
- Bypass allowed indicates if the PIN entry is mandatory or not. On SPm2, if bypass was allowed, pressing ENTER with a zero length PIN value would return a bypass event (zero length PIN returned). If bypass was disabled, ENTER key on a blank value would not work. SPm20 is expected to mirror the same behaviour (subject to supporting SDK library capabilities). Possible values are '0' disabled and '1' enabled.
- Max. PIN Digits has a value in the '4'-'12' range (passed value will be capped at 12).
- Keypad Timeout represents the timeout value between key presses in 1 seconds units. A value of '0' **Is Not Allowed!** as to enforce a timing-out exit route.
- Display Lines are UTF-8 encoded. The possible binary data for non-Latin alphabet are known not to clash with the ETX message end mark.
- PIN entry requests to use FIXED keys MUST indicate Key Type = 0 (MK/SK), Encrypting Key Length = 0, and MUST NOT include any PIN Encrypting Key data.

The mPOS device will then process the request, attempt to perform the PIN entry operation and finally reply with a corresponding message, whose structure is listed in the following table below:

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Result	Mandatory	Fixed	Numeric	2
PIN Length	Mandatory	Variable	Numeric	2
FS	Mandatory	FS	FS	1
Encrypted PIN Block	Optional	Fixed	Hex	16
US	Conditional	US	US	1
DUKPT Key Serial Number	Conditional	Fixed	Hex	20

Notes

- The Response field is the standard API messaging response code. It would indicate failure only if there was a considerable problem with the request (invalid formatting, failed to parse, corrupt data, etc.) or there were some error updating the session keys (at least

on Spm2 the keys handling would happen during the early message's processing and before the associated routine, namely PIN entry, was called).

- Result indicates the PIN entry outcome. The possible values are:
  - 00 = Good
  - 01 = Timeout
  - 02 = General Error
  - 04 = Cancelled
  - 05 = Bypassed
  - 42 = Bad Key Tag
  - 43 = Bad Master Key Index
  - 49 = PIN entry velocity exceeded

- Please note that unlike the API integrated transaction carried-out completely on the SPm devices, there will be only partially resolved API 49 - Status messages exchanged. The initial design is to only report the start of PIN entry operation via a 'C0' Status message. This will provide the EPOS with a potential cancellation exit route. Once started, the PIN entry operation may be aborted from the EPOS by sending an ENQ byte over the serial link.
- PIN Length is the number of PIN digits entered by user (the clear PIN length). Possible values are '0' if no value was captured (timing-out, cancellation, etc. events) or in the 4-12 range (up to the Max. PIN Digits as requested).
- DUKPT KSN is only present the operation result was successful and the Key Type PIN field requested a DUKPT scheme. To keep consistency with the general mPOS API, the KSN is US separated from the encrypted data field.

8.14 Display Text (21)

The purpose of this command is to display text on the PIN Pad screen. The message structure is detailed in the table below:

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Display Line 1	optional	Variable	UTF-8	64
FS	Mandatory	FS	FS	1
Display Line 2	optional	Variable	UTF-8	64
FS	Mandatory	FS	FS	1
Display Line 3	optional	Variable	UTF-8	64
FS	Mandatory	FS	FS	1
Display Line 4	optional	Variable	UTF-8	64

Notes

- If all of the optional lines are missing then the screen will be cleared (go blank).
- Upon receiving a request of this type, the mPOS devices will no longer display the regular idling screens. If reverting to one of those screens is required, the MPOS must either resend one of the API messages Stand-By (13) / Transaction Mode Initialise (12) or set directly the desired text via a new instance of this message.

As per usual mPosAPI protocol, a response is expected; its format is described in the following table:

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1

9 Message Content – Transaction Mode

This section describes the content of the messages that are used in Transaction mode.

9.1 Start Process (41 - ICC or Swipe)

Description:
This message is used to start a process on the mPOS. The EPOS system can choose what type of card to initially accept (ICC/contactless/ swipe)

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Process Type	Mandatory	Fixed	Alpha	1
POS Entry Mode Code	Mandatory	Fixed	Numeric	2
Transaction Date And Time	Conditional	Fixed	DateTime	12
FS	Conditional	FS	FS	1
Transaction Type	Conditional	Fixed	Numeric	2
FS	Conditional	FS	FS	1
Authorised Amount	Conditional	Variable	Numeric	12
FS	Conditional	FS	FS	1
Other Amount	Conditional	Variable	Numeric	12
FS	Conditional	FS	FS	1
Gratuity Amount	Conditional	Variable	Numeric	12

Notes:

- The *Process Type* field indicates the type of process that should be started on the mPOS. The following values may be used for this field:
  - '0' – Start ICC card only transaction
  - '1' – Start Swipe card only transaction
  - '2' – Start ICC card or swipe card transaction (fallback allowed)
  - '3' – Start ICC card or swipe card transaction (no fallback allowed)
  - '4' – Start logon transaction
  - '5' – Start card details transaction (ICC card or Swipe card – fallback allowed)
  - '8' – Start contactless card only transaction
  - '9' – Start contactless card transaction (fall forward to ICC/Swipe allowed)
  - 'B' – Start Balance Inquiry
  - 'C' – CVM/PIN Verification

  If fallback is allowed (value '2') then the transaction will fall back to using the card magnetic stripe in the event of an ICC failure.
  If fallback is not allowed (value '3') then the transaction will be voided in the event of an ICC failure.
- The *POS Entry Mode Code* field is dependent on the payment system requirements. For example, APACS may use the following value:
  - '32' – ICC, Customer Present, PIN
- The fields *Transaction Date And Time*, *Transaction Type*, *Authorised Amount*,*Other Amount and Gratuity Amount* are mandatory for contactless card transactions. They are optional for ICC and swipe card transactions
- If Gratuity amount is presented but of value zero then the application will prompt for a value. If non zero t will be applied to the authorised amount. In case of falling back to ICC, the gratuity value will be preserved and no second edit prompt will should be presented.

9.2 Get Transaction and Application Data (42 - ICC Only)

Description:
This message is used to obtain transaction and application payment related data during card application being selected. Expect the status message for AID selection completed to follow this exchange.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Application Identifier	Mandatory	Variable	Hex	32

Notes:
- The *Application Identifier* field identifies the card application (payment method) that was chosen by the card and/or cardholder at the start of the transaction.

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Transaction Date And Time	Mandatory	Fixed	DateTime	12
Transaction Type	Mandatory	Fixed	Numeric	2
Authorised Amount	Mandatory	Variable	Numeric	12
FS	Mandatory	FS	FS	1
Other Amount	Optional	Variable	Numeric	12
FS	Mandatory	FS	FS	1
Acquirer Identifier	Mandatory	Variable	Numeric	11
FS	Mandatory	FS	FS	1
Terminal Identifier	Mandatory	Fixed	Alpha	8
Merchant Identifier	Mandatory	Variable	Alpha	15
FS	Mandatory	FS	FS	1
Application Version Number	Mandatory	Fixed	Hex	4
TAC Default	Mandatory	Fixed	Hex	10
TAC Denial	Mandatory	Fixed	Hex	10
TAC Online	Mandatory	Fixed	Hex	10
Terminal Risk Management Data	Optional	Variable	Hex	16
FS	Conditional	FS	FS	1
Force Online	Optional	Fixed	Numeric	1
FS	Conditional	FS	FS	1
Target Percentage used in Random Selection	Optional	Fixed	Numeric	2
FS	Conditional	FS	FS	1
Max Target Percentage used in Random Selection	Optional	Fixed	Numeric	2
FS	Conditional	FS	FS	1
Threshold Value used in Random Selection	Optional	Variable	Numeric	12
FS	Conditional	FS	FS	1
Floor Limit	Optional	Variable	Numeric	12
FS	Conditional	FS	FS	1
TDOL	Optional	Variable	Hex	32

FS	Conditional	FS	FS	1
DDOL	Optional	Variable	Hex	32
FS	Conditional	FS	FS	1
Constraint Checks	Optional	Fixed	Hex	1
FS	Conditional	FS	FS	1
Additional Constraint Checks	Optional	Fixed	Hex	1

Notes:

- The value of the *Transaction Type* field should correspond to the first two digits of the Processing Codes given in ISO 8583: 1987
- The *Other Amount* field must be present if the transaction has a cashback amount (i.e. *Transaction Type* has been set to *Goods and Service with Cash Disbursement*)
- The *Acquirer Identifier* field identifies the acquirer that the transaction details are sent to for the chosen card application (payment method).
- The *Terminal Identifier* identifies the terminal to the acquirer
- The *Merchant Identifier* identifies the merchant to the acquirer
- The *TAC Default*, *TAC Denial* and *TAC Online* field values should correspond to those given in EMV 4 Book 3 Annex C.5 (Terminal Verification Results)
- The *Target Percentage*, *Max Target Percentage* and *Threshold Value* fields are mandatory for offline terminals with online capabilities
- The *Force Online* field indicates whether the transaction should be forced online. It is only appropriate for terminals that have online capabilities and that are allowed to force transactions online (as determined by payment system rules).
- The *Floor Limit* field is mandatory for offline only terminals or offline terminals with online capability
- The *Constraint Checks* field is used to determine whether the card should be checked against an exception file, whether the transaction should be checked against a transaction log, whether PIN entry bypass is allowed and whether DCC is allowed. The field may have one of the following values:

Value	Allow DCC	Check Exception File	Check Transaction Log	Allow PIN Entry Bypass
'0'	NO	NO	NO	NO
'1'	NO	NO	NO	YES
'2'	NO	NO	YES	NO
'3'	NO	NO	YES	YES
'4'	NO	YES	NO	NO
'5'	NO	YES	NO	YES
'6'	NO	YES	YES	NO
'7'	NO	YES	YES	YES
'8'	YES	NO	NO	NO
'9'	YES	NO	NO	YES
'A'	YES	NO	YES	NO
'B'	YES	NO	YES	YES
'C'	YES	YES	NO	NO
'D'	YES	YES	NO	YES
'E'	YES	YES	YES	NO
'F'	YES	YES	YES	YES

  If no *Constraint Checks* field is given in the response then a value of zero will be assumed. I.e. No DCC will be allowed; there will be no checks made against exception files and transaction logs; and no PIN entry bypass will be allowed
- The *Additional Constraint Checks* field is used to determine whether 'quick' refunds are permitted (this is where, for refunds, data is just read from the chip card and no other processing is performed), whether mPOS should prompt for gratuity to be entered, whether mPOS should request ICC data update (message 57), etc.
  The field may have one of the following values:

Value	Update ICC data	Prompt for Gratuity	Perform Quick Refunds
'0'	NO	NO	NO
'1'	NO	NO	YES
'2'	NO	YES	NO
'3'	NO	YES	YES
'4' to '7'	YES	As four cases above	As four cases above

If no *Additional Constraint Checks* field is given in the response then a value of zero will be assumed. I.e. No quick refunds will be performed and no prompt for gratuity will be displayed;

9.3 Update Transaction and Application Data (57 – ICC only)

Description:
This message may be used (market specific, subject to configuration) to update transaction and application payment related data once a card application has been selected.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
BIN range	Mandatory	Fixed	Numeric	6

Notes:
- The *Bin Range* field identifies the card scheme (payment method) for the selected AID application. This message helps setting-up different parameters for particular products of the same EMV application (BIN range scheme identification similar to swipe processing).
- The *Bin Range* represents the left six digits (MSB) of the PAN number.

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Acquirer Identifier	Mandatory	Variable	Numeric	11
FS	Mandatory	FS	FS	1
Application Version Number	Mandatory	Fixed	Hex	4
TAC Default	Mandatory	Fixed	Hex	10
TAC Denial	Mandatory	Fixed	Hex	10
TAC Online	Mandatory	Fixed	Hex	10
Terminal Risk Management Data	Optional	Variable	Hex	16
FS	Conditional	FS	FS	1
Force Online	Optional	Fixed	Numeric	1
FS	Conditional	FS	FS	1
Target Percentage used in Random Selection	Optional	Fixed	Numeric	2
FS	Conditional	FS	FS	1
Max Target Percentage used in Random Selection	Optional	Fixed	Numeric	2
FS	Conditional	FS	FS	1
Threshold Value used in Random Selection	Optional	Variable	Numeric	12
FS	Conditional	FS	FS	1
Floor Limit	Optional	Variable	Numeric	12

Notes:
- All fields have the same meaning and definition as per the initial Get Transaction Data message (42).

9.4 Get Cashback Amount (50 - ICC Only)

Description:
This message is used to obtain an optional cashback amount for a 'Goods and Service' transaction. This message will only be sent to the EPOS system if a cashback amount can be supplied without the transaction being declined offline.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Application Identifier	Mandatory	Variable	Hex	32

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Other Amount	Optional	Variable	Numeric	12

Notes:
- The *Other Amount* field in the response is optional. If no cashback is required for the transaction then no value should be sent in this field – it should just be empty.
- If a value is supplied in the *Other Amount* field then this will be added to the *Authorised Amount* that was given in *Get Transaction and Application Data*. The *Transaction Type* will also be changed to *Goods and Service with Cash Disbursement*.
- The message will only be sent to the EPOS if the following conditions are met:
  - A cashback amount has not yet been provided. I.e. the *Transaction Type* indicates *Goods and Service*
  - The POS supports cashback. I.e. bit 5 of byte 1 of *Additional Terminal Capabilities* is set
  - Supplying a cashback amount will not result in the transaction being declined offline (due to Processing Restrictions failing)

9.5 Get DCC Amount (51 - ICC or Swipe)

Description:
This message is used to request DCC information from the EPOS.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Application PAN or Track2 Card PAN	Mandatory	Variable	Numeric	19
FS	Mandatory	FS	FS	1
Authorised Amount	Mandatory	Variable	Numeric	12
FS	Conditional	FS	FS	1
Application Identifier	Optional	Variable	Hex	32
FS	Conditional	FS	FS	1
Cardholder Currency	Optional	Fixed	Numeric	3
FS	Conditional	FS	FS	1
Cardholder Currency Exponent	Optional	Fixed	Numeric	1

Notes:

- The *Cardholder Currency* and *Cardholder Currency Exponent* field values are optional and will be provided if they appear on the chip card. There may be circumstances where the card has just the currency code but no exponent, in which case the EPOS will need to determine the appropriate exponent value. Alternatively, the EPOS may choose to ignore these values altogether and use some other method to determine the cardholder currency – typically, by mapping the IIN (first 6 digits of the PAN) to a currency code.
- *Application Identifier* is omitted in the swipe version.
- The *PAN* or *Track2 PAN* will be masked with 0s to show only the first 6 and last 4 digits of the real PAN.

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Authorised Amount (in Cardholder Currency)	Optional	Variable	Numeric	12
Cardholder Currency	Optional	Fixed	Numeric	3
Cardholder Currency Exponent	Optional	Fixed	Numeric	1
FS	Conditional	FS	FS	1
Foreign Exchange Rate	Optional	Variable	Numeric	12
FS	Conditional	FS	FS	1
Foreign Exchange Rate Exponent	Optional	Variable	Numeric	1

Notes:

- The fields *Cardholder Currency*, *Cardholder Currency Exponent* and *Authorised Amount (in Cardholder Currency)* must be present if the cardholder is allowed to choose to pay in their home currency. These may be different from the values that may have been sent in the request
- The fields *Foreign Exchange Rate* and *Foreign Exchange Rate Exponent* may be present if the cardholder is allowed to choose to pay in their home currency

- If no values are provided in the fields *Authorised Amount (in Cardholder Currency)*, *Cardholder Currency* and *Cardholder Currency Exponent* then the cardholder will not be prompted for DCC.

9.6 Referral Performed (45 - ICC or Swipe or Contactless)

Description:
This message is used to send the result of a voice referral transaction to the EPOS system.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
FS	Mandatory	FS	FS	1
Referral Auth Code	Optional	Variable	Alpha	9
FS	Mandatory	FS	FS	1
Referral Result	Mandatory	Fixed	Numeric	1

Notes:

- The *Referral Auth Code* will contain the authorisation code. It should be left blank for a declined transaction.
- The *Referral Result* field indicates whether the referral was approved or declined.
  It shall have one of the following values:
  - '1' - The transaction was approved as a result of the referral
  - '2' - The transaction was declined as a result of the referral
- This message only informs the EPOS that a referral has been performed on the mPOS

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1

9.7 Go Online (46 - ICC & Contactless)

Description:
This message is used to indicate that the transaction should go online for authorisation.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Application Identifier	Mandatory	Variable	Hex	32
FS	Mandatory	FS	FS	1
Advice Required	Mandatory	Fixed	Numeric	1
FS	Conditional	FS	FS	1
Gratuity Amount	Optional	Variable	Numeric	12
FS	Conditional	FS	FS	1
Encrypted PIN	Optional	Fixed	Hex	16
US	Conditional	US	US	1
DUKPT Key Serial Number	Conditional	Fixed	Hex	20

Notes:

- The *Advice Required* field value indicates whether an advice message needs to be sent to the acquirer host. The value of the field will have one of the following values:
  - '0' – No advice is required
  - '1' – An advice is required
- If the card holder entered a PIN for online verification then its encrypted value will be present in the *Encrypted PIN* field. If DUKPT encryption is used then the key that was used to encrypt the PIN is identified by the *DUKPT Key Serial Number* field.
- If the card holder did not enter a PIN for online verification then the *Encrypted PIN* and *DUKPT Key Serial Number* fields will not be present

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Result	Mandatory	Fixed	Numeric	1
Issuer Response	Optional	Fixed	Numeric	1
Issuer Authorisation Response Code	Optional	Variable	Alpha	2
FS	Conditional	FS	FS	1
Issuer Authentication Data	Optional	Variable	Hex	32
FS	Conditional	FS	FS	1
Issuer Script	Optional	Variable	Hex	256
FS	Conditional	FS	FS	1
Encrypted Data Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1
Encrypted MAC Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1
Encrypted PIN Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1

Notes:

- The *Result* field indicates whether the EPOS system successfully went online and the type of request that was sent (authorisation or financial transaction). The value of the field will have one of the following values:
  - '0' – The EPOS system was unable to go online
  - '1' – The EPOS system failed to get a response to an authorisation request
  - '2' – The EPOS system successfully got a response to an authorisation request
  - '5' – The EPOS system failed to get a response to an EFT request
  - '6' – The EPOS system successfully got a response to an EFT request
  - '7' – The EPOS system successfully got a SEPA authorization
- The *Issuer Response* field is mandatory if the EPOS system successfully went online. This field should indicate whether the request was authorised, declined or referred. The value of the field will have one of the following values:
  - '1' – The host approved the request
  - '2' – The host declined the request
  - '3' – The host referred the request
- The *Issuer Authorisation Response Code* field is mandatory if the EPOS system successfully went online.
- The *Encrypted Data Key* is only present if the Data Encryption Key for Master/Session Key is to be updated. The field is the new data encryption session key encrypted under the master data encryption key.
- The *Encrypted MAC Key* is only present if the Data MAC Key for Master/Session Key is to be updated. The field is the new MAC session key encrypted under the master MAC key.
- The *Encrypted PIN Key* is only present if the PIN Encryption Key for Master/Session Key is to be updated. The field is the new PIN encryption session key encrypted under the master PIN encryption key.

9.8 Complete Transaction (47 - ICC & Contactless)

Description:
This message is used to indicate that the transaction is complete. Additional actions may be required on the part of the EPOS system to capture the transaction result and print a receipt.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Application Identifier	Mandatory	Variable	Hex	32
FS	Mandatory	FS	FS	1
Transaction Result	Mandatory	Fixed	Numeric	1
Completion Action	Mandatory	Fixed	Numeric	1
Card Checks	Optional	Fixed	Numeric	1
FS	Conditional	FS	FS	1
Gratuity Amount	Optional	Variable	Numeric	12

Notes:

- The *Transaction Result* field indicates whether the transaction was finally approved or declined. The value of the field can have one of the following values:
  - '0' – The transaction was approved
  - '1' – The transaction was declined
  - '2' – The transaction was approved after a referral
  - '3' – The transaction was declined after a referral
- The *Completion Action* field indicates whether
  - A reversal needs to be sent to the acquirer. This may happen, for example, if the transaction was approved online but finally declined by the card.
  - The transaction needs to be captured and sent to the acquirer, if it hasn't been captured online already
  - An advice needs to be created. This may be required if any issuer script results need to be sent back to the acquirer.

  The value may have one of the following values:
  - '0' – No capture, reversal or advice is required
  - '1' – An advice is required
  - '2' – A reversal is required
  - '4' – A capture is required
  - '6' – A reversal is required because there was no EFT response. A capture is also required because the transaction was approved offline
- The *Card Checks* field indicates whether additional card checks are required. The value of the field can have one of the following values:
  - '0' – No further card checks are required
  - '1' – A cardholder signature check is required
- This field is optional – if the field is not present then no further card checks are required.

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Attendant Action	Optional	Fixed	Numeric	1
FS	Conditional	FS	FS	1
Encrypted Data Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1
Encrypted MAC Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1
Encrypted PIN Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1

Notes:

- The *Attendant Action* field indicates whether any further action is required by the attendant in order to complete the transaction. E.g. Cardholder signature checks etc. If the value indicates that further action is required then the cardholder will be prompted to hand their card to the attendant. The value may have one of the following values:
  - '0' – No further action is required by the attendant. The cardholder can retain their card.
  - '1' – The attendant requires the card to check the cardholder's signature
  - '2' – The attendant requires the card to perform a referral
- If the *Attendant Action* field is not present then no further action will be required by the attendant

If the *Attendant Action* field is not zero and an Operator PIN was provided in the *Initialisation* message then the attendant will be prompted to enter the Operator PIN before the action can be carried out. Three attempts will be allowed to enter the Operator PIN. If three wrong entries are made then the result of the attendant action will be a negative response i.e. the signature was not verified or the referral was declined.

If the *Attendant Action* field indicates that a cardholder signature check is required (i.e. it has a value of '1') then the mPOS will prompt the attendant to check the cardholder signature.

The result of the signature check is returned to the EPOS using the *Signature Verified* message.

If the *Attendant Action* field indicates that a referral is required (i.e. it has a value of '2') then the mPOS will prompt the attendant to enter the referral result and referral auth code if applicable.

The result of the referral is returned to the EPOS using the *Referral Performed* message.

9.9 Terminate Transaction (48 - ICC or Swipe or Contactless or Logon)

Description:
This message is used to indicate that the transaction has been terminated. The reason for termination shall be provided in the message.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Reason	Mandatory	Fixed	Numeric	2

Notes:

- The *Reason* field value will give an indication of why the transaction was terminated:
  - '00' – (mPOS) General Failure
  - '01' – (Chip) Application Selection Failure
  - '02' – (Chip) Initiate Application Processing Failure
  - '03' – (Chip) Read Application Data Failure
  - '04' – (Chip) Offline Data Authentication Failure
  - '05' – (Chip) Process Restrictions Failure
  - '06' – (Chip) Terminal Risk Management Failure
  - '07' – (Chip) Cardholder Verification Method Failure
  - '08' – (Chip) Terminal Action Analysis Failure
  - '09' – (Chip) Card Action Analysis Failure
  - '10' – (Chip) Completion Failure
  - '11' – (EPOS) Transaction Terminated
  - '12' – (Chip) No Answer to Reset
  - '13' – (Swipe) Read Failure
  - '14' – (Chip) Card Removed
  - '15' – (mPOS) User Cancelled
  - '16' – (Chip) No Supported Applications
  - '17' – (Chip) Card Blocked
  - '18' – (Chip) Read Failure
  - '19' – (mPOS) User Time Out
  - '20' – (mPOS) DUKPT Key Failure
  - '21' – (mPOS) MK/SK Key Failure
  - '22' – (Contactless) Not Allowed
  - '23' – (Contactless) Aborted
- Generally, a transaction should be terminated and another method of payment needs to be sought if there is a chip processing error. However, some card issuers/acquirers may permit fallback to card swipe on certain chip errors – these may include:
  - No answer to reset (reason code 12)
  - No supported applications (reason code 16)
  - Unexpected response from the chip card (reason code 18) e.g. card responds with the status code '6985' on the 1st Generate AC command

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1

9.10 Signature Verified (54 - ICC or Swipe or Contactless)

Description:
This message is used to inform the EPOS of the result of the card holder verification that has taken place on the mPOS

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Signature Verification Result	Mandatory	Fixed	Numeric	1

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1

Notes:
- The *Signature Verification Result* field can have one of the following values:
  - '0' – Card holder signature was rejected
  - '1' – Card holder signature was accepted

9.11 Process Swiped Card (52 - Swipe Only)

Description:
This message is used to request that the EPOS should process the swiped card transaction. The EPOS should attempt to authorise the transaction either offline, by going online or by voice referral. The EPOS is also responsible for capturing any transaction data if necessary.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
ICC Fallback	Mandatory	Fixed	Numeric	1
Masked Card Track 2 Data	Mandatory	Variable	Alpha	40
US	Conditional	US	US	1
Encrypted Card Track 2 Data	Optional	Variable	Hex	2048
US	Conditional	US	US	1
DUKPT Key Serial Number or Initial Vector	Conditional	Fixed	Hex	20
FS	Conditional	FS	FS	1
Gratuity Amount	Optional	Variable	Numeric	12
FS	Conditional	FS	FS	1
Encrypted PIN	Optional	Fixed	Hex	16
US	Conditional	US	US	1
DUKPT Key Serial Number	Conditional	Fixed	Hex	20
FS	Conditional	FS	FS	1
Cardholder Mobile Number	Conditional	Variable	Hex	12
FS	Conditional	FS	FS	1
Masked Track 1 data	Conditional	Variable	Alpha	90

Notes:

- If DUKPT is used to encrypt the Track 2 Data then the *DUKPT Key Serial Number* field is mandatory.
- If Master Key/Session Key and CBC encryption are used then the Initial Vector may be present after the US
- If the card holder entered a PIN for online verification then its encrypted value will be present in the *Encrypted PIN* field. The key that was used to encrypt the PIN is identified by the *DUKPT Key Serial Number* field.
- If a single BDK is used for both data and PIN encryption then the KSN for both the Track 2 data and the Encrypted PIN will be the same, so the second DUKPT Key Serial Number will not be present.
- If the card holder did not enter a PIN for online verification then the *Encrypted PIN* and second *DUKPT Key Serial Number* fields will not be present
- If DUKPT is used to encrypt the PIN and the DUKPT BDK is different to the Track 2 Data BDK then the second *DUKPT Key Serial Number* field is mandatory. If the same BDK is used then the field will not be present.
- If Cardholder Mobile number was requested in Message 53 then the value will be present in *Cardholder Mobile Number* field
- If the Track 1 Data was requested in Message 53 then the Masked Track 1 will be present in *Masked Track 1 Data* field

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Transaction Result	Mandatory	Fixed	Numeric	1
FS	Conditional	FS	FS	1
Encrypted Data Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1
Encrypted MAC Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1
Encrypted PIN Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1

Notes:

- The field *ICC Fallback* indicates whether the swipe request follows and ICC failure. It may have one of the following values:
  - '0' – Card has been swiped at the beginning of the transaction, no ICC failure
  - '1' – Card has been swiped following an ICC process failure
- The field *Transaction Result* indicates whether the transaction was authorised, declined, cancelled or if additional actions are required to complete the transaction. It may have one of the following values:
  - '0' – Transaction Completed (i.e. Approved)
  - '1' – Transaction Declined
  - '2' – Transaction Cancelled
  - '3' – Transaction Void
  - '4' – Attendant requires card for referral
  - '5' – Attendant requires card for signature check

If the *Transaction Result* field indicates that a referral or cardholder signature check is required (i.e. it has a value of '4' or '5') then the mPOS will check if an Operator PIN was supplied in the *Initialisation* message. If an Operator PIN was supplied then the mPOS will prompt the attendant to enter the Operator PIN.

The attendant may attempt the Operator PIN entry 3 times. If the PIN is entered incorrectly 3 times or the attendant presses Cancel, the *Transaction Result* field will be changed to '2', Transaction cancelled.

If the Operator PIN is correctly entered or no Operator PIN was set in the *Initialisation* message the mPOS will prompt the attendant for a referral and/or a cardholder signature check. If a referral is performed then the result of the referral is returned using the *Referral Performed* message. The result of any signature check is returned to the EPOS using the *Signature Verified* message.

- The *Encrypted Data Key* is only present if the Data Encryption Key for Master/Session Key is to be updated. The field is the new data encryption session key encrypted under the master data encryption key.
- The *Encrypted MAC Key* is only present if the Data MAC Key for Master/Session Key is to be updated. The field is the new MAC session key encrypted under the master MAC key.
- The *Encrypted PIN Key* is only present if the PIN Encryption Key for Master/Session Key is to be updated. The field is the new PIN encryption session key encrypted under the master PIN encryption key.

9.12 Get Swiped Transaction Data (53 - Swipe Only)

Description:
This message is used to request the EPOS some data about the swiped transaction about to be performed. In this version only the total amount to be authorised is returned by EPOS but other data could be added in the future.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Masked Card Track 2 Data	Mandatory	Variable	Alpha	40
US	Mandatory	US	US	1
Encrypted Card Track 2 Data	Mandatory	Variable	Hex	2048
US	Conditional	US	US	1
DUKPT Key Serial Number or Initial Vector	Conditional	Variable	Hex	20

Notes:
- If DUKPT is used to encrypt the Track 2 Data then the *DUKPT Key Serial Number* field is mandatory otherwise it is not present.
- If Master Key/Session Key and CBC encryption are used then the Initial Vector may be present after the US

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Authorised Amount	Mandatory	Variable	Numeric	12
FS	Conditional	FS	FS	1
Constraint Checks	Optional	Fixed	Hex	1
FS	Conditional	FS	FS	1
Additional Constraint Checks	Optional	Fixed	Hex	1

- The *Constraint Checks* field is used to determine whether mPOS should prompt for gratuity to be entered.
  The field may have one of the following values:

Value	Allow Online PIN Bypass	Request Online PIN	Allow DCC	Prompt for Gratuity
'0'	NO	NO	NO	NO
'1'	NO	NO	NO	YES
'2'	NO	NO	YES	NO
'3'	NO	NO	YES	YES
'4'	NO	YES	NO	NO
'5'	NO	YES	NO	YES
'6'	NO	YES	YES	NO
'7'	NO	YES	YES	YES
'8'	NO	NO	NO	NO

'9'	NO	NO	NO	YES
'A'	NO	NO	YES	NO
'B'	NO	NO	YES	YES
'C'	YES	YES	NO	NO
'D'	YES	YES	NO	YES
'E'	YES	YES	YES	NO
'F'	YES	YES	YES	YES

If no *Constraint Checks* field is given in the response then a value of zero will be assumed. I.e. no prompt for gratuity will be displayed, no DCC will be performed and no online PIN verification will be required.

- The *Additional Constraint Checks* field is used to determine whether mPOS should prompt for User Data to be entered.
  The field may have one of the following values:

Value	**Request Track 1 Data**	**Prompt for Cardholder Mobile Number**
'0'	NO	NO
'1'	NO	YES
'2'	YES	NO
'3'	YES	YES

9.13 Logon Transaction (55 - Logon Only)

Description:
This message is used to perform a 'logon' transaction. The mPOS shall provide the appropriate transaction data for the EPOS to send to the acquiring bank.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Amount	Mandatory	Variable	Numeric	12
FS	Mandatory	FS	FS	1
Masked Card PAN	Mandatory	Variable	Numeric	19
FS	Mandatory	FS	FS	1
Encrypted Card PAN	Mandatory	Variable	Hex	2048
US	Conditional	US	US	1
DUKPT Key Serial Number or Initial Vector	Conditional	Variable	Hex	20
FS	Mandatory	FS	FS	1
Card Expiry Date	Mandatory	Fixed	Numeric	4
FS	Conditional	FS	FS	1
Card Start Date	Optional	Fixed	Numeric	4
FS	Conditional	FS	FS	1
Card Issue Number	Optional	Variable	Numeric	2

Notes:
- The card dates shall be in the format 'MMYY'.
- If DUKPT data encryption is used then the *DUKPT Key Serial Number* field is mandatory.
- If Master Key/Session Key and CBC encryption are used then the Initial Vector may be present after the US

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Encrypted Data Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1
Encrypted MAC Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1
Encrypted PIN Key	Optional	Variable	Hex	128
FS	Conditional	FS	FS	1

- The *Encrypted Data Key* is only present if the Data Encryption Key for Master/Session Key is to be updated. The field is the new data encryption session key encrypted under the master data encryption key.
- The *Encrypted MAC Key* is only present if the Data MAC Key for Master/Session Key is to be updated. The field is the new MAC session key encrypted under the master MAC key.
- The *Encrypted PIN Key* is only present if the PIN Encryption Key for Master/Session Key is to be updated. The field is the new PIN encryption session key encrypted under the master PIN encryption key.

9.14 Supplementary (ICC or Contactless)

Description:
This message is used to obtain additional data from the mPOS where insufficient data was provided in the initial request. It may be used during any message exchange.

Supplementary Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Tag List	Mandatory	Variable	Hex	256

Notes:

- The *Message Identifier* field value must be the same as the value given in the initial request message.
- The *Sequence Number* field should be set to the value of the last request that was received.
- The *Response* field value must indicate that Supplementary Data is required.
- The *Tag List* field should consist of a list of tags. Each tag identifies the data element that should be returned from the mPOS. A list of tag values can be found in EMV 4 Book 3 Annex A. 1 byte tags should be padded with a trailing 0x00 so *TagList* is multiple by 2 bytes
- A proprietary tag of D7 will be used to request the encrypted track 2 data. The response field will contain the encrypted track 2 data if available or the encrypted PAN if the track 2 data is not available. The data will be in ascii-hex format. If DUKPT keys are used for encryption then the encrypted data will be followed by a unit separator (US) byte followed by the key serial number. The tag of D8 shall also be available to request the length of the clear-text data (the track 2 data or PAN) that has been encrypted.
- A proprietary tag of D9 will be used to request the issuer script results. Note that the value of this data element will only be available when the transaction is complete (i.e. only request this data element in a *Supplementary* response to the *Complete Transaction* request
- Proprietary tag DA = reserved (live usage: VISA short AID printing)
- Proprietary tag DB = supervisor MAG card data
- Proprietary tag DC = contactless short Kernel ID
- Proprietary tag DD = RFU (contactless VISA decline reason)
- It is recommended that the data for a maximum of 8 tags is requested at one time. Subsequent supplementary messages should be used if more than 8 tags are required.

Supplementary Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Data	Mandatory	Variable	-	-
FS	Mandatory	FS	FS	1
: :	: :	: :	: :	: :
FS	Mandatory	FS	FS	1
Data	Mandatory	Variable	-	-

Notes:

- The *Message Identifier* field value will be identical to the one in the initial request message.
- The *Sequence Number* will be incremented to distinguish it from any previous requests that were repeated.

- The *Data* fields will be separated using the field separator (FS) character.
- The order of the *Data* fields will correspond to the order of the *Tag List* given in the supplementary response.
- The length and range of each *Data* field will be dependent on the data that it represents (they will all be ASCII encoded however). E.g. The Authorised Amount data element will have a numeric range and a variable length.

9.15 Supplementary MAC Generation (ICC or Swipe or Contactless)

Description:
This message is used to obtain a Message Authentication Code from the mPOS. It may be used during any message exchange.

Supplementary Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Data	Mandatory	Variable	Hex	64

Notes:
- The *Message Identifier* field value must be the same as the value given in the initial request message.
- The *Sequence Number* field should be set to the value of the last request that was received.
- The *Response* field value must indicate that a Supplementary MAC Generation is required.

Supplementary Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
MAC	Mandatory	Fixed	Hex	16
US	Conditional	US	US	1
DUKPT Key Serial Number	Conditional	Fixed	Hex	20

Notes:
- The *Message Identifier* field value will be identical to the one in the initial request message.
- The *Sequence Number* will be incremented to distinguish it from any previous requests that were repeated.
- If a DUKPT key was used to generate the MAC then the DUKPT Key Serial Number is mandatory

9.16 Supplementary MAC Verification (ICC or Swipe or Contactless)

Description:
This message is used to verify a Message Authentication Code sent to the mPOS. It may be used during any message exchange.

Supplementary Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1
Data	Mandatory	Variable	Hex	64
FS	Mandatory	FS	FS	1
MAC	Mandatory	Fixed	Hex	16
FS	Conditional	FS	FS	1
MAC Option	Optional	Fixed	Numeric	1

Notes:
- The *Message Identifier* field value must be the same as the value given in the initial request message.
- The *Sequence Number* field should be set to the value of the last request that was received.
- The *Response* field value must indicate that a Supplementary MAC Generation is required.
- The *MAC Option* field value determines which key variant to use. It can have one of the following values:
  - '0' – The response key variant is used to verify the *MAC* value
  - '1' – The request key variant is used to verify the *MAC* value

  This field is optional – if the message does not contain this field then the terminal shall verify the MAC using the response key variant.

Supplementary Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Result	Mandatory	Fixed	Numeric	1

Notes:
- The *Message Identifier* field value will be identical to the one in the initial request message.
- The *Sequence Number* field will be incremented to distinguish it from any previous requests that were repeated.
- The *Result* field will have a one of the following values:
  - '0' – the MAC of the data is invalid
  - '1' – the MAC of the data is valid

9.17 Status Report (49 - ICC or Swipe or Contactless)

Description:
This message is used to indicate to the EPOS the status of an ICC transaction. The EPOS may choose to terminate the transaction if external events require it to do so.

Request Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Status	Mandatory	Fixed	Hex	2

Notes:

- The *Status* may have one of the following values:
  - 0x11 – Battery Level Low Warning
  - 0x21 – User Input Started
  - 0x22 – User Input Completed
  - 0x23 – User Input Aborted
  - 0x24 – User Input Timed Out
  - **0xA0 – Card Entry Prompted**
  - **0xA1 – Smartcard Inserted**
  - **0xA2 – Smartcard Remove Prompted**
  - 0xA3 – Smartcard Removed
  - 0xA4 – Card Entry Bypassed
  - 0xA5 – Card Entry Timed Out
  - 0xA6 – Card Entry Aborted
  - **0xA7 – Card Swiped**
  - **0xA8 – Card Swipe Error**
  - **0xA9 – Contactless Card Tapped**
  - **0xAA – Contactless Card Tap Error**
  - **0xAB – Contactless onDeviceCVM (Follow mobile Instructions)**
  - **0xAC – Contactless Mastercard Declines (auto fallback to ICC)**
  - **0xB0 – Application Selection Started**
  - **0xB1 – Application Selection Completed**
  - **0xC0 – Pin Entry Started**
  - 0xC1 – Pin Entry Completed
  - 0xC2 – Pin Entry Aborted
  - 0xC3 – Pin Entry Bypassed
  - 0xC4 – Pin Entry Timed Out
  - 0xC5 – Last Pin Entry
  - 0xC6 – Invalid PIN entered
  - 0xC7 – PIN Blocked
  - **0xD0 – Amount Confirmation Started**
  - 0xD1 – Amount Confirmation Completed
  - 0xD2 – Amount Confirmation Aborted
  - 0xD3 – Amount Confirmation Bypassed
  - 0xD4 – Amount Confirmation Timed Out
  - **0xE0 – DCC Selection Started**
  - 0xE1 – DCC Cardholder Currency Selected
  - 0xE2 – DCC Cardholder Currency Not Selected
  - 0xE3 – DCC Selection Timed Out
  - **0xF0 – Gratuity Entry Started**
  - 0xF1 – Gratuity Entered
  - 0xF2 – Gratuity Not Entered

- 0xF3 – Gratuity Entry Timed Out

Status values marked with **Bold** will check the response value and will react to a transaction cancellation request.

Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1

Notes:

- If the EPOS chooses to terminate the transaction, it should use Response value '3' – Abort operation. In all other cases the terminal will expect Response value '0'.
- During Pin Entry operation, as well as all other prompts, EPOS can cancel the prompt (bypass the PIN entry) by sending a messages consisting in only one character, ENQ. Terminal should react in the same way when "NO" key is pressed at pin entry stage, and follow the rest of CVM rules (if any).

9.18 Stand-By (13)

Description:
This message is used to revert the mPOS into the stand-by mode waiting for an initialisation message.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1

Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1

Notes:

- This message will cause the mPOS to go from Transaction mode to stand-by mode. It can be used to "park" the mPOS overnight or to allow reconfiguration of the mPOS

9.19 Add Record (30)

Description:
This message is used to add a record to the mPOS.offline transaction store.
This message is only supported by the SPm20 terminals.

Request Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Record Content	Mandatory	Variable	Base64	1968

Response Content (mPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1

9.20 Card Details (56)

Description:
This message is used to send card details to the EPOS and to perform card and card holder verification without a value transaction.

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Masked Card PAN	Mandatory	Variable	Numeric	19
FS	Mandatory	FS	FS	1
Card Expiry Date	Mandatory	Fixed	Numeric	4
PIN Verified	Conditional	Fixed	Numeric	1
Encrypted Card PAN	Conditional	Variable	Hex	2048
US	Conditional	US	US	1
DUKPT Key Serial Number or Initial Vector	Conditional	Variable	Hex	20

Notes:

- The card dates shall be in the format 'MMYY'.
- PIN Verified is only returned for the CVM Validation transaction type
  0=Verified
  1=Not verified
- Encrypted PAN is only returned for the CVM Validation transaction type
- DUKPT KSN is only returned for the CVM Validation transaction type where the encryption type is DUKPT

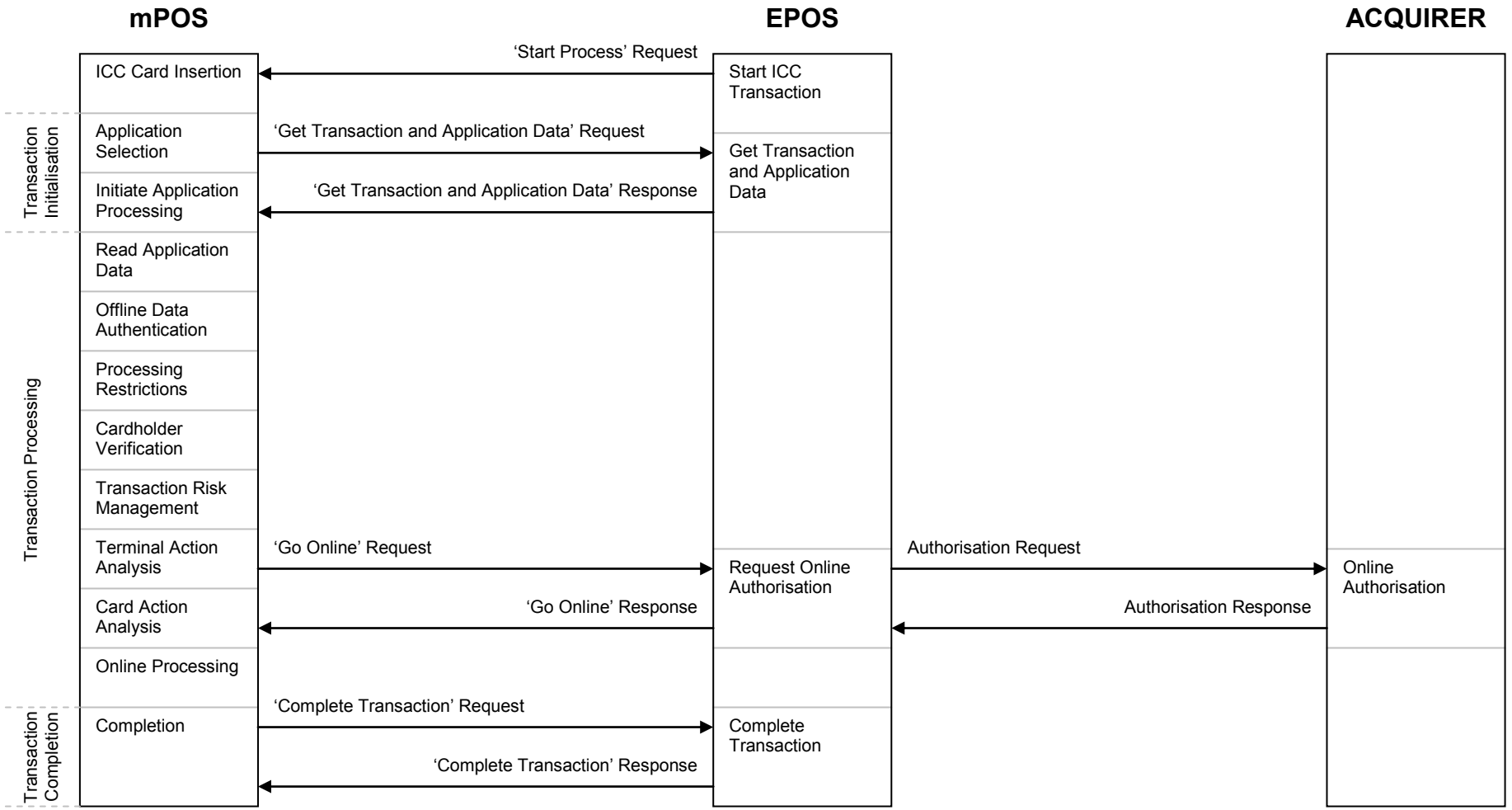
Response Content (EPOS):

Field	Requirement	Type	Range	Max Length
Message Identifier	Mandatory	Fixed	Numeric	2
Sequence Number	Mandatory	Fixed	Numeric	1
Response	Mandatory	Fixed	Numeric	1

10 Appendix A – Example ICC Transaction

10.1 Transaction Flow

The diagram below illustrates the processes that take place during a typical ICC transaction that requires online authorisation together with the message exchanges that get sent between the mPOS, the EPOS system and an acquirer host.



10.2 Starting a Transaction

An ICC transaction is started by the EPOS sending a 'Start Process' request to the mPOS. The mPOS will then wait for a card to be inserted into the smartcard reader by the cardholder or the attendant. Once a card is inserted, the mPOS will then initialise the transaction.

'Start Process' Request Message (EPOS)

An example of a 'Start Process' request message is shown below:

41	1	0	05

The description of each of the fields is provided in the following table:

Field	Value	Description
Message Identifier	41	Start Process
Sequence Number	1	Initial request
Process Type	0	Start ICC Transaction
POS Mode Entry Code	05	ICC card transaction

The mPOS does not send a response message to this request. Instead, it goes on to initialise the transaction – this is described in the following section.

10.3 Initialising a Transaction

A card may contain several payment applications that may be used to carry out a transaction (e.g. a card may contain both a debit payment application and a credit payment application). A payment application must first be selected by the mPOS which may require the cardholder to either select or confirm the choice of payment. Once a payment application has been selected, the appropriate transaction and application data must be retrieved by the mPOS from the EPOS system. This is achived by the mPOS sending a 'Get Transaction And Application Data' request message. The request shall contain a field identifying the payment application that was chosen for the transaction. The EPOS may use this field to determine the data values (floor limit, transaction risk management data etc.) that are appropriate for the selected payment application and return them to the mPOS in the 'Get Transaction And Application Data' response

'Get Transaction And Application Data' Initial Request Message (mPOS)

An example of the content of a 'Get Transaction And Application Data' request message is shown below:

42	1	A000000003101001

The description of each of the fields is given in the table below:

Field	Value	Description
Message Identifier	**42**	Get Transaction And Application Data
Sequence Number	**1**	Initial Request
Application Identifier	**A000000003101001**	Visa Debit

'Get Transaction And Application Data' Final Response Message (EPOS)

An example of the content of a 'Get Transaction And Application Data' response message is shown below:

42	1	0	030724113021	00	123	FS	FS	10003	FS	20000001	6815355	FS	0087	F00040C000	0070000000	F08840D000	FS	FS	30	60	2500	FS	5000	FS	9F02069F0306	FS

9F37049F1C089F1A029A03

The following table describes the data in each of the fields

Field	Value	Description
Message Identifier	42	Get Transaction And Application Data
Sequence Number	1	Must be the same value as the request
Response	0	Successful
Transaction Date And Time	030724113021	24th July 2003 at 11:30:21
Transaction Type	00	Goods and service
Authorised Amount	123	£1.23 The currency is implicit and is taken from the currency that was provided in the Merchant and Terminal Data
Other Amount	***NONE***	No other amount is provided since it is not a cashback transaction
Acquirer Identifier	10003	Identifies an acquirer
Terminal Identifier	20000001	Identifies the terminal to the acquirer
Merchant Identifier	6815355	Identifies the merchant to the acquirer
Application Version Number	0087	The value is provided in hex. In this case it is equal to 135 in decimal
TAC Default	F00040C000	• Offline data authentication was not performed • Offline static data authentication failed • ICC data missing • Card appears on terminal exception file • Unrecognised CVM • Transaction exceeds floor limit • Lower consecutive offline limit exceeded
TAC Denial	0070000000	• Expired application • Application not yet effective • Requested service not allowed for card product
TAC Online	F08840D000	• Offline data authentication was not performed • Offline static data authentication failed • ICC data missing • Card appears on terminal exception file • ICC and terminal have different application versions • New card • Unrecognised CVM

		• Transaction exceeds floor limit • Lower consecutive offline limit exceeded • Transaction selected randomly for online processing
Target Percentage used in Random Selection	**30**	30 percent
Max. Target Percentage used in Random Selection	**60**	60 percent
Threshold Value used in Random Selection	**2500**	£25.00 The currency is implicit and is taken from the currency that was provided in the Merchant and Terminal Data
Floor Limit	**5000**	£50.00 The currency is implicit and is taken from the currency that was provided in the Merchant and Terminal Data
TDOL	**9F02069F0306**	• Amount, Authorised (Length 6) • Amount, Other (Length 6)
DDOL	**9F37049F1C089F1A029A03**	• Unpredictable Number (Length 4) • Terminal Identifier (Length 8) • Terminal Country Code (Length 2) • Transaction Date (Length 3)
Constraint Checks	***NONE***	The mPOS will assume that the EPOS does not have an exception file or a transaction log, DCC is not supported and that PIN entry cannot be bypassed
Additional Constraint Checks	***NONE***	The mPOS will assume that 'quick' refunds are not performed (not applicable in this case as we're doing a sale)

10.4 Processing a Transaction

Once the transaction has been initialised, the mPOS will continue with processing the transaction. This may involve authenticating the data on the card as well as performing risk management and cardholder verification. If necessary, the cardholder may be required to enter their PIN on the mPOS for verification.

It may also be necessary for the transaction to go online for authorisation. In this case, the mPOS will send a 'Go Online' request message to the EPOS system. In order to create an appropriate authorisation request to send to the acquirer host, the EPOS system will need to obtain appropriate transaction data from the mPOS such as the card PAN, CVM Results, TVR etc. These can be obtained by sending supplementary messages to the mPOS. Any number of these may be sent to the mPOS – in the following example, just a single message is used to get the required information

'Go Online' Initial Request Message (mPOS)

An example of this request is shown below:

46	1	A000000003101001	FS	0

The fields of the above message are described in the following table:

Field	Value	Description
Message Identifier	**46**	Go Online
Sequence Number	**1**	Initial Request
Application Identifier	**A000000003101001**	Visa Debit
Advice Required	**0**	No advice message is required

'Go Online' Supplementary Response Message (EPOS)

An example of a supplementary response is shown below:

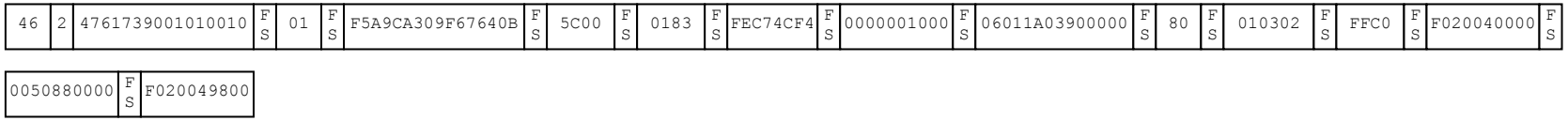
46	1	2	5A005F349F2682009F369F3795009F109F279F349F079F0D9F0E9F0F

The following table describes the transaction data elements that were requested by the EPOS in the above request.

Field	Value	Description
Message Identifier	**46**	Go Online
Sequence Number	**1**	Must be the same value as the last request
Response	**2**	Supplementary data required
Tag List	**5A005F349F2682009F369F3795009F 109F279F349F079F0D9F0E9F0F**	• Application PAN (5A) • Application PAN Sequence Number (5F34) • Application Cryptogram (9F26) • AIP (82) • ATC (9F36) • Unpredictable Number (9F37) • TVR (95) • IAD (9F10) • CID (9F27) • CVM Results (9F34) • AUC (9F07) • IAC Default (9F0D) • IAC Denial (9F0E) • IAC Online (9F0F)

'Go Online' Supplementary Request Message (mPOS)

In response to the the supplementary message, the mPOS will return the requested data in the order given by the tag list. Each data value is seperated using a field seperator.



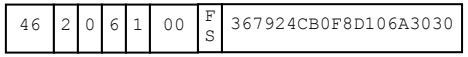
The data values returned in the above example request are described below:

Field	Value	Description
Message Identifier	**46**	Go Online
Sequence Number	**2**	Incremented from last request
Data (Application PAN)	**4761730000000010**	Primary account number held that is held on the card (masked with zeros)
Data (Application PAN Sequence Number)	**01**	Primary account sequence number that is held on the card
Data (Application Cryptogram)	**F5A9CA309F67640B**	ARQC generated by the ICC
Data (AIP)	**5C00**	• Offline static data authentication is supported • Cardholder verification is supported • Terminal risk management is to be performed • Issuer authentication is supported
Data (ATC)	**0183**	Transaction counter that is maintained by the card
Data (Unpredictable Number)	**FEC74CF4**	Generated by the mPOS
Data (TVR)	**0000001000**	Transaction selected randomly for online processing
Data (IAD)	**06011A03900000**	Used to authenticate the card to the card issuer
Data (CID)	**80**	ARQC
Data (CVM Results)	**010302**	• Last CVM Code = 1 • CVM Condition = 'If terminal supports the CVM' • CVM Successful
Data (AUC)	**FFC0**	• Valid for domestic cash transactions

		• Valid for international cash transactions • Valid for domestic goods • Valid for international goods • Valid for domestic services • Valid for international services • Valid at ATMs • Valid at terminals other than ATMs • Domestic cashback allowed • International cashback allowed
Data (IAC – Default)	**F020040000**	• Offline data authentication was not performed • Offline static data authentication failed • ICC data missing • Card appears on terminal exception file • Application not yet effective • Online PIN entered
Data (IAC – Denial)	**0050880000**	• Expired application • Requested service not allowed for card product • Cardholder verification was not successful • PIN entry required, PIN pad present, but PIN was not entered
Data (IAC – Online)	**F020049800**	• Offline data authentication was not performed • Offline static data authentication failed • ICC data missing • Card appears on terminal exception file • Application not yet effective • Online PIN entered • Transaction exceeds floor limit • Transaction selected randomly for online processing • Merchant forced transaction online

'Go Online' Final Response Message (EPOS)

Once the online authorisation is complete, the EPOS shall return details of the online authorisation response to the mPOS using a final 'Go Online' response message. An example of the response is shown below:



The following table describes the each of the fields in the above example

Field	Value	Description
Message Identifier	**46**	Go Online
Sequence Number	**2**	The same as the last (supplementary) request
Response	**0**	Success
Result	**6**	Financial transaction request successfully sent online
Issuer Response	**1**	Approved
Issuer Authorisation Response Code	**00**	Response code sent back from the issuer
Issuer Authentication Data	**367924CB0F8D106A3030**	Cryptogram sent back from the issuer that gets authenticated by the card

10.5 Completing a Transaction

Once a transaction has been processed, it needs to be completed. This may involve capturing transaction details - if they have not been captured online already; sending a reversal – if the transaction was finally declined by the card after having been approved online; or creating an advice – if there any issuer script results that need to be returned to the acquirer.

'Complete Transaction' Initial Request Message (mPOS)

An example of a 'Complete Transaction' request is given below.

47	1	A000000003101001	FS	0	0	0

A description of each of the field values is given in the following table

Field	Value	Description
Message Identifier	**47**	Complete Transaction
Sequence Number	**1**	Initial request
Application Identifier	**A000000003101001**	Visa Debit
Transaction Result	**0**	Transaction approved
Completion Action	**0**	No reversal, capture or advice is required
Card Checks	**0**	No further card checks are required

'Complete Transaction' Final Response Message (EPOS)

The EPOS system may send supplementary messages in order to retrieve any data that may be required at the end of the transaction. The transaction finishes when a final 'Complete Transaction' response message is sent by the EPOS system. An example of a final response message is shown below:

47	1	0

The fields of the above message are described in the following table:

Field	Value	Description
Message Identifier	**47**	Complete Transaction
Sequence Number	**1**	Must be the same value as the last request
Response	**0**	Success

11 Appendix B – Configuration File Format

All of the configuration files that are used by the mPOS use the same format.

Each configuration file may be split into a number of 'sections'. The start of a section is denoted by a line that starts with a '**#**' character followed by the name of the section. Each section shall contain a number of lines that define key-value pairs in the form:
'**<key> = <value>**'

Note that a semi-colon is used to delimit the lines in the configuration file (not carriage returns or line feeds or combinations of both). All control characters and spaces that occur in between lines are ignored.

11.1 ICC Applications File

This configuration file contains information on all of the payment card applications that are supported by the mPOS.

The file name of the ICC Applications File is '**f:\iccapp.cfg**'

The ICC Applications File shall contain a section for each payment card application that is required to be supported by the mPOS. Each section name for a payment card application shall be derived from its AID – in the form of:
'**APP_<AID>**'
The key values that should be given in these sections are as follows:

Configuration Key Name	Description
APP_PartialMatch	Indicates whether card applications may be partially matched against the AID. Set this to **TRUE** to enable partial matching or **FALSE** to disable it
APP_CountryCode	This country code where the card was issued. This is optional and should only be used for 'domestic processing'. E.g. The country code for the UK domestic Maestro card application (A0000000050001) should be set to **826**

Example:
A simple example of the content of an ICC Applications File is shown below:

```
#APP_A0000000031010;
APP_PartialMatch = FALSE;

#APP_A0000000050001;
APP_PartialMatch = TRUE;
APP_CountryCode = 826;
```

11.2 CA Public Keys File

This configuration file contains all of the CA public keys that are to be used by the mPOS to authenticate payment cards and their data.

The file name of the CA Public Key File is '**`f:\cakeys.cfg`**'

The CA Public Key File shall contain a main **`CAK_Index`** section that provides various attributes for all of the CA public keys that are held in the file.
The key values that should be given in this section are as follows:

Configuration Key Name	Description
`CAK_DefaultKeyAlgorithm`	The default key type. Currently this should have the value **`1`** (which indicates RSA).
`CAK_DefaultChecksumAlgorithm`	The default algorithm used to generate the checksum. Currently this should have the value **`1`** (which indicates SHA-1).
`CAK_ModulusChunkSize`	The number of nibbles (4 bits) that a key modulus is split into. This should be set to **`64`** (no other values are currently supported).
`CAK_CrlSerialsPerBlock`	The number of serial numbers that can be given in a CRL block. This should be set to **`5`**.

The CA Public Key File shall also contain a section for each CA public key. Each section name for a CA public key shall be derived from its RID and key index – in the form of:
'**`CAK_<RID>_<KeyIndex>`**'
The key values that should be given in these sections are as follows:

Configuration Key Name	Description
`CAK_Checksum`	The public key checksum. It is calculated using the SHA-1 hash of the following values (concatenated together) - RID (as a 5 byte binary value) - Key Index (as a one byte binary value) - Modulus (as a binary value) - Exponent (as a binary value)
`CAK_Exponent`	The public key exponent value (in decimal). It should either be set to **`3`** or **`65537`** (an exponent of **`2`** is not supported).
`CAK_ModulusChunks`	The number of 'chunks' that the modulus has been split into.
`CAK_ModulusChunk<n>`	A chunk of the public key modulus (as an ASCII encoded binary value). The most significant byte is given first. Each chunk should have 64 characters - the last chunk may be less than or equal to 64 characters.
`CAK_CrlBlocks`	The number of CRL blocks that are present. This value is optional
`CAK_CrlBlock<n>`	A list of certificate serial numbers that have been revoked. The serial numbers should be given in decimal and separated with a comma.

Example:
A simple example of the content of a CA Public Key File is shown below:

```
#CAK_Index;
CAK_DefaultKeyAlgorithm = 1;
CAK_DefaultChecksumAlgorithm = 1;
CAK_ModulusChunkSize = 64;
CAK_CrlSerialsPerBlock = 5;

#CAK_A000000003_01;
CAK_Checksum = D34A6A776011C7E7CE3AEC5F03AD2F8CFC5503CC;
CAK_Exponent = 3;
CAK_ModulusChunks = 4;
CAK_ModulusChunk1 = C696034213D7D8546984579D1D0F0EA519CFF8DEFFC429354CF3A871A6F7183F;
CAK_ModulusChunk2 = 1228DA5C7470C055387100CB935A712C4E2864DF5D64BA93FE7E63E71F25B1E5;
CAK_ModulusChunk3 = F5298575EBE1C63AA617706917911DC2A75AC28B251C7EF40F2365912490B939;
CAK_ModulusChunk4 = BCA2124A30A28F54402C34AECA331AB67E1E79B285DD5771B5D9FF79EA630B75;
CAK_CrlBlocks = 1;
CAK_CrlBlock1 = 10102547,12345678,66668859,78965478,88888888;

#CAK_A000000004_01;
CAK_Checksum = EA950DD4234FEB7C900C0BE817F64DE66EEEF7C4;
CAK_Exponent = 3;
CAK_ModulusChunks = 3;
CAK_ModulusChunk1 = D2010716C9FB5264D8C91A14F4F32F8981EE954F20087ED77CDC5868431728D3;
CAK_ModulusChunk2 = 637C632CCF2718A4F5D92EA8AB166AB992D2DE24E9FBDC7CAB9729401E91C502;
CAK_ModulusChunk3 = D72B39F6866F5C098B1243B132AFEE65F5036E168323116338F8040834B98725;
```

11.3 Logon Transaction File

This configuration file contains the information that the mPOS requires to perform a logon transaction.

The file name of the Logon Transaction File is '**f:\logon.cfg**'

The Logon Transaction File shall contain a main **TXN_Logon** section that provides the transaction details.
The key values that should be given in this section are as follows:

Configuration Key Name	Description
TXN_Amount	The amount for the logon transaction (in the currency's minor units).
TXN_PAN	The card PAN.
TXN_ExpiryDate	The card expiry date (formatted as MMYY).
TXN_StartDate	The card start date (formatted as MMYY). This value is optional.
TXN_IssueNumber	The card issue number. This value is optional.

Example:
A simple example of the content of a Logon Transaction File is shown below:

```
#TXN_Logon;
TXN_Amount = 1000;
TXN_PAN = 4444333322221111;
TXN_ExpiryDate = 1212;
```

11.4 Currency File

This file contains the list of supported currencies. Upon receiving the message 12 (L1_Initialisation), the currency code from the message is looked-up in this configuration file. If no match is found the terminal is considered initialised and the processing transactions would be rejected.

The file name is '**f:\currency.cfg**'. Each currency group is defined as #<ISO4217::Numeric Code>; for example **#978;** for Euro

Configuration Key Name	Description
Name	Generic label of the currency (US Dollar, Euro, etc)
AlphaCode	3 letter code ISO 4217 (USD, EUR, CHF)
SymbolCode	ISO 8859 code
SymbolTable	Specific table of the ISO 8859 where the symbol is found
Exponent	Minor digits to represent amounts (usually 2)
CodeIsPrefix	Boolean that indicates if the currency code prefixes the value (during amount prompts) Default value is true.
CodeIsSpaced	Boolean that indicates if there is a space between the currency code and the amount value (during amount prompts). Default value is true.

Example:

```
#826;
Name=POUND STERLING;
AlphaCode=GBP;
SymbolCode=163;
SymbolTable=1;
Exponent=2;
CodeIsPrefix=false;
CodeIsSpaced=false;

#840;
Name=US DOLLAR;
AlphaCode=USD;
SymbolCode=36;
Exponent=2;
```

will display sterling amounts as: **15.00GBP**

11.5 Terminal Configuration File

This configuration file contains the information that configures the mPOS application.

The file name of the generic terminal configuration is '**f:\terminal.cfg**'

The Terminal Configuration File shall contain a **COM_BLUETOOTH** section that provides Bluetooth settings.

The key values that should be given in this section are as follows:

Section	Configuration Key Name	Description
TML_TERMINAL	**TML_PinEditable**	Flag to indicate if the Supervisor PIN is editable Range – TRUE or FALSE Default value : FALSE
	TML_SupervisorPin	4 digit Supervisor PIN**
	TML_MerchantLanguage	Alphabetic code for merchant language Default value : If not present then a language selection menu will be presented at startup
	TML_DefaultMerchantLanguage	Alphabetic code for Default Merchant Language Default value : same as TML_MerchantLanguage
	TML_LanguagePreference	Languages supported by the terminal (masks cardholder and messages and menu operation). The order will also count as priority for menu rendering (language select)
	TML_MerchantName	Merchant Name Default Value : Blank
	TML_SupplierName	Supplier Name Default Value : Blank
	TML_IdleTimeout	Timeout (in sec) to enter Low Power Mode when Idle Default value : 0sec
	TML_WarningBatteryLvl	Battery Level (in %) for the terminal to indicate Warning Battery Level Default value : 0%
	TML_CriticalBatteryLvl	Battery Level (in %) for the terminal to indicate Critical Battery Level Default value : 0%
	TML_ShamsiCalendar	Flag to indicate the type of calendar to be used TRUE – Use Shamsi Calendar FALSE – Use Western Calendar Default Value : FALSE
	TML_CommsMode	Type of Communication Mode to be used Default value if the field is

		absent – Bluetooth 2 modes available USB and Bluetooth
	TML_AllowManualUSBSelection	Enables manual data bearer selection of Bluetooth or USB
	TML_Region	Defines an economic region for the terminal to apply specific processing. See 'Regions' table in Appendix C section
	TML_AdjustSN	TRUE or FALSE Default Value: FALSE Changes the first two digits of the terminal serial number (API reported value) with a value derivate from the full serial ID. (duplicate last 8 digits helper)
	TML_BTAdjustSN	TRUE / FALSE Default Value: FALSE Applies the same scheme as TML_AdjustSN but for the Bluetooth pairing name.
COM_BLUETOOTH	**COM_BTNamePrefix**	Section of the Bluetooth pairing name before the terminal ID. This field has a maximum length of 7 and will always be followed by " – XXXXXXXX" where X is the mPOS Serial Number.
	COM_BTNCFirst	TRUE / FALSE Default Value: FALSE Changes the priority of the Bluetooth pairing scheme. When set to TRUE the pairing code confirmation has priority over manual code entry

Default Values are used if the field is not present in Terminal Configuration File

Example:

A simple example of the content of a Terminal Configuration File is shown below:

```
#TML_TERMINAL;
TML_PinEditable=FALSE;
TML_SupervisorPin=1234;
TML_MerchantLanguage=en;
TML_DefaultMerchantLanguage=en;
TML_MerchantName=Spire Payments;
TML_SupplierName=Spire Payments;
TML_IdleTimeout=300;
TML_WarningBatteryLvl=20;
TML_CriticalBatteryLvl=10;
TML_ShamsiCalendar=FALSE;
TML_CommsMode=Bluetooth;
#COM_BLUETOOTH;
COM_BTNamePrefix = Spire;
```

When pairing the mPOS device, the discoverable name for the above example would be:

```
"Spire – 20081188"
```

**For Supervisor PIN value following are the conditions

Device	Condition	Example
SPm2	Default PIN (8497)	Do not add this field in terminal.cfg
	No Supervisor PIN	`TML_SupervisorPin=;`
	Defined Supevisor PIN	`TML_SupervisorPin=1234;`
SPm20	Default PIN (8497)	Not Applicable
	No Supervisor PIN	Do not add this field in terminal.cfg
	Defined Supevisor PIN	`TML_SupervisorPin=1234;`

11.6 Contactless Configuration File

If an mPOS device is to perform contactless configuration then it must have sufficient configuration data to be able to complete that transaction off line.

The correct configuration of contactless parameters is complex and details of how to specify the correct value defined below is given in a separate document, “mPOS API Contactless Configuration.pdf”.

This configuration file contains the information that configures the mPOS application for contactless transactions. It is mandatory if contactless transactions are supported.

The file name of the Contactless File is ‘**`f:\contactless.cfg`**’

The Contactless Configuration File shall contain the following sections:

CTL_DynamicLimit<n>
CTL_AmountLimit<n>
CTL_KernelConfiguration<n>
CTL_<aid>_<kernel-id>

CTL_DynamicLimit<n> contains the following parameters:

ProgramId=<xx>;
PerformStatusCheck=<boolean>;
AllowStatusCheck=<boolean>;
PerformZeroAmountCheck=<boolean>;
AllowZeroAmount=<boolean>;
OnlineCryptogramOnZeroAmount=<boolean>;
PerformFloorLimitCheck=<boolean>;
PerformTransactionLimitCheck=<boolean>;
PerformCvmRequiredLimitCheck=<boolean>;
FloorLimit=<amount>;
TransactionLimit=<amount>;
CvmRequiredLimit=<amount>;

CTL_AmountLimit<n> contains the following parameters:

AllowMobileDevices=<boolean>;
AllowCards=<boolean>;
AllowSale=<boolean>;
AllowCash=<boolean>;
AllowCashback=<boolean>;
AllowRefund=<boolean>;
FloorLimit=<amount>;
TransactionLimit=<amount>;
CvmRequiredLimit=<amount>;
OnDeviceCvmTransactionLimit=<amount>;
TerminalFloorLimit=<amount>;

CTL_KernelConfiguration<n> contains the following parameters:

PriorityIndicator=<numeric>;
PerformStatusCheck=<boolean>;
AllowStatusCheck=<boolean>;
PerformZeroAmountCheck=<boolean>;
AllowZeroAmount=<boolean>;
OnlineCryptogramOnZeroAmount=<boolean>;
PerformFloorLimitCheck=<boolean>;
PerformTransactionLimitCheck=<boolean>;
PerformCvmRequiredLimitCheck=<boolean>;
EmvSupported=<boolean>;

MsdSupported=<boolean>;
AllowPartialMatch=<boolean>;
OnDeviceCvmSupported=<boolean>;
VisaTTQPresent=<boolean>;
VisaPreProcessingRequired=<boolean>;
AmexProcessingRrequired=<boolean>;
MasterCardProcessingRequired=<boolean>;
RebootAfterGPO=<boolean>;
NoCardholderConfirmation=<boolean>;
AllowLOA=<boolean>;
TerminalCapabilities=<binary>;
TerminalCapabilitiesNoCvm=<binary>;
MasterCardMagStripeCvmCapability=<binary>;
MasterCardMagStripeNoCvmCapability=<binary>;
AdditionalTerminalCapabilities=<binary>;
EmvApplicationVersionList=<version-list>;
MsdApplicationVersionList=<version-list>;
TerminalTransactionQualifier=<binary>;
TerminalTransactionQualifierCash=<binary>;
TerminalTransactionQualifierRefund=<binary>;
TerminalTransactionQualifierCashback=<binary>;
TerminalActionCodeOnline=<binary>;
TerminalActionCodeDefault=<binary>;
TerminalActionCodeDenial=<binary>;
AdditionalTags=<binary>; 'insert here 9F1D tag
DefaultTDOL=<binary>;
DefaultDDOL=<binary>;
DefaultUDOL=<binary>;
ExpressPayTerminalCapabilities=<binary>;
ExpressPayRandomNumberScope=<nn>;
ExpressPayTerminalTransactionCapabilities;

CTL_<aid>_<kernel-id> contains the following parameters:
AmountLimit=AmountLimit<n>;
DynamicLimit=DynamicLimit<n>;
KernelConfiguration=KernelConfiguration<n>;

There is a CTL_<aid>_<kernel-id> section for each AID+kernel combination. These reference the appropriate amount limit (used for the entry point), kernel configuration and (optionally) dynamic limit sections

11.7 Logo Configuration File

This configuration file contains all of the Logos to be displayed when the terminal is connected in idle mode

The file name of the Logo Configuration File is '**`f:\logob.cfg`**'

The Logo Configuration File shall also contain a section for each Logo. Each section name for a Logo shall be in the form of:
'**`LOG_logo<LogoNumber>`**'
The Logo values that should be given in these sections are as follows:

Configuration Key Name	Description
`LOG_XPos`	Start Pixel Location along the X axis w.r.t. origin (Top-left)
`LOG_YPos`	Start Pixel Location along the Y axis w.r.t. origin (Top-left)

LOG_Width	Logo Width in pixels
LOG_Height	Logo Height in pixels
LOG_Chunks	The number of 'chunks' that the Logo has been split into.
LOG_Chunk<n>	A chunk of the Logo (as an ASCII encoded binary value). The most significant byte is given first. Each chunk should have 64 characters - the last chunk may be less than or equal to 64 characters.

Example:
A simple example of the content of a Logo Configuration File is shown below:

```
#LOG_logo1;
LOG_XPos=15;
LOG_YPos=16;
LOG_Width=40;
LOG_Height=32;
LOG_Chunks=5;
LOG_Chunk1=FFFFFE01FFFFFFF0003FFFFFE0001FFFFFC00007FFFF800003FFFF000003FFFE;
LOG_Chunk2=0000FDFFFE0000FEFFFC00073EFFFC000FC6FFFC0018F9C07C00307F801E00F0;
LOG_Chunk3=3F000F03F03F0007FC701F0003F3B01F0001CFB01F80003FB01F80003F701FC0;
LOG_Chunk4=0000783FE00000F83FF00001F87FF80003F87FFE000FB0FFFFC07F83FFFFFFC3;
LOG_Chunk5=FFFFFFF181FFFFFFEE01FFFFFFEC03FFFFFFE003FFFFFFF007FFFFFFFC1FFFFF;

#LOG_logo2;
LOG_XPos=70;
LOG_YPos=18;
LOG_Width=40;
LOG_Height=28;
LOG_Chunks=5;
LOG_Chunk1=FFFFFFFFFFFFFFFF807FFFFFFFFFFC3FFFC001FFFFFFFFFF007FC0001FFFFF;
LOG_Chunk2=FFFFFF800F80003FFFFFFFFFFF800200007FFFFFFFFFFFE0000001FFFFFFFFF;
LOG_Chunk3=FFF000000FFFFFFFFFFFFFFE0003FFFFFFFFFFFFFFFFE0001FFFFFFFFFFFFFF;
LOG_Chunk4=FE0001FFFFFFFFFFFFFFFC0F801FFFFFFFFFFFFFFC07E00FFFFFFFFFFFFFFE07;
LOG_Chunk5=FC1FFFFFFFFFFFFFFCFFFF;
```

Notes:
1. If the Logo Configuration File is present as per the expected format the Logos shall be displayed.
2. In order to remove the display of Logos then load the logob.cfg file with only '0' written it and nothing else
Example:
A simple example of the content of Logo Configuration File for this case is shown below:

```
0
```

3. Defining Logo
- Bit Value = 1 indicates the pixel is bright whereas Bit Value = 0 indicated the pixel is dark.
- Direction of Calculating Logo bit values is from Left to Right starting from the topmost line and moving downwards.
- Combine 8 bits to one byte and make an entry into the Logo Configuration File.

12 Appendix C - Data Element Codes

This section lists the codes that are required by some of the fields in the request/response messages. It does not provide an exhaustive list but is just intended as a handy reference. The codes are defined by a number of standards – for a definitive list please refer to the appropriate one.

12.1 Transaction Type

This is defined by the first 2 digits of ISO-8583:1987 (Processing Code). Typical values are:

Code	Description
00	Goods and Service
01	Cash
09	Goods and Service with Cash Disbursement
20	Returns (Refund)

12.2 Terminal Country Code

These codes are defined by ISO3166. Typical values are:

Code	Country
826	United Kingdom
840	United States of America
036	Australia
124	Canada
250	France
276	Germany

12.3 Terminal Currency Code

These codes are defined by ISO-4217. Typical values are:

Code	Currency
826	UK Pound Sterling
840	US Dollar
036	Australian Dollar
124	Canadian Dollar
978	Euro

12.4 Transaction and Merchant Category Codes

Transaction category codes are defined by MasterCard. Possible values are:

TCC Value	Description
C	Manual Cash Disbursement
Z	ATM Cash Disbursement
O	College/School Expense. Hospital and Nursing Care
H	Hotels, Motels and Cruise Ships
X	Transportation
A	Automobile and Vehicle Rental
F	Restaurants
T	Non Face-To-Face Transactions
P	Payment Transaction
U	Unique Transaction/Quasi-Cash Disbursement
R	Retail/Other Transactions

Note that the codes for manual cash disbursement (C), ATM cash disbursement (Z) and for non-face-to-face transactions (T) are not valid for use on the mPOS.

Merchant category codes are defined by ISO-8583:1993 (Card Acceptor Business Code). Typical values are (but not limited to):

MCC Value	Description
4112	Passenger Railways
4722	Travel Agencies and Tour Operators
5211	Home Supply Warehouse Stores
5251	Hardware Stores
5261	Lawn and Garden Supply Stores
5309	Duty Free Stores
5310	Discount Stores
5311	Department Stores
5331	Variety Stores
5399	Miscellaneous General Merchandise Stores
5411	Grocery Stores, Supermarkets
5441	Candy, Nut, Confectionery Stores
5451	Dairy Products Stores
5462	Bakeries
5499	Miscellaneous Food Stores (Convenience Stores, Markets, Specialty Stores, and Vending Machines)
5651	Family Clothing Stores
5661	Shoe Stores
5712	Equipment, Furniture, and Home Furnishings Stores (except Appliances)
5722	Household Appliance Stores
5732	Electronic Sales
5735	Record Shops
5812	Eating Places, Restaurants
5813	Bars, Cocktail Lounges, Discotheques, Nightclubs, and Taverns (Drinking Places - Alcoholic Beverages)
5814	Fast Food Restaurants
5912	Drug Stores, Pharmacies
5921	Package Stores, Beer, Wine, and Liquor
5942	Book Stores
5992	Florists
5994	News Dealers and Newsstands
7011	Lodging - Hotels, Motels, Resorts (not elsewhere classified)
7832	Motion Picture Theatres

The following table provides the mapping that the mPOS uses to determine the transaction category code from the merchant category code (when a TCC value has not provided in the *Transaction Initialisation* request)

MCC Value	TCC Value	Description
3000-3299	X	Airlines, Air Carriers
4011	X	Railroads (Freight)
4111	X	Transportation (Suburban and Local Commuter Passenger, including Ferries)
4112	X	Passenger Railways
4131	X	Bus Lines
4511	X	Air Carriers, Airlines (not elsewhere classified)
4722	X	Travel Agencies and Tour Operators
4789	X	Transportation Services (not elsewhere classified)
3501-3999	H	Lodging - Hotels, Motels, Resorts
4411	H	Cruise Lines
7011	H	Lodging - Hotels, Motels, Resorts (not elsewhere classified)
5811	F	Caterers
5812	F	Eating Places, Restaurants
5813	F	Bars, Cocktail Lounges, Discotheques, Nightclubs, and Taverns (Drinking Places - Alcoholic Beverages)
5814	F	Fast Food Restaurants
4829	U	Money Transfer (Merchant)
6050	U	Quasi Cash (Member Financial Institution)
6051	U	Quasi Cash (Merchant)
6529	U	Remote Stored Value Load (Member Financial Institution)
6530	U	Remote Stored Value Load (Merchant)
6534	U	Money Transfer (Member Financial Institution)
7511	U	Truck Stop Transactions
7995	U	Gambling Transactions
3351-3441	A	Car Rental Agencies
7512	A	Automobile Rental Agency (not elsewhere classified)
7513	A	Truck Rental
7519	A	Motor Home and Recreational Vehicle Rental
6532	P	Payment Transaction Provider (Member Financial Institution)
6533	P	Payment Transaction Provider (Merchant)
8050	O	Nursing and Personal Care Facilities
8062	O	Hospitals
8220	O	Colleges, Universities, Professional Schools, and Junior Colleges
All Other	R	All other transaction environments

Note: that merchant category codes that normally correspond to manual cash disbursement (C), ATM cash disbursement (Z) and non face-to-face (T) transaction category codes will be mapped to a retail transaction category code (R).

Please refer to the MasterCard 'Quick Reference Booklet' for more detailed information on merchant and transaction category codes.

12.5 Regions Codes

Region Value	Description
0	--- EUROPE section ---
1	The UK
2	Northern EU
3	Western EU
4	Southern EU
5	Eastern EU
6	Russia
20	--- ASIA section ---
21	China
22	Central
23	Eastern
24	Southern
25	South-East
26	Western
40	--- AMERICAS section ---
41	Latin
42	Caribbean
43	Central
44	Southern
45	Northern
60	--- AFRICA section ---
61	Eastern
62	Middle
63	Northern
64	Southern
65	Western
80	--- OCEANIA section ---
81	Australia & New Zeeland
82	Melanesia
83	Micronesia
84	Polynesia

The scope of the regions configuration is to enable the terminal implement behaviour specific to targeted markets (as there could be difference in requirements and accreditation tests).

For example, a region value in the European group (0 to 6 included) will implement the VPTT requirements whilst a region value in the Asian group (20 to 26 included) will trigger the CDET expectations.

13 Appendix D - ASCII Control Characters

The table below lists the values (in hexadecimal) of the control characters that are used for the communication protocol and messages

Control Character	Value
STX	0x02
ETX	0x03
EOT	0x04
ENQ	0x05
ACK	0x06
NAK	0x15
FS	0x1C
US	0x1F