



الاتحاد للمدفوعات
AI Etihad Payments

UAESWITCH Interface Technical Specifications

30 Jun, 2025
Version 1.6.1



COPYRIGHT

This document, including any referenced documents in the appendices and any amended versions, shall be at all times the property of AI Etihad Payments (AEP), who shall also own the copyright of these documents. All brand or product names mentioned are trademarks or registered trademarks of their respective holders. These documents may not be reproduced, transmitted electronically or otherwise, in whole or in part, without the prior written permission of AEP.

1.	About This Manual.....	9
1.1	Audience	9
1.2	Related Publication.....	9
1.3	Document Control	10
2.	Introduction	11
2.1	UAESWITCH Switching Service	11
2.2	Network Participants	12
2.3	Card Acceptors.....	12
2.4	Transaction Acquirers.....	12
2.5	Card Issuers.....	12
2.6	The UAESWITCH	12
2.7	Remote Switches	12
2.8	Terminal Devices	12
2.9	Functions of the switch.....	13
2.9.1	Routing	13
2.9.2	Logging.....	13
2.9.3	Network Management	13
2.9.4	Settlement	13
3.	Interface Messages	14
3.1	Authorization Message.....	14
3.2	Financial Message.....	14
3.3	Reversal Message	14
3.4	Reconciliation Message	15
3.5	File update Message	15
3.6	Administration Advice Message	15
3.7	Network Management Message	16
4.	Transaction Processing.....	17
4.1	Supported Transactions.....	17
4.2	General Requirements.....	18
4.2.1	Transaction Logging.....	19
4.2.2	Response timer Control.....	20
4.2.3	Message Routing Checks	21
4.2.4	Message Validation	21
4.2.5	Reconciliation Totals.....	21
4.2.6	Reversal Processing	23
4.2.7	Authorization Checks.....	27
4.2.8	Network Control	28
4.2.9	EMV Based Transactions Receipts & Journal.....	28
4.3	Financial.....	29
4.3.1	ATM Transactions	29
4.3.2	Cash Withdrawal / Balance Enquiry	29
4.3.3	ATM Reversal.....	30
4.4	Point of Sale.....	30

4.4.1 POS Purchase	31
4.4.2 Pre-Authorization & Incremental Pre-Authorization	31
4.4.3 Pre-authorization & Pre-authorization Completion	33
4.4.4 Refund	34
4.4.5 Void.....	35
4.4.6 Reversal	36
4.4.7 POS Balance Inquiry.....	37
4.5 Ecommerce	37
4.5.1 ECOM Purchase/Sale	37
4.5.2 Recurring Transactions	38
4.5.3 ECom Refund	39
4.5.4 Void.....	39
4.5.5 Reversal	39
4.6 Tokenization	40
4.6.1 Token Provisioning	40
4.6.1.1 Jaywan Mono Badge Card - Token Provisioning.....	40
4.6.1.2 Jaywan Co-Badge Card - Token Provisioning.....	41
4.6.2 Life Cycle Management	44
4.6.2.1. Jaywan Mono Badge Card - Life cycle Management from Issuer.....	44
4.6.2.2 Jaywan Mono Badge Card - Life cycle Management from TR.....	45
4.6.2.3 Jaywan Co-Badge Card - Life Cycle Management from Issuer	46
4.6.2.4 Jaywan Co-Badge Card - Life Cycle Management from TR.....	48
4.7 Network Management	49
4.7.1 Logon	50
4.7.2 Logoff.....	51
4.7.3 Cutover	52
4.7.4 Echo Test.....	53
4.7.5 Key Change	54
4.8 Reconciliation	55
4.9 9-Series Message	56
4.9.1 9200 ATM Balance Inquiry Transaction from Acquirer	56
4.9.2 9210 ATM Balance Inquiry Transaction Response from Issuer	56
4.10 EMV Transactions	57
5. Message Structure	58
5.1 Message Header	58
5.1.1 Message Header ATM Transaction Set.....	59
5.1.2 Message Header POS Transaction Set.....	59
5.2 Message Type Identifier	59
5.3 Bitmap	61
5.4 Data Elements.....	62
6. Message Formats	63
6.1 ATM Financial Transaction Request/ Response	63
6.2 ATM Reversal Request/ Response.....	65
6.3 ATM & POS Reconciliation Request/ Response.....	66

6.4 Network Management	67
6.5 POS Purchase Request / Response	68
6.6 POS Pre-authorization Request / Response	70
6.7 Incremental Pre Authorization Request/Response	72
6.8 POS Pre-authorization Completion	74
6.9 Ecommerce Request/Response	76
6.10 MOTO Transaction Request / Response	78
6.11 Recurring Transaction Request/Response	80
6.12 Refund Request/Response	82
6.13 Void/Cancel/Reversal Transaction Request/Response	84
6.14 Account Verification	86
6.15 Wallet Based Token Provisioning Request / Response	88
6.16 Send OTP	90
6.17 COF Token Provisioning Request / Response	91
6.18 Life Cycle Management	92
6.18.1 Life Cycle Management – Token Completion/Event Notification (Request and Response)	92
6.18.2 Life Cycle Management- Token status update Initiated from Issuer (request and response)	93
6.19 Onus transaction Detokenization	95
6.20 Offline Transactions/Financial Transaction Advice (Debit/Credit)	97
6.21 POS Balance Enquiry	99
7. Detailed Description of Data Elements	101
7.1 DE-2 Primary Account Number	101
7.2 DE-3, Processing Code	102
7.3 DE-4, Amount Transaction	104
7.4 DE-6, Amount Cardholder Billing	105
7.5 DE-7, Date Time, Transmission	106
7.6 DE-10, Conversion Rate, Cardholder Billing	107
7.7 DE-11, Systems Trace Audit Number	108
7.8 DE-12, Time, Local Transaction	108
7.9 DE-13, Date, Local Transaction	109
7.10 DE-14, Date, Expiration	109
7.11 DE-15, Date, Settlement	110
7.12 DE-16, Date, Conversion	110
7.13 DE-17, Capture Date	111
7.14 DE-18, Merchant Category Code	111
7.15 DE-19, Acquiring Country Code	112
7.16 DE-22, Point of Service (POS) Entry Mode	113
7.17 DE-23, Card Sequence Number	114
7.18 DE-25, Point of Service (POS) Condition Code	115
7.19 DE-32, Acquiring Institution ID	116
7.20 DE-33, Forwarding Acquiring Institution ID	116
7.21 DE-35, Track II Data	117
7.22 DE-37, Retrieval Reference Number (RRN)	117
7.23 DE-38, Authorization Identification Response	117
7.24 DE-39, Response Code	119

7.25 DE-41, Card Acceptor Terminal ID	122
7.26 DE-42, Card Acceptor Identification Code	122
7.27 DE-43, Card Acceptor Acquirer Name	123
7.28 DE-44, Additional Data, Response Data	124
7.29 DE-47, Additional Data, National.....	126
7.30 DE-48, POS retailer Data	127
7.31 DE-49, Transaction Currency Code	127
7.32 DE-50, Currency Code, Settlement	128
7.33 DE-51, Currency Code, Cardholder Billing	128
7.34 DE-52, Personal Identification Number (PIN) Data	129
7.35 DE-53, Security Related Control Information	130
7.36 DE-54, Additional Amounts	131
7.37 DE-55, ICC System Related Data	132
7.38 DE-57, EMV System Related Data.....	136
7.39 DE-60, Additional Data	137
7.40 DE-61, Point of Service Data, Private.....	138
7.41 DE-63, Network Data , Private.....	142
7.42 DE-66, Settlement Code	143
7.43 DE-70, Network Management Information Code	143
7.44 DE-74, Credits, Number	144
7.45 DE-75, Credits , Reversals Number	144
7.46 DE-76, Debits, Number	145
7.47 DE-77, Debits, Reversal Number	145
7.48 DE-80, Inquires, Number	146
7.49 DE-86, Credits ,Amount	146
7.50 DE-87, Credits , Reversal Amount.....	147
7.51 DE-88, Debits, Amount	147
7.52 DE-89, Debits, Reversal Amount.....	148
7.53 DE-90, Original Data Element	149
7.54 DE-95, Replacement Amounts.....	150
7.55 DE-97, Amount, Net Settlement.....	151
7.56 DE-99, Settlement Institution Identification Code	151
7.57 DE-100, Receiving Institution Identification Code.....	152
7.58 DE-104, Additional data – Payment Services	153
7.59 DE-105, Token Data	155
7.60 DE-115, Additional Trace Data.....	162
7.61 DE-122, Remaining Open to use	162
7.62 DE-123, Address Verification Data	164
8. Communication Protocol.....	168
9. Security Protocol.....	169
9.1 PIN ENCRYPTION SCHEME	169
9.1.1 ANSI X9.8 PIN Block	170
9.1.2 Zone Control Master Keys	170
9.1.3 Issuer/Acquirer Working Keys	171

9.1.4 AWK Change Procedure	171
9.1.5 IWK Change Procedure	172
9.1.6 IWK/AWK Validation	172
10. Change of Business Day	173
10.1 Stand in Authorization	173
10.2 Store and forward (SAF)	173
10.3 Totaling (For Reconciliation Messages)	174
10.4 Settlement	174
11. Exceptions Transactions Processing	177
11.1 Rules for exceptions processing	177
11.2 Issuer Response timeouts	177
11.3 Message Format Error	177
11.4 Data Security Error	178
11.5 Communication exceptions	178
11.5.1 Case 1 The Acquirer Cannot Forward Request from the Terminal	178
11.5.2 Case 2 UAESWITCH Cannot Receive Request	179
11.5.3 Case 3 UAESWITCH Cannot Forward Request to the Issuer	179
11.5.4 Case 4 The Issuer Cannot Receive Request	180
11.5.5 Case 5 The Issuer Cannot Send Request Response to UAESWITCH	180
11.5.6 Case 6 UAESWITCH Cannot Receive Response from the Issuer	181
11.5.7 Case 7 UAESWITCH Receives Late Response from the Issuer	181
11.5.8 Case 8 UAESWITCH Cannot Forward Request Response to the Acquirer	182
11.5.9 Case 9 UAESWITCH Receives Early Reversal from the Acquirer	182
11.5.10 Case 10 The Acquirer Cannot Receive Response from UAESWITCH	183
11.5.11 Case 11 The Acquirer Receives Late Acceptance Response from UAESWITCH	183
11.5.12 Case 12 The Acquirer Cannot Send Terminal Operation Instruction	184
11.6 Terminal Operations exceptions	184
12. Compliance	185
12.1 Card/Customer Authentication	185
12.2 Customer Authentication	185
12.3 General compliance	185
12.4 Purchase	186
12.5 Pre-Authorization & Pre-Authorization Completion	186
12.6 Refund Transaction	188
12.7 Partial Authorization	190
12.8 Purchase with Cashback	191
12.9 Contactless Transactions no CVM thresholds	191
12.10 POS Transaction Displays and Transaction Process Flows	192
12.11 POS Transaction Record Receipts	192
12.11.1 Approved UAESWITCH POS transactions	192
12.11.2 Declined UAESWITCH POS Transactions	193
12.12 MIT/Recurring Transactions	193
12.13 Tokenization	194

12.13.1 Token Life Cycle Management (TLCM)	196
12.14 Ecommerce Transaction	197
12.15 MOTO Transactions	199
12.16 Offline Transaction/Financial Transaction Advice	199
12.16.1 On-Board/Transit Use Cases.....	200
12.16.2 Special Offline Use Cases.....	201
12.17 Deferred Authorization	202
13. Appendix	203
13.1 Document Revision History	203
13.2 Abbreviations in Data Element / Message format	218
13.3 Data Formats & Data Encoding Standards	219
13.4 Conditional Data Element in message field.....	221
13.5 Envisaged Services	223
13.6 Additional Business Use cases	224
13.7 ISO8583 Sample Layout for Specific Data Element	228
13.7.1 Key Exchange Data Layout.....	228
13.7.2 Key Exchange Fixed 41 Digits.....	228
13.7.3 Key Exchange TLV format Variant	228
13.7.4 Key Exchange TLV format Key Block.....	229
13.7.5 Reconciliation Data Layout.....	229
13.7.6 TLV Format DE-74,DE-75,DE-76,DE-77,DE-80	229
13.7.7 TLV Format DE-86,DE-87,DE-88,DE-89	230

1. About This Manual

This manual documents the technical details of UAESWITCH transaction processing. The manual contains detailed specifications for ATM, POS message formats and associated technical details

1.1 Audience

This manual is intended for technical staff and managers and customer support personnel of the member banks.

1.2 Related Publication

EMV Integrated Circuit Card Specifications for Payment Systems
EMVCo Payment Tokenization Guide
EMVCo Payment Account Reference
EMVCo Payment Tokenization Use cases Guide

1.3 Document Control

Document Name: UAESWITCH Interface Technical Specifications

Distribution Lists: Participants

Version History

Version	Issue Date	Effective Date
1.0	June 30 th , 2022	June 30 th , 2022
1.1	July 12 th , 2022	July 13 th , 2022
1.2	Sep 5 th , 2022	Sep 6 th , 2022
1.3	April 3 rd , 2023	April 3 rd , 2023
1.4	August 15 th , 2023	Aug 12 th , 2024
1.5	Aug 12 th , 2024	Aug 12 th , 2024
1.6	Apr 20 th , 2025	Apr 20 th , 2025
1.6.1	June 30 th 2025	June 30 th 2025

Document Revision History

Please review Appendix 13.1 Document Revision history

2. Introduction

AI Etihad Payments is the national payments entity created in 2023 as part of the National Payment Systems Strategy to develop and operate best-in-class financial markets infrastructure for the UAE. It is a fully owned subsidiary of The Central Bank of UAE. AEP is formed to Establish and operationalize best-in-class payment services and infrastructure, contributing to financial stability and financial inclusion in the country.

The UAE Domestic Card scheme (Jaywan) is one of the initiatives of the CBUAE National Payment System Strategy (NPSS). This initiative, launched in 2024, aims to enhance the country's financial infrastructure by providing a secure, efficient, and cost-effective card payment method for both consumers and merchants within the UAE. The primary goals of the Jaywan scheme include reducing reliance on international payment networks, keeping transaction fees within the country, and enhancing financial inclusion making payment services more accessible to all segments of the population by keeping the transaction fees low when compared to international schemes.

The UAESWITCH is designed to act as a switch for Electronic Funds Transfer (EFT) and authorizations. It allows groups of institutions to provide a wider area of service to their customers by sharing their card processing facilities. Customers are not then restricted to using terminal devices owned by their own card issuing institution but are free to use any terminal device that is connected to the network.

The basic purpose of the UAESWITCH is to allow member institutions the ability to authorize the transactions of its customers initiated at other UAESWITCH bank locations.

In addition, a switch can communicate with other "remote" switches to further broaden the area in which institutions can offer customers their services.

2.1 UAESWITCH Switching Service

UAESWITCH Switching service supports routing of interbank POS and ATM transactions through UAESWITCH network.

UAESWITCH validates the request message from the acquirer and prepares it for processing. This processing and validation include identifying the message type, identifying the Issuing bank, checking of structural, format and value validation.

If UAESWITCH encounters an error condition at any point in the process, then further processing is halted. Messages rejected or declined by CBUAE are sent back to the respective participants with a proper response code indicating occurrence of an error condition wherever possible and the message is not forwarded to the issuer.

For e.g., if a message does not contain a mandatory field in the request, or a field contains an alphabet in place of a number then that message would be rejected with 9XXX series message

2.2 Network Participants

The various parties that participate in the flow of transactions through the network are identified here. The inter-relationships are shown diagrammatically below in figure 1.

2.3 Card Acceptors

A card acceptor is the party accepting the card from the customer and presenting the transaction data to the acquirer. Within the UAESWITCH system this would normally either be a merchant sponsored by a bank, or the banks themselves via their branches.

2.4 Transaction Acquirers

A transaction acquirer is the bank (as opposed to a particular bank branch) that receives the transaction from a card acceptor. Usually, the acquiring bank controls a network of directly connected terminal devices in its branches, but it may also control bank sponsored merchant terminal devices.

An acquirer bank's transaction processing system will process its own customer's transactions ("on-us" transactions) and will forward all other bank customer transactions ("not-on-us" transactions) to the switch.

2.5 Card Issuers

The card issuer is the bank that has issued the card to the customer. It receives transactions from the switch and provides the authorization function for the transaction. PIN verification, card expiration date, daily withdrawal limits, and account status are some of the checks an issuer will have to perform in order to either approve or deny a transaction.

2.6 The UAESWITCH

The UAESWITCH is the central participant in the switch network. It receives transaction requests from acquirers and routes them to issuers. It then routes the issuer's authorization outcome back to the acquirer for transaction completion. Other functions performed by the UAESWITCH are described in section 2.9, Functions of the Switch.

2.7 Remote Switches

The UAESWITCH intend that in the future the UAESWITCH network should be connected to other international networks through "remote" switches

The UAESWITCH also connects to the GCCNet Switch enabling participating banks connected to this Switch to deliver to, and receive transactions from other participating banks via their switch processor.

2.8 Terminal Devices

Terminal devices are the originators of customer transactions, which require authorization. The UAESWITCH network supports transactions originating from the following terminal "types":

- Automated Teller Machines (ATMs)
- Automatic Cash Dispensers (ACDs).
- Point-of-Sale Terminals (POS terminals)
- Bank Branch "Teller" Terminals
- Remote switches.
- E-commerce Channels

The UAESWITCH demands that PIN, if entered at a terminal must be secure within the device and must also be securely transferred between the terminal and the bank using a 3DES encrypted PIN block under a communication key that is securely changed on a regular basis. Full details of PIN management are provided in chapter 10, Security Protocol.

2.9 Functions of the switch

2.9.1 Routing

The primary function of the UAESWITCH is the routing of messages between the parties involved in a transaction (usually the acquirer and the relevant card issuer). This involves identifying the destination of a message based on information contained in the message. Once a transaction request is delivered to the relevant issuer bank it is the responsibility of the switch to monitor for a response from the destination. When a response is expected but not received the switch will respond back to the bank that sent the original request message with a time out response.

2.9.2 Logging

Another function that the UAESWITCH performs is the logging of each transaction handled by the switch. This provides a record of the transactions that each bank has performed through the network.

2.9.3 Network Management

The UAESWITCH is responsible for the management of the communications lines and devices directly connected to it in the network. It provides network management facilities to assist in the monitoring and control of the network.

2.9.4 Settlement

Settlement is a complex function that provides the basis for balancing with each bank connected to the switch. Each bank has to reconcile to every other bank on the switch. This could be a very complicated process since a switch could have hundreds of banks that subscribe to its services. The UAESWITCH can solve this problem by providing a middle ground for banks to settle with. Each bank settles with the UAESWITCH, and the UAESWITCH settles with each bank. This way each bank does not need to settle with every other bank. The actual process by which funds are transferred is outside the scope of the UAESWITCH switching system, but the UAESWITCH does produce various accounting reports, which can help in settlement processing.

All financial transactions acquired by UAESWITCH member banks ATMS/POS/ECOMMERCE terminals and processed via UAESWITCH will be sent online to the issuer for authorization. Full financial transactions contain both authorization and clearing information to be settlement in a single message format

Please review section 10.4 Settlement

3. Interface Messages

UAESWITCH interface messages are based on Bank Card Organizational Messages—Interchange Message Specifications—Content for Financial Transactions, International Organization for Standardization (ISO) 8583; 1987 (E).

UAESWITCH system messages generally consist of a pair of messages. A request message followed by a response message and can be classified into two categories Request message & Advice message

Request message is sent from the acquirer to the issuer to inform the receiver that a transaction is in progress and response must be sent back after completion of the transaction. After receiving the transaction request, the receiver should directly give the response of approving or refusing the transaction.

Advice message generally refers to a transaction message in which the sender informs the receiver of an action the sender has taken, and the sender requests no authorization but a response.

This section provides a brief overview and defines various types of messages supported by the UAESWITCH system. Chapter 9 Message Format details on the individual message types and associated data elements

3.1 Authorization Message

This message authorizes a transaction before the final amount of the purchase is known. It determines if funds are available, gets an approval and blocks the funds in the account. These messages do not have a settlement impact hence, to clear and settle an approved transaction the acquirer must submit the transaction to the clearing system.

Message Type Identifier for Authorization Message

- 0100 - Authorization request
- 0110 - Authorization response

3.2 Financial Message

This message determines if funds are available, gets an approval and debits the account. Financial messages have a settlement impact.

Message Type Identifier for Financial Message

- 0200 - Financial Request
- 0210 - Financial Response
- 0220 - Financial Advice Request
- 0230 - Financial Advice Response

3.3 Reversal Message

This message reverses the action of a previous authorization. It notifies CBUAE and/or the issuer of an error condition regarding an earlier financial transaction if:

- An approved transaction is cancelled at the POS/ATM/ECOMMERCE
- Acquirer does not receive a response to a financial request
- Acquirer cannot send an approved response to the POS/ATM

If, for any reason, these messages cannot be immediately delivered to their intended destination, acquirer or CBUAE stores these messages in SAF and forwards them to the intended destination when communication is re-established with the appropriate destination processor. The Acquirer needs to send 0400/0401/0420/0421 message to CBUAE and CBUAE will forward the same to the Issuer. The issuer needs to respond with a 0410 message. CBUAE generates reversals only for time-out cases for issuer responses. CBUAE will also generate reversal, if the response from issuer fails for format validation or issuer fails to respond within the allowed time limit. If any response comes for Reversal message from the Issuer, CBUAE treats that the reversal is completed and the same is not to be forwarded again, removed from SAF.

Message Type Identifier for Reversal Message

- 0420/0421- Reversal Message Advice
- 0430 - Reversal Message Advice Response
- 0400/0401 - Reversal Message
- 0410 - Reversal Message Response

3.4 Reconciliation Message

Totals related to the UAESWITCH inter-bank transaction traffic are exchanged using reconciliation messages. These message types are used by the UAESWITCH to notify a Member Bank of the acquirer/issuer totals that reflect the previous business day's UAESWITCH position as determined by the last cutoff transaction from the switch to the bank

Message Type Identifier for Reconciliation Message

- 0500 - Acquirer reconciliation request
- 0501 - Acquirer reconciliation repeat
- 0510 - Acquirer reconciliation request/repeat response
- 0502 - Card Issuer reconciliation request
- 0503 - Card Issuer reconciliation repeat
- 0512 - Card Issuer reconciliation request response

3.5 File update Message

File update message is an issuer generated message to be sent to UAESWITCH. File update message is used to update the cardholder records in the UAESWITCH database for the specific use cases.

- 0302 - File update message request
- 0312 - File updates message response

3.6 Administration Advice Message

These messages are generated to notify the issuer about a change inside the system. The message are currently used to update the issuers for any token creation for their cards or change in the status for the tokens attached to the cards

- 0620 – Administration Advice request
- 0630 – Administration Advice response

3.7 Network Management Message

Network management messages are required to support the administration of the UAESWITCH network. These messages can be initiated either by members or by UAESWITCH. These messages are used to communicate that the member is available for processing transactions.

Message Type Identifier for Network Management Message

- 0800 - Network management request
- 0801 - Network management repeat
- 0810 - Network management request/repeat response

4. Transaction Processing

This section provides a high-level overview of the processing sequence for the messages as supported by the interface and the processing requirements

4.1 Supported Transactions

This section identifies all the transactions that are supported by the UAESWITCH network at the present time. Transactions are divided into three types, financial, network management and reconciliation. Each of these is presented in separate subsections below. The information is presented in the form of tables with the following columns:

Transaction : Name of the transaction

Transaction Type : States whether the transaction is monetary (M) or non-monetary (NM).

Message Types : Lists the message types that are used in processing the transaction.

ATM Transactions

No	Transaction	Tran. Type (M/NM)*	Message Type
1	ATM Balance Enquiry	NM	0200,0210
2	ATM Cash Withdrawal	M	0200,0210
3	ATM Cash Withdrawal Reversal	M	0400,0401,0410
4	ATM Cash Withdrawal Partial Reversal	M	0400,0401,0410

POS/E-commerce Transaction

No	Transaction	Tran. Type (M/N)*	Message Type
1	Purchase / Sale	M	0100, 0200,0110, 0210
2	Pre Authorization	M*	0100,0110
3	Pre Authorization Topup	M*	0100,0110
4	Pre Authorization Completion	M	0220,0230
5	E-commerce (CIT/MIT)	M	0100/0110
6	Refund	M	0100/0200, 0110/0210
7	Void	M	0400,0401,0410
8	Reversal	M	0420,0421,0430
9	Balance Enquiry	M*	0100,0200,0110,0210
10	Account Verification Inquiry	M*	0100, 0110

*Based on MCC Category

Network Management Transactions

No	Transaction	Tran. Type (M/N)*	Message Type
1	Cutover	NM	0800,0801,0810
2	UAESWITCH Log-on	NM	0800,0810
3	UAESWITCH Log-off	NM	0800,0810
4	Bank Log-on	NM	0800,0810
5	Bank Log-off	NM	0800,0810
6	UAESWITCH Echo Test	NM	0800,0810
7	Bank Echo Test	NM	0800,0810
8	Key Exchange	NM	0800,0810

Reconciliation Transactions

No	Transaction	Tran. Type (M/N)*	Message Type
1	Acquirer Reconciliation	NM	0500,0501,0510
2	Issuer Reconciliation	NM	0502,0503,0512

4.2 General Requirements

This section gives details of various general-processing requirements that are common to all or several types of transaction. These are considered in separate subsections as follows:

- Transaction Logging
- Response Timer Control
- Message Routing Checks
- Message Validation
- Reconciliation Totals
- Reversal Processing
- Advice Processing
- Authorization Checks
- Network Control

The requirements described in these subsections should be borne in mind when referring to the individual transaction processing scenarios described in sections 4.3.

4.2.1 Transaction Logging

Banks must log all transactions related to the UAESWITCH network. This log may be used to generate reports of bank "seen" network activity, which will be useful to banks in resolving any settlement discrepancies that occur. It is recommended that banks also log a minimum the same data as the UAESWITCH will log, defined below.

The UAESWITCH logs all transaction traffic that it has processed in a given business day to a Transaction Log File (TLF). After switch cutover each day, the UAESWITCH will run batch processes against the TLF and produce reports of switch activity. These reports may be used in the reconciliation process. A settlement report is also produced using the contents of the TLF, which may be used in settlement.

The following data, where available, will always be logged on the TLF for each transaction:

- Message type identifier of the last message processed for a given transaction (e.g., 0110, 0210, 0410, etc.)
- primary account number (DE-2)
- processing code (DE-3)
- amount, transaction (DE-4)
- systems trace audit number (DE-11)
- date, expiration (DE-14)
- date, settlement (DE-15)
- date, capture (DE-17)
- merchant's type (DE-18)
- point of service entry mode (DE-22)
- point of service condition code (DE-25)
- retrieval reference number (DE-37)
- authorization identification response (DE-38)
- response code (DE-39)
- card acceptor terminal identification (DE-41)
- card acceptor identification code (DE-42)
- card acceptor name/location (DE-43)
- EMV data (DE-55)
- original data elements (DE-90)
- replacement amounts (DE-95)
- Additional Data (DE – 104)
- Token Data (DE-105)
- remaining open-to-use (DE-122)

4.2.2 Response timer Control

The UAESWITCH will operate timer controls on all responses to request messages (0100/0200/0302/0620/0400/0401/0420/0421/0800). Acquirers are also required to maintain timer controls, both for their terminals, and transaction processing systems. Recommended time out values, in seconds, for each type of request/response exchange are provided in the following table.

Transaction	Message	Issuer	UAESWITCH	Acquirer	Terminal
ATM Cash Withdrawal	0200/0210	15	30	45	60
ATM Balance Enquiry	0200/0210	15	30	45	60
Purchase/Sale/Ecommerce	0100/0200/0110/0210	6	12	45	60
Pre-authorization	0100/0110	6	12	45	60
Token LCM by Issuer	0302/0312	20	15	N/A	N/A
ATM Reversals	0400 or 0401/0410 0420, 0421/0430	15	30	20	60
POS/ECOM Reversals	0400 or 0401/0410 0420, 0421/0430	6	8	20	60
Reconciliation	0500/0501/0510 0502/0503/0512	6	8	20	N/A
Token Management by N/W	0620/0630	6	8	N/A	N/A
Key Exchange	0800/0801/0810	10	12	20	N/A
Log-on/Log-off	0800/0810	10	12	20	N/A
Echo Test	0800/0810	10	12	20	N/A

Acquirer time out values should be set to a longer period than the UAESWITCH time out values. This will reduce the incidence of late response processing for acquirers. The exception to this is in the case of reversals and advices, where the values may be the same, since UAESWITCH responds directly to the acquirer without waiting for an issuer response first (see sections 4.2.6, Reversal Processing).

Recovery action that the UAESWITCH and acquirers will perform on timer Expiry (no response) and late response processing action is defined in detail in the individual transaction processing scenarios described in sections 4.3.

It is important that issuers respond to requests well within the time out values set by the UAESWITCH even at peak times. Consecutive message time outs can lead to the issuer member bank node to be set offline.

4.2.3 Message Routing Checks

The UAESWITCH obtains its message routing information from the Primary Account Number (DE-2).

On receiving a message to be routed from an acquirer, the UAESWITCH will verify that the network supports the card issuer institution, using the information supplied in DE-2. If it is not, the UAESWITCH will send the acquirer an appropriate denial response message with a "Financial institution or intermediate network facility cannot be found for routing" response code value of "92" in DE-39.

If the card issuer is recognized but, for some reason, the UAESWITCH is unable to process the request at the present time, the UAESWITCH will send the acquirer an appropriate denial response message with an "Issuer or switch is inoperative" response code value of "91", contained in DE-39.

4.2.4 Message Validation

When the UAESWITCH receives a message containing an invalid message type identifier, it will status log the message and return the message to the sender with a "9" prefix (i.e., a 9xxx message will be forwarded). The Field in Error, field in the message header, will contain the value of the first offending field that caused the message validation failure. If the message header is invalid, then the Field in Error field will contain "999".

4.2.5 Reconciliation Totals

Banks must maintain totals related to the UAESWITCH inter-bank transaction traffic they have sent to or received from the UAESWITCH network.

Banks should maintain two sets of totals, "acquirer" totals and "issuer" totals. The first set relates to transactions that the bank has acquired for other Member Bank cardholders, the second set relates to transactions initiated at other bank locations that a bank has authorized for its cardholders. Banks should maintain two separate sets of "acquirer" and "issuer" totals. These may be thought of as the "current day" and the "next day", from the point of view of reconciliation. The UAESWITCH will always supply the business day that applies to a transaction in DE-15, (Date, and Settlement). Further details of the use of these separate sets of totals are provided in 4.5, Reconciliation and 10.3, Totaling (For Reconciliation Messages).

Within each set of totals the following information should be maintained:

- Number of approved credits
- Amount of approved credits
- Number of approved credit reversals
- Amount of approved credit reversals
- Number of approved debits
- Amount of approved debits
- Number of approved debit reversals
- Amount of approved debit reversals
- Number of approved inquiries

The following two subsections define "acquirer" and "issuer" totals separately. Details of the situations when particular totals should be updated are provided in the section 4.3 Financial Transactions, where the specific processing requirements of financial transactions supported by UAESWITCH are discussed.

Acquirer Totals

For "acquirer" totals "approved" means that the bank received a 0110/0210/0230/0410/0430 response to the 0100/0200/0400/0401/0420/0421 transaction request with a response code value of "00".

The following table indicates which "amount" and/or "number" totals need to be updated for each transaction supported by the network. Where relevant the value by which "amounts" should be incremented is also given

Total	Transactions	Amount Value
Credit Reversals	ATM Reversal (Full or Partial) ATM Forced Credit	Amount, Transaction (DE-4)
Debits	ATM Cash Withdrawal	Amount, Transaction (DE-4)
	ATM Partial Reversal	Actual amount, Transaction (DE-95.1)
Inquiries	ATM Balance Inquiry	Not Applicable

Issuer Totals

For "issuer" totals "approved" means that the bank sent a 0110/0210/0410/0430 response to the received 0100/0200/0400/0401/0420/0421 transaction request with a response code value of "00".

The following table indicates which "amount" and/or "number" totals need to be updated for each transaction supported by the network. Where relevant the value by which "amount" totals should be incremented is also given.

Total	Transactions	Amount Value
Credit Reversals	ATM Reversal (Full or Partial) ATM Forced Credit POS Purchase Reversal EFT (Full or Partial)	Amount, Transaction (DE-4)
Debits	ATM Cash Withdrawal	Amount, Transaction (DE-4)
	ATM Partial Reversal	Actual amount, Transaction (DE-95.1)
Inquiries	ATM Balance Inquiry	Not Applicable

4.2.6 Reversal Processing

This section describes the common features of reversal processing. Specific details are provided in the relevant subsections of section 4.3, Financial Transactions, where each expected instance for which a reversal would be generated is considered for each type of transaction. To ensure that reversal processing proceeds smoothly, banks should follow the recommendations described in this section at all times.

Reversal request messages (0400/0401/0420/0421) are generated whenever a customer transaction that has been approved by the card issuer has to be partially or completely canceled. They are normally generated by an acquirer bank for an issuer bank destination, but in some situations reversal requests may be generated directly by the UAESWITCH, for delivery to issuer banks. Issuer banks never generate 0400/0401/0420/0421 reversal requests; they only receive them and respond to them using a 0410/0430 reversal response message. Similarly, acquirer banks never generate 0410/0430 reversal responses. The UAESWITCH may generate either requests (0400/0401/0420/0421) or responses (0410/0430).

Failure to generate a reversal when it is required, or failure to process a reversal correctly could result in a customer being billed for a transaction either that did not take place or occurred for a different amount to that billed. For this reason, as far as it is possible, reversal delivery should be guaranteed. In order to keep customer account balance information accurate for authorization purposes, it is important that reversals are delivered to the issuer in a timely fashion.

The design of an efficient reversal processing system involves some compromise. It is not possible to meet the requirements mentioned above one hundred percent of the time given the practical constraints of a real system. The system described in this section is designed to meet the most important needs of Member Banks and the UAESWITCH. In particular, the system is designed to keep issuer banks and the UAESWITCH consistent with each other.

The central philosophy of the design is that it is the responsibility of the UAESWITCH to ensure that all reversal messages received from an acquirer, or generated by the UAESWITCH, are delivered, and responded to by the relevant issuer. This is achieved using a store and forward (SAF) processing mechanism. All reversal request messages received, or generated, are kept in a SAF file, rather than sent directly to the issuer. Each issuer bank destination has its own unique SAF file. Entries in the SAF file are sent to the issuer in chronological order, i.e., first-in, first-out. Entries in the SAF file have a "lifetime" of one business day. When the UAESWITCH performs cutover to the next business day, all entries in the SAF file which are dated the previous business day will be deleted by the SAF processing mechanism. The UAESWITCH end-of-day batch "extract" process will generate reports of all activity "seen" by the UAESWITCH on a given business day. These may be used in the reconciliation of any outstanding unprocessed reversal messages.

For this procedure to work, an issuer cannot deny reversal messages as long as the system is operational, except in situations where a duplicate is detected, or certain validation checks fail. In the rare situations where the issuer is unable to process a reversal because of an unrecoverable field format error, or validation error, the UAESWITCH will log the transaction information in the Transaction Log File but will not respond back to the acquirer with this information. Thus, it is possible using this design for acquirer bank reconciliation totals to lose consistency with issuer bank and the UAESWITCH held totals. However, these discrepancies will be resolved at the end of every business day, during reconciliation. In order for reconciliation to work smoothly all parties must ensure that an accurate log is kept of all reversals processed in a given business day. Reports of reversal activity are required for reconciliation.

Specific details of the processing requirements for the UAESWITCH, acquirers and issuers are presented in individual sections below.

UAESWITCH reversal processing

When UAESWITCH receives a 0400/0401/0420/0421 request from an acquirer it will store the request in the issuer bank's SAF file. If this is successful, the UAESWITCH will respond back to the acquirer bank immediately with an "approved" 0410/0430 acquirer reversal response (response code set to "00"). The UAESWITCH will then log the transaction to the Transaction Log File. Note that this is before the request has actually been sent to the issuer. This is because the UAESWITCH takes responsibility for delivery of the message to the issuer via its SAF mechanism. The UAESWITCH will forward entries from the SAF file to the issuer bank and will wait for a response in the usual way, i.e., the UAESWITCH will set a timer to wait for a response. If the timer expires waiting for the 0410/0430 Acquirer reversal request response from the issuer, then the SAF mechanism will maintain the reversal transaction and generate periodic 0401/0420 Acquirer reversal request repeats until a 0410/0430 is successfully received.

When the UAESWITCH receives a 0400/0401/0420/0421 message its format will be validated. Should the format be invalid then the message will be returned to the sender with a "9" prefix (i.e., a 9xxx message will be forwarded). The Field in Error field in the message header will contain the value of the first offending field that caused the message validation failure. If the message header is invalid, then the Field in Error field will contain "999".

When the UAESWITCH receives a 0410/0430 message its format will be validated. Should the format be invalid then the message will be logged and will be returned to the sender with a "9" prefix (i.e., a 9xxx message will be forwarded). The Field in Error field in the message header will contain the value of the first offending field that caused the message validation failure. If the message header is invalid, then the Field in Error field will contain "999".

The UAESWITCH will adjust the reconciliation totals of the issuer bank to reflect the reversed amount after the reversal message has been successfully written to the SAF file.

When a 0410/0430 response is received, the UAESWITCH will check the value of the response code field (field 39).

If a "No action taken" response code value of "21" has been returned in the 0410/0430 response, indicating that the issuer has processed this transaction before, the UAESWITCH will discard the response and remove the message from the store and forward file. The response will be written to status log file.

If the response code is one of the other non-zero values listed in Issuer reversal processing below, the UAESWITCH will log the response information. The UAESWITCH will not adjust the issuer bank's switch reconciliation totals. This will leave the reconciliation of the customer's account as an administrative procedure. The acquirer and issuer will be required to provide reports of all reversals processed to the UAESWITCH for reconciliation purposes. The UAESWITCH will also provide the reversal information to banks in its daily reporting.

The UAESWITCH does not attempt to detect "duplicate" reversal messages. It is always the responsibility of the issuer bank's processing system to detect and correctly process "duplicate" 0400/0401/0420/0421 reversal messages. This is described below in the subsection on Issuer reversal processing.

Acquirer reversal processing

Whenever an acquirer bank needs to generate a reversal transaction the following procedure should be observed.

Banks will need to implement some form of processing system that will maintain the reversal transaction until a 0410/0430 response message is successfully received from the UAESWITCH. The system should be capable of sending periodic 0401 repeat message until a timely 0410 response is received to the original 0400 request, or if the UAESWITCH indicates in the 0410 response that it was unable to process the original 0400 request. The UAESWITCH uses a SAF mechanism to maintain reversal transactions, and acquirer banks are strongly recommended to follow a similar design.

When an acquirer receives a 0410/0430 message its format should be validated. Should the format be invalid then the message should be returned to the UAESWITCH with a “9” prefix (i.e., a 9xxx message will be forwarded). The Field in Error, field in the message header, should be encoded with the value of the first offending field that caused the message validation failure. If the message header is invalid, then the Field in Error field should contain “999”.

The total amount to be reversed must be provided in field 4 (Amount, Transaction). For partial reversals, the value of the Actual amount, transaction sub-field of Replacement Amounts (field 95) should be set to the value of the partially completed transaction. The response code (field 39) should be set to a value that indicates the cause of the problem. Valid response code values that should be used in these situations are as follows:

Value	Description
00	Approved
05	Do Not Honor
06	General Error
13	Invalid Amount
17	Customer Cancellation
21	No Action Taken
22	Suspect Malfunction
32	Completed Partially
34	Suspected Fraud
68	Response Received Too Late
91	Timeout
96	System Malfunction

The bank should also set the value of the authorization identification response (DE-38) in the 0400/0401/0420/0421 message to match the value in the original 0110/0210 approval received from the UAESWITCH, together with the value of Original Data Elements (DE-90). This information will enable the

issuer to match the reversal to the original transaction and also to determine whether or not the reversal has already been processed (i.e., to detect duplicates).

After a 0400/0401/0420/0421 request is sent to the UAESWITCH, the acquirer's reversal processing mechanism should set a timer to wait for a response, in the usual way. If the acquirer's timer expires waiting for the 0410/0430 Acquirer reversal request response from the UAESWITCH, then the acquirer's reversal processing system should maintain the reversal transaction and generate periodic 0401/0421 Acquirer reversal request repeats until a 0410/0430 is successfully received.

When a 0410/0430 response is received from the UAESWITCH with a "00" response code value indicating successful completion, the acquirer should log details of the transaction and update its acquirer "reversal" reconciliation totals. The message should then be removed from the acquirer's reversal maintenance processing system.

Acquirer banks for use in reconciliation should produce reports of all reversals generated, whether or not they were successfully sent to UAESWITCH.

Issuer reversal processing

Whenever an issuer bank receives a 0400/0401/0420/0421 reversal message from the UAESWITCH it should observe the following procedure.

The bank's system should verify that the reversal message has not already been processed by checking against the authorization identification response (DE-38) and original data elements (DE-90) in the 0400/0401/0420/0421 message. If the bank thinks this is a reversal message that it has already processed a "No action taken" response code value of "21" should be returned in the 0410/0430 response.

If this is a new reversal transaction the bank should perform relevant validation checks against the reversal request message in the same way recommended in section 4.2.7, Authorization Checks. If any validation check fails, the bank should return the appropriate response code value in DE-39 of the 0410/0430 response corresponding to one of the values below.

Reversal request message always respond with successful response. In case of any issue while responding back to reversal request, then such transactions has to be manually handled offline.

Whenever these response code values are used in the 0410/0430 response, the issuer should not update any customer account information or its issuer "reversal" reconciliation totals.

If all the validation checks are successful and no other processing errors occur the bank should log the transaction and adjust the totals relating to the customer's account, i.e., balance and number and amount of withdrawals as well as the relevant bank issuer "reversal" reconciliation totals. These adjustments should be based on the transaction amount value (DE-4) in the 0400/0401/0420/0421 message, with an exemption as follows. If the response code of reversal message is '13' (invalid amount), the issuer should reverse the actual debited amount to the customer's account. The bank should then return a 0410/0430 response with an "Approved or completed successfully" response code value of "00".

Issuer banks should produce reports detailing all reversal activity it has seen in a single given UAESWITCH business day for use in reconciliation.

When an issuer receives a 0400/0401/0420/0421 message its format should be validated. Should the format be invalid then the message should be returned to the UAESWITCH with a "9" prefix (i.e., a 9xxx message will be forwarded). The Field in Error, field in the message header, will contain the value of the

first offending field that caused the message validation failure. If the message header is invalid, then the Field in Error field will contain "999".

4.2.7 Authorization Checks

Following is a list of basic controls the issuer bank's processing system might implement when approving transactions. Failure of any of these checks should result in the transaction being denied. The reason for denial should be indicated by the use of an appropriate non-zero response code value being returned in DE-39 of the relevant response message. A full list of available response codes, values and their meanings are provided in the entry under the DE-39, Response Code in chapter 5, and Data Element Descriptions.

- Verify that the transaction selected is valid for the customer at the acquiring institution. If not, then return an "Invalid Transaction" response code value of "12".
- For card-related transactions where a PIN is entered, verify that the PIN entered by the customer is correct. If not, and the maximum number of pin retries has not been reached for the day, then return an "Incorrect Personal Identification Number" response code value of "55". If the maximum number of PIN tries for the day has been exceeded return an "Allowable number of PIN tries exceeded" response code value of "75". The issuer should inhibit further access for that card. The inhibition should remain in effect until it is lifted through an administrative procedure upon cardholder request.
- For monetary and authorization transactions, verify that the transaction amount selected is within the valid range. If lower than the minimum allowed return an "Invalid Amount" response code value of "13" or if greater than the maximum allowed return an "Exceeds Withdrawal Amount Limit" response code value of "61".
- For card-related transactions, verify the card number. If the card account number is invalid, then return an "Invalid card number" response code value of "14".
- For card-related transactions, verify the expiration date of the card against the current date. If the card is expired, then return an "Expired Card" response code value of "54".
- Verify the customer's account number. If the account number is not valid then return the appropriate response code value from those below.

Value	Description
39	No Credit Account
52	No Checking Account
53	No Savings Account

- Verify the customer's account status. If the account status is not valid for the transaction required, then return the appropriate response code as defined in the entry for field 39 in chapter 4.
- For monetary and authorization transactions, verify that the customer's account has sufficient funds to perform the requested transaction. If not return a "Not sufficient funds" response code value of "51".

- For monetary and authorization transactions, verify that the customer's daily maximum withdrawal/POS "number" limit has not been exceeded for the current business day. If it has then return an "Exceeds withdrawal/POS frequency limit" response code value of "65".

4.2.8 Network Control

This section describes how the status of the connection between the UAESWITCH and a Member Bank controls transaction traffic to and from that bank.

The status of a particular connection between the UAESWITCH and a Member Bank may be either "up" or "down". When a session is in an "up" state all traffic to and from the bank will be allowed. When a session is in a "down" state only logon request traffic will be allowed (a special case is made however for cutover and reconciliation messages which may still be exchanged). The only way that a session's status may be changed from "down" to "up" is via a successful logon request transaction (either bank or the UAESWITCH initiated). Similarly, the only way that a session's status may be changed from "up" to "down" is via a successful logoff request transaction (again, either bank or the UAESWITCH initiated).

Note: Any outstanding responses will still be sent between the parties.

Whenever the UAESWITCH receives messages for a bank whose connection status is down, it will issue an appropriate denial response, with the response code value set to "91" in field 39, indicating that the issuer is unavailable.

4.2.9 EMV Based Transactions Receipts & Journal

The acquirer ATM should have the following items added to the ATM receipts and journal in case of an EMV based transaction:

- 9F06 "Application Identifier (AID)"
- 9F12 "Application preferred name" if present; otherwise, print tag 50 "Application Label"

The receipt may, at the acquirer's discretion, additionally contain the cryptogram (ARPC) and the data elements used to calculate the cryptogram.

4.3 Financial

This section contains details of how the various financial transactions defined by the UAESWITCH network should be processed in normal and abnormal situations

4.3.1 ATM Transactions

This section discusses the requirements of processing ATM transactions through the UAESWITCH. At present the UAESWITCH defines the following basic ATM transactions:

- Cash Withdrawal
- Balance Inquiry

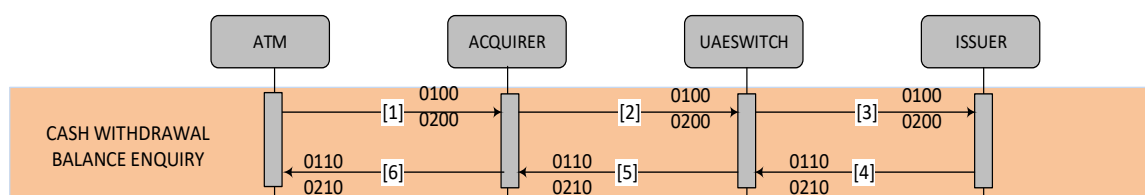
For cash withdrawals, the processing required for the following scenarios are discussed in turn:

- Normal Transaction Completion (approved or denied)
- Acquirer unavailable for response from the Issuer
- Late (or duplicate) approval response received by the UAESWITCH from Issuer
- Late approval response received by the Acquirer from the UAESWITCH
- Reversal by the Acquirer due to an ATM problem
- Forced Credit by the Acquirer due to an ATM partial reversal problem

These scenarios serve to illustrate the processing requirements in all conceivable situations.

For balance inquiry transactions a single scenario is sufficient to describe all the processing requirements.

4.3.2 Cash Withdrawal / Balance Enquiry



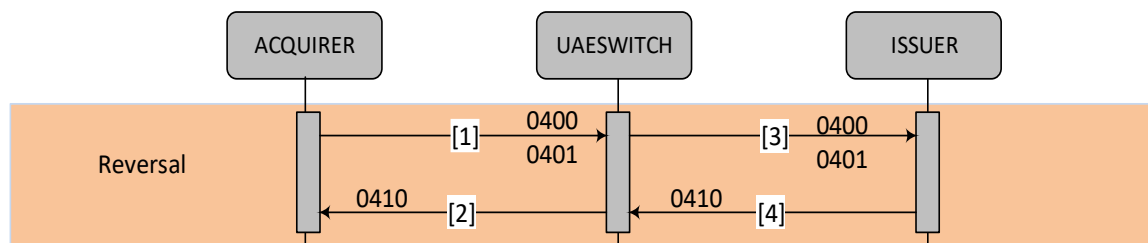
1. Card Holder initiates Cash Withdrawal/Balance enquiry Service request (0100/0200) on ACQUIRER ATM
2. ACQUIRER submits transaction request (0100/0200) to UAESWITCH
3. UAESWITCH routes the transaction request (0100/0200) to the ISSUER
4. ISSUER responds (0110/0210) to UAESWITCH
5. UAESWITCH routes the response (0110/0210) to the ACQUIRER
6. ACQUIRER forwards the response (0110/0210) to the ATM

Note: - In the future, when Jaywan cards are accepted outside UAE, the transaction will be performed in DMS mode and issuers should process cash withdrawals with 0100 message type and followed by the clearing file.

4.3.3 ATM Reversal

For the cash withdrawal requests reversal must be generated if the Acquirer is unable to process an authorized response due to any reason.

Store-and-forward will be adopted in case the sender of the reversal advice cannot receive any response



1. ACQUIRER generates a reversal (0400/0401) request to UAESWITCH
2. After performing the required check UAESWITCH acknowledges the response (0410) to ACQUIRER
3. UAESWITCH forwards the 0400/0401 request to the ISSUER
4. The Issuer responds (0410) to the UAESWITCH

4.4 Point of Sale

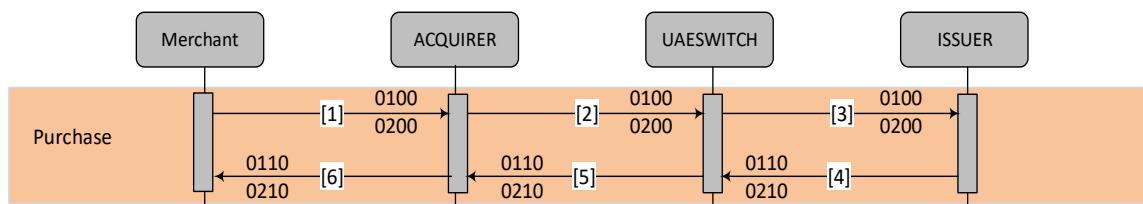
This section discusses the requirements of processing POS transactions through the UAESWITCH. At present the UAESWITCH defines the following basic POS transactions:

- Purchase/Sale
- Pre-authorization
- Pre-authorization top-up
- Pre-Authorization Completion
- Refund
- Void
- Reversal
- POS Balance Inquiry

4.4.1 POS Purchase

The basic service which allows the cardholder to pay for the purchase of goods and services from a card acceptor using their card.

It refers to the procedure of completing payment with bankcard accounts at POS terminals or through other channels when Merchants sell commodities or provide services.



1. MERCHANT submits purchase request (0100/0200) to ACQUIRER
2. ACQUIRER submits a purchase request (0100/0200) to UAESWITCH
3. UAESWITCH (detokenize if it is token) routes the transaction request (0100/0200) to the ISSUER
4. ISSUER responds (0110/0210) to UAESWITCH
5. UAESWITCH (tokenize if it is tokenized transaction) routes the response (0110/0210) to the ACQUIRER
6. ACQUIRER forwards the response (0110/0210) to the MERCHANT

Please review the following sections

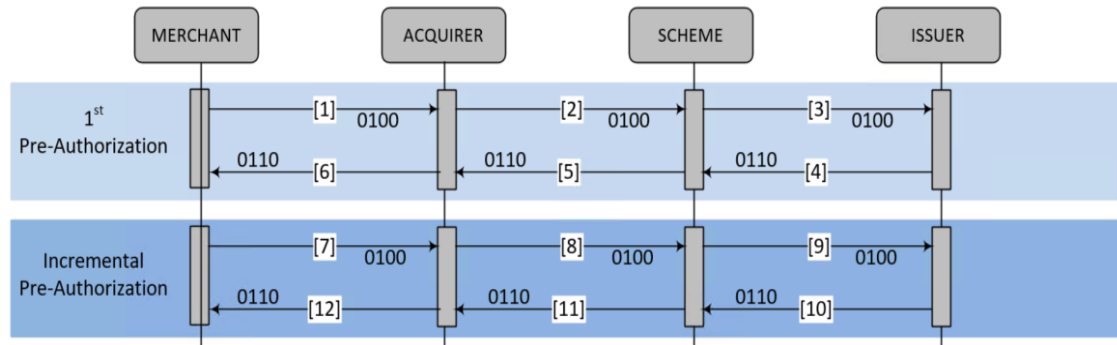
- 12.4 Purchase
- 12.7 Partial Authorization
- 12.8 Purchase with Cashback
- 12.13 Tokenization

4.4.2 Pre-Authorization & Incremental Pre-Authorization

The purpose of the incremental authorization is to increase the previously authorized amount.

If the final amount will exceed or is likely to exceed the amount of the pre-authorization, a further incremental authorization may be obtained. The incremental authorization will be for the difference between the original pre-authorization and the actual or estimated final amount. The sum of all linked estimated and incremental authorizations represent the total amount on hold in the cardholder's account for a given transaction.

By using incremental authorizations merchants can ensure the cardholder's open-to-buy accurately reflects their transaction activity.



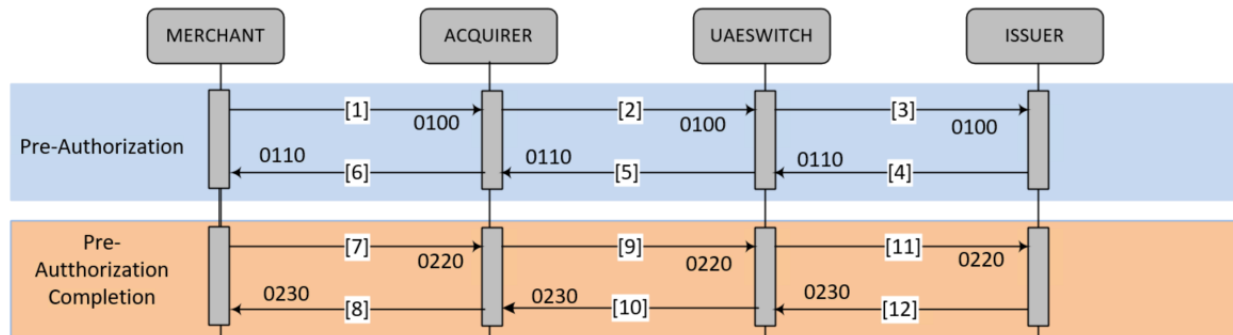
1. MERCHANT submits Pre-Auth request (0100) to ACQUIRER
2. ACQUIRER submits Pre-Auth request (0100) to UAESWITCH
3. UAESWITCH routes Pre-Auth request (0100) to the ISSUER
4. The ISSUER responds (0110) to UAESWITCH
5. UAESWITCH routes the Issuers response (0110) to the ACQUIRER
6. ACQUIRER routes response (0110) to the MERCHANT
7. MERCHANT submits incremental Pre-authorization request (0100) to ACQUIRER
8. ACQUIRER sends the incremental pre-authorization request (0100) to UAESWITCH
9. UAESWITCH forwards the incremental pre-authorization request (0100) to the ISSUER
10. The ISSUER shall associate the incremental pre-authorization with the 1st pre-authorization transaction. After required processing, the issuer acknowledges the response (0110) to UAESWITCH
11. UAESWITCH returns the incremental pre-authorization response (0110) to the ACQUIRER
12. ACQUIRER forwards 0110 response to the MERCHANT

Please review section 12.5. Pre-Authorization & Pre-Authorization Completion

4.4.3 Pre-authorization & Pre-authorization Completion

For an approved pre-authorization transaction, the pre-authorization completion (request) is used to complete the payment and settlement of the transaction.

This transaction is included in daily settlement and reconciliation and supports reversal advice.



1. MERCHANT submits Pre-Auth request (0100) to ACQUIRER
2. ACQUIRER submits Pre-Auth request (0100) to UAESWITCH
3. UAESWITCH routes the transaction request (0100) to the ISSUER
4. ISSUER responds (0110) to UAESWITCH
5. UAESWITCH routes the response (0110) to the ACQUIRER
6. ACQUIRER routes the response (0110) to the MERCHANT
7. MERCHANT submits pre-authorization completion advice (0220) to the ACQUIRER
8. ACQUIRER acknowledges Pre-Authorization completion advice (0230) to the MERCHANT
9. ACQUIRER submits the pre-authorization completion advice as an online 0220 advice to UAESWITCH
10. UAESWITCH acknowledges Pre-Authorization completion advice (0230) to the ACQUIRER
11. UAESWITCH forwards (0220) as an online message to the ISSUER
12. ISSUER acknowledges with (0230) response

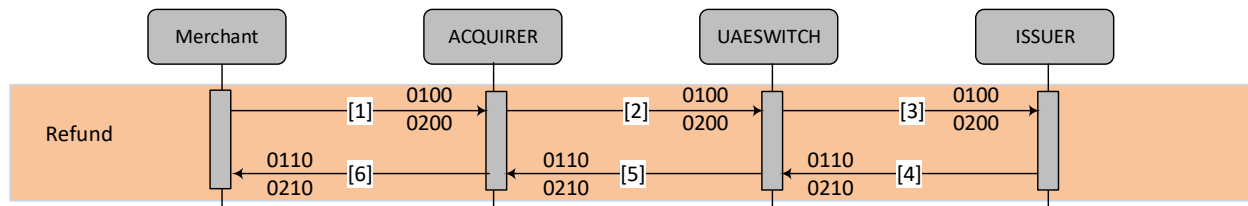
Note: - In view of DMS Support in future, issuers can expect pre-Auth completion messages either through ISO Message with MTI 0220 or through the clearing file.

Please review section 12.5. Pre-Authorization & Pre-Authorization Completion

4.4.4 Refund

A service which allows the card acceptor to reimburse the cardholder partially or totally.

Unlike Cancellation, Refund is not necessarily linked to any previous transaction

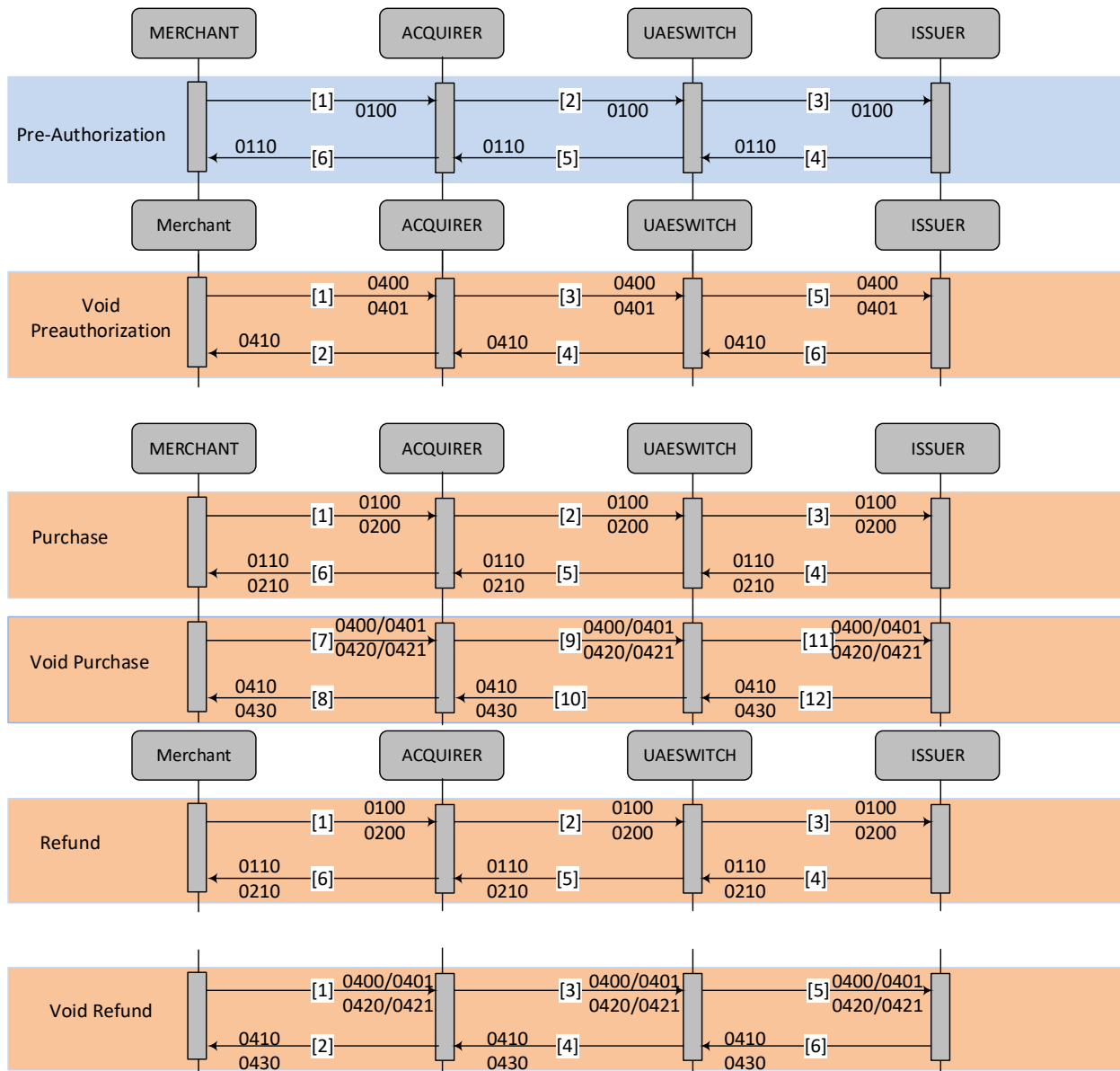


1. MERCHANT submits Refund (0100/0200) request to ACQUIRER
2. ACQUIRER submits Refund request (0100/0200) to UAESWITCH
3. UAESWITCH (detokenize, if it is token based transaction) routes the Refund request (0100/0200) to the ISSUER
4. ISSUER responds (0110/0210) to the UAESWITCH
5. UAESWITCH (tokenize if it is token) routes the ISSUER'S response (0110/0210) to the ACQUIRER
6. ACQUIRER forwards (0110/0210) to the MERCHANT

Please review section 12.6. Refund

4.4.5 Void

For a successful purchase/pre-authorization/refund, merchant cancel the payment commitment prior to settlement or prior to initiating a pre-authorization completion.



1. MERCHANT submits Purchase/Refund/Pre-Auth request (0100/0200) to ACQUIRER
2. ACQUIRER Submits Purchase/Refund/Pre-Auth request (0100/0200) to UAESWITCH
3. UAESWITCH routes the Purchase/Refund/Pre-Auth request (0200/0100) to the ISSUER
4. ISSUER responds (0110/0210) to UAESWITCH
5. UAESWITCH routes the response (0110/0210) to the ACQUIRER
6. ACQUIRER routes the response (0210/0110) to the MERCHANT

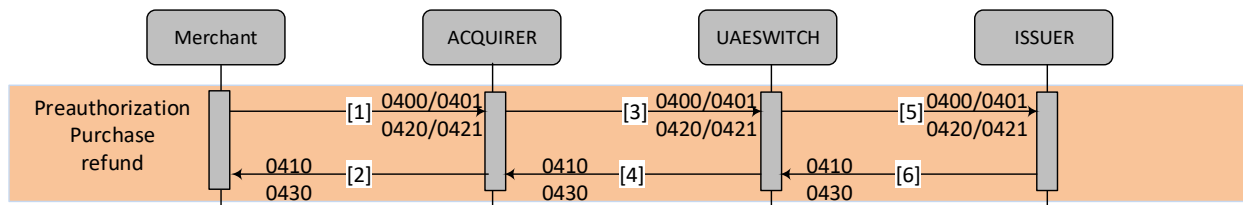
7. For authorized Pre-Auth (0100)/Purchase/Refund (0100/0200) requests, the MERCHANT initiates a cancellation request (0400/0401/0420/0421) *
8. After performing the required check ACQUIRER acknowledges the response (0410/0430) to MERCHANT
9. ACQUIRER submits the 0400/0401/0420/0421 advice ONLINE to the UAESWITCH
10. UAESWITCH acknowledges 0410/0430 response to the ACQUIRER
11. UAESWITCH forwards 0400/0401/0420/041 as an online message to the issuer
12. ISSUER acknowledges with 0410/0430 message

4.4.6 Reversal

For the requests with the message type identifier 0100 and 0200, except for inquiry requests, Reversal advice must be generated if the Acquirer and Scheme cannot receive any response to the transaction request within a specified timeframe.

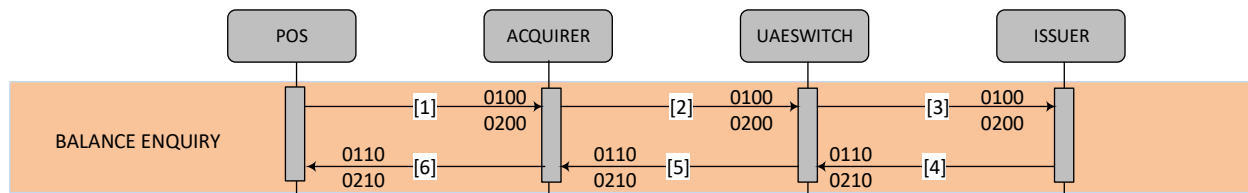
When the Acquirer receives reversal advice from the terminal or Scheme receives reversal advice from the Acquirer, a response must be given immediately. If the original transaction is successful, it shall be firstly set to reversed transaction and then reversal advice will be sent to the next institution, to which the original transaction is sent.

Store-and-forward will be adopted in case the sender of the reversal advice cannot receive any response. But reversal advice shall not be sent on another settlement day.



1. On Pre-Auth (0100)/Purchase, (0100/0200)/Refund (0100/0200) request timeouts, the MERCHANT generates a reversal (0400/0401/0420/0421) request
2. After performing the required check ACQUIRER acknowledges the response (0410/0430) to MERCHANT
3. ACQUIRER forwards the 0400/0401/0420/0421 request to the UAESWITCH
4. UAESWITCH acknowledges a 0410/0430 response
5. UAESWITCH detokenize and forwards the reversal request to the ISSUER
6. The Issuer responds (0410/0430) to the UAESWITCH

4.4.7 POS Balance Inquiry



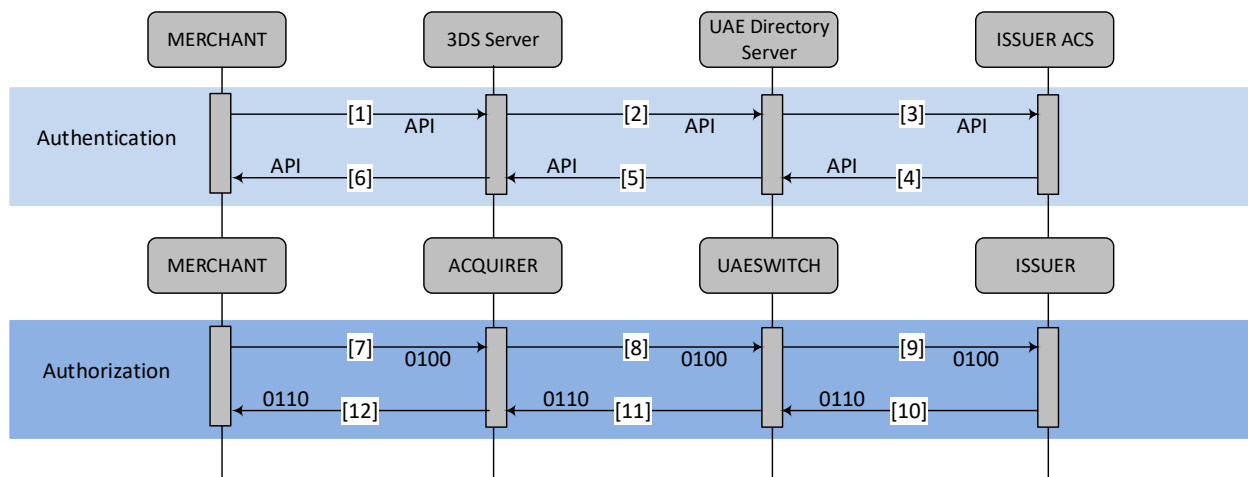
1. Card Holder initiates Balance enquiry transaction request (0100/0200) on ACQUIRER terminal
2. ACQUIRER submits transaction request (0100/0200) to UAESWITCH
3. UAESWITCH routes the transaction request (0100/0200) to the ISSUER
4. ISSUER responds (0110/0210) to UAESWITCH
5. UAESWITCH routes the response (0110/0210) to the ACQUIRER
6. ACQUIRER forwards the response (0110/0210) to Terminal

4.5 Ecommerce

This section discusses the requirements of processing E-commerce transactions through the UAESWITCH. At present the UAESWITCH defines the following basic E-commerce transactions:

- Purchase/Sale
- Recurring/Installment Payments
- Incremental Auth
- Refund
- Void/Cancel
- Reversal

4.5.1 ECOM Purchase/Sale

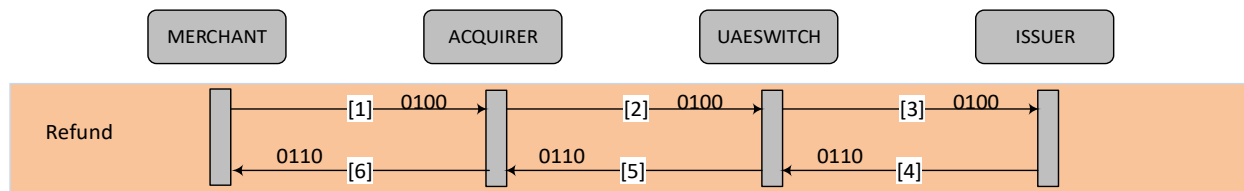


1. 3DS Server initiates 3DS flow with Directory Server. Merchant initiates transaction on behalf of cardholder, with its 3DS Server.
2. 3DS Server initiates 3DS flow with Directory server.

3. Directory Server forwards the request to respective ACS (Access Control Server)
4. ACS sends response to DS and Authentication methods to Directory Server.
5. Directory servers forwards the response back to 3DS Server
6. 3DS Servers sends the response back to Merchant using its integration with merchant and then cardholder authentication with ACS is completed. After successful authentication transaction route to acquirer for Authorization.
7. Post successful cardholder authentication, merchant initiate's authorization leg with its acquirer.
8. Acquirer Switch forms the authorization message and sends it to UAE Network.
9. UAENETWORK detokenize if it is token and send the authorization leg to respective Issuer host for Debit
10. Issuer host sends a successful response to UAE Network.
11. UAE Network will re-tokenize the Issuer host response, if applicable and sends a successful response to Acquirer.
12. Acquirers sends the received response back to Merchant.

Note: Please refer to AEP SecureNxt Specification document to get information about the authentication leg.

4.5.2 Recurring Transactions

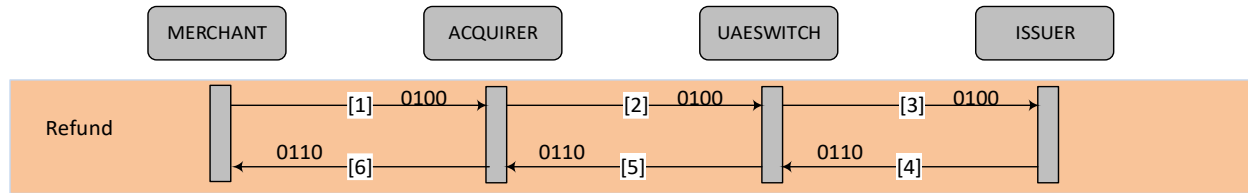


Merchant send Recurring transactions periodically to issuer to debit customers account for any service customer has opted.

1. MERCHANT submits recurring transaction request to ACQUIRER
2. ACQUIRER Submits recurring transaction to UAESWITCH
3. UAESWITCH routes this transaction to the ISSUER
4. ISSUER reply for the transaction request to UAESWITCH
5. UAESWITCH routes the response to ACQUIRER
6. ACQUIRER routes the response message to the MERCHANT

4.5.3 ECom Refund

A service which allows the card acceptor to reimburse the cardholder partially or totally. Unlike Cancellation, Refund is not necessarily linked to any previous transaction



1. MERCHANT submits Refund (0100) request to ACQUIRER
2. ACQUIRER submits Refund request (0100) to UAESWITCH
3. UAESWITCH (detokenize if it is token) routes the Refund request (0100) to the ISSUER
4. ISSUER responds (0110) to the UAESWITCH
5. UAESWITCH (tokenize if it is token) routes the ISSUERS response (0110) to the ACQUIRER
6. ACQUIRER forwards (0110/0210) to the MERCHANT

Please review section 12.6. for Refund

4.5.4 Void

Please refer section 4.3.2.5 for Void.

4.5.5 Reversal

Please refer section 4.3.2.6 for Reversal.

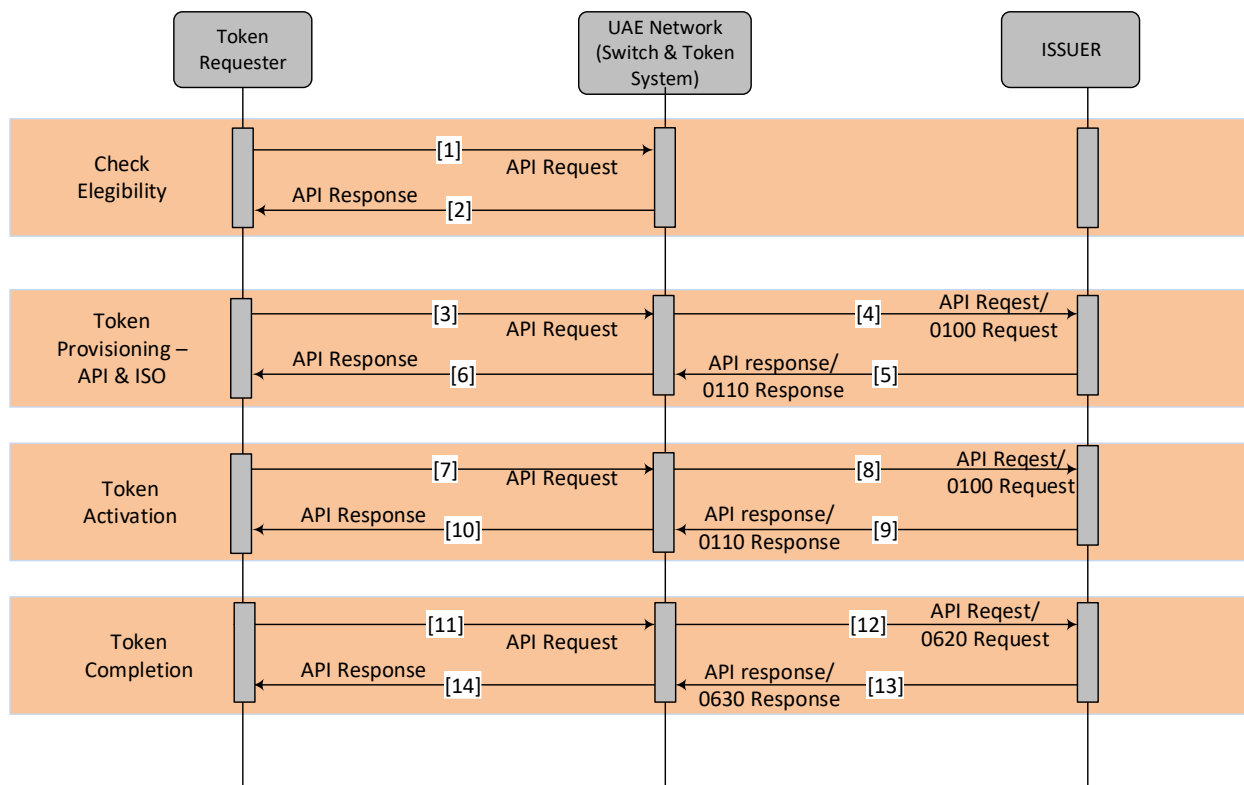
4.6 Tokenization

This section discusses the requirements of supporting Tokenization through the UAESWITCH. At present the UAESWITCH defines the following functionalities for Tokenization

4.6.1 Token Provisioning

4.6.1.1 Jaywan Mono Badge Card - Token Provisioning

Payment tokenization is the process of replacing the traditional payment card account number with a unique digital token in online and mobile transactions. Tokens can be restricted for transactions with a specific mobile device, merchant or transaction type.



1. Cardholder wants to provision (add) a card on device. TR (Token Requestor) initiates Check Eligibility call to UAE Token system to check if BIN is eligible for Tokenization.
2. UAE token system checks the Card BIN mapping against on-boarded issuer BINs, and it will send either a successful or decline response back to Token Requestor. If it is decline, then flow will stop and if it is approved then it will move ahead with next step.
3. TR triggers token provisioning request to UAE token system to token provisioning.
4. UAE Token system will send provisioning request either 0100 TAR (token account request) or API call to Issuer.
5. Issuer responses to TAR mentioning the Additional step-up authentication required for token creation.

6. UAE Token system now generates token and keeps the initial state as in-active at this stage. Then TR receives the Token Ref ID for the respective token.
7. Cardholder now selects the OTP as authentication method to complete the authentication. TR generates the OTP and sends it to UAE token system.
8. UAE token system will pass that received OTP value to the issuer to deliver to the respective cardholder.
9. Issuer sends OTP to customer and responds back to UAE Token System
10. UAE Token system will send response back to TR.
11. After successful ID & V process, TR will send update token state request to UAE Token System.
12. UAE Token System updates the token state to active at its end and also sends a LCM notification to the Issuer.
13. Issuer gets notified about the event and Issuer system sends acknowledgement back to UAE Token system.
14. UAE Token provide will send response back to TR for update token state request.

4.6.1.2 Jaywan Co-Badge Card - Token Provisioning

In case of co-badge cards, there will be two tokens provisioned on the wallet.

1. Jaywan token (For domestic usage)
2. International scheme token. (For international usage)

International card scheme will be the primary party responsible for the token provisioning supported by the required authentication (ID & V) with an auxiliary Jaywan token also provisioned in the back end.

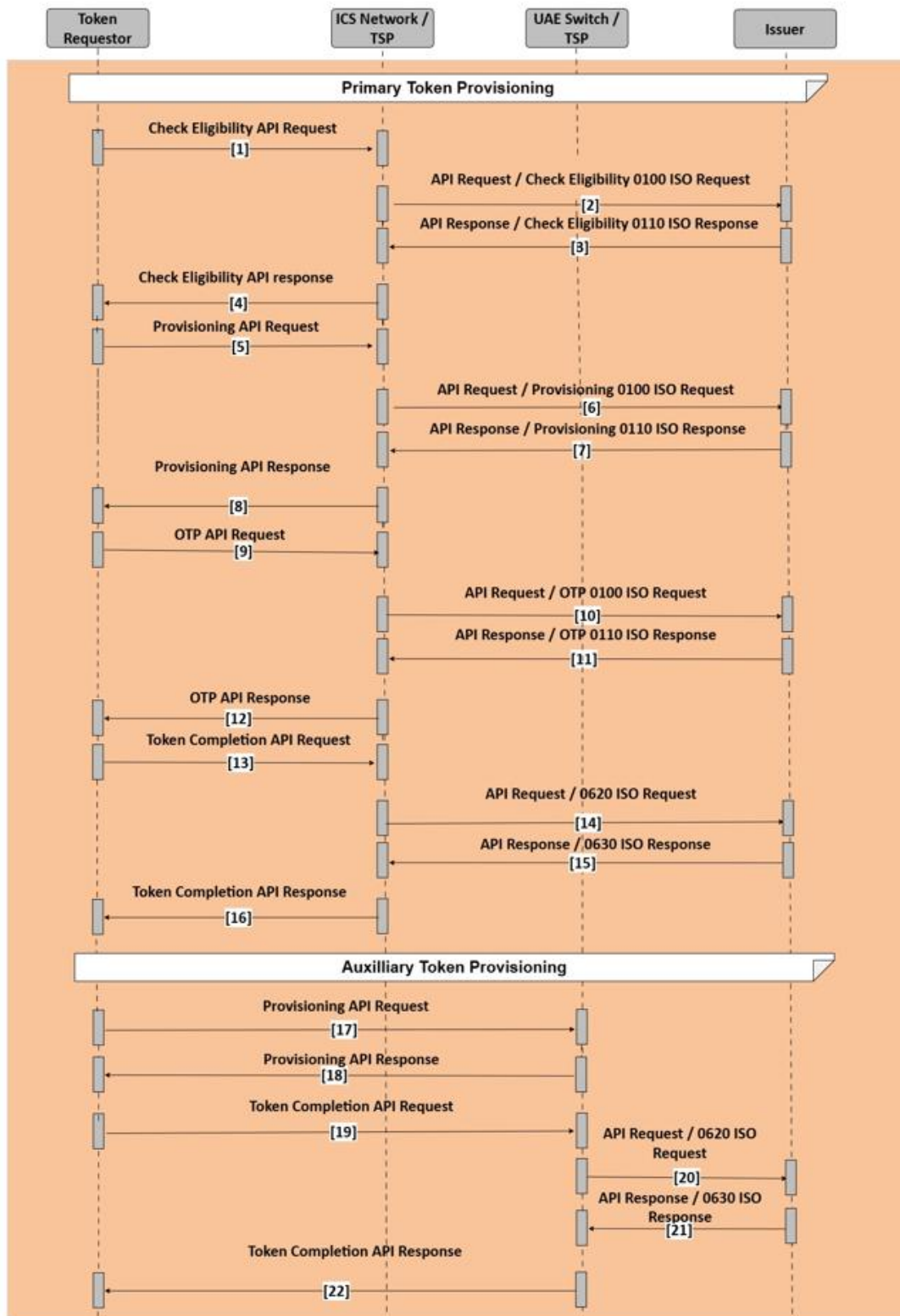
Upon successful completion of the token provisioning process, the Issuer will receive two separate completion notifications:

- One from the ICS Token System (ICS TSP) for the primary token, and
- One from the Jaywan TSP for the auxiliary (domestic) token.

The Jaywan notification will contain Issuer Card Reference id and Token reference id, which will be required to perform LCM activities with Jaywan TSP in both ISO and API integrations.

In case of Card On File(COF) provisioning issuers must support Jaywan token provisioning request coming from UAE Switch. COF provisioning requests can be identified using DE105 tag 21 = M4M_PAY.

This flow outlines the end-to-end process of provisioning a payment card on a device, including both international (ICS) and domestic (Jaywan TSP) tokenization components.



The Cardholder initiates the provisioning process by attempting to add their card to an OEM Wallet using the mobile device.

1. The Token Requestor (TR) sends a Check Eligibility API call to the ICS Token System.
2. The ICS Network Switch forwards a Check BIN request to the Issuer to perform eligibility validation. This may be optional for some issuers, as issuers may not opted.
3. The Issuer responds to the ICS Network with a success response if the card is eligible for tokenization.
4. The ICS Network forwards the successful eligibility response back to the TR.
5. The TR then initiates a Token Provisioning Request to the ICS Token System.
6. The ICS Token System sends a Token Authorization Request (TAR) message to the Issuer to request approval for token creation.
7. The Issuer responds to the TAR, indicating that step-up authentication (e.g., OTP) is required for token issuance.
8. The ICS Token System generates the token and keeps its state as inactive. It returns a Token Reference ID to the TR.
9. The Cardholder selects OTP as the authentication method. The TR generates the OTP and sends it to the ICS Token System.
10. The ICS Token System forwards the OTP value to the Issuer for delivery to the cardholder.
11. The Issuer sends the OTP to the customer and responds back to the ICS Token System confirming the delivery.
12. The ICS Token System relays this confirmation response back to the TR.
13. After the cardholder completes OTP verification (ID&V), the TR sends an Update Token State request to the ICS Token System.
14. The ICS Token System updates the token status to active and sends a Lifecycle Management (LCM) Notification to the Issuer.
15. The Issuer acknowledges receipt of the LCM notification by responding to the ICS Token System.
16. The ICS Token System sends a final response back to the TR confirming the token activation.
17. The TR now initiates a Provisioning Request to the Jaywan TSP to create a corresponding auxiliary token for domestic use.
18. The Jaywan TSP generates the auxiliary token and sends it back to the TR in the response.
19. The TR sends an Activation Request to the Jaywan TSP for the newly generated auxiliary token.
20. The Jaywan TSP activates the auxiliary token and sends LCM notifications to the Issuer.
21. The Issuer acknowledges the LCM notifications with a success response.
22. Jaywan TSP completes the flow by confirming token state activation to the TR.

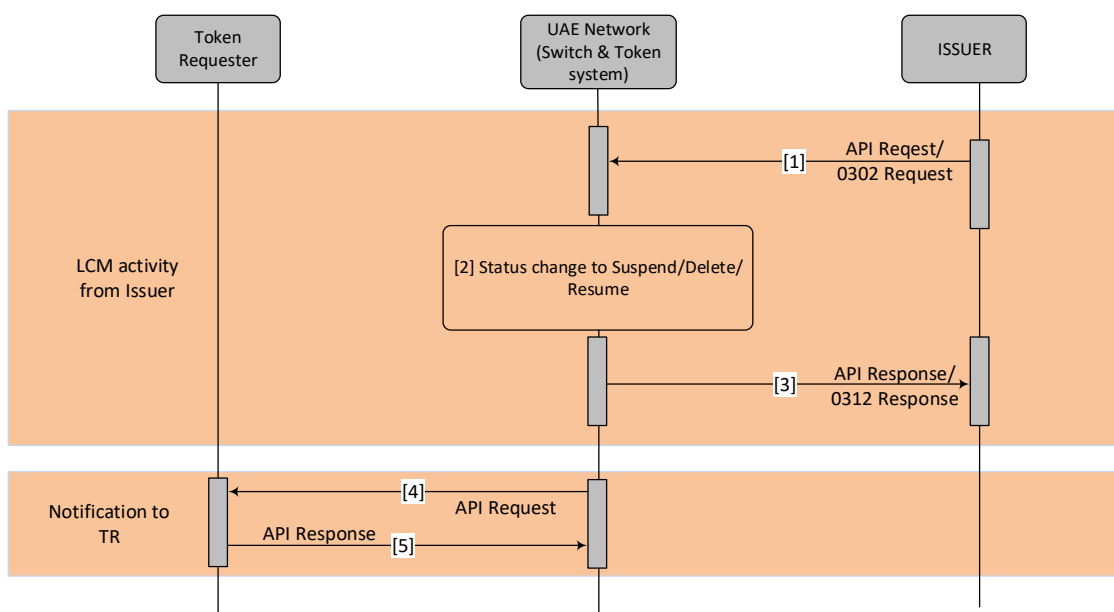
Upon successful completion of the token provisioning process, the Issuer will receive two separate completion notifications:

- One from the ICS Token System (ICS TSP) for the primary token, and
- One from the Jaywan TSP for the auxiliary (domestic) token.

4.6.2 Life Cycle Management

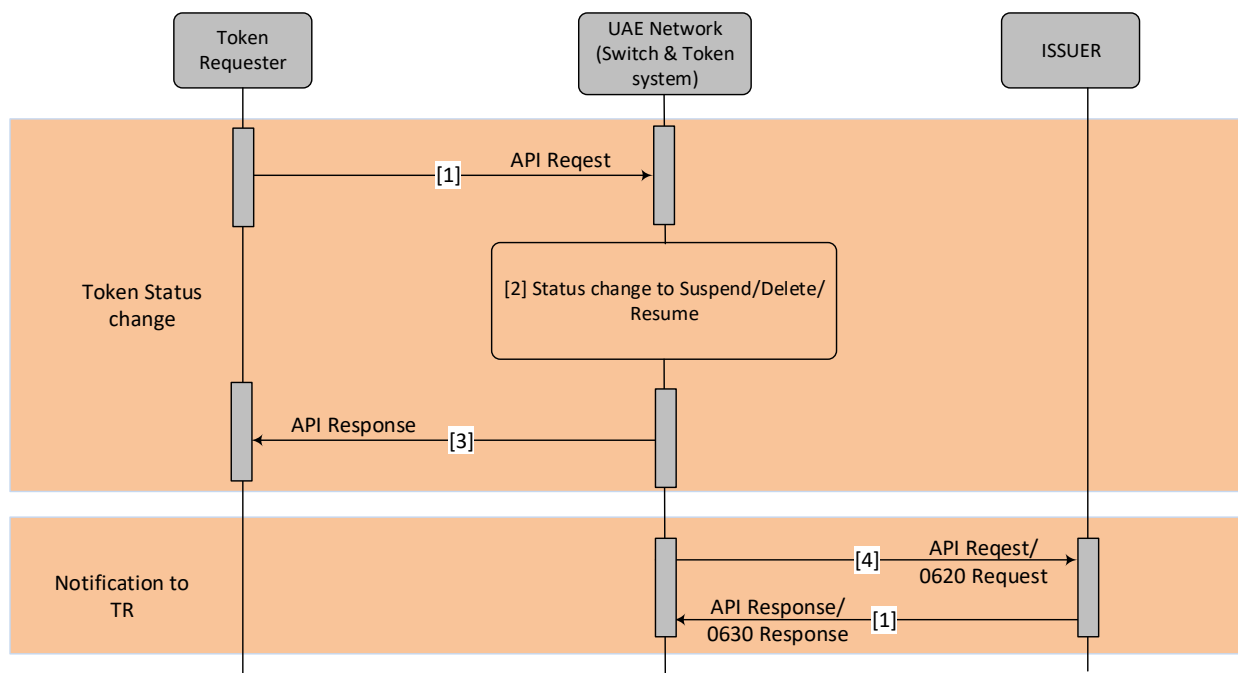
4.6.2.1. Jaywan Mono Badge Card - Life cycle Management from Issuer

Please find below message where bank/Cardholder want to take any action on case, below are the messages send to Tokenization system to synchronizing state for the card.



1. Issuer calls update card with desired Token state change & request reason to Jaywan TSP
2. Tokenization system changes the status
3. After changing state, it will respond back to Issuer
4. Tokenization system send update to TR (Token Requestor)
5. TR will send response back to the Tokenization system.

4.6.2.2 Jaywan Mono Badge Card - Life cycle Management from TR



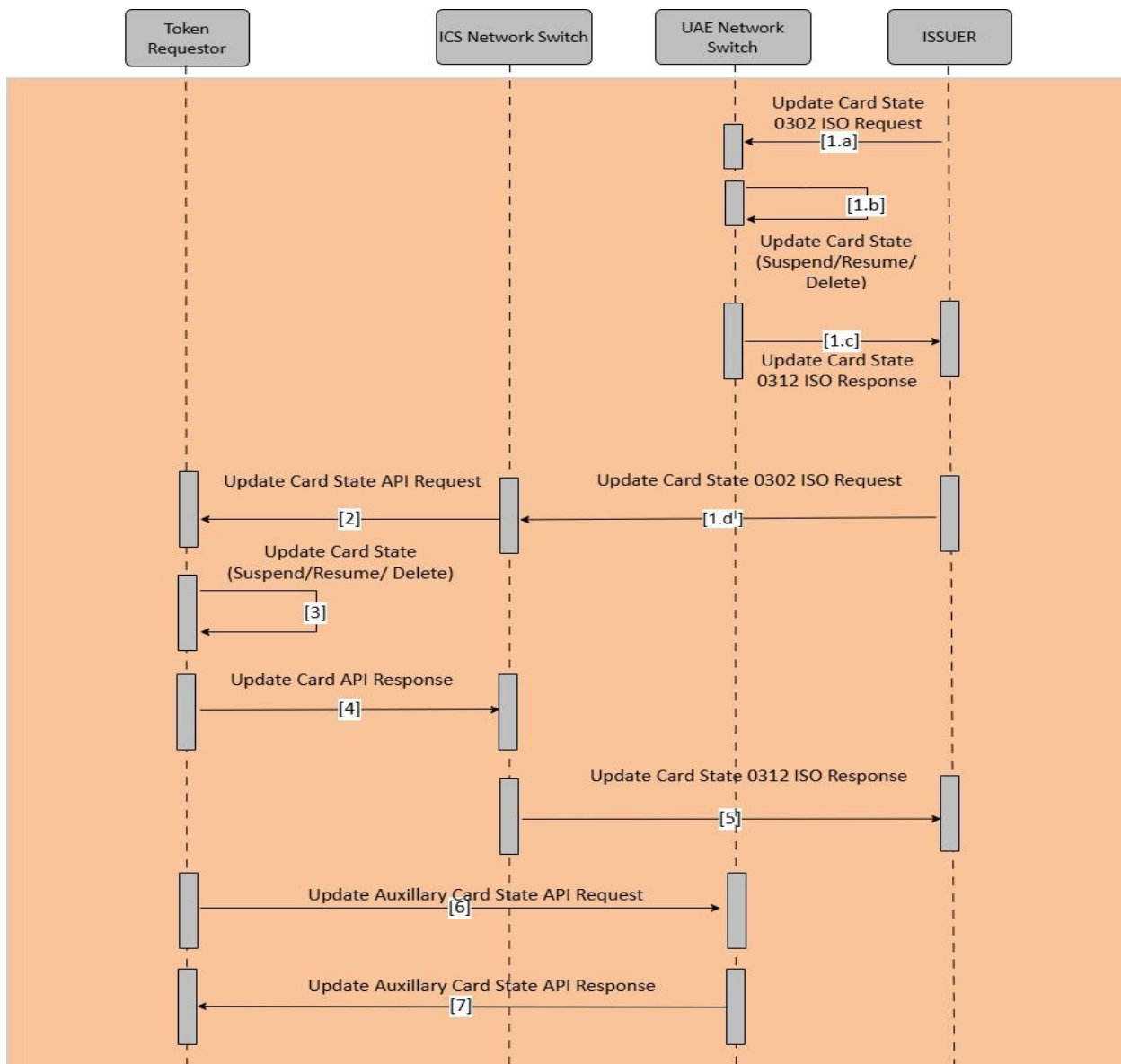
1. TR calls Update Token State API call to UAE Network with the token state & request reason.
2. Tokenization system will update token state as per request locally.
3. Tokenization system responds back to TR
4. Tokenization system calls Issuer to notify token state change
5. Issuer responds back to Tokenization system

4.6.2.3 Jaywan Co-Badge Card - Life Cycle Management from Issuer

For Token life cycle management related to card status change, OEM Pay will update the status to Jaywan TSP and issuers not required to perform any update with Jaywan TSP.

For Token Life Cycle Management related to Card renewal, replacement and product transfer, issuers are required to make additional API/ISO call to Jaywan TSP for updating Jaywan tokens.

This flow describes how the issuer initiates a lifecycle change for a Jaywan Co-Badge card, and how it propagates across the ICS and Jaywan Token Systems.



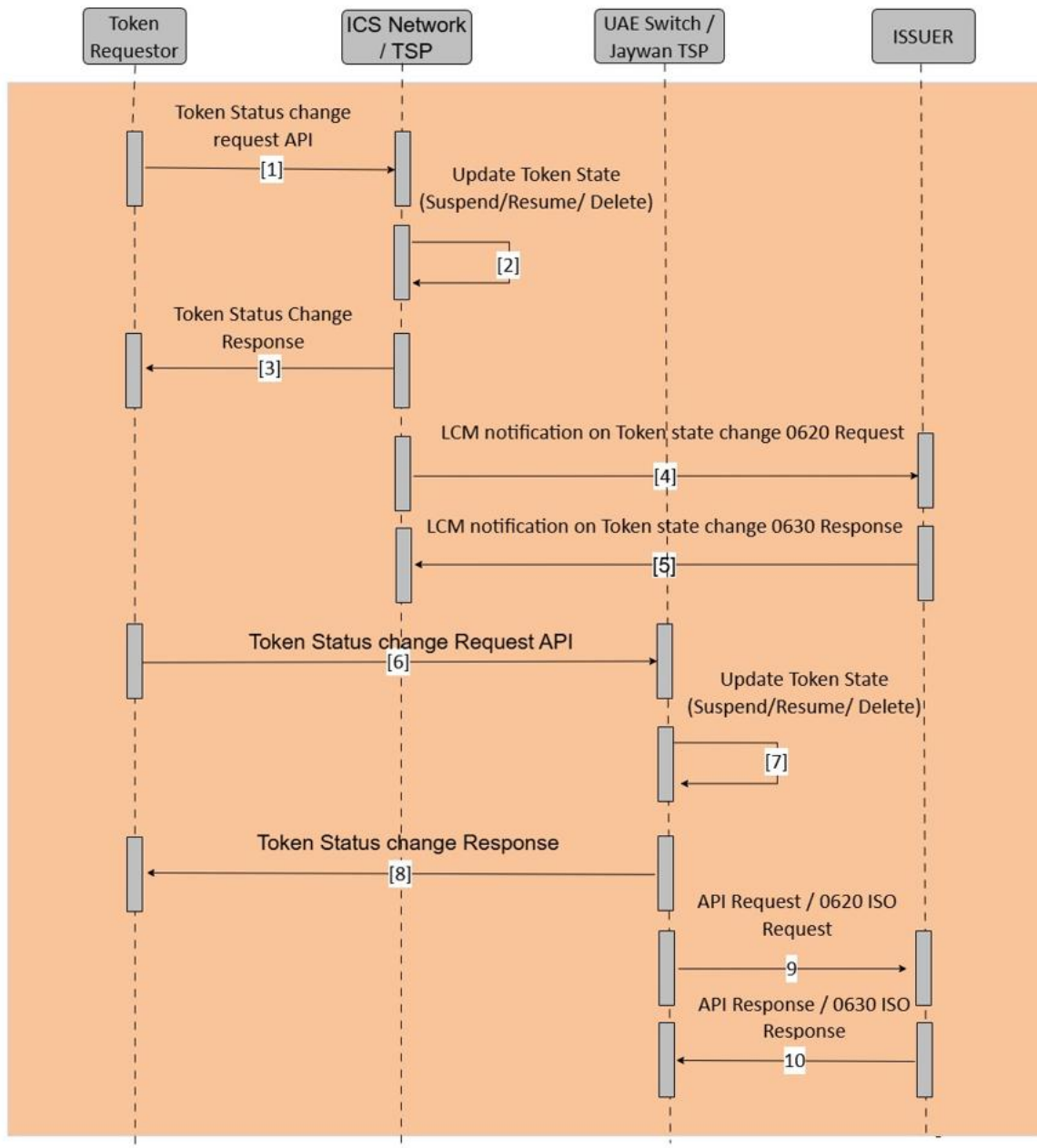
1. The Issuer sends an Update Card request to the Jaywan Token System and ICS Token System, specifying the desired Primary Token state change (e.g., suspend, resume, deactivate) along with the reason for the request.
2. The ICS Token System processes the request, updates the token state in its internal system, and forwards the token update request to the Token Requestor (TR).
3. The Token Requestor (TR) performs the token state update (e.g., changes status to suspended or deactivated) at its end.
4. Once the update is complete, the TR sends a confirmation response back to the ICS Token System.
5. The ICS Token System responds to the Issuer, confirming that the token state update has been successfully applied.
6. Separately, the TR initiates a second Update Card request to the Jaywan Token System, ensuring that the Jaywan (domestic) token reflects the same updated state.
7. The UAE Token System processes the request, updates the token state, and sends a confirmation response back to the TR.
8. On successful completion of the status update, Jaywan TSP sends an event notification to the Issuer regarding the status change of the auxiliary token.

As a result, the Issuer will receive two notifications:

- One from the ICS Token System (for the primary token)
- One from the Jaywan TSP (for the auxiliary token)

4.6.2.4 Jaywan Co-Badge Card - Life Cycle Management from TR

This flow describes how a Token Requestor (TR) initiates a token state change (e.g., suspend, resume, deactivate) for a Jaywan Co-Badge card, and how it is propagated across both ICS and Jaywan TSP.



1. The Token Requestor (TR) initiates an Update Token State API call to the ICS Tokenization System, providing the desired token state and request reason.
2. The ICS Tokenization System updates the token state locally in its internal system based on the received request.
3. The ICS Tokenization System sends a response back to the TR, confirming the state update.
4. The ICS Tokenization System then sends a token state change notification to the Issuer, informing them of the updated token status.
5. The Issuer sends an acknowledgment response back to the ICS Tokenization System.
6. The TR separately initiates another Update Token State API call to the Jaywan TSP, with the same token state and request reason, in order to update the auxiliary (domestic) token.
7. The Jaywan TSP processes the request and updates the token state in its system.
8. The Jaywan TSP sends a confirmation response back to the TR.
9. On Successful completion of status update, Jaywan TSP send a token event notification to issuer on successful status update. As a result, the Issuer will receive two notifications:
 - One from the ICS Token System (for the primary token)
 - One from the Jaywan TSP (for the auxiliary token)

4.7 Network Management

This section describes the processing requirements of the network management transactions that control the smooth administration of the UAESWITCH network. The following subsections are present:

- Logon transactions
- Logoff transactions
- Cutover transactions
- Echo Test transactions
- Key Change transactions

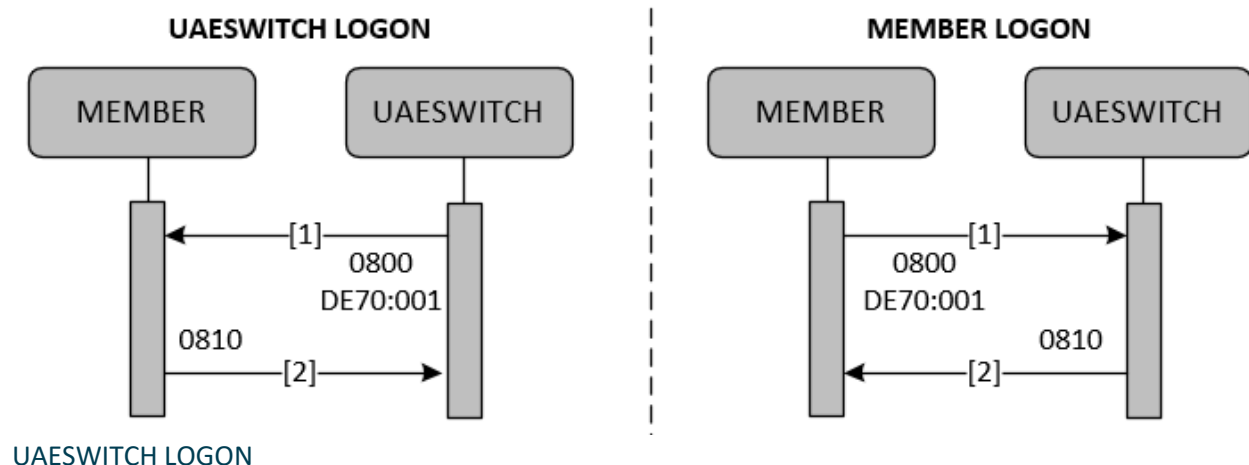
It should be noted that these transactions only involve a single bank and the UAESWITCH. Thus, the terms acquirer and issuer do not apply to the transactions in this section.

4.7.1 Logon

The logon facility is designed to establish application to application connection between a Member Bank and the UAESWITCH. Both banks and the UAESWITCH may initiate logon requests. In the case of the UAESWITCH this will be an operator level command.

The following logon transaction scenarios are considered:

- UAESWITCH Logon
- MEMBER Logon



1. UAESWITCH sends a LOGON request (0800 with DE 70 value of '001') to a MEMBER
2. MEMBER acknowledges with LOGON response (0810 response with DE39 00) to UAESWITCH

MEMBER LOGON

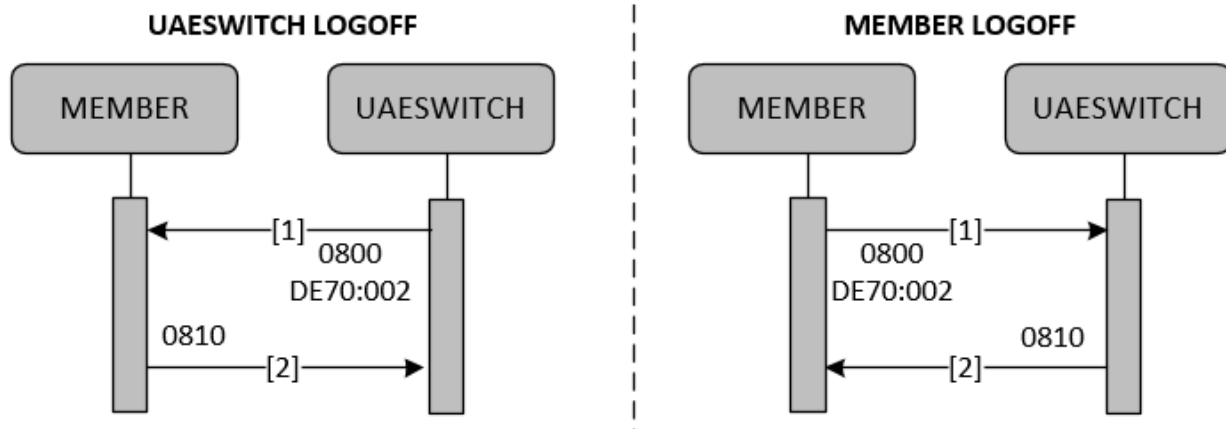
1. MEMBER sends a LOGON request (0800 with DE 70 value of '001') to UAESWITCH
2. UAESWITCH acknowledges with LOGON response (0810 response with DE39 00) to MEMBER

4.7.2 Logoff

The logoff facility is designed to terminate an established application to application connection between a Member Bank and the UAESWITCH. Both banks and the UAESWITCH may initiate logoff transactions, in the case of the UAESWITCH this will be an operator level command.

The following logoff transaction scenarios are considered:

- UAESWITCH Logoff
- MEMBER Logoff



UAESWITCH LOGOFF

1. UAESWITCH sends a LOGOFF request (0800 with DE 70 value of '002') to a MEMBER
2. MEMBER acknowledges with LOGOFF response (0810 response with DE39 00) to UAESWITCH

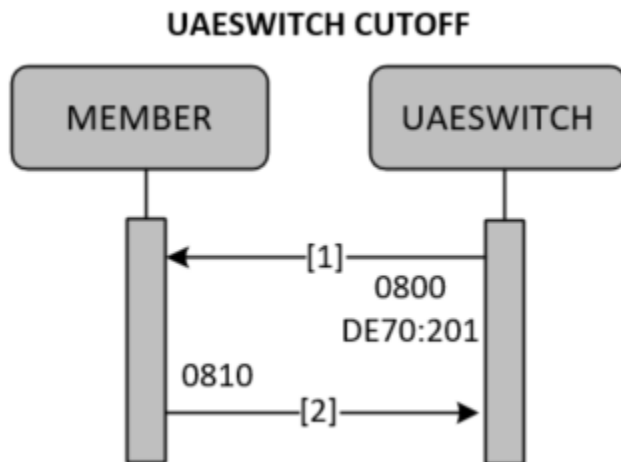
MEMBER LOGON

1. MEMBER sends a LOGOFF request (0800 with DE 70 value of '002') to UAESWITCH
2. UAESWITCH acknowledges with LOGOFF response (0810 response with DE39 00) to MEMBER

4.7.3 Cutover

The cutover transaction is used to inform banks that the UAESWITCH business day has changed.

Deliveries of cutover requests are guaranteed. This means that the same SAF mechanism used for reversal processing is also used for cutover processing. This is fully described in section 4.2.6, Reversal Processing. The only differences are in the message types involved (08xx, rather than 04xx).



UAESWITCH CUTOFF

1. UAESWITCH sends a CUTOFF request (0800 with DE-70 value of '201') to a MEMBER. DE-15 will contain then new UAESWITCH Business Day
2. MEMBER acknowledges with CUTOFF response (0810 response with DE39 00) to UAESWITCH.

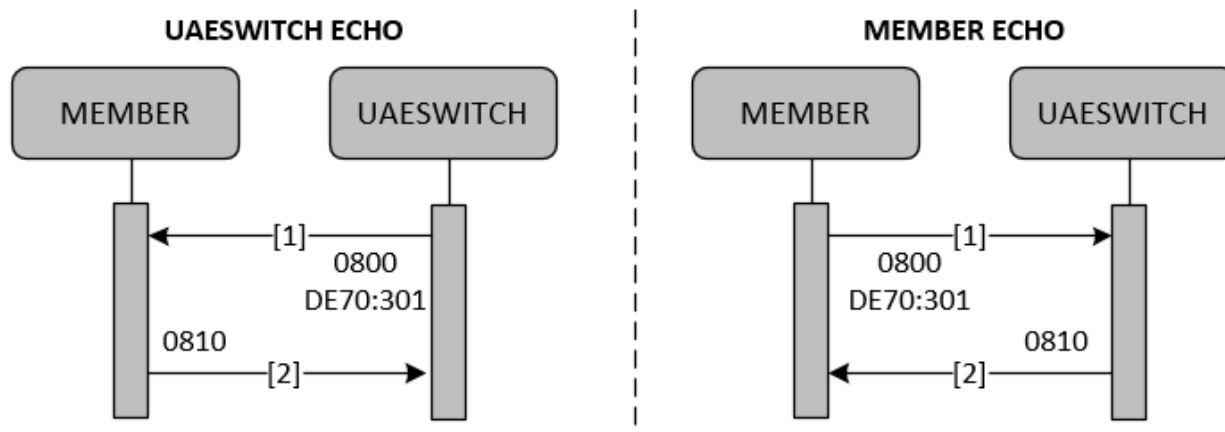
After all the interfaces have been cutoff for a given business day, the UAESWITCH will freeze the reconciliation totals for the old business day and generate reconciliation transactions.

4.7.4 Echo Test

The UAESWITCH will automatically generate an echo test transaction to a bank whenever a configurable time period has elapsed without any message traffic on the UAESWITCH /bank connection.

The following echo test scenarios are considered:

- UAESWITCH Echo Test
- MEMBER Echo Test



UAESWITCH ECHO

1. UAESWITCH sends an ECHO request (0800 with DE-70 value of '301') to a MEMBER
2. MEMBER acknowledges with ECHO response (0810 response with DE-39 00) to UAESWITCH

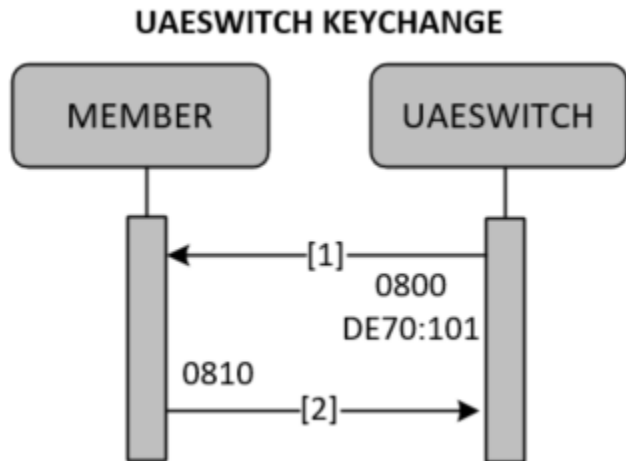
MEMBER LOGON

1. MEMBER sends an ECHO request (0800 with DE-70 value of '301') to UAESWITCH
2. UAESWITCH acknowledges with ECHO response (0810 response with DE-39 00) to MEMBER

4.7.5 Key Change

Key change transactions are generated at configurable intervals by the UAESWITCH to maintain security of network messages. Details of key generation and use are provided in chapter 9, Security Protocol. This section only deals with the key change transaction itself. The following scenario is sufficient to describe all aspects of key change transactions.

- UAESWITCH EXCHANGE



UAESWITCH KEYCHANGE

1. UAESWITCH sends a KEYCHANGE request (0800 with DE-70 value of '101') to a MEMBER
2. MEMBER acknowledges with KEYCHANGE response (0810 response with DE-39 00) to UAESWITCH

If MEMBER acknowledges the KEYCHANGE response the MEMBER should check the value of the Key Type and Key Sequence Number sub-fields of Additional Data, National (DE-47) to identify which key is being changed by the UAESWITCH.

The MEMBERS processing system should then enable the new key value contained in the Key Value sub-field of Additional Data, National (DE-47) using the procedure described in chapter 9, Security Protocol. If this is successful, the bank should return an 810-response message to the UAESWITCH with a response code value of "00" indicating that the key change has been implemented.

Note: The UAESWITCH will only implement the key change if it receives a timely approval response from the bank. A late or a denial response to a key change request will be status logged by the UAESWITCH, but the UAESWITCH will not then implement the key change. The key management mechanism, described in chapter 10, Security Protocol, is designed to handle these types of situations without causing key incompatibility problems.

4.8 Reconciliation

This section describes the processing of reconciliation transactions between the UAESWITCH and a bank. Reconciliation is designed to enable the exchange of those totals held by the UAESWITCH and a bank that monitors the volume of the UAESWITCH transaction traffic that the bank has processed in a particular UAESWITCH business day. These totals are fully defined in section 10.3 Reconciliation totals.

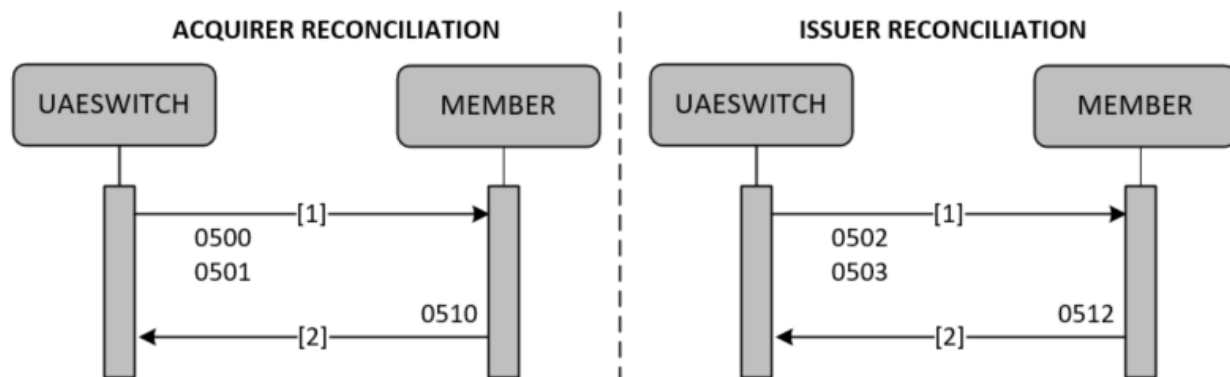
Since two sets of reconciliation totals are maintained, two types of reconciliation transaction are possible, as follows:

- Acquirer reconciliation transaction
- Card issuer reconciliation transaction

It is expected that Member Banks will always act as both issuers and acquirers of transactions, and hence each bank will always receive both transactions every business day.

A UAESWITCH generates reconciliation transactions, normally after all bank interfaces have been cutover.

Like cutover requests, deliveries of reconciliation requests are guaranteed. This means that the same SAF mechanism used for reversal processing is also used for reconciliation processing. This is fully described in section 4.2.6, Reversal Processing. The only differences are in the message types involved (05xx, rather than 04xx).



Acquirer Reconciliation

1. UAESWITCH initiates acquirer reconciliation request (0500) to a MEMBER
2. MEMBER acknowledges with acquirer reconciliation response (0510 response) to UAESWITCH

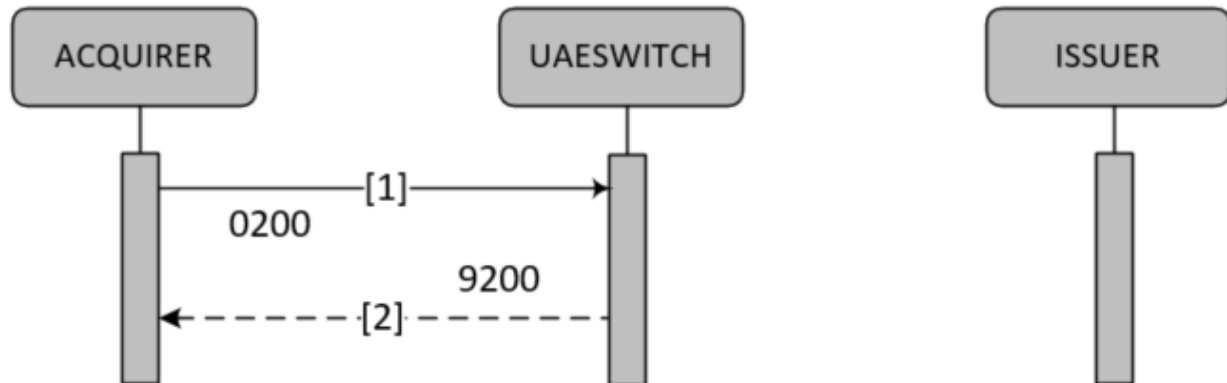
Issuer Reconciliation

1. UAESWITCH initiates Issuer reconciliation request (0500) to a MEMBER
2. MEMBER acknowledges with Issuer reconciliation response (0510 response) to UAESWITCH

4.9 9-Series Message

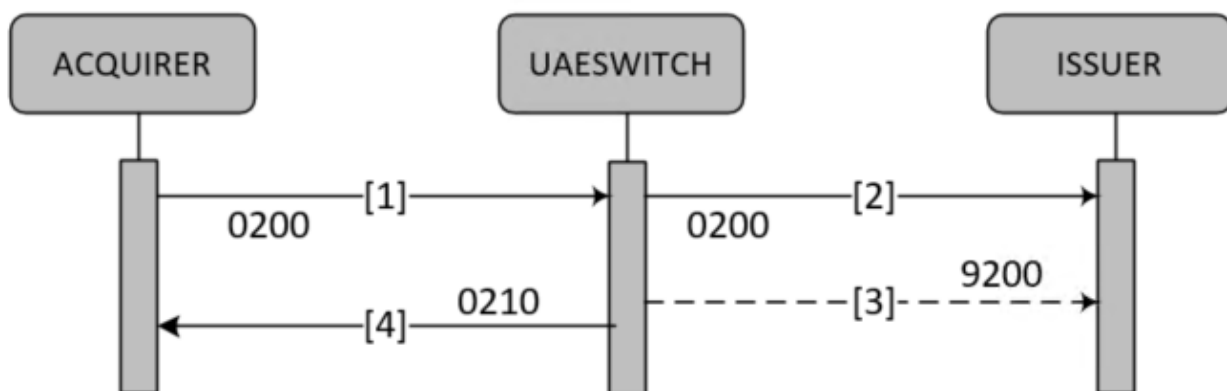
This section describes the processing of 9-series messages resulting from message format errors in messages from a bank to the UAESWITCH or from the UAESWITCH to a bank.

4.9.1 9200 ATM Balance Inquiry Transaction from Acquirer



1. ACQUIRER bank forwards a balance enquiry request to UAESWITCH with DE 4 populated with nonzero value
2. UAESWITCH rejects the balance enquiry request with a 9200 message indicating field in error as DE4

4.9.2 9210 ATM Balance Inquiry Transaction Response from Issuer



1. ACQUIRER bank forwards a balance enquiry request to UAESWITCH with DE 4 populated with zero value
2. UAESWITCH forwards the balance enquiry request to the ISSUER
3. ISSUER acknowledges 0210 response without DE39
4. UAESWITCH rejects the 0210 response with a 9210 message to the ISSUER
5. UAESWITCH acknowledges 0210 to the ACQUIRER with DE39 as '68'

4.10 EMV Transactions

An EMV terminal (ATM/POS) shall always attempt to process the transaction using the chip if the chip is present and readable. “Fallback” means that the EMV Terminal is unable to complete processing the transaction using the chip, and so uses magnetic stripe processing to provide a service to the cardholder. The EMV terminal should attempt to re-try accessing the chip a number of times (minimum three) prior to falling back. If feasible, the EMV Terminal should attempt to restage the card in the chip reading station, or retract and re-land the chip contacts in order to complete the transaction.

Fallback to magnetic stripe circumvents the improved security offered by chip. Therefore, it is at the issuing bank’s discretion whether to approve or decline a chip card that has fallen back to magnetic stripe.

If both the Chip and the magnetic stripe are unreadable, the transaction should be declined and aborted.

UAESWITCH may send no value in ‘Issuer Authentication Data’ to the acquirer in DE-55 of 0110/0210/0230 in the form of ‘9100’.

5. Message Structure

UAESWITCH online messages are based on Bank Card Organizational Messages—Interchange Message Specifications—Content for Financial Transactions, International Organization for Standardization (ISO) 8583; 1987 (E).

System messages have four basic components, as shown below. The message structure is based on ISO 8583 standard as defined in the following table

Message Header	MTI	Bit Map Primary	Bit Map Secondary	Data Elements 2-64	Data Elements 65-128
----------------	-----	--------------------	----------------------	-----------------------	-------------------------

A message structure comprises of the following components:

Message Element	Description
Message Header	Contains the length of the message
MTI	Message Type Identifier. Specifies general category of message
Bit Map	Specifies which data elements are present Primary: presence of Data elements between 2 and 64 Secondary: presence of Data elements between 65 and 128
Data Elements	Detailed data elements 2-64: Data elements between 2 and 64 65-128: Data elements between 65 and 128

5.1 Message Header

Message header consists of 2 bytes binary value which contains the length of message including the header length.

The UAESWITCH message header is provided to enhance the routing and error determination capabilities of the UAESWITCH network. The fields in the UAESWITCH message header are:

- The Application Message Protocol field specifies which protocol version the following message uses.
- The Network Product Indicator and Network Version Number will be used to allow an orderly migration between versions of the UAESWITCH system software, and to aid member banks in their migration to new versions.
- The UAESWITCH and member banks will use the Field in Error field, which detect message format errors to identify to the sender the field, which is in error.
- The Acquirer Type and Issuer Type fields are reserved for future use.

5.1.1 Message Header ATM Transaction Set

Position	Field Name	Length	Allowable values
1-12	Application Message Protocol	12	ISO8583-1987
13-14	Network Product Indicator	2	00 - ATM
15-16	Network Version Number	2	10
17-19	Field in Error	3	Numeric, in the range 000 to 128 and 999.
20	Acquirer Type	1	0
21	Issuer Type	1	0

5.1.2 Message Header POS Transaction Set

Position	Field Name	Length	Allowable values
1-12	Application Message Protocol	12	ISO8583-1987
13-14	Network Product Indicator	2	01 – POS/ECOM
15-16	Network Version Number	2	10
17-19	Field in Error	3	Numeric, in the range 000 to 128 and 999.
20	Acquirer Type	1	0
21	Issuer Type	1	0

5.2 Message Type Identifier

The Message Type Identifier consists of four (4) digits whose each digit starting from the left indicates - ISO 8583 version, the message class, the message function, and the message origin.

Position 1- Version Number

MTI	Signifies	CBUAE Implementation
0XXX	ISO 8583:1987 Version	Yes
1XXX	ISO 8583:1993 Version	No
2XXX	ISO 8583-1:2003 Version	No

Position 2 – Message Class

MTI	Signifies	CBUAE Implementation
01XX	Authorization Message	Yes
02XX	Financial Transaction Message	Yes
03XX	Issuer File update Message	Yes
04XX	Reversal Message	Yes
05XX	Reconciliation messages	Yes
06XX	Administration Message	Yes
08XX	Network Management messages	Yes
9XXX*	9 Series to indicate format errors	Yes

*Proprietary to UAESWITCH

Position 3 – Message Function

MTI	Signifies	CBUAE Implementation
XX00	Request	Yes
XX10	Request Response	Yes
XX20	Advice	Yes
XX30	Advice Response	Yes

Position 4 – Message Source

MTI	Signifies	CBUAE Implementation
XXX0	Acquirer	Yes
XXX1	Acquirer repeat	Yes
XXX2	Issuer	Yes
XXX3	Issuer repeat	Yes

Following are the valid message type identifiers

Msg Type	Message Type Definition
0100	Authorization request
0110	Authorization response
0200	Financial request
0210	Financial response
0220	Financial advice request
0230	Financial advice response
0302	Issuer file update request
0312	Issuer file update response
0400	Reversal request

0401	Reversal Repeat
0410	Reversal response
0420	Reversal advice request
0421	Reversal Advice Repeat
0430	Reversal advice response
0500	Acquirer Reconciliation request
0501	Acquirer Reconciliation repeat
0510	Acquirer Reconciliation response
0502	Card Issuer Reconciliation request
0503	Card Issuer Reconciliation repeat
0512	Card Issuer Reconciliation response
0620	Administrative Message Request
0630	Administrative Message Response
0800	Network Management request
0801	Network Management repeat
0810	Network Management response
9XXX	Format Errors 9100/9110 9200/9210 9302/9312 9400/9401/9410 9420/9430 9500/9501/9510 9502/9503/9512 9602/9612 9800/9801/9810

5.3 Bitmap

Within an ISO 8583 message, a bitmap is a field or subfield that indicates which data elements may be present in a message. The message text segment of all messages transmitted through Central Switch is of variable length. For this segment, bit maps specify the fields that are present and those that are missing.

The valid combinations of the bit maps are:

- Primary bitmap
- Primary and secondary bitmap

Primary Bitmap

Each message includes the primary bitmap. It is a control field consisting of 64 bits (8 bytes) located after the message type identifier. Except for the first bit, each bit in the bitmap relates to the corresponding data field (fields 2–64) in the message. The value in the bit indicates whether the data field is present in the message:

- If a bit is 0, the field related to that bit is not present in the message
- If a bit is 1, the field related to that bit is present in the message.

Data field number 1 does not exist. The first bit of the primary map is used to indicate if another bitmap called the second bitmap (see the next section) immediately follows this primary one.

Secondary Bitmap

The first bit of the first bitmap indicates the presence or absence of a second map called the second bitmap. Like the primary map, the secondary map is a control field consisting of 64 bits (8 bytes). It can be considered an extension of the primary map because it is associated with fields 66 through 128. Data field 65 does not exist. This position, like that of field 1 in the primary map, is used to indicate the presence of another bitmap. A 1 in this position indicates the presence of a third bitmap.

The second bitmap is present only when the message contains information in any field from 66 through 128. When present, the secondary map immediately follows the primary bitmap and precedes the data fields.

5.4 Data Elements

Data elements are fields carrying the information of the transaction itself. Each Data element has a specified meaning and format. The detailed description of the data elements is described in the next chapter.

For example: Bit value 2 is assigned to Primary Account Number, 3 is assigned to Processing Code, 4 is for Transaction Amount similarly bit value 128 is for message authentication code field and so on. For each data element there is specific data format, size, constraints and description, which are been mentioned in below

Section 7 (Detailed Description of Data Elements) Cover all the data elements

6. Message Formats

Please review Appendix 13.2/13.3 for list of all Abbreviations used in the message formats

6.1 ATM Financial Transaction Request/ Response

Financial Transaction Request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/ 0200		0110/ 0210	
ISO	Primary Bit Map		M	M	M	M
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	
7	Date Time, Transmission	N10(MMDDHHMMSS)	M	→	M	→
10	Conversion rate, card holder billing	N8		C10	C10	
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	M	→	M	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Type (Category Code)	N4	M	→	O	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
23	Card Sequence No	N3	C23	→	C23	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
35	Track II Data	Z..37(LLVAR)	C35	→		
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6			C38	→
39	Response Code	AN2			M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→

Financial Transaction Request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	M	→
49	Transaction Currency Code	AN3	M	→	M	→
51	Cardholder Billing Currency Code	N3		C51	C51	
52	PIN Data	AN16	M	→		
53	Security Related Control Information	N16	M	→		
55	ICC System Related Data	B..255(LLVAR)	C55	→	C55	→
57	EMV System Related Data	N6	C57	→	C57	→
100	Receiving Institution ID	N..11(LLVAR)			O	→
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		M	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		M	→	
105 Tag 21	Wallet Provider ID	ANS32		M	→	
122	Remaining Open To Use	AN..25(LLVAR)			C122	→

6.2 ATM Reversal Request/ Response

Reversal request and Response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
	Message Type identifier		0400		0410	
	Primary Bit Map		M	M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	
7	Date Time, Transmission	N10(MMDDHHMMSS)	M	→	M	→
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	M	→	O	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Category Code	N4	M	→	M	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
25	POS Condition Code	N2+C25	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6	M	→	M	→
39	Response Code	AN2	M	→	M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	O	→

UAESWITCH Interface Technical Specifications

Reversal request and Response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
49	Transaction Currency Code	AN3	M	→	M	→
51	Cardholder Billing Currency Code	N3		C51	C51	
90	Original Data Elements	N42	M	→	M	→
95	Replacement Amounts	N42	C95	→	M	→
105	Token Data	ANS..999(LLLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		M	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		M	→	
105 Tag 21	Wallet Provider ID	ANS32		M	→	

6.3 ATM & POS Reconciliation Request/ Response

Reconciliation message request and Response						
Field	Data Element	Data Type	Transmission Requirement			
			SW		IS	
	Message Type identifier		0500/0501 0502/0503		0510 0512	
	Primary Bit Map		M		M	
	Secondary Bit Map					
7	Date Time, Transmission	N10(MMDDHHMMSS)	M		M	
11	Systems Trace Number	N6	M		M	
15	Date, Settlement	N4(MMDD)	M		M	
37	Retrieval Ref. No.	AN12	M		M	
50	Currency Code, Settlement	N3	M		M	
66	Settlement Code	N1			M	
74	Credits Number	N TLV (Max 999 bytes)	M		C66	
75	Credits Reversal Number	N TLV (Max 999 bytes)	M		C66	

UAESWITCH Interface Technical Specifications

Reconciliation message request and Response						
Field	Data Element	Data Type	Transmission Requirement			
			SW		IS	
76	Debits Number	N TLV (Max 999 bytes)	M		C66	
77	Debits Reversal Number	N TLV (Max 999 bytes)	M		C66	
80	Inquires Number	N TLV (Max 999 bytes)	M		C66	
86	Credits Amount	N TLV (Max 999 bytes)	M		C66	
87	Credits Reversal Amount	N TLV (Max 999 bytes)	M		C66	
88	Debits Amount	N TLV (Max 999 bytes)	M		C66	
89	Debits Reversal Amount	N TLV (Max 999 bytes)	M		C66	
97	Amount, Net Settlement	X+N 16	M		M	
99	Settlement Institution Identification Code	N..11(LLVAR)	M		M	

6.4 Network Management

Network Management request and Response						
Field	Data Element	Data Type	Transmission Requirement			
			SW		ISD	
	Message Type identifier		0800/0801		0810	
	Primary Bit Map		M		M	
	Secondary Bit Map					
7	Date Time, Transmission	N10(MMDDHHMMSS)	M		M	
11	Systems Trace Number	N6	M		M	
15	Date, Settlement	N4(MMDD)	C15		C15	
37	Retrieval Ref. No.	AN12	M		M	
39	Response Code	AN2			M	
47	Additional Data National	ANS TLV	C47			
70	Network Management Information code	N3	M		M	

6.5 POS Purchase Request / Response

The Cardholder asks for approval from the Issuer when purchasing goods or services.

POS Purchase transaction request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/0200		0110/0210	
ISO	Primary Bit Map		M	M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	C6
7	Date Time, Transmission	N10(MMDDH HMMSS)	M	→	M	→
10	Conversion rate, card holder billing	N8		C6	C6	
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	M	→	M	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
16	Date, Conversion	N4(MMDD)		C16	C16	
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Category Code	N4	M	→	M	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
23	Card Sequence No	N3	C23	→	C23	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
33	Forwarding Institution ID	N..11(LLVAR)	M	→	M	→
35	Track II Data	Z..37(LLVAR)	C35	→		
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6			C38	→
39	Response Code	AN2			M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	M	→
44	Additional Response Data	AN15			C44	C44
48	POS retailer Data	AN..27(LLVAR)	M	→	M	→
49	Transaction Currency Code	N3	M	→	M	→

POS Purchase transaction request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/0200		0110/0210	
51	Currency Code, Cardholder billing	N3		C51	C51	C51
52	PIN Data	AN16	C52	→		
53	Security Related Control Information	N16	C53	→		
54	Additional Amounts	AN...20	C54	→	C54	→
55	ICC System Related Data	B..255 (LLVAR)	C55	→	C55	→
57	EMV Data Element 2	N6	C57	→	C57	→
60	Additional Data	AN..16(LLVAR)	M	→	M	→
61	POS terminal data	AN..255(LLVAR)	M	→	M	→
63	Network Data	ANS..255(LLVAR)				
063 Tag 02	Transaction Identifier	AN15		C063	→	→
063 Tag 03	Token PAR	ANS29				C063
100	Receiving Institution ID	N..11(LLVAR)			M	→
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		M	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		M	→	
105 Tag 21	Wallet Provider ID	ANS32		M	→	

Please review the following sections

- 12.4 Purchase
- 12.7 Partial Authorization
- 12.8 Purchase with Cashback
- 12.13 Tokenization

6.6 POS Pre-authorization Request / Response

Pre-authorization transaction is used by the acquirer to confirm the issuer's approval of the cardholder transaction. Pre-authorization transaction only controls the cardholder's available balance. Funds settlement will be accomplished by pre-authorization completion transaction. An approved pre-authorization transaction is only valid within a specified timeframe.

POS Pre Authorization request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100		0110	
ISO	Primary Bit Map		M	M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	C6
7	Date Time, Transmission	N10(MMDDHHMMSS)	M	→	M	→
10	Conversion rate, card holder billing	N8		C10	C10	
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YMM)	M	→	M	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
16	Date, Conversion	N4(MMDD)		C16	C16	
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Category Code	N4	M	→	M	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
23	Card Sequence No	N3	C23	→	C23	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
33	Forwarding Institution ID	N..11(LLVAR)	M	→	M	→
35	Track II Data	Z..37(LLVAR)	C35	→		
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6			C38	→
39	Response Code	AN2			M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	M	→
44	Additional Response Data	AN15			C44	C44
48	POS retailer Data	AN..27(LLVAR)	M	→	M	→
49	Transaction Currency Code	N3	M	→	M	→

POS Pre Authorization request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100		0110	
51	Currency Code, Cardholder billing	N3		C51	C51	C51
52	PIN Data	AN16	C52	→		
53	Security Related Control Information	N16	C53	→		
55	ICC System Related Data	B..255(LLVAR)	C55	→	C55	→
57	EMV Data Element 2	N6	C57	→	C57	→
60	Additional Data	AN..16(LLVAR)	M	→	M	→
61	POS terminal data	AN..255(LLVAR)	M	→	M	→
63	Network Data	ANS..255(LLVAR)				
063 Tag 01	Preauthorization Time Limit	AN4			C063	→
063 Tag 02	Transaction Identifier	AN15		C063	→	→
063 Tag 03	Token PAR	ANS29				C063
100	Receiving Institution ID	N..11(LLVAR)			M	→
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		M	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		M	→	
105 Tag 21	Wallet Provider Id	ANS32		M	→	

Please review section 12.5. Pre-Authorization & Pre-Authorization Completion

6.7 Incremental Pre Authorization Request/Response

An Incremental Authorization can be used to increase the total amount authorized for a transaction if the amount of the estimate or initial authorization (pre-authorization) is insufficient. An Incremental Authorization request can also be based on a revised estimate of what the cardholder might spend.

In Incremental Pre-authorization request should attempt to mirror the values of DE-2, DE-3, DE-11, DE-32, DE-37 and DE63.2 sent in the original pre-authorization message.

Incremental Pre-authorization request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100		0110	
ISO	Primary Bit Map		M	M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	C6
7	Date Time, Transmission	N10(MMDDHHMMS S)	M	→	M	→
10	Conversion rate, card holder billing	N8		C6	C6	
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	M	→	M	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
16	Date, Conversion	N4(MMDD)		C16	C16	
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Category Code	N4	M	→	M	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
23	Card Sequence No	N3	C23	→	C23	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
33	Forwarding Institution ID	N..11(LLVAR)	M	→	M	→
35	Track II Data	Z..37(LLVAR)	C35	→		
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6			C38	→
39	Response Code	AN2			M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	M	→
44	Additional Response Data	AN15			C44	C44

Incremental Pre-authorization request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100		0110	
48	POS retailer Data	AN..27(LLVAR)	M	→	M	→
49	Transaction Currency Code	N3	M	→	M	→
51	Currency Code, Cardholder billing	N3		C51	C51	C51
52	PIN Data	AN16	C52	→		
53	Security Related Control Information	N16	C53	→		
55	ICC System Related Data	B..255(LLVAR)	C55	→	C55	→
57	EMV Data Element 2	N6	C57	→	C57	→
60	Additional Data	AN..16(LLVAR)	M	→	M	→
61	POS terminal data	AN..255(LLVAR)	M	→	M	→
63	Network Data	ANS..255(LLVAR)				
063 Tag 01	Preauthorization Time Limit	AN4			C063	→
063 Tag 02	Transaction Identifier	AN15	C063	C063	→	→
063 Tag 03	Token PAR	ANS29				C063
100	Receiving Institution ID	N..11(LLVAR)			M	→
104	Additional Data – Payment Services	ANS..999(LLLVAR)				
104 Tag 07	Token Cryptogram	ANS..28	C104			
104 Tag 09	Payment Facilitator ID	AN11	C104	C104	→	→
105	Token Data	ANS..999(LLLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		C105	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		C105	→	
105 Tag 21	Wallet Provider Id	ANS32		M	→	
105 Tag 26	Merchant ID	ANS36		C105	→	
105 Tag 27	Merchant Name	ANS15		C105	→	
105 Tag 28	TR Name	ANS45		C105	→	

Please review section 12.5. Pre-Authorization & Pre-Authorization Completion

6.8 POS Pre-authorization Completion

For the approved pre-authorization transaction, the pre-authorization completion (request) is used to complete the payment and settlement of the transaction.

Acquirers may send pre-authorization completion in the existing online SMS(0220) message for POS transactions only if the Issuer Acceptance Capability in the BIN file is marked as 'S'. However, if the indicator is 'D' or for any eCommerce transactions, the pre-authorization completion must be processed through the clearing file.

POS Preauthorization Completion request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0220		0230	
ISO	Primary Bit Map		M	M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	C6
7	Date Time, Transmission	N10(MMDDHHMMS S)	M	→	M	→
10	Conversion rate, card holder billing	N8		C6	C6	
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	M	→	M	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
16	Date, Conversion	N4(MMDD)		C16	C16	
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Category Code	N4	M	→	M	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
23	Card Sequence No	N3	C23	→	C23	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
33	Forwarding Institution ID	N..11(LLVAR)	M	→	M	→
35	Track II Data	Z..37(LLVAR)	C35	→		
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6	M	→	M	→
39	Response Code	AN2			M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	M	→

POS Preauthorization Completion request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0220		0230	
44	Additional Response Data	AN15				
48	POS retailer Data	AN..27(LLVAR)	M	→	M	→
49	Transaction Currency Code	N3	M	→	M	→
51	Currency Code, Cardholder billing	N3		C51	C51	C5 1
55	ICC System Related Data	B..255(LLVAR)		C55		C5 5
57	EMV Data Element 2	N6	C57	→	C57	→
60	Additional Data	AN..16(LLVAR)	M	→	M	→
61	POS terminal data	AN..255(LLVAR)	M	→	M	→
63	Network Data	ANS..255(LLVAR)				
063 Tag 01	Preauthorization Time Limit	AN4			C063	→
063 Tag 02	Transaction Identifier	AN15		C063	→	→
063 Tag 03	Token PAR	ANS29				C06 3
100	Receiving Institution ID	N..11(LLVAR)			M	→
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		M	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		M	→	
105 Tag 21	Wallet Provider Id	ANS32		M	→	

Please review section 12.5. Pre-Authorization & Pre-Authorization Completion

6.9 Ecommerce Request/Response

The following table describes Ecommerce messages handles at Acquirer and Issuer. We need to identify the type of Ecommerce transaction (CIT/MIT) based on DE-22, DE-25, DE-61 and DE-104.

Ecommerce request and response							
Field	Data Element	Data Type		Transmission Requirement			
				AQ	SW	IS	SW
ISO	Message Type identifier			0100		0110	
ISO	Primary Bit Map			M	M	M	M
	Secondary Bit Map						
2	Primary Account. Number.	N..19(LLVAR)		M	→	M	→
3	Processing Code	N6		M	→	M	→
4	Amount, Transaction	N12		M	→	M	→
6	Amount, Cardholder Billing	N12			C6	C6	C6
7	Date Time, Transmission	N10(MMDDHHMMSS)		M	→	M	→
10	Conversion rate, card holder billing	N8			C6	C6	
11	Systems Trace Number	N6		M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)		M	→	M	→
13	Date, Local Transaction	N4(MMDD)		M	→	M	→
14	Date, Expiration	N4(YYMM)		C14	→	C14	→
15	Date, Settlement	N4(MMDD)		M	→	M	→
16	Date, Conversion	N4(MMDD)			C16	C16	
17	Date, Capture	N4(MMDD)		M	→	M	→
18	Merchant Category Code	N4		M	→	M	→
19	Acquiring Country Code	N3		M	→	M	→
22	POS Entry Mode	N3		M	→	M	→
25	POS Condition Code	N2		M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)		M	→	M	→
33	Forwarding Institution ID	N..11(LLVAR)		M	→	M	→
37	Retrieval Ref. No.	AN12		M	→	M	→
38	Authorization Id Response	AN6				C38	→
39	Response Code	AN2				M	→
41	Card Acceptor, Terminal Id	AN8		M	→	M	→
42	Card Acceptor. Id Code	AN15		M	→	M	→
43	Card Acceptor Acquirer Name	AN40		M	→	M	→
44	Additional Response Data	AN15				C44	C44
48	POS retailer Data	AN..27(LLVAR)		M	→	M	→
49	Transaction Currency Code		N3	M	→	M	→

Ecommerce request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100		0110	
51	Currency Code, Cardholder billing	N3		C51	C51	C51
54	Additional Amounts	AN...20	C54	→	C54	→
55	ICC System Related Data	B..255(LLVAR)	C55	-		
60	Additional Data	AN..16(LLVAR)	M	→	M	→
61	POS terminal data	AN..255(LLVAR)	M	→	M	→
63	Network Data	ANS..255(LLVAR)				
063 Tag 01	Preauthorization Time Limit	AN4			C063	→
063 Tag 02	Transaction Identifier	AN15		C063	→	→
063 Tag 03	Token PAR	ANS29				C063
100	Receiving Institution ID	N..11(LLVAR)			M	→
104	Additional Data – Payment Services	ANS..999 (LLLVAR)				
104 Tag 01	CVD2	N3	C104	→		
104 Tag 02	CVD2 result code	A1			C104	→
104 Tag 03	ECOM Indicator	N2	C104	→		
104 Tag 04	CAVV Data	ANS..99	C104	→		
104 Tag 05	CAVV Result	A1		C104	C104	→
104 Tag 07	Token Cryptogram	ANS..28	C104			
104 Tag 09	Payment Facilitator ID	AN11	C104	C104	→	→
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		C105	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		C105	→	
105 Tag 21	Wallet Provider Id	ANS32		M	→	
105 Tag 26	Merchant ID	ANS36		C105	→	
105 Tag 27	Merchant Name	ANS15		C105	→	
105 Tag 28	TR Name	ANS45		C105	→	

UAESWITCH Interface Technical Specifications

Please review the following sections

- 12.13 Tokenized transaction
- 12.14 Ecommerce transaction

6.10 MOTO Transaction Request / Response

This is Manual transaction initiated by merchant by entering card manually on the terminal. Only DE-22 will be '01', DE-25 will be '08' and DE-61.4=2/3 for this transaction.

MOTO Transaction Request and Response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/0200		0110/0210	
ISO	Primary Bit Map		M	M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	C6
7	Date Time, Transmission	N10 (MMDDHHMMS S)	M	→	M	→
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	C14	→	C14	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
16	Date, Conversion	N4(MMDD)		C16	C16	
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Category Code	N4	M	→	M	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
33	Forwarding Institution ID	N..11(LLVAR)	M	→	M	→
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6			C38	→
39	Response Code	AN2			M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→

MOTO Transaction Request and Response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/0200		0110/0210	
43	Card Acceptor Acquirer Name	AN40	M	→	M	→
44	Additional Response Data	AN15			C44	C44
48	POS retailer Data	AN..27(LLVAR)	M	→	M	→
49	Transaction Currency Code	N3	M	→	M	→
51	Currency Code, Cardholder billing	N3		C51	C51	C51
54	Additional Amounts	AN...20	C54	→	C54	→
60	Additional Data	AN..16(LLVAR)	M	→	M	→
61	POS terminal data	AN..255(LLVAR)	M	→	M	→
63	Network Data	ANS..255(LLVAR)				
063 Tag 02	Transaction Identifier	AN15		C063	→	→
100	Receiving Institution ID	N..11(LLVAR)			M	→
104	Additional Data – Payment Services	ANS..999 (LLLVAR)				
104 Tag 01	CVD2	N3	C104	→		
104 Tag 02	CVD2 result code	A1			C104	→
104 Tag 09	Payment Facilitator ID	AN11	C104	C104	→	→

Note: - In this transaction we will not expecting token data from acquirer as this is a manual entry transaction.

Please review the following section

- 12.15 MOTO Transactions

6.11 Recurring Transaction Request/Response

Recurring/Subscription (SI) transactions are automated payments made at regular intervals for ongoing services or subscriptions. These transactions occur in both e-commerce and point-of-sale (POS) platforms, enabling businesses to charge customers for recurring services like memberships, subscriptions, or installment plans.

Recurring transaction request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/ 0200		0110/ 0210	
ISO	Primary Bit Map		M	M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	C6
7	Date Time, Transmission	N10(MMDDHHMMS S)	M	→	M	→
10	Conversion rate, card holder billing	N8		C6	C6	
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	C14	→	C14	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
16	Date, Conversion	N4(MMDD)		C16	C16	
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Category Code	N4	M	→	M	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
33	Forwarding Institution ID	N..11(LLVAR)	M	→	M	→
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6	O	→	C38	→
39	Response Code	AN2			M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	M	→
48	POS retailer Data	AN..27(LLVAR)	M	→	M	→

Recurring transaction request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/ 0200		0110/ 0210	
49	Transaction Currency Code	N3	M	→	M	→
51	Currency Code, Cardholder billing	N3		C51	C51	C5 1
60	Additional Data	AN..16(LLVAR)	M	→	M	→
61	POS terminal data	AN..255(LLVAR)	M	→	M	→
63	Network Data	ANS..255(LLVAR)				
063 Tag 02	Transaction Identifier	AN15	C063	C063	→	→
063 Tag 03	Token PAR	ANS29				C06 3
100	Receiving Institution ID	N..11(LLVAR)			M	→
104	Additional Data – Payment Services	ANS..999 (LLLVAR)				
104 Tag 01	CVD2	N3	C104	→		
104 Tag 02	CVD2 result code	A1			C104	→
104 Tag 03	ECOM Indicator	N2	C104	→		
104 Tag 06	Original Transaction ID	AN15	C104	→		
104 Tag 07	Token Cryptogram	ANS..28	C104			
104 Tag 09	Payment Facilitator ID	AN11	C104	C104	→	→
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		C105	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		C105	→	
105 Tag 21	Wallet Provider Id	ANS32		M	→	
105 Tag 26	Merchant ID	ANS36		C105	→	
105 Tag 27	Merchant Name	ANS15		C105	→	
105 Tag 28	TR Name	ANS45		C105	→	

Please review the following section

- 12.12 MIT/Recurring Transactions

6.12 Refund Request/Response

Refund is a financial transaction that instructs the issuer to credit the cardholders account for the return of goods, tickets etc. Refund amount should be less than or equal to the amount of original purchase.

Refund request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/ 0200		0110/ 0210	
ISO	Primary Bit Map		M	M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	C6
7	Date Time, Transmission	N10(MMDDHHMMS S)	M	→	M	→
10	Conversion rate, card holder billing	N8		C6	C6	
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	C14	→	C14	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
16	Date, Conversion	N4(MMDD)		C16	C16	
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Category Code	N4	M	→	M	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
23	Card Sequence No	N3	C23	→	C23	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
33	Forwarding Institution ID	N..11(LLVAR)	M	→	M	→
35	Track II Data	Z..37(LLVAR)	C35	→		
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6	O	→	C38	→
39	Response Code	AN2			M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	M	→
44	Additional Response Data	AN15			C44	C4 4
48	POS retailer Data	AN..27(LLVAR)	M	→	M	→

Refund request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/ 0200		0110/ 0210	
49	Transaction Currency Code	N3	M	→	M	→
51	Currency Code, Cardholder billing	N3		C51	C51	C5 1
52	PIN Data	AN16	C52	→		
53	Security Related Control Information	N16	C53	→		
55	ICC System Related Data	B..255(LLVAR)	C55	→	C55	→
57	EMV Data Element 2	N6	C57	→	C57	→
60	Additional Data	AN..16(LLVAR)	M	→	M	→
61	POS terminal data	AN..255(LLVAR)	M	→	M	→
63	Network Data	ANS..255(LLVAR)				
063 Tag 01	Preauthorization Time Limit	AN4			C063	→
063 Tag 02	Transaction Identifier	AN15	C063	C063	→	→
063 Tag 03	Token PAR	ANS29				C06 3
100	Receiving Institution ID	N..11(LLVAR)			M	→
104	Additional Data – Payment Services	ANS..999 (LLLVAR)				
104 Tag 01	CVD2	N3	C104	→		
104 Tag 02	CVD2 result code	A1			C104	→
104 Tag 03	ECOM Indicator	N2	C104	→		
104 Tag 03	ECOM Indicator	N2	C104	→		
104 Tag 04	CAVV Data	ANS..99	C104	→		
104 Tag 05	CAVV Result	A1		C104	C104	→
104 Tag 06	Original Transaction ID	AN15	C104	→		
104 Tag 07	Token Cryptogram	ANS..28	C104			
104 Tag 09	Payment Facilitator ID	AN11	C104	C104	→	→
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		C105	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		C105	→	

Refund request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/ 0200		0110/ 0210	
105 Tag 21	Wallet Provider Id	ANS32		M	→	
105 Tag 26	Merchant ID	ANS36		C105	→	
105 Tag 27	Merchant Name	ANS15		C105	→	
105 Tag 28	TR Name	ANS45		C105	→	

Please review section 12.6. Refund

6.13 Void/Cancel/Reversal Transaction Request/Response

Transactions that generate reversal advice include:

- pre-authorization, pre-authorization completion (request)
- purchase, sale
- Refunds
- ECOM (CIT/MIT)

Void/Cancel/Reversal – request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0400/ 0420/ 0401/ 0421		0410 0430	
ISO	Primary Bit Map		M	M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	C6
7	Date Time, Transmission	N10(MMDDHHMMSS)	M	→	M	→
10	Conversion rate, card holder billing	N8		C6	C6	
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	C14	→	C14	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
16	Date, Conversion	N4(MMDD)		C16	C16	

UAESWITCH Interface Technical Specifications

Void/Cancel/Reversal – request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0400/ 0420/ 0401/ 0421		0410 0430	
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Category Code	N4	M	→	M	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
23	Card Sequence No	N3	C23	→	C23	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
33	Forwarding Institution ID	N..11(LLVAR)	M	→	M	→
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6	O	→	O	→
39	Response Code	AN2	M	→	M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	M	→
44	Additional Response Data	AN15			C44	C44
48	POS retailer Data	AN..27(LLVAR)	M	→	M	→
49	Transaction Currency Code	N3	M	→	M	→
51	Currency Code, Cardholder billing	N3		C51	C51	C51
52	PIN Data	AN16				
53	Security Related Control Information	N16				
54	Additional Amounts	AN...20	C54	→	C54	→
55	ICC System Related Data	B..255(LLVAR)				
57	EMV Data Element 2	N6				
60	Additional Data	AN..16(LLVAR)	M	→	M	→
61	POS terminal data	AN..255(LLVAR)	M	→	M	→
63	Network Data	ANS..255(LLVAR)				
063 Tag 02	Transaction Identifier	AN15		C063	→	→
90	Original Data Element	N42	M	→	M	→
100	Receiving Institution ID	N..11(LLVAR)			M	→
104	Token Data	ANS..999(LLVAR)				
104 Tag 09	Payment Facilitator ID	AN11	C104	→	→	→
105	Token Data	ANS..999(LLVAR)				

Void/Cancel/Reversal – request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0400/ 0420/ 0401/ 0421		0410 0430	
105 Tag 01	Token ID	AN19		M		
105 Tag 02	Token Expiration Date	N4		M		
105 Tag 03	Token Reference ID	ANS36		M		
105 Tag 04	Wallet ID	ANS..99		C105		
105 Tag 05	Token Type	AN2		M		
105 Tag 06	Token Status	AN1		M		
105 Tag 07	Payment Account Reference (PAR)	ANS29		M		
105 Tag 08	Token Requestor ID	ANS11		M		
105 Tag 09	TSP Validation Result	AN2		M		
105 Tag 10	Device Type	AN2		C105		
105 Tag 21	Wallet Provider Id	ANS32		M		
105 Tag 26	Merchant ID	ANS36		C105		
105 Tag 27	Merchant Name	ANS15		C105		
105 Tag 28	TR Name	ANS45		C105		

6.14 Account Verification

In Account verification for token provisioning transaction below data elements are mandatory to check.

In this transaction DE-25 should be '51' and CVV2 must be present.

Account Verification Request and Response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/0200	→	0110/0210	→
ISO	Primary Bit Map		M		M	M
	Secondary Bit Map				M	M
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	C6
7	Date Time, Transmission	N10(MMDDHHM MSS)	M	→	M	→
10	Conversion rate, card holder billing	N8		C6	C6	
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→

UAESWITCH Interface Technical Specifications

Account Verification Request and Response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/0200	→	0110/0210	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	C14	→	C14	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Category Code	N4	M	→	M	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
33	Forwarding Institution ID	N..11(LLVAR)	M	→	M	→
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6			C38	→
39	Response Code	AN2			M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	M	→
44	Additional Response Data	AN15		→	C44	→
48	POS retailer Data	AN..27(LLVAR)	M	→	M	→
49	Transaction Currency Code	N3	M	→	M	→
51	Currency Code, Cardholder billing	N3		C51	C51	C51
55	ICC System Related Data	B..255(LLVAR)	C55			
60	Additional Data	AN..16(LLVAR)	M	→	M	→
61	POS terminal data	AN..255(LLVAR)	M	→	M	→
63	Network Data	ANS..255(LLVAR)				
063 Tag 02	Transaction Identifier	AN15		C063	→	→
063 Tag 03	Token PAR	ANS29				C063
100	Receiving Institution ID	N..11(LLVAR)			M	→
104	Additional Data – Payment Services	ANS..999 (LLLVAR)				
104 Tag 01	CVD2	N3	C104	→		
104 Tag 02	CVD2 result code	A1			C104	→

6.15 Wallet Based Token Provisioning Request / Response

In Account verification for wallet based token provisioning transaction below data elements are mandatory to check.

DE-25 should be '51'

MCC has to come as '6012'. And DE-105 for Token related data.

Wallet Based Token Provisioning request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier			0100/0200	0110/0210	
ISO	Primary Bit Map			M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)		M	M	
3	Processing Code	N6		M	M	
4	Amount, Transaction	N12		M	M	
7	Date Time, Transmission	N10(MMDDHHMMSS)		M	M	
11	Systems Trace Number	N6		M	M	
12	Time, Local Transaction	N6(HHMMSS)		M	M	
13	Date, Local Transaction	N4(MMDD)		M	M	
14	Date, Expiration	N4(YYMM)		C14	C14	
15	Date, Settlement	N4(MMDD)		M	→	
17	Date, Capture	N4(MMDD)		M	→	
18	Merchant Category Code	N4		M	M	
19	Acquiring Country Code	N3		M	M	
22	POS Entry Mode	N3		M	M	
25	POS Condition Code	N2		M	M	
32	Acquirer Institution ID	N..11(LLVAR)		M	M	
33	Forwarding Institution ID	N..11(LLVAR)		M	M	
37	Retrieval Ref. No.	AN12		M	M	
38	Authorization Id Response	AN6			C38	
39	Response Code	AN2			M	
41	Card Acceptor, Terminal Id	AN8		M	M	
42	Card Acceptor. Id Code	AN15		M	M	
43	Card Acceptor Acquirer Name	AN40		M	M	
49	Transaction Currency Code	N3		M	M	
61	POS terminal data	AN..255(LLVAR)		M	M	
100	Receiving Institution ID	N..11(LLVAR)			M	
104	Additional Data – Payment Services	ANS..999 (LLLVAR)				

UAESWITCH Interface Technical Specifications

Wallet Based Token Provisioning request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier			0100/0200	0110/0210	
104 Tag 01	CVD2	N3		C104		
104 Tag 02	CVD2 result code	A1			C104	
105	Token Data	ANS..999(LLLVAR)				
105 Tag 04	Wallet ID	ANS..99		M	M	
105 Tag 08	Token Requestor ID	ANS11		M	M	
105 Tag 10	Device Type	AN2		M	→	
105 Tag 16	User Account Score	N2		O		
105 Tag 17	Device Score	N2		O		
105 Tag 19	Device Location	ANS16		O	O	
105 Tag 21	Waller Provider Id	ANS32		M	M	
105 Tag 25	Issuer Card Ref ID	ANS36		M	M	
105 Tag 29	Masked Email	ANS64		O	O	
105 Tag 30	Provisioning Attempts on Device in 24 hours	N99		O	O	
105 Tag 31	Wallet Account Country	ANS2		M	M	
105 Tag 32	Card Holder Name	ANS99		M	M	
105 Tag 33	Level Of Trust	N2		M	M	
105 Tag 34	Reason Codes	AN2		O	O	
105 Tag 36	Device Country	AN2		M	M	
105 Tag 38	Wallet Score	N1		O	O	
105 Tag 39	Manufacturer	ANS32		O	O	
105 Tag 40	Model	ANS16		O	O	
105 Tag 41	OS Version	ANS16		O	O	
105 Tag 42	Phone number	N20		O	O	
105 Tag 43	IMEI	ANS24		O	O	
105 Tag 44	Platform	ANS32		O	O	
105 Tag 48	ID&V Method	ANS99			C105	
105 Tag 49	ID&V Values	ANS99			C105	
105 Tag 52	Pan Source	N2		M	M	
105 Tag 53	Card Art Indicator	AN15			O	
105 Tag 54	Level Of Trust Standard Version	ANS16		O	O	
105 Tag 55	Device Name	ANS..99		O	O	
105 Tag 56	Language	ANS3		O	O	
105 Tag 57	Tnc Status	N1		O	O	
105 Tag 58	Tnc Accepted Date	ANS64		O	O	

Please review the following section

- 12.13 Tokenization

6.16 Send OTP

Below message depicts the message for OTP send to Issuer for Token Provisioning.

Send OTP Request and Response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier			0100/0200	0110/0210	
ISO	Primary Bit Map			M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)		M	M	
3	Processing Code	N6		M	M	
4	Amount, Transaction	N12		M	M	
7	Date Time, Transmission	N10(MMDDHHMMSS)		M	M	
11	Systems Trace Number	N6		M	M	
12	Time, Local Transaction	N6(HHMMSS)		M	M	
13	Date, Local Transaction	N4(MMDD)		M	M	
15	Date, Settlement	N4(MMDD)		M	→	
17	Date, Capture	N4(MMDD)		M	→	
18	Merchant Category Code	N4		M	M	
19	Acquiring Country Code	N3		M	M	
22	POS Entry Mode	N3		M	M	
25	POS Condition Code	N2		M	M	
32	Acquirer Institution ID	N..11(LLVAR)		M	M	
33	Forwarding Institution ID	N..11(LLVAR)		M	M	
37	Retrieval Ref. No.	AN12		M	M	
38	Authorization Id Response	AN6			C38	
39	Response Code	AN2			M	
41	Card Acceptor, Terminal Id	AN8		M	M	
42	Card Acceptor. Id Code	AN15		M	M	
43	Card Acceptor Acquirer Name	AN40		M	M	
49	Transaction Currency Code	N3		M	M	
100	Receiving Institution ID	N..11(LLVAR)			M	
105	Token Data	ANS999(LLVAR)				
105 Tag 03	Token Reference ID	ANS36		M	M	
105 Tag 04	Wallet ID	ANS..99		M	M	
105 Tag 08	Token Requestor ID	ANS11		M	M	
105 Tag 10	Device Type	AN2		M	→	
105 Tag 45	OTP Value	N10		M		
105 Tag 46	OTP expiration Date	ANS99		M		
105 Tag 47	OTP Method ID	N2		M		

UAESWITCH Interface Technical Specifications

Please review the following section

- 12.13 Tokenization

6.17 COF Token Provisioning Request / Response

In Account verification for COF provisioning transaction below data elements are mandatory to check.

DE-25 should be '51'

MCC has to come as '6012'. And DE-105 for Token related data.

COF Token Provisioning request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier			0100/0200	0110/0210	
ISO	Primary Bit Map			M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)		M	M	
3	Processing Code	N6		M	M	
4	Amount, Transaction	N12		M	M	
7	Date Time, Transmission	N10(MMDDHHMMSS)		M	M	
11	Systems Trace Number	N6		M	M	
12	Time, Local Transaction	N6(HHMMSS)		M	M	
13	Date, Local Transaction	N4(MMDD)		M	M	
14	Date, Expiration	N4(YYMM)		C14	C14	
15	Date, Settlement	N4(MMDD)		M	→	
17	Date, Capture	N4(MMDD)		M	→	
18	Merchant Category Code	N4		M	M	
19	Acquiring Country Code	N3		M	M	
22	POS Entry Mode	N3		M	M	
25	POS Condition Code	N2		M	M	
32	Acquirer Institution ID	N..11(LLVAR)		M	M	
33	Forwarding Institution ID	N..11(LLVAR)		M	M	
37	Retrieval Ref. No.	AN12		M	M	
38	Authorization Id Response	AN6			C38	
39	Response Code	AN2			M	
41	Card Acceptor, Terminal Id	AN8		M	M	
42	Card Acceptor. Id Code	AN15		M	M	
43	Card Acceptor Acquirer Name	AN40		M	M	
49	Transaction Currency Code	N3		M	M	
61	POS terminal data	AN..255(LLVAR)		M	M	

COF Token Provisioning request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier			0100/0200	0110/0210	
100	Receiving Institution ID	N..11(LLVAR)			M	
104	Additional Data – Payment Services	ANS..999 (LLLVAR)				
104 Tag 01	CVD2	N3		M		
104 Tag 02	CVD2 result code	A1			M	
105	Token Data	ANS..999(LLVAR)				
105 Tag 08	Token Requestor ID	ANS11		M	M	
105 Tag 21	Waller Provider Id	ANS32		M	M	
105 Tag 25	Issuer Card Ref ID	ANS36		M	M	
105 Tag 26	Merchant ID	ANS36		M	M	
105 Tag 27	Merchant Name	ANS15		M	M	
105 Tag 28	TR Name	ANS45		M	M	
105 Tag 33	Level Of Trust	N2		M	M	
105 Tag 36	Device Country	AN2		M	M	
105 Tag 52	Pan Source	N2		M	M	

Please review the following section

- 12.13 Tokenization

6.18 Life Cycle Management

The Token completion and Event notifications will be triggered by Jaywan TSP to issuer on successful provisioning and also in case of any status change.

6.18.1 Life Cycle Management – Token Completion/Event Notification (Request and Response)						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier			0620	0630	
ISO	Primary Bit Map			M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)		M	M	→
7	Date Time, Transmission	N10(MMDDHHMMSS)		M	M	→
11	Systems Trace Number	N6		M	M	→
18	Merchant Category Code	N4		M	M	→
32	Acquirer Institution ID	N..11(LLVAR)		M	M	→
33	Forwarding Institution ID	N..11(LLVAR)		M	M	→
37	Retrieval Ref. No.	AN12		M	M	→
39	Response Code	AN2			M	→
42	Card Acceptor. Id Code	AN15		C	C	

6.18.1 Life Cycle Management – Token Completion/Event Notification (Request and Response)						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier			0620	0630	
43	Card Acceptor Acquirer Name	AN40		C	C	
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19		M	M	
105 Tag 02	Token Expiration Date	N4		M	M	
105 Tag 03	Token Reference ID	ANS36		M		
105 Tag 04	Wallet ID	ANS..99		M	M	
105 Tag 08	Token Requestor ID	ANS11		M		
105 Tag 10	Device Type	AN2		M	→	
105 Tag 21	Waller Provide Id	ANS32		M	M	
105 Tag 22	Token Advice Reason	N2		M		
105 Tag 23	Token Previous Status	N2		M		
105 Tag 24	Token Current Status	N2		M		
105 Tag 25	Issuer Card Ref ID	ANS36		M	M	
105 Tag 26	Merchant ID	ANS15		C105		
105 Tag 27	Merchant Name	ANS45		C105		
105 Tag 28	TR Name	ANS45		C105		

Whenever there is any change in the card status, renewal or replacement, issuers are required to perform real time updates to Jaywan TSP to ensure that the token status is accurately reflected both in the Jaywan TSP and the OEM Pay wallet.

6.18.2 Life Cycle Management- Token status update Initiated from Issuer (request and response)						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier				0302	0312
ISO	Primary Bit Map				M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)			M	M
7	Date Time, Transmission	N10(MMDDHHMMSS)			M	M
11	Systems Trace Number	N6			M	M
18	Merchant Category Code	N4			M	M
32	Acquirer Institution ID	N..11(LLVAR)			M	M
37	Retrieval Ref. No.	AN12			M	M
39	Response Code	AN2				M

6.18.2 Life Cycle Management- Token status update Initiated from Issuer (request and response)

Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier				0302	0312
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19			M	M
105 Tag 02	Token Expiration date	N4			C105	
105 Tag 03	Token Reference ID	ANS36			M	
105 Tag 22	Token Advice Reason	N2			C105	
105 Tag 23	Token Previous Status	N2			C105	
105 Tag 24	Token Current Status	N2			C105	
105 Tag 50	Replacement PAN	AN19			C105	
105 Tag 51	Replacement Expiry Date	N4			C105	
105 Tag 52	PAN Source	N2			C105	

This message is applicable when we need to change status of the card like Card block/ Card Expiry change/Card replacement/Token status change. Please refer compliance section for details.

Issuers will be provided with Jaywan TSP Portal to perform token life cycle management activities on behalf of the customers. Issuers will be onboarded to Jaywan TSP portal as part of the onboarding process.

Please review the following section

- 12.13.1 Token Life Cycle Management (TLCM)

6.19 Onus transaction Detokenization

Onus transactions need to send to UAE switch to detokenize card if the transaction initiate with token.

Member banks who want to support Onus Detokenization transaction must expect FPAN in DE-02 and DPAN in DE35 & DE 105 Tag 01 in response.

Onus Transaction request and response for detokenize card						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	AQ	SW
ISO	Message Type identifier		0100/ 0200		0110/02 10	
ISO	Primary Bit Map		M	M	M	
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	
3	Processing Code	N6	M	→	M	
4	Amount, Transaction	N12	M	→	M	
7	Date Time, Transmission	N10(MMDDH HMMSS)	M	→	M	
11	Systems Trace Number	N6	M	→	M	
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	
13	Date, Local Transaction	N4(MMDD)	M	→	M	
14	Date, Expiration	N4(YYMM)	M	→	M	
15	Date, Settlement	N4(MMDD)	M	→	M	
17	Date, Capture	N4(MMDD)	M	→	M	
18	Merchant Category Code	N4	M	→	O	
19	Acquiring Country Code	N3	M	→	M	
22	POS Entry Mode	N3	M	→	M	
23	Card Sequence No	N3	C23	→		
25	POS Condition Code	N2	M	→	M	
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	
33	Forwarding Institution ID	N..11(LLVAR)	M	→	M	
35	Track II Data	Z..37(LLVAR)	C35	→	→	
37	Retrieval Ref. No.	AN12	M	→	M	
38	Authorization Id Response	AN6			C38	
39	Response Code	AN2			M	
41	Card Acceptor, Terminal Id	AN8	M	→	M	
42	Card Acceptor. Id Code	AN15	M	→	M	
43	Card Acceptor Acquirer Name	AN40	M	→	M	
49	Transaction Currency Code	N3	M	→	M	
52	PIN Data	AN16	C52	→		
53	Security Related Control Information	N16	C53	→		

Onus Transaction request and response for detokenize card						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	AQ	SW
ISO	Message Type identifier		0100/ 0200		0110/02 10	
55	ICC System Related Data	B..255(LLVAR)	C55	→	C55	
57	EMV Data Element 2	N6	C57	→		
60	Additional Data	AN..16(LLVAR)	M	→	M	
61	POS terminal data	AN..255(LLVAR)	M	→	M	
100	Receiving Institution ID	N..11(LLVAR)			M	
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		M	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		M	→	
105 Tag 21	Wallet Provider Id	ANS32		M	→	

6.20 Offline Transactions/Financial Transaction Advice (Debit/Credit)

Offline transactions are used when the acquirer approves transactions offline at the terminal, due to the nature of the business (e.g., airlines, transit, etc.). In such cases, acquirers can submit these as offline transactions using 0220 message with POS Condition code as 09/10.

For Discover co-badge transactions, processing is done in DMS mode. If a Discover co-badge card is used on the Discover network, the authorization is processed using an 0110 message, and the corresponding clearing file is submitted as an online 0220 message using adjustment transactions.

This same functionality will be extended in the future to support international bilateral transactions, where DMS-mode processing is required. These will also utilize the adjustment transaction message format to ensure compatibility.

Debit/Credit Adjustment transactions						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0220		0230	
ISO	Primary Bit Map		M	M	M	M
	Secondary Bit Map					
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	C6
7	Date Time, Transmission	N10(MMDDHHMMS S)	M	→	M	→
10	Conversion rate, card holder billing	N8		C6	C6	
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	M	→	M	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
16	Date, Conversion	N4(MMDD)		C16	C16	
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Category Code	N4	M	→	M	→
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
23	Card Sequence No	N3	C23	→	C23	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
33	Forwarding Institution ID	N..11(LLVAR)	M	→	M	→
35	Track II Data	Z..37(LLVAR)	C35	→		

Debit/Credit Adjustment transactions						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0220		0230	
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6	M	→	M	→
39	Response Code	AN2			M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	M	→
48	POS retailer Data	AN..27(LLVAR)	M	→	M	→
49	Transaction Currency Code	N3	M	→	M	→
51	Currency Code, Cardholder billing	N3		C51	C51	C5 1
55	ICC System Related Data	B..255(LLVAR)	C55	C55	C55	C5 5
57	EMV Data Element 2	N6	C57	→	C57	→
60	Additional Data	AN..16(LLVAR)	M	→	M	→
61	POS terminal data	AN..255(LLVAR)	M	→	M	→
63	Network Data	ANS..255(LLVAR)				
063 Tag 02	Transaction Identifier	AN15		C063	→	→
063 Tag 03	Token PAR	ANS29				C06 3
063 Tag 04	Function Code	N3	C063	C063	→	→
100	Receiving Institution ID	N..11(LLVAR)			M	→
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		C105	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		C105	→	
105 Tag 21	Wallet Provider Id	ANS32		M	→	

Please review the following section

- 12.16 Offline Transaction/Financial Transaction Advice

6.21 POS Balance Enquiry

Transaction Request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
ISO	Message Type identifier		0100/ 0200		0110/ 0210	
ISO	Primary Bit Map		M	M	M	M
2	Primary Account. Number.	N..19(LLVAR)	M	→	M	→
3	Processing Code	N6	M	→	M	→
4	Amount, Transaction	N12	M	→	M	→
6	Amount, Cardholder Billing	N12		C6	C6	
7	Date Time, Transmission	N10(MMDDHHMMSS)	M	→	M	→
10	Conversion rate, card holder billing	N8		C10	C10	
11	Systems Trace Number	N6	M	→	M	→
12	Time, Local Transaction	N6(HHMMSS)	M	→	M	→
13	Date, Local Transaction	N4(MMDD)	M	→	M	→
14	Date, Expiration	N4(YYMM)	M	→	M	→
15	Date, Settlement	N4(MMDD)	M	→	M	→
17	Date, Capture	N4(MMDD)	M	→	M	→
18	Merchant Type (Category Code)	N4	M	→	O	O
19	Acquiring Country Code	N3	M	→	M	→
22	POS Entry Mode	N3	M	→	M	→
23	Card Sequence No	N3	C23	→	C23	→
25	POS Condition Code	N2	M	→	M	→
32	Acquirer Institution ID	N..11(LLVAR)	M	→	M	→
35	Track II Data	Z..37(LLVAR)	C35	→		
37	Retrieval Ref. No.	AN12	M	→	M	→
38	Authorization Id Response	AN6			C38	→
39	Response Code	AN2			M	→
41	Card Acceptor, Terminal Id	AN8	M	→	M	→
42	Card Acceptor. Id Code	AN15	M	→	M	→
43	Card Acceptor Acquirer Name	AN40	M	→	M	→
49	Transaction Currency Code	AN3	M	→	M	→

Transaction Request and response						
Field	Data Element	Data Type	Transmission Requirement			
			AQ	SW	IS	SW
51	Cardholder Billing Currency Code	N3		C51	C51	
52	PIN Data	AN16	C52	→		
53	Security Related Control Information	N16	M	→		
55	ICC System Related Data	B..255(LLVAR)	C55	→	C55	→
57	EMV System Related Data	N6	C57	→	C57	→
100	Receiving Institution ID	N..11(LLVAR)			O	→
105	Token Data	ANS..999(LLVAR)				
105 Tag 01	Token ID	AN19		M	→	
105 Tag 02	Token Expiration Date	N4		M	→	
105 Tag 03	Token Reference ID	ANS36		M	→	
105 Tag 04	Wallet ID	ANS..99		M	→	
105 Tag 05	Token Type	AN2		M	→	
105 Tag 06	Token Status	AN1		M	→	
105 Tag 07	Payment Account Reference (PAR)	ANS29		M	→	
105 Tag 08	Token Requestor ID	ANS11		M	→	
105 Tag 09	TSP Validation Result	AN2		M	→	
105 Tag 10	Device Type	AN2		M	→	
105 Tag 21	Wallet Provider ID	ANS32		M	→	
122	Remaining Open To Use	AN..25(LLVAR)			C122	→

7. Detailed Description of Data Elements

7.1 DE-2 Primary Account Number

Type	N..19
Format	LLVAR
Description	A series of digits used to identify customer account or relationship. Identifies the cardholder PAN.
Field Edits	This remains same for a particular transaction and cannot be changed.
Constraints	When present, it should be echoed in response and all Subsequent messages.
Validation	It should be a 12-19 digit PAN number and should not be less than 12 and not more than 19.
Compliance	Card number in request and response should always be the same. In reversal, the Card number should be the same as original request message
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0100/0110 – E-Commerce Request/Response 0200/0210 – ATM/POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM/POS Reversal Request/Repeat/Response

7.2 DE-3, Processing Code

The processing code is used in conjunction with the message type to define the type of transaction being sent by the terminal to the host. It also includes account selection information. (Refer to the Message Type / Processing Code Table section for processing code definitions.)

Type	N6																														
Format	Fixed																														
Description	A series of digits that describe the type of transaction and the accounts affected by the transaction. <table> <tr> <th><i>Digit 1 and 2</i></th><th><i>Transaction Code</i></th></tr> <tr> <td>00</td><td>Purchase /Pre-Authorization / Incremental Auth / Pre-Authorization completion/Token Provisioning</td></tr> <tr> <td>01</td><td>Cash Withdrawal/ Cash Advance</td></tr> <tr> <td>09</td><td>Purchase with Cashback</td></tr> <tr> <td>20</td><td>Credit/Refund</td></tr> <tr> <td>31</td><td>Balance Enquiry</td></tr> <tr> <td>26</td><td>OCT</td></tr> <tr> <td>90</td><td>Detokenize request (Only for Onus transaction)</td></tr> <tr> <th><i>Digit 3 and 4</i></th><th><i>From Account type</i></th></tr> <tr> <td>00</td><td>Unspecified/Unknown</td></tr> <tr> <td>10</td><td>Savings</td></tr> <tr> <td>20</td><td>Checking</td></tr> <tr> <td>30</td><td>Credit card</td></tr> <tr> <th><i>Digit 5 and 6</i></th><th><i>To Account type</i></th></tr> <tr> <td>00</td><td>Unspecified/Unknown</td></tr> </table>	<i>Digit 1 and 2</i>	<i>Transaction Code</i>	00	Purchase /Pre-Authorization / Incremental Auth / Pre-Authorization completion/Token Provisioning	01	Cash Withdrawal/ Cash Advance	09	Purchase with Cashback	20	Credit/Refund	31	Balance Enquiry	26	OCT	90	Detokenize request (Only for Onus transaction)	<i>Digit 3 and 4</i>	<i>From Account type</i>	00	Unspecified/Unknown	10	Savings	20	Checking	30	Credit card	<i>Digit 5 and 6</i>	<i>To Account type</i>	00	Unspecified/Unknown
<i>Digit 1 and 2</i>	<i>Transaction Code</i>																														
00	Purchase /Pre-Authorization / Incremental Auth / Pre-Authorization completion/Token Provisioning																														
01	Cash Withdrawal/ Cash Advance																														
09	Purchase with Cashback																														
20	Credit/Refund																														
31	Balance Enquiry																														
26	OCT																														
90	Detokenize request (Only for Onus transaction)																														
<i>Digit 3 and 4</i>	<i>From Account type</i>																														
00	Unspecified/Unknown																														
10	Savings																														
20	Checking																														
30	Credit card																														
<i>Digit 5 and 6</i>	<i>To Account type</i>																														
00	Unspecified/Unknown																														
Field Edits	This remains same for a particular transaction and cannot be changed.																														
Constraints	When present, it should be echoed in response and all Subsequent messages.																														
Validation	Processing code should be from the list above																														
Compliance	Transaction code in request and response should be same. In reversal it should be the same as original request.																														
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM/POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM/POS Reversal Request/Repeat/Response																														

The processing code is used in conjunction with the message type to define the type of transaction being sent to the host. The following is a table specifying the message type and processing code for each transaction below:

Transaction	Processing Code
Cash withdrawal	01 00 00
Balance Enquiry	31 00 00
Pre-authorization	00 aa 00
Purchase	00 aa 00
Purchase with cash-back	09 aa 00
Refund	20 aa 00
Recurring Payments	00 aa 00
Incremental Auth	00 aa 00
Token provisioning	00 00 00
Detokenization	90 00 00
Void	Same as original Transaction
Reversal	Same as original Transaction

Please review the following sections

- 12.4 Purchase
- 12.5 Pre-Authorization & Pre-Authorization Completion
- 12.6 Refund
- 12.7 Partial Authorization
- 12.8 Purchase with Cashback
- 12.13 Tokenization
- 12.14 Ecommerce CIT

7.3 DE-4, Amount Transaction

Type	N12
Format	Fixed
Description	Contains the transaction amount to be transferred i.e., specified by the currency code in DE-49. This field contains the total amount carried for a transaction.
Field Edits	• This remains same for a particular transaction and cannot be changed. • For balance enquiry amount will be zero in request and response. • Amount, Transaction is a fixed length field and a leading zero is always required, right Justified • For Tokenization ASI transaction, this field will contain Zero value in request and response.
Constraints	When present, it should be echoed in response and all Subsequent messages. Exception in case of partial authorization
Validation	Amount should be only in numeric
Compliance	• Transaction amount should be same in request and response. Also, transaction currency code should be present in DE-49. • In reversal transaction amount should be same as original request. • In balance inquiry and account status inquiry transactions this field should be Zero. • If there is any transaction fee, it is included in field 4 in case it is present. For a purchase with cashback transaction this field should contain the purchase amount + the cash amount For partial authorization, issuer will populate • DE-4 with actual debited amount • DE-54 with the original transaction amount • DE-39 with '10' For Tokenization provisioning transaction /Account Verification transaction this field should populate values with Zeros. For Domestic/GCC Transactions, Issuers to use this amount for the actual transaction amount. For international acceptance, if DE49 is not 784 (i.e., not in AED), this field will contain the transaction amount in the acquirer's currency For an incremental authorization transaction, this field should contain the additional amount authorized. For example, if the initial authorization was for 100 AED and an incremental authorization was initiated for 20 AED, this field should reflect 20 AED.
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM/POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response

	0400/0401/0410/0420/0421/0430 – ATM/POS Reversal Request/Repeat/Response
--	--

Please review the following sections

- 12.7 Partial Authorization
- 12.8 Purchase with Cashback
- 12.14. Tokenization

7.4 DE-6, Amount Cardholder Billing

Type	N12
Format	Fixed
Description	Amount billed to the cardholder in the currency of the cardholder account Exclusive of cardholder billing fees. This is a fixed-length field, lead zero fills are always required. No decimal point appears in this field; the decimal place is implied based on the DE-51. This field may be inserted by network switch or issuer. It must NOT be included in acquirer request messages. If an issuer receives a request with this field present, the same value must be echoed in the response. If an issuer receives a request with this field absent, the issuer may optionally insert it in the response message as an informational field. DE-6, DE-10 and DE-51 must be inserted together, i.e., if a message contains any one of them, it must contain all of them.
Field Edits	• Used where the billing currency is different from the transaction currency. • If not present, it is assumed that the two currencies are the same • Data will be set by the Switch • Issuer might optionally insert it in the response message
Constraints	When present, it should be echoed in response
Validation	Amount should be only in numeric
Compliance	• DE-6, DE-10, DE-51 will be present • If DE49 is not 784, issuers should refer to this field for the AED equivalent amount for processing and posting to the cardholder's account.
Presence	Conditional-This field is present in the below messages where billing currency is different from the transaction currency. 0100/0110 – POS Authorization Request/Response 0200/0210 – POS Financial Request/Response 0400/0401/0410/0420/0421/0430 – POS Reversal Request/Repeat/Response

7.5 DE-7, Date Time, Transmission

Type	N10
Format	Fixed. MMDDhhmmss
Description	Date and time a message is entered into the data interchange system. It is represented in GMT/UTC
Field Edits	This field can be changed for a particular transaction. The original date and time will be restored in the response.
Constraints	This should be echoed back in response
Validation	Date and Time, Transmission should be only in numeric
Compliance	In reversal this value can differ from original request.
Presence	Mandatory- This field is mandatory across all the messages

7.6 DE-10, Conversion Rate, Cardholder Billing

Type	N8
Format	Fixed
Description	The factor used in the conversion from transaction to cardholder billing amount. The amount transaction is multiplied by the billing conversion rate to give the cardholder billing amount. The leftmost digit of this field signifies the number of decimal places in the rate, and the remaining 7 digits give the actual rate. For example: 69972522 represents 9.972522 22190391 represents 21903.91 This field should only be included if the billing currency is different from the transaction currency. This field may be inserted by network switch or issuer. It must NOT be included in acquirer request messages. If an issuer receives a request with this field present, the same value must be echoed in the response. If an issuer receives a request with this field absent, the issuer may optionally insert it in the response message as an informational field.
Field Edits	- Used where the billing currency is different from the transaction currency. - If not present, it is assumed that the two currencies are the same - Data will be set by the Switch - Issuer might optionally insert it in the response message
Constraints	When present, it should be echoed in response
Validation	Amount should be only in numeric
Compliance	DE-6, DE-10, DE-51 will be present
Presence	Conditional-This field is present in the below messages where billing currency is different from the transaction currency. 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM/POS Financial Request/Response 0400/0401/0410/0420/0421/0430 – ATM/POS Reversal Request/Repeat/Response

7.7 DE-11, Systems Trace Audit Number

Type	N6
Format	Fixed
Description	- This is assigned by the acquirer device that uniquely identifies a cardholder transaction. - Remains unchanged for all messages throughout the life the transaction. - Issuer has to respond back with the same STAN in their response. It may happen that acquirer STAN and Issuer STAN may be different for the same transaction. - Acquirer should send STAN & RRN of original transaction in reversal messages.
Field Edits	This field remains the same for a particular transaction.
Constraints	The same is echoed in the response
Validation	STAN should be a 6-digit numeric value.
Compliance	System trace Audit Number should be same in request as well as in response.
Presence	Mandatory- Present across all the messages

7.8 DE-12, Time, Local Transaction

Type	N6
Format	Fixed. HHMMSS
Description	Time entered by the POS device. Local time at which the transaction began at the card acceptor location.
Field Edits	This field remains the same for a particular transaction.
Constraints	The same is echoed in the response
Validation	Local time should be of this format
Compliance	Local transaction time should be same in request as well as in response. And this field remains same in complete transaction cycle. Time must be specified in local time zone, NOT in GMT
Presence	Mandatory- Present across all the messages

7.9 DE-13, Date, Local Transaction

Type	N4
Format	Fixed. MMDD
Description	Date entered by the acquirer device. Local date at which the transaction began at the card acceptor location
Field Edits	This field remains the same for a particular transaction.
Constraints	The same is echoed in the response
Validation	Local date should be of this format and for domestic, Acquirer should send this date as per the UAE date else transaction will be rejected
Compliance	Local transaction date should be same in request as well as in response. And this field remains same in complete transaction cycle.
Presence	Mandatory- This field is mandatory across all the messages

7.10 DE-14, Date, Expiration

Type	N4
Format	Fixed. YYMM
Description	Contains the month and the year after which the card expires.
Field Edits	This remains same for a particular transaction
Constraints	Element is present if DE-35 (Track 2) is not present or if it is online transactions.
Validation	- For eCommerce customer initiated and POS transactions this field should be mandatory. - For MIT, Manual, MOTO, and Recurring transactions, this field is optional and issuers are required to validate it if present in the request. - Acquirer may verify the format but should not verify its content
Compliance	This field should be present in card not present transactions such as E-commerce, manual entry, token provisioning and tokenized financial transaction
Presence	Conditional- For CNP transactions this field should be present 0100/0110 – POS Authorization Request/Response 0100/0110 – Ecommerce Authorization Request/Response 0200/0210 –ATM/POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – POS Reversal Request/Repeat/Response

7.11 DE-15, Date, Settlement

Type	N4
Format	Fixed. MMDD
Description	Contains the date and the month on which Host will settle the transaction.
Field Edits	Host can add settlement date as per the cases. But when present should be echoed back in the response.
Constraints	
Validation	Settlement Date should be of this format
Compliance	This field remains same in complete transaction cycle Should indicate the switch settlement date In Cutover message the value will indicate the new business date that the UAESWITCH has cutover to
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM & POS Reversal Request/Repeat/Response 0500/0501/0510 – Acquirer Recon 0502/0503/0512 – Issuer Recon 0800/0801/0810 (cutover)

7.12 DE-16, Date, Conversion

Type	N4
Format	Fixed. MMDD
Description	Contains the month and the day used to convert the transaction from the local currency into the currency of the issuer. DE-16 indicates the effective date (month and day) of the DE-9 (Conversion Rate, Settlement) and the DE-10 (Conversion Rate, Cardholder Billing). DE-16 must be present whenever either of these data elements is present within a message.
Field Edits	Switch can add conversion date as per the cases. But when present should be echoed back in the response.
Constraints	For a cross-currency conversion, DE-9, DE-10
Validation	
Compliance	Set by Switch DE-9, DE-10, DE-16
Presence	Conditional- present in the following messages for cross border transaction 0100/0110 – POS Authorization Request/Response 0200/0210 – POS Financial Request/Response 0400/0401/0410/0420/0421/0430 – POS Reversal Request/Repeat/Response

7.13 DE-17, Capture Date

Type	N4
Format	Fixed. MMDD
Description	Contains the date and the month on which transaction was acquired Reflects the date after cutover
Field Edits	Should be echoed back in the response.
Constraints	NA
Validation	Capture Date should be of this format
Compliance	This field remains same in complete transaction cycle.
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM & POS Reversal Request/Repeat/Response

7.14 DE-18, Merchant Category Code

Type	N4
Format	Fixed
Description	Contains a 4-digit code describing a merchant's type of business For POS, valid values as per ISO 18245 for list of MCC's For ATM, the value must be set to "6011" for ATM transactions.
Field Edits	This remains same for a transaction.
Constraints	It is not to be echoed in response for ATM transactions but mandatory echo for POS transactions
Validation	This field should be from the standard list.
Compliance	This is mandatory field. The value should be present as per the MCC code as per ISO 18245 For ATM transactions, this must be set to 6011
Presence	Mandatory for the below messages 0100 /0110– POS Authorization Request /Response 0200/0210 – ATM Financial Request/Response 0400/0410 – ATM reversal request/Response 0200/0210 – POS Financial Request /Response 0220/0230 – POS Authorization Completion Request 0400/0401/0420/0421/0410/0430 – POS Reversal Request

7.15 DE-19, Acquiring Country Code

Type	N3
Format	Fixed
Description	Contains a code identifying the country of the acquiring institution for the ATM/POS. Refer to ISO 3166 for country code list.
Field Edits	This remains same for a transaction.
Constraints	If present is to be echoed back in response.
Validation	This field should be from the standard list.
Compliance	For UAE Acquirers the value should be set to 784
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM & POS Reversal Request/Response

7.16 DE-22, Point of Service (POS) Entry Mode

Type	N3																																																				
Format	Fixed																																																				
Description	Contains a 3-digit code indicating the method used to enter the account number. <table> <tr> <th><i>Digit 1&2</i></th><th><i>Pan Entry Mode</i></th></tr> <tr><td>00</td><td>PAN entry mode unknown</td></tr> <tr><td>01</td><td>Manual</td></tr> <tr><td>02</td><td>Magnetic Stripe Read</td></tr> <tr><td>03</td><td>Barcode reader</td></tr> <tr><td>04</td><td>Optical card reader</td></tr> <tr><td>05</td><td>ICC</td></tr> <tr><td>06</td><td>IVR</td></tr> <tr><td>07</td><td>Contactless payment using chip card.</td></tr> <tr><td>08</td><td>QR code</td></tr> <tr><td>09</td><td>PAN/Token entry via electronic commerce containing Digital secure remote payment (DSRP) cryptogram in DE-55</td></tr> <tr><td>10</td><td>Credential on file</td></tr> <tr><td>80</td><td>Fall-back Transactions</td></tr> <tr><td>81</td><td>E-commerce</td></tr> <tr><td>97</td><td>Reserved for private use</td></tr> <tr><td>90</td><td>Full and Unaltered magnetic stripe read (enables CVD validation)</td></tr> <tr><td>91</td><td>Contactless using CVD, iCVD checking possible.</td></tr> <tr><td>95</td><td>Chip card with unreliable CVD or iCVD</td></tr> <tr><td>99</td><td>Reserved for private use</td></tr> <tr> <th><i>Digit 3</i></th><th><i>Pin Entry capability</i></th></tr> <tr><td>0</td><td>Unspecified</td></tr> <tr><td>1</td><td>PIN Entry Capability</td></tr> <tr><td>2</td><td>No PIN Entry Capability</td></tr> <tr><td>6</td><td>PIN pad inoperative</td></tr> <tr><td>8</td><td>Reserved for private use</td></tr> <tr><td>9</td><td>Reserved for private use</td></tr> </table>	<i>Digit 1&2</i>	<i>Pan Entry Mode</i>	00	PAN entry mode unknown	01	Manual	02	Magnetic Stripe Read	03	Barcode reader	04	Optical card reader	05	ICC	06	IVR	07	Contactless payment using chip card.	08	QR code	09	PAN/Token entry via electronic commerce containing Digital secure remote payment (DSRP) cryptogram in DE-55	10	Credential on file	80	Fall-back Transactions	81	E-commerce	97	Reserved for private use	90	Full and Unaltered magnetic stripe read (enables CVD validation)	91	Contactless using CVD, iCVD checking possible.	95	Chip card with unreliable CVD or iCVD	99	Reserved for private use	<i>Digit 3</i>	<i>Pin Entry capability</i>	0	Unspecified	1	PIN Entry Capability	2	No PIN Entry Capability	6	PIN pad inoperative	8	Reserved for private use	9	Reserved for private use
<i>Digit 1&2</i>	<i>Pan Entry Mode</i>																																																				
00	PAN entry mode unknown																																																				
01	Manual																																																				
02	Magnetic Stripe Read																																																				
03	Barcode reader																																																				
04	Optical card reader																																																				
05	ICC																																																				
06	IVR																																																				
07	Contactless payment using chip card.																																																				
08	QR code																																																				
09	PAN/Token entry via electronic commerce containing Digital secure remote payment (DSRP) cryptogram in DE-55																																																				
10	Credential on file																																																				
80	Fall-back Transactions																																																				
81	E-commerce																																																				
97	Reserved for private use																																																				
90	Full and Unaltered magnetic stripe read (enables CVD validation)																																																				
91	Contactless using CVD, iCVD checking possible.																																																				
95	Chip card with unreliable CVD or iCVD																																																				
99	Reserved for private use																																																				
<i>Digit 3</i>	<i>Pin Entry capability</i>																																																				
0	Unspecified																																																				
1	PIN Entry Capability																																																				
2	No PIN Entry Capability																																																				
6	PIN pad inoperative																																																				
8	Reserved for private use																																																				
9	Reserved for private use																																																				
Field Edits	This remains same for a particular transaction.																																																				
Constraints	This is to be echoed back in response																																																				
Validation	This field should be from the standard list.																																																				
Compliance	The value should be from the table mentioned above. Card present: This field should compare with DE-25, DE-35/DE-45, DE-52, DE-55, DE-61, DE-63 and DE-23. Card not present: This field should be compare with DE-14, DE-25, DE-48, DE-52 , DE-61, DE-63, DE-104. If PAN entry mode is set to 05, then DE-23, DE-55, DE-57 to be populated If PAN entry mode is set to 08, then DE-57 to be populated																																																				
Presence	Mandatory for the below messages																																																				

	0100/0110 – POS Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM & POS Reversal Request/Repeat/Response
--	--

7.17 DE-23, Card Sequence Number

Type	N3
Format	Fixed
Description	(Applicable for Chip) If cards have the same PAN Number, then card sequence number is used to differentiate these cards
Field Edits	This remains same for a particular transaction.
Constraints	- DE 23 shall be echoed in response - Should be in the range of 000-999
Validation	It should be a 3-digit numeric code
Compliance	This field should be present if it is a chip transaction
Presence	Mandatory for the following message if transaction has EMV data 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response 0220/0230 – POS Authorization Completion Response

7.18 DE-25, Point of Service (POS) Condition Code

Type	N2	
Format	Fixed	
Description	<i>Value</i>	<i>Meaning</i>
	00	Normal
	01	Customer Not present
	02	Unattended Terminal
	03	Merchant suspicious
	05	Customer present, card not present
	06	Preauthorization completion advice
	07	Telephone Request (IVR)
	08	MO/TO request
	09	Financial Transaction Advice Debit
	10	Financial Transaction Advice Credit
	51	Request for Account status inquiry or Token Provisioning.
	53	Send OTP for Token Provisioning
	58	Merchant Initiated Transactions (Recurring / Incremental Auth)
	59	E-Commerce transaction (Customer Initiated Transaction)
	71	Card present, Magnetic stripe cannot be read.
Field Edits	This remains same for a particular transaction.	
Constraints	DE25 shall be mandatory echoed in response.	
Validation	This field should be from the standard list	
Compliance	The value should be same as mentioned above. This field should compare with DE-22 and DE-61. For ATM transaction value to be set to 00	
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0100/0110 – Ecommerce Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM & POS Reversal Request/Repeat/Response	

7.19 DE-32, Acquiring Institution ID

Type	N..11
Format	LLVAR
Description	Unique Code allotted by CBUAE for determining the financial institution acting as an acquirer.
Field Edits	This remains same for a particular transaction.
Constraints	This is to be echoed back in response.
Validation	This is allotted by CBUAE and should be numeric.
Compliance	The value should present in table maintained by CBUAE. The values should remain same during the complete transaction cycle. For UAE Acquirers: First three digit value will start with 784 For Non-UAE Acquirers: First three digits will indicate the acquiring country code For Token Provisioning: This value will be 784200200
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0100/0110 – Ecommerce request/response 0200/0210 – ATM & POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM & POS Reversal Request/Repeat/Response

7.20 DE-33, Forwarding Acquiring Institution ID

Type	N..11
Format	LLVAR
Description	Unique Code allotted by CBUAE for determining the institution operating as a terminal acquirer for other entities.
Field Edits	This remains same for a particular transaction.
Constraints	This is to be echoed back in response.
Validation	This is allotted by CBUAE and should be numeric.
Compliance	The value should present in table maintained by CBUAE. The values should remain same during the complete transaction cycle. For UAE Acquirers: First three digit value will start with 784 For Non-UAE Acquirers: First three digits will indicate the acquiring country code
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0430 – ATM & POS Reversal Request/Repeat/Response

7.21 DE-35, Track II Data

Type	Z..37
Format	LLVAR
Description	The information encoded on Track 2 of the magnetic stripe of the plastic card (per ISO 7813) used for the transaction, excluding start and end sentinel and LRC characters.
Field Edits	This remains same for a particular transaction. This is not used in reversal.
Constraints	This is not echoed in response.
Validation	None
Compliance	- This field should be a permanent field for a card based transaction. - When PAN entry capability is 05, 07 or 95 then EMV tag 57 should be captured in DE-35 by the acquirer and EMV tag 57 should not be carried in DE-55. - When PAN entry capability is 91 i.e., for a contactless card, Tag 9F6B should be captured in DE-35 by the acquirer. - For tokenized transaction, this field will contain Token PAN information - For Manual, MOTO and eCommerce transactions this field may not be present.
Presence	Mandatory for non-tokenized card present transaction for the below messages 0100 – POS Authorization Request 0200 – ATM & POS Financial Request sections 0220 – Pre-Auth Completion

7.22 DE-37, Retrieval Reference Number (RRN)

Type	AN12
Format	FIXED
Description	It is used to identify and track all messages related to a given cardholder transaction.
Field Edits	This field remains same for a particular transaction and is to be echoed back in a response.
Constraints	This field should be echoed back in a response
Validation	This field should be of this format
Compliance	The value should be same in request as well as response. And this value should remain same during complete transaction cycle.
Presence	Mandatory-Should be present for all messages

7.23 DE-38, Authorization Identification Response

Type	AN6
Format	Fixed
Description	A unique code assigned by the issuer
Field Edits	This Field present in all successfully approved transaction response message

	This field should never be present in the message requests from Acquirer except in case of refund/void message
Constraints	Purchase: assigned by issuer Refund: Present in Request (optional) Reversal: must be present if its present in the original transaction
Validation	This is a 6 character authorization code generated by the issuer / CBUAE and should not be filled by the acquirer except in case of refund/void
Compliance	This field should be present in all authorizations. In reversal, if this is present in the original transactions, this field is present In Refund request if present it will contain reference to the original purchase transaction
Presence	Mandatory for the below messages 0110 – POS Authorization Response 0210 – ATM & POS Financial Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM & POS Reversal Request/Repeat/Response

7.24 DE-39, Response Code

Type	AN2
Format	Fixed
Description	This defines the response to a request for a transaction.
Field Edits	This field is echoed back in a response for a successful and an unsuccessful transaction. This data element must be present in all response messages
Constraints	Assigned by the issuer.
Validation	This field is assigned by the issuer. But for a reversal transaction this can be filled by the acquirer from the original transaction.
Compliance	This value should be from the table mentioned in the section. If response code value is set to 00, then DE-38 should be populated
Presence	Mandatory for the below messages 0110 – POS Authorization Response 0210 – ATM & POS Financial Response 0230 – POS Authorization Completion Response 0312 – Issuer Update response 0410/430 – ATM & POS Reversal Response 0630 – Administration advice response 0810 – Network Management Response

Action	Meaning
A	Accept
D	Decline
C	Capture

Response Code Table								
00	Approved or completed Successfully.	A	34	Suspected fraud, capture.	C	74	Transactions declined by Issuer based on Risk Score	D
01	Refer to card issuer	D	35	Contact Acquirer	C	75	Allowable number of PIN tries exceeded	D
			36	Restricted card, capture	C			
02	Refer to card issuer	D	37	Contact Acquirer	C	76	Invalid Account	D
			38	Allowable PIN tries exceeded, capture.	C			
03	Invalid merchant.	D	39	No credit account.	D	77	CAVV Validation failed	D
			40	Requested function not supported.	D			
04	Pick-up.	C	41	Lost card, capture.	C	78	Jaywan TSP Declined	D
05	Do not honor. In case CVD, CVD2, iCVD verification	D	42	No universal account.	D			
			43	Stolen card, capture.	C			
			45	DMS Not Supported	D			

UAESWITCH Interface Technical Specifications

	fails, Inactive or Dormant account		51	Not sufficient funds.	D	81	Cryptographic Error	D
			52	No checking account	D			
06	Error.	D	53	No savings account.	D	85	Conditional Approval	A
07	Pick-up Card	D	54	Expired card, decline	D			
10	Partial approval	A	55	Incorrect personal identification number.	D	90	Cut-off is in process.	D
12	Invalid transaction or if member is not able to find any appropriate response code	D	56	No card record.	D	91	Issuer or switch is inoperative	D
			57	Transaction not permitted to Cardholder	D	92	No routing available	D
			58	Transaction not permitted to terminal.	D	93	Transaction cannot be completed. Compliance violation.	D
13	Invalid amount.	D	59	Suspected fraud, decline / Transactions declined based on Risk Score	D			
14	Invalid card number (no such Number).	D	60	Card acceptor contact acquirer, decline.	D	94	Duplicate transmission.	D
15	No such issuer.	D	61	Exceeds withdrawal amount limit.	D	95	Reconcile error	D
17	Customer cancellation.	D	62	Restricted card, decline.	D	96	System malfunction	D
19	Re-enter transaction	D	63	Security violation.	D			
20	Invalid response.	D	64	Original Amount Incorrect	D			
21	No action taken.	D	65	Exceeds withdrawal frequency limit.	D	Q0	Enter PIN	D
22	Suspected malfunction.	D	66	Card acceptor calls acquirer's.	D			
25	Unable to locate record	D	67	Hard capture (requires that card be picked up at ATM).	C			
27	File Update field edit error	D	68	Acquirer time-out	D			
28	Record already exists in the file	D	69	Mobile number record not found/ mismatch	D			
29	File Update not successful	D						
30	Format error.	D						
31	Bank not supported by switch	D						
32	Completed Partially							
33	Expired card, capture	C						

Issuer response Timed Out/Late response

When UAESWITCH sends 0100 / 0200 request to Issuer member bank and do not receive response within the stipulated time, UAESWITCH response back to acquirer with response code '68' and sends reversal to issuing member bank with response code '68' indicating a full reversal.

Issuer offline/Signed off

If Issuer member bank is in offline/signed off and UAESWITCH receives 0100 / 0200 request from the acquirer, then UAESWITCH will response back with '91' response code to Acquirer member bank. Acquirer need not generate reversal for this transaction.

Acquirer Time-out

When an acquirer sends a 0100/ 0200 message to UAESWITCH but do not receive the response within the stipulated time, then acquirer sends a reversal 0400/0401/0420/0421 message with response code '68'.

Terminal Failure

When an acquirer has received an approved response 0110/ 0210 with a valid DE-38 but fails to send the response to the terminal, then acquirer sends a reversal 0400/0401/0420/0421 message with response code '22'. For ATM transactions response code may be '21'.

Customer Cancellation

When an acquirer sends a 0100/0200 and has received an approved response 0110/0210 with a valid DE-38 but customer cancels the transaction by sending a void transaction at POS terminal, then acquirer sends this void as reversal with response code '17' to UAESWITCH.

Contactless Transactions no CVM thresholds

For contactless transactions received without a PIN i.e., no CVM was performed and the issuer requires a PIN due to single transaction limit exceeding the CVM limit OR the contactless cumulative limit is exceeded, the issuer bank will respond in DE-39 with value "Q0" to ask for PIN; the POS Acquirer will force the Pin when the Issuer responds with Value (Q0) in DE-39

If the Issuer responds with Q0, the following should be considered for the "next transaction"

- The transaction will have a new Transmission Date and Time (DE-7)
- The transaction will have a new Local Transaction Date and Time (DE-12)
- The STAN will be incremented (DE-11)
- The transaction will have a new Retrieval Reference Number (DE-37)
- The POS Condition Code (DE-22) Position 1 (Card data input capability) and Position 7 (Card data input mode) will be "7" i.e., contactless
- The EMV data (DE-55) will be duplicated from the previous transaction request which was declined with Action Code "Q0" and Issuers must accept this as valid and not reject it or any parts of the EMV data e.g., ATC

Partial Authorization

If a card issuer is supporting partial authorization, issuer has to indicate the response code as '10' Please review the following section 12.6 Partial Authorization

7.25 DE-41, Card Acceptor Terminal ID

Type	AN8
Format	Fixed
Description	Contains an ID that identifies a card acceptor terminal.
Field Edits	This remains same for a transaction.
Constraints	When present this is to be echoed back in a response.
Validation	None
Compliance	The value should be same in request as well as response. The values should remain same during the complete transaction cycle.
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM & POS Reversal Request/Repeat/Response

7.26 DE-42, Card Acceptor Identification Code

Type	AN15
Format	Fixed
Description	Contains the identifier of the card acceptor operating the terminal
Field Edits	This remains same for a transaction.
Constraints	When present this is to be echoed back in a response.
Validation	None
Compliance	The value should be same in request as well as response. The values should remain same during the complete transaction cycle. For Card-on-File (CoF) provisioning, issuers will receive the Merchant ID in this field.
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM & POS Reversal Request/Repeat/Response

7.27 DE-43, Card Acceptor Acquirer Name

Type	AN40																	
Format	Fixed																	
Description	The name and location of the card acceptor i.e., POS Terminal owner name and city to be right padded with spaces. <table><tr><th>No</th><th>Terminal</th><th>Description</th></tr><tr><td>1</td><td>POS</td><td>01-23-Terminal Owner name</td></tr><tr><td></td><td></td><td>24-36-Terminal City</td></tr><tr><td></td><td></td><td>37-38-Terminal State Code</td></tr><tr><td></td><td></td><td>39-40-Terminal country Code ISO3166 Standard BH: Bahrain KW: Kuwait OM: Oman QA: Qatar SA: Saudi Arabia AE: United Arab Emirates</td></tr></table>			No	Terminal	Description	1	POS	01-23-Terminal Owner name			24-36-Terminal City			37-38-Terminal State Code			39-40-Terminal country Code ISO3166 Standard BH: Bahrain KW: Kuwait OM: Oman QA: Qatar SA: Saudi Arabia AE: United Arab Emirates
No	Terminal	Description																
1	POS	01-23-Terminal Owner name																
		24-36-Terminal City																
		37-38-Terminal State Code																
		39-40-Terminal country Code ISO3166 Standard BH: Bahrain KW: Kuwait OM: Oman QA: Qatar SA: Saudi Arabia AE: United Arab Emirates																
Field Edits	This remains same for a transaction.																	
Constraints	When present this should not be echoed back in a response. For Card-on-File (CoF) provisioning, issuers will receive the Merchant Name in this field. In the case of transactions originating from aggregator merchants, this field must contain the actual merchant's name																	
Validation	This field should be of this format.																	
Compliance	Check Terminal country code for domestic transaction only.																	
Presence	Mandatory for the below messages 0100 – POS Authorization Request 0200 – ATM & POS Financial Request 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0420/0421– ATM & POS Reversal Request/Repeat																	

7.28 DE-44, Additional Data, Response Data

Type	AN15																																				
Format	Fixed																																				
Description	Contains miscellaneous response message data. Acquirers receive field 44 in all 0110/210 authorization responses, and it contains transaction specific validation codes. 44.1—Address Verification Result Code (1 Byte) It is used in responses to original card-present and Card Not Present (CNP) requests that include address verification data in field 123. The result code is provided by the party verifying the address. <table border="1"> <thead> <tr> <th>Code</th><th>Definition</th></tr> </thead> <tbody> <tr> <td>A</td><td>Address matches, ZIP does not. Acquirer rights not implied.</td></tr> <tr> <td>B</td><td>Street addresses match. Postal code not verified due to incompatible formats. (Acquirer sent street address and postal code.)</td></tr> <tr> <td>C</td><td>Street address and postal code not verified due to incompatible formats. (Acquirer sent street address and postal code.)</td></tr> <tr> <td>D</td><td>Street addresses and postal codes match.</td></tr> <tr> <td>F</td><td>Street address and postal code match. Applies to U.K.-issued cards.</td></tr> <tr> <td>G</td><td>Address information not verified for international transaction. Issuer is not an AVS participant, or AVS data was present in the request, but issuer did not return an AVS result, there was no address record on file for this account.</td></tr> <tr> <td>I</td><td>Address information not verified.</td></tr> <tr> <td>M</td><td>Street address and postal code match.</td></tr> <tr> <td>N</td><td>No match. Acquirer sent postal/ZIP code only, or street address only, or postal code and street address. Also used when acquirer requests AVS but sends no AVS data in field 123.</td></tr> <tr> <td>P</td><td>Postal code match. Acquirer sent postal code and street address, but street address not verified due to incompatible formats.</td></tr> <tr> <td>R</td><td>Retry: System unavailable or timed out</td></tr> <tr> <td>S</td><td>Not applicable. If present, replaced with U (for domestic) or G (for international) by CBUAE.</td></tr> <tr> <td>U</td><td>Address not verified for domestic transaction. Issuer is not an AVS participant, or AVS data was present in the request but issuer did not return an AVS result, There was no address record on file for this account.</td></tr> <tr> <td>W</td><td>Not applicable. If present, replaced with Z by CBUAE.</td></tr> <tr> <td>X</td><td>Not applicable. If present, replaced with Y by CBUAE.</td></tr> <tr> <td>Y</td><td>Street address and postal code match.</td></tr> <tr> <td>Z</td><td>Postal/ZIP matches; street address does not match or street address not included in request.</td></tr> </tbody> </table>	Code	Definition	A	Address matches, ZIP does not. Acquirer rights not implied.	B	Street addresses match. Postal code not verified due to incompatible formats. (Acquirer sent street address and postal code.)	C	Street address and postal code not verified due to incompatible formats. (Acquirer sent street address and postal code.)	D	Street addresses and postal codes match.	F	Street address and postal code match. Applies to U.K.-issued cards.	G	Address information not verified for international transaction. Issuer is not an AVS participant, or AVS data was present in the request, but issuer did not return an AVS result, there was no address record on file for this account.	I	Address information not verified.	M	Street address and postal code match.	N	No match. Acquirer sent postal/ZIP code only, or street address only, or postal code and street address. Also used when acquirer requests AVS but sends no AVS data in field 123.	P	Postal code match. Acquirer sent postal code and street address, but street address not verified due to incompatible formats.	R	Retry: System unavailable or timed out	S	Not applicable. If present, replaced with U (for domestic) or G (for international) by CBUAE.	U	Address not verified for domestic transaction. Issuer is not an AVS participant, or AVS data was present in the request but issuer did not return an AVS result, There was no address record on file for this account.	W	Not applicable. If present, replaced with Z by CBUAE.	X	Not applicable. If present, replaced with Y by CBUAE.	Y	Street address and postal code match.	Z	Postal/ZIP matches; street address does not match or street address not included in request.
Code	Definition																																				
A	Address matches, ZIP does not. Acquirer rights not implied.																																				
B	Street addresses match. Postal code not verified due to incompatible formats. (Acquirer sent street address and postal code.)																																				
C	Street address and postal code not verified due to incompatible formats. (Acquirer sent street address and postal code.)																																				
D	Street addresses and postal codes match.																																				
F	Street address and postal code match. Applies to U.K.-issued cards.																																				
G	Address information not verified for international transaction. Issuer is not an AVS participant, or AVS data was present in the request, but issuer did not return an AVS result, there was no address record on file for this account.																																				
I	Address information not verified.																																				
M	Street address and postal code match.																																				
N	No match. Acquirer sent postal/ZIP code only, or street address only, or postal code and street address. Also used when acquirer requests AVS but sends no AVS data in field 123.																																				
P	Postal code match. Acquirer sent postal code and street address, but street address not verified due to incompatible formats.																																				
R	Retry: System unavailable or timed out																																				
S	Not applicable. If present, replaced with U (for domestic) or G (for international) by CBUAE.																																				
U	Address not verified for domestic transaction. Issuer is not an AVS participant, or AVS data was present in the request but issuer did not return an AVS result, There was no address record on file for this account.																																				
W	Not applicable. If present, replaced with Z by CBUAE.																																				
X	Not applicable. If present, replaced with Y by CBUAE.																																				
Y	Street address and postal code match.																																				
Z	Postal/ZIP matches; street address does not match or street address not included in request.																																				

44.2—CVV/iCVV Results Code (requests and responses) - 1 Byte

Code indicating Card Verification Value (CVV), iCVV

(Integrated Chip Card CVV), or dCVV (dynamic CVV) verification results. When acquired as a contactless transaction, the field may contain the Online Card Authentication Method (Online CAM) results. The system assumes that the data used for authentication is from the chip and not the magnetic stripe.

Code	Definition
Blank) or not present	CVV, iCVV, or dCVV was not verified.
1	CVV, iCVV, dCVV, or Online CAM failed verification, or Offline PIN authentication was interrupted.
2	CVV, iCVV, dCVV, or Online CAM passed verification.
3	Transaction passed CVV, Emergency Replacement Card (ERC) service value only, Which is used exclusively by the Global Customer Assistance Service (GCAS).

44.3—Card Authentication Results Code (1 byte)

Code to indicate Online CAM results.

Code	Definition
Blank) or not present	Online CAM was not performed, or some other situation or problem prevented Verification. For example, issuer is not participating in Online CAM, or a system or Cryptographic error occurred.
1	The Authorization Request Cryptogram (ARQC) was checked but failed verification
2	The ARQC was checked and passed verification

44.4—CVM Requirement for PIN-less (1 Byte)

Informs acquirers of the Cardholder Verification Method (CVM) requirement For PIN-less transactions.

Code	Definition
0	No CVM required.
1	Signature prompt required.

44.6—Reserved (2 Bytes)**44.7—Reserved (2 byte)****44.8—Reserved (2 byte)****44.9—Reserved (1 byte)**

	44.10—Reserved (1 byte) 44.11—Reserved (1 byte) 44.12 – Reserved (1 byte) 44.13 – Reserved (1 byte)
Field Edits	This data element should be present in all response messages
Constraints	Assigned by the issuer
Validation	This field should be of this format.
Compliance	NA
Presence	Optional. Reserved for Future Use

7.29 DE-47, Additional Data, National

Variant/Key Block Format

Type	ANS			
Format	TLV Format			
Description	This element carries information that identifies the new key value in reference to key exchange transaction.			
	TAG	Length	Format	Content of Sub-Element
	01	032...999	AN	New Key Value
	02	006...099	AN	Contains check digit value
	03	001	N	Key Type 1: Acquirer Working Key 2: Issuer Working Key
	04	002	N	Key Sequence Number to be changed 01: First Sequence 02: Second Sequence 03: Third Sequence
	Please review 13.7.3. Key Exchange TLV format Variant Please review 13.7.4. Key Exchange TLV format Key Block			
Field Edits	This remains same for a transaction.			
Constraints	When present this should not be echoed back in a response.			
Validation	This field should be of this format.			
Compliance	NA			
Presence	Mandatory- in Key Exchange messages 0800 – Network management request (Key Exchange)			
	Note: Both Variant and key block will be supported in same tag <01>			

7.30 DE-48, POS retailer Data

Type	AN..27		
Format	LLVAR		
Description	This element carries information that identifies the retailer involved in the transaction.		
	Position	Length	Description
	01 -19	19	Retailer ID - the ID of the retailer initiating the Transaction.
	20-23	4	Retailer Group - the group to which the retailer belongs.
	24-27	4	Retailer Region - code that indicates the region of the Retailer initiating the transaction.
Field Edits	This remains the same for a transaction.		
Constraints	When present this should be echoed back in a response.		
Validation	This field should be of this format.		
Compliance	NA		
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request / Response 0200/0210 – POS Financial Request / Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420//0421/0430– POS Reversal Request/Repeat		

7.31 DE-49, Transaction Currency Code

Type	N3
Format	Fixed
Description	3-digit code that identifies the currency of the source location of the transaction For example: - 784: United Arab Emirates Dirham
Field Edits	This remains same for a particular transaction.
Constraints	It is echoed in response.
Validation	The currency code should be from the standard list.
Compliance	Must be present if DE-4 is present. The values should remain same during the complete transaction cycle. For UAE Acquirers: Value to be set a 784 For GCC Acquirers: The scheme will set the value as 784 (AED). For International Bilateral Transactions: The value should be set to the acquirer's local currency code.
Presence	Mandatory for the below messages 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – ATM & POS Reversal Request/Repeat/Response

7.32 DE-50, Currency Code, Settlement

Type	N3
Format	Fixed
Description	3-digit code that identifies the currency of the source location of the transaction 784: United Arab Emirates Dirham
Field Edits	This remains same for a particular transaction.
Constraints	It is echoed in response.
Validation	The currency code should be from the standard list.
Compliance	Value to be set a 784
Presence	Mandatory for the below messages 0100/0200/0400/0401/0420/0421/0110/0210/0410/0430 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response

7.33 DE-51, Currency Code, Cardholder Billing

Type	N3
Format	Fixed
Description	Cardholder account currency code
Field Edits	- Used where the billing currency is different from the transaction currency. - If not present, it is assumed that the two currencies are the same - Data will be set by the Switch - Issuer might optionally insert it in the response message
Constraints	When present, it should be echoed in response
Validation	Amount should be only in numeric
Compliance	DE-6, DE-10, DE-51 will be present
Presence	Conditional-This field is present across the messages where billing currency is different from the transaction currency. 0100/0110 – POS Authorization Request/Response 0200/0210 – POS Financial Request/Response 0400/0401/0410/0420/0421/0430 – POS Reversal Request/Repeat/Response

7.34 DE-52, Personal Identification Number (PIN) Data

Type	B16
Format	Fixed, ANSI format
Description	- The block of data containing encrypted PIN block. PIN should be encrypted as a block of 16 hexadecimal digits. - Mandatory for all EMV and fallback pin-based transactions. - Optional for Mag-Stripe POS transactions
Field Edits	This remains same for a particular transaction. For a reversal message this field is not required. For Mag-Stripe POS transaction without pin this field is optional
Constraints	This is not echoed in response.
Validation	This field should be of this format.
Compliance	The values should be in Standard ANSI DES format.
Presence	Mandatory-Should be present in the following messages which is transporting PIN as authentication mechanism. 0100 – POS Authorization Request 0200 – ATM &POS Financial Request

7.35 DE-53, Security Related Control Information

Type	N16		
Format	Fixed		
Description	This element carries information required by the issuer to process PIN based transactions.		
	<i>Position</i>	<i>Length</i>	<i>Description</i>
	01 -02	2	Security Format: Zone encryption Value 20.
	03-04	1	PIN Encryption Algorithm Identifier: ANSI DES Value 01
	05-06	1	PIN Block Format Code In outgoing requests, this field describes the PIN block format used by the acquirer center. In incoming requests, it describes the PIN block format used by the issuer center. Value: 01
	07-08	1	Working Key Sequence Number In request messages from the acquirer to UAESWITCH this specifies the key sequence number of the AWK. In request messages from UAESWITCH to the issuer this specifies the key sequence number of the IWK. Values: 01 / 02 /03
	09-10	1	Future Use Values: 0
	11-16	7	Future Use Values: Zeros
Field Edits	This remains same for a transaction.		
Constraints	When present this should not be echoed back in a response.		
Validation	This field should be of this format.		
Compliance	UAESWITCH will perform PIN block transaction between the Acquirer Working Key (AWK) and the Issuer Working Key (IWK)		
Presence	Mandatory-Should be present in the following messages which is transporting PIN as authentication mechanism 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response		

7.36 DE-54, Additional Amounts

Type	AN...20
Format	LLVAR
Description	This DE contains amount used in several types of transactions such as purchase with cashback and Partial authorization. For purchase with cashback, - Acquirer should populate this in request and the same should echo back by issuer in response - For e.g., A purchase with cashback transaction with cashback amount of 100 would be: 0C000000010000 For Partial Auth, - Issuer should populate this Field in response - For Partial Authorization transaction, Approved amount by Issuer would present in DE4 and actual amount would present in DE54 - Format 0C000000010000
Field Edits	None
Constraints	If present in a request this is to be echoed in a response.
Validation	Additional amount should be of this format as given in the description.
Compliance	For a purchase with a cashback transaction this field should contain the cash amount, and value should be less than the transaction amount in DE-4. For partial authorization, issuer will populate DE-54 with the original transaction amount
Presence	Mandatory for the below messages 0100/0110 – Authorization Request/Response (Partial authorization /POS Cashback) 0200/0210 – Financial Request/Response (Partial authorization /POS Cashback)

Please review the following sections

- 12.7 Partial Authorization
- 12.8 Purchase with Cashback
- 12.X.X.X Merchant Initiated Transactions

7.37 DE-55, ICC System Related Data

Type	B...255								
Format	LLVAR								
Description	This data element is present in full-issuance chip transactions. DE-55 must be 'TLV' encoded and must contain the information (mandatory and optional) as specified in the message layouts (see below). Each element will consist of three sub components, a "Tag", a "Length" and a "Value". The tag and the length are hexadecimal values. <table border="1"> <thead> <tr> <th>Name</th><th>Length (Bytes)</th></tr> </thead> <tbody> <tr> <td>Tag</td><td>1-2</td></tr> <tr> <td>Tag length</td><td>1</td></tr> <tr> <td>Tag Value</td><td>Variable</td></tr> </tbody> </table> This field will contain as many tags as required in the above manner as long as the maximum length of the field does not exceed the maximum permissible limit. The length of DE-55 will be equal to the total length of all the tag-length-value sets. Unexpected EMV Tags: This field may contain tags that the receiving issuer or acquirer does not recognize or does not expect. The receiver must ignore such tags and continue parsing the next tag in DE-55	Name	Length (Bytes)	Tag	1-2	Tag length	1	Tag Value	Variable
Name	Length (Bytes)								
Tag	1-2								
Tag length	1								
Tag Value	Variable								
Field Edits	None								
Constraints	For full chip issuer transactions, - DE-55 will be sent to the issuer in request. - DE-55 may be sent by the issuer in the response. In a 0110/0210 response for a chip transaction UAESWITCH may send TAG 91 with value of '00'. In this case the acquirer switch should accept the 0110/0210 message from UAESWITCH and pass on the contents of bitmap 55 to the terminal In a 0220 completion/financial transaction advice request for a chip transaction, DE-55 can be populated with empty value (no EMV tags). Issuer switch should accept the 0220 request message. In a 0230 completion/financial transaction advice response for a chip transaction, TAG 91 in DE-55 can be populated with value of '00'. Acquirer switch should accept the 0230 response message. For decline transactions if the issuer is not able to generate the ARPC then they should respond with value 00 in Tag 91. For Tokenized transaction, Issuer will not get this field in transaction request. For Remote Pay transactions, if the OEM Pay sends remote payment tags in the EMV data, acquirers are required to populate this information in DE55 when sending the transaction to the UAE Switch. In this case, UCAF data (DE-104 Tag 07) will not be received from the OEM Pay.								
Validation	The tags that are mentioned as mandatory should be present for a chip based transaction.								

UAESWITCH Interface Technical Specifications

Compliance	Mandatory tags should be present in 0100/0200 request mentioned in below table.
Presence	Mandatory-Should be present for card present EMV transactions in the following messages which carry EMV Data 0100/0110 – Authorization Request/Response 0200/0210 – Financial Request/Response 0220/0230 – Pre-Auth Completion

EMV Tag	Tag Name	Length	Format	0100 0200	0110 0210	040X 042X	0410/ 0430	Usage
9F02	Amount Authorized	6	N12	M	-	-	-	Authorized amount of the transaction (excluding adjustments)
9F03	Amount Other	6	N12	M	-	-	-	Mandatory if cash over (cash back) transaction OR if input to application cryptogram
9F26	Application Cryptogram	8	B	M	-	-	-	Cryptogram returned by the ICC in response of the GENERATE AC command
9F06	Application Identifier (AID) – Terminal	5-16	B	O	-	-	-	Identifies the application as described in ISO/IEC 7816-5
82	Application Interchange Profile (AIP)	2	B	M	-	-	-	Indicates the capabilities of the card to support specific functions in the application
9F36	Application Transaction Counter (ATC)	2	B	M	-	-	-	Counter maintained by the application in the ICC (incrementing the ATC is managed by the ICC)
9F07	Application Usage Control	2	B	O	-	-	-	Indicates issuer's specified restrictions on the geographic usage and services allowed for the application
9F27	Cryptogram Information Data (CID)	1	B	M	-	-	-	Indicates the type of cryptogram and the actions to be performed by the terminal
9F34	CVM Results	3	B	O	-	-	-	Indicates the results of the last CVM performed
84	Dedicated File Name	5-16	B	C	-	-	-	Identifies the name of the DF, this needs to be sent if it is available.
9F1E	Interface Device (IFD) Serial Number	8	An8	M	-	-	-	Unique and permanent serial number assigned to the IFD by the manufacturer

UAESWITCH Interface Technical Specifications

EMV Tag	Tag Name	Length	Format	0100 0200	0110 0210	040X 042X	0410/ 0430	Usage
9F10	Issuer Application Data (IAD)	Var. up to 32	b	M	-	-	-	Contains proprietary application data for transmission to the issuer in an online transaction
91	Issuer Authentication Data	8-16	B	-	C	-	-	Data sent back to the ICC as response data for online issuer authentication. Mandatory for online successful transactions OR if any script/s are sent to the card by the issuer
9F5B	Issuer Script Results	Var. Up to 25	B	-	-	-	-	Present if scripts were sent by issuer in original response
71	Issuer Script Template 1	Var. Up to 27	B	-	C	-	-	Contains proprietary issuer data for transmission to the ICC before issuing the second GENERATE AC command. Present if sent by Issuer
72	Issuer Script Template 2	Var. Up to 127	B	-	C	-	-	Contains proprietary issuer data for transmission to the ICC after completion of the second GENERATE AC command. Present if sent by Issuer
9F09	Terminal Application Version Number	2	B	O	-	-	-	Version number assigned for the application
9F33	Terminal Capabilities	3	B	C	-	-	-	Indicates the capabilities of the terminal, like card data input method, CVMs, security functions etc. This field is optional for issuers when the transactions are acquired on GCC terminals
9F1A	Terminal Country Code	2	N3	M	-	-	-	Indicates the country of the terminal, represented according to ISO 3166
9F35	Terminal Type	1	N2	O	-	-	-	Indicates the environment of the terminal, its communications capability, and its operational control
95	Terminal Verification Results (TVR)	5	B	M	-	-	-	Status of the different functions as seen from the terminal
5F2A	Transaction Currency Code	2	N3	M	-	-	-	Indicates the currency code of the -transaction according -to ISO 4217

UAESWITCH Interface Technical Specifications

EMV Tag	Tag Name	Length	Format	0100 0200	0110 0210	040X 042X	0410/ 0430	Usage
9A	Transaction Date	3	n 6 YYMMDD	M	-	-	-	Local date that the transaction was authorized
9F41	Transaction Sequence Counter	2-4	N4-8	O	-	-	-	Counter maintained by the terminal that is incremented by one for each transaction
9C	Transaction Type	1	N2	M	-	-	-	Indicates the type of transaction,
9F37	Unpredictable Number	4	B	M	-	-	-	Random number generated by terminal unique for each transaction.
4F	ICC Application ID	Var (...16)	B	O	-	-	-	ADF name (AID) returned by ICC, as read from directory file, in template 61
DF15	ICC Application ID Service Management info.	2	B	C	-	-	-	Terminal uses this data element in service based transaction in order to advise the card on the request for service i.e., update service data, create a new service area etc.
DF7C	LUC ID	4	B	C	-	-	-	To be used by transaction manager for cryptogram verification. Note: It will not be present in request message to issuer. It will be dropped by transaction manager after cryptogram validation
9F24	PAR	29	B	C	-	-	-	To be present if personalized by Issuer
9F6E	Form Factor Indicator	4-32	N	C	-	-	-	If the form factor is available on the card, merchants/acquirers are required to populate it for all the transactions.
9F19	Token requestor ID	6	N	C	-	-	-	Mandatory for all token-based transactions.
9F25	FPAN suffix	4	N	C	-	-	-	This tag will contain the last 4 digits of the Jaywan FPAN

***Note:** - 'X' is mentioned as '0/1'

7.38 DE-57, EMV System Related Data

Type	N6		
Format	Fixed (EBCDIC)		
Description	EMV System Related Data – Contains the EMV Chip Condition code and the Terminal data.		
	The field structure is as follows:		
	Position	Length	Description
	01-03	3	Value set to 003
	04	1	Terminal Data, valid values are as follows: 3- for Contactless Chip and ICC EMV Reader 4- for Contactless Mag-Stripe 5- for Magnetic Stripe Reader and EMV compatible ICC reader 6- Key Entry only 7- Magnetic Stripe Reader and Key Entry 8- Magnetic Stripe reader, Key Entry and EMV Compatible ICC Reader. 9-EMV Compatible ICC Reader
	05	1	Last EMV Chip Condition Code. 0- Last transaction was from a non-chip card. 1- Last EMV read successful, or was not a chip transaction, or unknown. 2- Last Transaction at the chip capable terminal was unsuccessful.
06	1	Card Authentication Results code. 0- ARQC not checked. 1- ARQC was checked, but failed verification. 2- ARQC was checked and passed verification.	
Field Edits	None		
Constraints	None		
Validation	The tags that are mentioned as mandatory should be present for an EMV chip-based transaction.		
Compliance	Mandatory tags should be present in request mentioned in below table.		
Presence	Mandatory-Should be present in the following messages transporting EMV Data 0100/0110 – POS Authorization Request/Response 0200/0210 – ATM & POS Financial Request/Response		

7.39 DE-60, Additional Data

Type	AN16		
Format	LLVAR		
Description	Terminal Data carries terminal information required for processing. This data element is mandatory in request messages and must be set by the acquirer switch/bank. It is optional to echo back this data in message response. The field structure is as follows:		
	Position	Length	Description
	01-04	4	Terminal owner FIID - identifier of the institution owning the Terminal. Should be set by the acquirer to “0000” since the value will be changed when sending to the issuer.
	05-08	4	Terminal logical network - the logical network in which the terminal is located. Should be set by the acquirer to “0000” since this value will be changed by Switch when sending to the issuer.
	09-12	4	Terminal time offset (PIC S999) - a signed number of minutes to be added to the system time to arrive at the local time of the terminal originating the transaction. Currently, as the components of the Network (Member Bank and systems, are in the same time zone, this should always be set to “+000”.
	13-16	4	Pseudo Terminal ID - (POS only). For POS transactions, this contains a value used to identify the terminal involved.
Field Edits	This remains same for a transaction.		
Constraints			
Validation	This field should be of this format.		
Compliance	NA		
Presence	Mandatory-Should be present in the following messages 0100 – POS Authorization Request (POS Transaction) 0200 – POS Financial Request (POS Transaction) 0220/0230 – POS Authorization Completion Request/Response		

7.40 DE-61, Point of Service Data, Private

Type	AN..255																																		
Format	LLVAR																																		
Description	(Point-of-Service [POS] Data) indicates the conditions that exist at the Point of service at the time of the transaction. Subfield 1 (POS Terminal Attendance) Contents of position 1 DE-61, subfield 1 (POS Terminal Attendance) indicates if the card acceptor is Attending the terminal. <table border="1"> <thead> <tr> <th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>0</td><td>Attended terminal</td></tr> <tr> <td>1</td><td>Unattended terminal (cardholder-activated terminal [CAT], home PC, mobile phone, PDA)</td></tr> <tr> <td>2</td><td>No terminal used (voice/audio response unit [ARU] authorization);</td></tr> <tr> <td>9</td><td>Unknown data</td></tr> </tbody> </table> Subfield 2 (POS Additional Authorization Indicators) Contents of position 2 Subfield 2 (POS Additional Authorization Indicators) indicates additional terminal supported transactions indicator. <table border="1"> <thead> <tr> <th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>0</td><td>Indicates Acquirer doesn't supports partial Authorization</td></tr> <tr> <td>1</td><td>Indicates Acquirer supports partial Authorization</td></tr> </tbody> </table> Subfield 3 (POS Terminal Location) Contents of position 3 DE-61, subfield 3 (POS Terminal Location) indicates the terminal location. <table border="1"> <thead> <tr> <th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>0</td><td>On premises of card acceptor facility</td></tr> <tr> <td>1</td><td>Off premises of card acceptor facility (merchant terminal—remote location)</td></tr> <tr> <td>2</td><td>Off premises of card acceptor facility (cardholder terminal including home PC, mobile phone, and PDA)</td></tr> <tr> <td>3</td><td>No terminal used (voice/ARU authorization); server</td></tr> <tr> <td>4</td><td>On premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA)</td></tr> <tr> <td>6</td><td>Off cardholder premises, unattended (Single Message System Use Only)</td></tr> <tr> <td>8</td><td>Additional POS terminal locations</td></tr> <tr> <td>9</td><td>Unknown data not available (Single Message System Use Only)</td></tr> </tbody> </table> Subfield 4 (POS Cardholder Presence) Contents of position 4 DE-61, subfield 4 (POS Cardholder Presence) indicates whether the cardholder is present at the point of service and explains the condition if the cardholder is not	Value	Description	0	Attended terminal	1	Unattended terminal (cardholder-activated terminal [CAT], home PC, mobile phone, PDA)	2	No terminal used (voice/audio response unit [ARU] authorization);	9	Unknown data	Value	Description	0	Indicates Acquirer doesn't supports partial Authorization	1	Indicates Acquirer supports partial Authorization	Value	Description	0	On premises of card acceptor facility	1	Off premises of card acceptor facility (merchant terminal—remote location)	2	Off premises of card acceptor facility (cardholder terminal including home PC, mobile phone, and PDA)	3	No terminal used (voice/ARU authorization); server	4	On premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA)	6	Off cardholder premises, unattended (Single Message System Use Only)	8	Additional POS terminal locations	9	Unknown data not available (Single Message System Use Only)
Value	Description																																		
0	Attended terminal																																		
1	Unattended terminal (cardholder-activated terminal [CAT], home PC, mobile phone, PDA)																																		
2	No terminal used (voice/audio response unit [ARU] authorization);																																		
9	Unknown data																																		
Value	Description																																		
0	Indicates Acquirer doesn't supports partial Authorization																																		
1	Indicates Acquirer supports partial Authorization																																		
Value	Description																																		
0	On premises of card acceptor facility																																		
1	Off premises of card acceptor facility (merchant terminal—remote location)																																		
2	Off premises of card acceptor facility (cardholder terminal including home PC, mobile phone, and PDA)																																		
3	No terminal used (voice/ARU authorization); server																																		
4	On premises of card acceptor facility (cardholder terminal including home PC, mobile phone, PDA)																																		
6	Off cardholder premises, unattended (Single Message System Use Only)																																		
8	Additional POS terminal locations																																		
9	Unknown data not available (Single Message System Use Only)																																		

Present.

Value	Description
0	Cardholder present
1	Cardholder not present (unspecified)
2	Cardholder not present (mail/facsimile order)
3	Cardholder not present (phone or Automated Response Unit [ARU])
4	Standing order/Recurring Transactions
5	Cardholder not present (Electronic order [home PC, Internet, mobile phone, PDA])
9	Unknown data

Subfield 5 (POS Card Presence) Contents of position 5

DE-61, subfield 5 (POS Card Presence) indicates if the card is present at the point of service.

Value	Description
0	Card present
1	Card not present
9	Unknown data

Subfield 6 (POS Card Retention) Contents of position 6

DE-61, subfield 6 (POS Card Capture Capabilities) indicates whether the terminal has card capture capabilities.

Value	Description
0	Terminal/operator does not have card capture capability
1	Terminal/operator has card capture capability
9	Unknown data

Subfield 7 (POS Transaction Status) Contents of position 7

DE-61, Subfield 7 (POS Transaction Status) indicates the purpose or status of the request.

Value	Description
0	Normal request (original presentment)
1	Deferred authorization
2	Identity check phone order/ MOTO transaction
3	Time based payment authorization request or Subscriptions or Installments
4	Preauthorization request
5	Related/Delayed Charges
6	Incremental Pre-auth/Pre-auth Topup/Incremental Auth
7	Purchase with cash back
8	Account status inquiry service
9	Tokenization request/notification

A	Un Schedule Transactions COF (CIT/MIT)
B	No Show
C	Partial Shipment
D	Resubmissions/Reauthorizations

Subfield 8 (POS Transaction Security) Contents of position 8
DE-61, subfield 8 (POS Transaction Security) indicates the card acceptor’s confidence in the transaction security level.

Value	Description
0	No security concern
1	Suspected fraud
2	Identification verified
9	Unknown Data

Subfield 9 (Reserved for Future Use) Contents of position 9
DE-61, subfield 9 (Reserved) is reserved.

Value
Zero-filled

Subfield 10 (Cardholder-Activated Terminal Level) Contents of position 10
DE-61, subfield 10 (Cardholder-Activated Terminal Level) indicates the type of Cardholder activated terminal used by the cardholder to initiate the transaction.

Value	Description
0	Not a CAT transaction
1	Authorized Level 1 CAT: automated dispensing machine with PIN
2	Authorized Level 2 CAT: self-service terminal
3	Authorized Level 3 CAT: limited amount terminal
4	Authorized Level 4 CAT: in-flight commerce
5	Scrip device
6	Authorized Level 6 CAT: electronic commerce transactions
7	Authorized Level 7 CAT: transponder
8	Reserved for future use
9	MPOS acceptance device

Subfield 11 (POS Card Data Terminal Input Capability) Contents of position 11
DE-61, subfield 11 indicates the set of methods supported by the terminal for the input of account number, card, or mobile device data.

Value	Description
0	Input capability unknown or unspecified
1	No terminal used (voice/ARU authorization); server
2	Terminal supports magnetic stripe input only

	3	Terminal supports contactless EMV input. The terminal may also support one or more other card input types, including contactless mag-stripe input, EMV contact chip input, magnetic stripe input and key Entry input.	
	4	Contactless mag stripe (proximity chip) Terminal supports contactless Mag-Stripe input but not contactless EMV input. The terminal also may support one or more other card input types, including EMV contact chip input, magnetic stripe input, and key Entry input.	
	5	Terminal supports EMV contact chip input and magnetic stripe input.	
	6	Terminal supports key entry input only	
	7	Terminal supports magnetic stripe input and key entry input	
	8	Terminal supports EMV contact chip input, magnetic stripe input and Key entry input.	
	9	Terminal supports EMV contact chip input only.	
	Subfield 12 (POS Postal Code [or Sub-Merchant Information, if applicable]) Contents of position (12 -21)		
	DE-61, subfield 12 (POS Postal Code) indicates the geographic code of the POS (Merchant) location (not the acquirer’s location).		
	<table><tr><th>Value</th></tr><tr><td>Subfield 12 must be present if postal codes are available in the acquiring country. If data is unknown or unavailable, acquirers may populate this field with the value UNKNOWN, all nines, or all zeros followed by trailing spaces.</td></tr></table>		Value
Value			
Subfield 12 must be present if postal codes are available in the acquiring country. If data is unknown or unavailable, acquirers may populate this field with the value UNKNOWN, all nines, or all zeros followed by trailing spaces.			
Field Edits	This remains same for a transaction.		
Constraints	Should be echoed back in a response.		
Validation	This field should be of this format.		
Compliance	NA		
Presence	Mandatory-Should be present in the following messages 0100/0110 – POS Authorization Request/Response (POS Transaction) 0200/0210 – POS Financial Request/Response (POS Transaction) 0220/0230 – POS Authorization Completion Request/Response 0400/0401/0410/0420/0421/0430 – POS Reversal Request/Repeat/Response		

Please review the following sections

- 12.4 Purchase
- 12.5 Pre-Authorization & Pre-Authorization completion
- 12.7 Partial Authorization
- 12.8 Purchase with Cashback
- 12.3 Tokenization
- 12.4 Ecommerce
- 12.5 MOTO
- 12.12 MIT/Recurring Transactions

7.41 DE-63, Network Data , Private

Type	ANS																												
Format	TLV format (Max 255 bytes)																												
Description	DE-63 is a private-use field for various kinds of authorization message information. Identifying the acquirer's network ID is a primary use of this field, which is also used for various reason codes. <table border="1"> <thead> <tr> <th>TAG</th><th>Length</th><th>Value</th><th>Format</th><th>Content of Sub-Element</th></tr> </thead> <tbody> <tr> <td>01</td><td>4</td><td>Preauthorization Time Limit</td><td>AN</td><td>It's an optional field set by issuer in POS preauthorization response. Acquirer can use this value to manage the settlement process more effectively. IF issuer not responded with any value, country policy is taking into consideration for settlement process.</td></tr> <tr> <td>02</td><td>15</td><td>Transaction Identifier</td><td>AN</td><td>This field is using for PREAUTHORIZATION/INCREMENTAL AUTHORISATION and any DMS transaction request. This field value should be populated from original pre-authorization response</td></tr> <tr> <td>03</td><td>29</td><td>Token PAR</td><td>ANS</td><td>Payment Account Reference for Tokenized transaction. This tag may be present in response message to Acquirer.</td></tr> <tr> <td>04</td><td>3</td><td>Function Code</td><td>N</td><td>In case of Financial Transaction Advice, the function code represents the nature of the transaction. 260- Offline Presentment (Without Auth) 263- Offline Refund (Without Auth) 200- Presentment (With Auth) 262- Refund (With Auth)</td></tr> </tbody> </table>				TAG	Length	Value	Format	Content of Sub-Element	01	4	Preauthorization Time Limit	AN	It's an optional field set by issuer in POS preauthorization response. Acquirer can use this value to manage the settlement process more effectively. IF issuer not responded with any value, country policy is taking into consideration for settlement process.	02	15	Transaction Identifier	AN	This field is using for PREAUTHORIZATION/INCREMENTAL AUTHORISATION and any DMS transaction request. This field value should be populated from original pre-authorization response	03	29	Token PAR	ANS	Payment Account Reference for Tokenized transaction. This tag may be present in response message to Acquirer.	04	3	Function Code	N	In case of Financial Transaction Advice, the function code represents the nature of the transaction. 260- Offline Presentment (Without Auth) 263- Offline Refund (Without Auth) 200- Presentment (With Auth) 262- Refund (With Auth)
TAG	Length	Value	Format	Content of Sub-Element																									
01	4	Preauthorization Time Limit	AN	It's an optional field set by issuer in POS preauthorization response. Acquirer can use this value to manage the settlement process more effectively. IF issuer not responded with any value, country policy is taking into consideration for settlement process.																									
02	15	Transaction Identifier	AN	This field is using for PREAUTHORIZATION/INCREMENTAL AUTHORISATION and any DMS transaction request. This field value should be populated from original pre-authorization response																									
03	29	Token PAR	ANS	Payment Account Reference for Tokenized transaction. This tag may be present in response message to Acquirer.																									
04	3	Function Code	N	In case of Financial Transaction Advice, the function code represents the nature of the transaction. 260- Offline Presentment (Without Auth) 263- Offline Refund (Without Auth) 200- Presentment (With Auth) 262- Refund (With Auth)																									
Field Edits																													
Constraints	Transaction id as populated by central operator (UAESWITCH) to be echoed back in response.																												
Validation	This field should be of this format.																												
Compliance	NA																												
Presence	Mandatory-Should be present in the following messages 0100/0110 – Authorization Request/Response (POS/ECOM Transaction) 0200/0210 – Financial Request/Response (POS Transaction) 0220/0230 – POS Authorization Completion Request/Response																												

7.42 DE-66, Settlement Code

Type	N1
Format	Fixed
Description	Code indicating the result of a reconciliation request Value 1: In Balance 2: Out of Balance 3: Error
Field Edits	This remains same for a particular transaction.
Constraints	It is echoed in response.
Validation	This field should be of this format.
Compliance	Value set as indicated
Presence	Mandatory-Should be present in the following messages 0510 – Acquirer Reconciliation response 0512 – Issuer Reconciliation response

7.43 DE-70, Network Management Information Code

Type	N3
Format	Fixed
Description	Code to identify network status the result of a reconciliation request Value 001: Logon 002: Logoff 101: Key Change 201: Cutoff 301: Echo Test
Field Edits	This remains same for a particular transaction.
Constraints	It is echoed in response. 0801 Network Management request repeat is only used for cutoff transactions
Validation	
Compliance	Value to be set as indicated
Presence	Mandatory-Should be present in the following messages 0800/0810 – Network Management Request/Response 0801/0810 – Network Management Repeat/Response (cutoff)

7.44 DE-74, Credits, Number

Type	N			
Format	TLV format (Max length 999 bytes)			
Description	Contains the sum number of all credit transactions processed by the bank since the last business day cutover.			
	TAG	Length	Format	Content of Sub-Element
	01	010	N	For ATM
	02	010	N	For POS
	03	010	N	Others
	Please review 13.7.3.TLV Format DE-74, DE-75, DE-76, DE-77, DE-80			
Field Edits	This remains same for a particular transaction.			
Constraints	It is echoed in response.			
Validation	This field should be of this format.			
Compliance	It is also required in 0510/0512 responses whenever the value of settlement Code (DE-66) is "2" or "3".			
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response			

7.45 DE-75, Credits , Reversals Number

Type	N																			
Format	TLV format (Max length 999 bytes)																			
Description	Contains the sum number of all reversal credit transactions processed by the bank since the last business day cutover. <table><tr><th>TAG</th><th>Length</th><th>Format</th><th>Content of Sub-Element</th></tr><tr><td>01</td><td>010</td><td>N</td><td>For ATM</td></tr><tr><td>02</td><td>010</td><td>N</td><td>For POS</td></tr><tr><td>03</td><td>010</td><td>N</td><td>Others</td></tr></table> Please review 13.7.3.TLV Format DE-74, DE-75, DE-76, DE-77, DE-80				TAG	Length	Format	Content of Sub-Element	01	010	N	For ATM	02	010	N	For POS	03	010	N	Others
TAG	Length	Format	Content of Sub-Element																	
01	010	N	For ATM																	
02	010	N	For POS																	
03	010	N	Others																	
Field Edits	This remains same for a particular transaction.																			
Constraints	It is echoed in response.																			
Validation	This field should be of this format.																			
Compliance	It is also required in 0510/0512 responses whenever the value of settlement Code (DE-66) is "2" or "3".																			
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response																			

7.46 DE-76, Debits, Number

Type	N																			
Format	TLV format (Max length 999 bytes)																			
Description	Contains the sum number of all debit transactions processed by the bank since the last business day cutover. <table><tr><th>TAG</th><th>Length</th><th>Format</th><th>Content of Sub-Element</th></tr><tr><td>01</td><td>010</td><td>N</td><td>For ATM</td></tr><tr><td>02</td><td>010</td><td>N</td><td>For POS</td></tr><tr><td>03</td><td>010</td><td>N</td><td>Others</td></tr></table> Please review 13.7.3.TLV Format DE-74, DE-75, DE-76, DE-77, DE-80				TAG	Length	Format	Content of Sub-Element	01	010	N	For ATM	02	010	N	For POS	03	010	N	Others
TAG	Length	Format	Content of Sub-Element																	
01	010	N	For ATM																	
02	010	N	For POS																	
03	010	N	Others																	
Field Edits	This remains same for a particular transaction.																			
Constraints	It is echoed in response.																			
Validation	This field should be of this format.																			
Compliance	It is also required in 0510/0512 responses whenever the value of settlement Code (DE-66) is "2" or "3".																			
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response																			

7.47 DE-77, Debits, Reversal Number

Type	N																			
Format	TLV format (Max length 999 bytes)																			
Description	Contains the sum number of all reversal debit transactions processed by the bank since the last business day cutover. <table><tr><th>TAG</th><th>Length</th><th>Format</th><th>Content of Sub-Element</th></tr><tr><td>01</td><td>010</td><td>N</td><td>For ATM</td></tr><tr><td>02</td><td>010</td><td>N</td><td>For POS</td></tr><tr><td>03</td><td>010</td><td>N</td><td>Others</td></tr></table> Please review 13.7.3.TLV Format DE-74, DE-75, DE-76, DE-77, DE-80				TAG	Length	Format	Content of Sub-Element	01	010	N	For ATM	02	010	N	For POS	03	010	N	Others
TAG	Length	Format	Content of Sub-Element																	
01	010	N	For ATM																	
02	010	N	For POS																	
03	010	N	Others																	
Field Edits	This remains same for a particular transaction.																			
Constraints	It is echoed in response.																			
Validation	This field should be of this format.																			
Compliance	It is also required in 0510/0512 responses whenever the value of settlement Code (DE-66) is "2" or "3".																			
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response																			

7.48 DE-80, Inquires, Number

Type	N																
Format	TLV format (Max length 999 bytes)																
Description	Contains the sum number of all balance enquiry transactions processed by the bank since the last business day cutover. <table><tr><th>TAG</th><th>Length</th><th>Format</th><th>Content of Sub-Element</th></tr><tr><td>01</td><td>010</td><td>N</td><td>For ATM</td></tr><tr><td>02</td><td>010</td><td>N</td><td>For POS</td></tr><tr><td>03</td><td>010</td><td>N</td><td>Others</td></tr></table> Please review 13.7.3.TLV Format DE-74, DE-75, DE-76, DE-77, DE-80	TAG	Length	Format	Content of Sub-Element	01	010	N	For ATM	02	010	N	For POS	03	010	N	Others
TAG	Length	Format	Content of Sub-Element														
01	010	N	For ATM														
02	010	N	For POS														
03	010	N	Others														
Field Edits	This remains same for a particular transaction.																
Constraints	It is echoed in response.																
Validation	This field should be of this format.																
Compliance	It is also required in 0510/0512 responses whenever the value of settlement Code (DE-66) is "2" or "3".																
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response																

7.49 DE-86, Credits ,Amount

Type	N			
Format	TLV format (Max length 999 bytes)			
Description	Contains the sum number of all approved credit transactions processed by the bank since the last business day cutover.			
	TAG	Length	Format	Content of Sub-Element
	01	016	N	For ATM
	02	016	N	For POS
	03	016	N	Others
Please review 13.7.4.TLV Format DE-86, DE-87, DE-88, DE-89				
Field Edits	This remains same for a particular transaction.			
Constraints	It is echoed in response.			
Validation	This field should be of this format.			
Compliance	It is also required in 0510/0512 responses whenever the value of settlement Code (DE-66) is "2" or "3".			
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response			
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response			

7.50 DE-87, Credits , Reversal Amount

Type	N																
Format	TLV format (Max length 999 bytes)																
Description	Contains the sum amount of all reversal credit transactions processed by the bank since the last business day cutover. <table><thead><tr><th>TAG</th><th>Length</th><th>Format</th><th>Content of Sub-Element</th></tr></thead><tbody><tr><td>01</td><td>016</td><td>N</td><td>For ATM</td></tr><tr><td>02</td><td>016</td><td>N</td><td>For POS</td></tr><tr><td>03</td><td>016</td><td>N</td><td>Others</td></tr></tbody></table> Please review 13.7.4.TLV Format DE-86, DE-87, DE-88, DE-89	TAG	Length	Format	Content of Sub-Element	01	016	N	For ATM	02	016	N	For POS	03	016	N	Others
TAG	Length	Format	Content of Sub-Element														
01	016	N	For ATM														
02	016	N	For POS														
03	016	N	Others														
Field Edits	This remains same for a particular transaction.																
Constraints	It is echoed in response.																
Validation	This field should be of this format.																
Compliance	It is also required in 0510/0512 responses whenever the value of settlement Code (DE-66) is "2" or "3".																
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response																

7.51 DE-88, Debits, Amount

Type	N			
Format	TLV format (Max length 999 bytes)			
Description	Contains the sum number of all approved debit transactions processed by the bank since the last business day cutover.			
	TAG	Length	Format	Content of Sub-Element
	01	016	N	For ATM
	02	016	N	For POS
	03	016	N	Others
Please review 13.7.4.TLV Format DE-86, DE-87, DE-88, DE-89				
Field Edits	This remains same for a particular transaction.			
Constraints	It is echoed in response.			
Validation	This field should be of this format.			
Compliance	It is also required in 0510/0512 responses whenever the value of settlement Code (DE-66) is "2" or "3".			
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response			
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response			

7.52 DE-89, Debits, Reversal Amount

Type	N			
Format	TLV format (Max length 999 bytes)			
Description	Contains the sum amount of all reversal debit transactions processed by the bank since the last business day cutover.			
	TAG	Length	Format	Content of Sub-Element
	01	016	N	For ATM
	02	016	N	For POS
	03	016	N	Others
	Please review 13.7.4.TLV Format DE-86, DE-87, DE-88, DE-89			
Field Edits	This remains same for a particular transaction.			
Constraints	It is echoed in response.			
Validation	This field should be of this format.			
Compliance	It is also required in 0510/0512 responses whenever the value of settlement Code (DE-66) is "2" or "3".			
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response			

7.53 DE-90, Original Data Element

Type	N42												
Format	Fixed												
Description	Contains information for tracking the current message back to prior messages for same cardholder transaction. <table border="1"> <thead> <tr> <th>Position</th><th>Description</th></tr> </thead> <tbody> <tr> <td>1-4</td><td>Original message type</td></tr> <tr> <td>5-10</td><td>Original STAN number DE 11 data from original request</td></tr> <tr> <td>11-20</td><td>Original Transmission date and time DE-7 from original request</td></tr> <tr> <td>21-31</td><td>Original acquirer ID DE-32 from original request</td></tr> <tr> <td>32-42</td><td>Original forwarding institution id Set to all zeros</td></tr> </tbody> </table>	Position	Description	1-4	Original message type	5-10	Original STAN number DE 11 data from original request	11-20	Original Transmission date and time DE-7 from original request	21-31	Original acquirer ID DE-32 from original request	32-42	Original forwarding institution id Set to all zeros
Position	Description												
1-4	Original message type												
5-10	Original STAN number DE 11 data from original request												
11-20	Original Transmission date and time DE-7 from original request												
21-31	Original acquirer ID DE-32 from original request												
32-42	Original forwarding institution id Set to all zeros												
Field Edits	This remains same for a particular transaction. For reversal, this field is required.												
Constraints	If present this is to be echoed in response as well.												
Validation	Original data elements should be of this format as described in the description. If DE-90 is absent in request /not matching with the original transaction then the transaction will not be sent to the issuer.												
Compliance	Values in this field should match with the original transaction and use for matching purpose.												
Presence	Mandatory-Should be present in the following messages 0400/0401/0410/0420/0421/0430 – ATM & POS Reversal Request/Repeat/Response												

7.54 DE-95, Replacement Amounts

Type	N42										
Format	Fixed										
Description	Contains the new actual amount data elements that are necessary to perform a partial reversal on a financial transaction. <table border="1"> <thead> <tr> <th>Position</th><th>Description</th></tr> </thead> <tbody> <tr> <td>01-12</td><td>Actual amount transaction Contains the actual amount of the customer transaction</td></tr> <tr> <td>13-24</td><td>Actual amount, settlement Set to zeros</td></tr> <tr> <td>25-33</td><td>Actual amount, transaction fee Set to zeros</td></tr> <tr> <td>34-42</td><td>Actual amount, settlement fee Set to zeros</td></tr> </tbody> </table>	Position	Description	01-12	Actual amount transaction Contains the actual amount of the customer transaction	13-24	Actual amount, settlement Set to zeros	25-33	Actual amount, transaction fee Set to zeros	34-42	Actual amount, settlement fee Set to zeros
Position	Description										
01-12	Actual amount transaction Contains the actual amount of the customer transaction										
13-24	Actual amount, settlement Set to zeros										
25-33	Actual amount, transaction fee Set to zeros										
34-42	Actual amount, settlement fee Set to zeros										
Field Edits	This remains same for a particular transaction. For reversal, this field is required.										
Constraints	If present this is to be echoed in response as well.										
Validation	Original data elements should be of this format as described in the description. If DE-90 is absent in request /not matching with the original transaction then the transaction will not be sent to the issuer.										
Compliance	Will only be present when the reversal transaction is for an amount other than the original transaction amount (DE-4). Not present in full reversal transaction										
Presence	Mandatory-Should be present in the following messages 0400/0401/0410 – Reversal Request/Repeat/Response (Partial Reversal)										

7.55 DE-97, Amount, Net Settlement

Type	N16
Format	Fixed
Description	Contains the value of all gross amounts The value of this field is calculated using the other reconciliation amount fields as follows: $\text{Net Settlement Amount} = (\text{Credit Amount} + \text{Reversal Credit Amount}) \text{ minus } (\text{Debit Amount} + \text{Reversal Debit Amount}).$
Field Edits	This remains same for a particular transaction.
Constraints	It is echoed in response.
Validation	This field should be of this format.
Compliance	If the resulting value is zero or positive it should be preceded by the character "C" (credit) otherwise, it should be preceded by the character "D" (debit). The amount following the sign character should be all numeric.
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response

7.56 DE-99, Settlement Institution Identification Code

Type	N..11
Format	LLVAR
Description	Contains the code identifying the settlement institution
Field Edits	This remains same for a particular transaction.
Constraints	It is echoed in response.
Validation	This field should be of this format.
Compliance	
Presence	Mandatory-Should be present in the following messages 0500//0501/0510 – Acquirer Reconciliation request/repeat/response 0502//0503/0512 – Issuer Reconciliation request/repeat/response

7.57 DE-100, Receiving Institution Identification Code

Type	N..11												
Format	LLVAR												
Description	Receiving Institution Identification Code identifies the institution receiving a request message. This element is mandatory for 0110, 0210, 0400, 0401, 0420, and 0421 messages. It will be set by the issuer to appropriate value. In 0400, 0401, 0420 messages, the Receiving Institution Identification Code is copied from the 0110/0210 message. <table><thead><tr><th>Position</th><th>Length</th><th>Description</th></tr></thead><tbody><tr><td>01-02</td><td>2</td><td>Length Indicator</td></tr><tr><td>03-05</td><td>3</td><td> Country Code - The country code where the Card Issuer is located. Few examples are: Bahrain - 048 Oman - 512 Kuwait - 414 Qatar - 634 Saudi Arabia - 682 United Arab Emirates – 784 Other country code can be expected in this field. Acquirer shouldn't decline the transaction for values that are not present in the specification </td></tr><tr><td>06-13</td><td>8</td><td>Institution Code (Switch or Bank) - The value of this code is decided by the Issuer Participant</td></tr></tbody></table>	Position	Length	Description	01-02	2	Length Indicator	03-05	3	Country Code - The country code where the Card Issuer is located. Few examples are: Bahrain - 048 Oman - 512 Kuwait - 414 Qatar - 634 Saudi Arabia - 682 United Arab Emirates – 784 Other country code can be expected in this field. Acquirer shouldn't decline the transaction for values that are not present in the specification	06-13	8	Institution Code (Switch or Bank) - The value of this code is decided by the Issuer Participant
Position	Length	Description											
01-02	2	Length Indicator											
03-05	3	Country Code - The country code where the Card Issuer is located. Few examples are: Bahrain - 048 Oman - 512 Kuwait - 414 Qatar - 634 Saudi Arabia - 682 United Arab Emirates – 784 Other country code can be expected in this field. Acquirer shouldn't decline the transaction for values that are not present in the specification											
06-13	8	Institution Code (Switch or Bank) - The value of this code is decided by the Issuer Participant											
Field Edits	For reversal, this field is required.												
Constraints	It will be set by the issuer to appropriate value.												
Validation	In 0420 messages, the Receiving Institution Identification Code is copied from the 0210 message.												
Compliance	Value to be set by issuer												
Presence	Mandatory-Should be present in the following messages 0110 – Authorization Response (POS transaction) 0210 – Financial Response (POS transaction) 0220/0230 – Authorization Completion Request/Response 0400/0401/0420/0421 – Not required in reversal Message												

7.58 DE-104, Additional data – Payment Services

Please find the below additional data

Type	ANS..999					
Format	LLLVAR					
Description	Tag	Type & Length (LLVAR)	Description	Comments		
	01	N3	CVD2	CVD2 value		
	02	A1	CVD2 Match Code	CVD2 match Code M- CVD2 matched N – CVD2 unmatched U – CVD2 match not done		
	03	N2	ECOM Indicators	05 — Secure Ecommerce with 3D Secure 06 — Not authenticated security transaction. Merchant attempted to authenticate using 3D secure. 07 — Non-authenticated Security Transaction. 08 — Non secure transaction		
	04	ANS..99	CAVV DATA	Position	Field Name	Data
				1-2	3-D Secure Authentication Results Code	“00” – Successful Authentication (status Y) “05” – Authentication could not be performed (status U) “07” – Attempt Processed by ICS ACS “08” –Attempt Processed by ICS DS “09” – Authentication failed (status N)
				3-4	Second Factor Authentication Results Code	• 01 = Static Passcode • 02 = SMS OTP • 03 = Key fob or EMV card reader OTP • 04 = App OTP • 05 = OTP Other • 06 = KBA • 07 = OOB Biometrics • 08 = OOB Login • 09 = OOB Other • 10 = Other • 11 = Push Confirmation • 12 = Decoupled • 98 = EMV 3DS Attempt • 99 = Frictionless

				5-6	CAVV Key indicator	01: Issuer CAVV Key Prod 02: Issuer CAVV Key Test 10: DS CAVV Key Prod 11: DS CAVV Key Test
				7-10	CAVV output	CAVV Output computed by ACS or DS A leading zero is required to pad the first unused byte of the CAVV.
				11-14	Unpredictable Number	Last 4 digits of ATN.
				15-30	ATN	16-digit transaction identifier generated by the ACS
				31-34	Reserved	Zero filled
				35-40	Date	YYDDD
	05	A1	CAVV result	CAVV verification result code M- CAVV verified. N – CAVV verification failed U – CAVV verification not done		
	06	AN15	Original Transaction ID	Transaction ID received in DE.63 SF2 from the original response to be sent in case of recurring transactions.		
	07	ANS..28	Token Cryptogram	This field will contain the Token Cryptogram during remote payments and Card on file transactions performed using Jaywan Scheme token		
	09	AN11	Payment Facilitator ID	Payment Facilitator ID sent by acquirer.		
	Field Edits		None.			
Constraints		Present in Online transaction in request.				
Validation		This field should be of this format				
Compliance		Any additional tags received issuers should ignore the additional tags and process without any format error.				
Presence		Conditional-Should be present in the following messages 0200/0210 – POS Manual transactions CVV2 tag may present in Tag 01. 0100/0110 – E-commerce Authorization Request/Response 0100/0110 – Tokenize ASI transactions this field is present Tag 06 – should present for all recurring/installment transactions.				

7.59 DE-105, Token Data

Type	ANS...999			
Format	LLLVAR			
Description	Tag	Type & Length (LLVAR)	Description	Comments
	01	AN19	Token ID	Token Value corresponding to the PAN
	02	N4	Token Expiration Date	Expiry Date for the Token. The date is in yymm format, where yy = year (00–99) and mm = month (01–12).
	03	ANS36	Token Reference ID	Reference ID corresponding to the Token.
	04	ANS..99	Wallet ID	ID allocated for the Particular Wallet Optional for COF based E-com transaction. Mandatory in other scenarios
	05	AN2	Token Type	EC - ECOM/COF (e-commerce/ card on file) SE - secure element HC - cloud-based payment TE – Trusted environment
	06	AN1	Token Status	A - Active for payment I - Inactive for payment (not yet active) S - Temporarily Suspended for payments D - Permanently deactivated for payments
	07	ANS29	Payment Account Reference (PAR)	PAR value populated by the Jaywan TSP system.
	08	ANS11	Token Requestor ID	Contains the assigned Token Requestor ID 08600010001 - Google Pay

				08600010002 - Samsung Pay 08600010003 - Apple Pay 0861XXXXXX – M4M_PAY* * Jaywan will assign a unique token requestor ID for merchants/ COF provisioning with 0861
	09	AN2	TSP Validation Result	01 –Token / Cryptogram Validation Successful 02 – Token / Cryptogram Validation Failed 03 – Token Validation Successful (token cryptogram is absent) 04 – Token Validation Failed (token cryptogram is absent)
	10	AN2	Device Type	Device from which the transaction was initiated as below • 01 - HCE • 02 - SPAY_PHONE • 03 - SPAY_TABLET • 04 - SPAY_WATCH • 05 - SPAY_TV • 06 - IPHONE • 07 - IWATCH • 08 - IPAD • 09 - MAC_BOOK • 10 - ANDROID_PHONE • 11 - ANDROID_TABLET • 12- ANDROID_WATCH • 13 - MOBILE_PHONE • 14 - TABLET • 15 - WATCH • 16 - MOBILE_PHONE_OR_TABLET • 17 - BRACELET • 18 - PC • 19 - HOUSEHOLD • 20 - WEARABLE • 21 - AUTOMOBILE • 22 – REALITY • 23 -- UNKNOWN Optional for COF based E-com transaction. Mandatory in other scenarios
	11	ANS64	Device ID	Contains Device ID
	13	N2	Number of Active Tokens	Number of Tokens Currently Active for this PAN
	14	N2	Number of Inactive Tokens	Number of Token currently Inactive for this PAN

	15	N2	Number of Suspended Tokens	Number of Token currently Suspended for this PAN
	16	N2	User Account Score	A score between 1 and 5 indicating how trustworthy the device user's account is. Five is most trusted. A value of 0 (zero) means that the account was not checked by wallet or wallet owner.
	17	N2	Device Score	A score between 1 and 5 indicating how trustworthy the device is. Five is most trusted. A value of 0 (zero) means that the account was not checked by wallet or wallet owner
	19	ANS16	Device Location	Latitude and longitude coordinates of device location
	20	ANS64	Device IP	Cardholder's device IP address
	21	ANS32	walletProviderId	Wallet Provider identifier, defined by Jaywan TSP. APPLE_PAY: Apple Pay Wallet SAMSUNG_PAY: Samsung Pay Wallet ANDROID_PAY: Google Pay Wallet M4M_PAY : Merchant/COF Provisioning
	22	N2	Token Advice Reason	01. Provision complete notification. 02. State of token changed on device upon lifecycle management request from Issuer. 03. State of token changed on vault upon lifecycle management request from wallet. 04. State of token changed on vault upon lifecycle management request from TSP CSP. 05. Meta data changed
	23	N2	Previous Token State	Possible Values are 01- LINKED(ACTIVE) 02-RESUME 03-SUSPENDEED 04- UNLINKED(Delete)
	24	N2	New Token State	Possible Values are 01-LINKED(ACTIVE) 02-RESUME 03-SUSPENDEED 04- UNLINKED(Delete)
	25	ANS36	Issuer Card Ref ID	Reference ID assigned for each funding pan
	26	ANS15	Merchant ID	ID of the merchant requesting the token Mandatory for Card on file scenarios

	27	ANS45	Merchant Name	Name of the merchant requesting the token Mandatory for Card on file scenarios
	28	ANS45	TR Name	Token requestor name Mandatory for Card on file scenarios
	29	ANS64	MaskedEmail	Masked Email ID of the customer. It will be received if the customer has enabled sharing of information on their mobile device.
	30	N99	provisioningAttemptsOnDeviceIn24Hours	No of Attempts made on 24 Hours Mandatory for token Provision request.
	31	ANS2	WalletAccountCountry	Wallet country code as per ISO-3166-Alpha-2 This field will contain spaces if the token requestor has not provided the information
	32	ANS99	Card holder name	Card holder name on the card Mandatory for Token provision request
	33	N2	levelOfTrust	'01'-'green': good level of trust, no particular ID&V requested. '02' -'yellow': warning, ID&V is required needed. '03' 'orange': suspect a fraud. '04' 'red' : reject the provisioning '99' 'Not Available' if not passed by the token requestor Mandatory for token Provision request.
	34	AN2	reasonCodes	IN CASE OF YELLOW FLOW DESCRIPTION: 01: User Wallet Account ID too new relative to launch. 02: User Wallet Account ID too new relative to provisioning request 03: User Wallet Account ID/Card Pair is newer than date threshold 04: Changes made to account data within date threshold 05: Suspicious transactions linked to this account. 06: The Account has not had activity in the last year. 07: Suspended cards in the secure element

				08: The device was put in lost mode in the last 7 days for longer than the duration threshold 09: The number of provisioning attempts on this device in 72 hours exceeds the threshold 0A: There have been more than the threshold number of different cards attempted at provisioning to this phone in 24 hours. 0B: The card provisioning request contains a distinct name more than the permitted threshold. 0C: Device Score is less than 3 0D: Account Score is less than 4 0E: Device provisioning location outside of OEM marketplace store home country 0F: Model rules not available currently (in cases where back-end systems time out). 0G: Orange path flag 0H: Phone Number Score is less than 3
	36	AN2	deviceCountry	Device country code as per ISO-3166-Alpha-2 Mandatory for token Provision request. This field will contain spaces if the token requestor has not provided the information
	38	N1	walletScore	Wallet Provider Account scoring Mandatory for token Provision request.
	39	ANS32	manufacturer	Device Manufacturer
	40	ANS16	model	Device Model
	41	ANS16	osVersion	Device OS Version
	42	N20	phoneNumber	Mobile number of the card holder
	43	ANS24	IMEI	IMEI Number of the device.
	44	ANS32	Device Platform	ANDROID, IOS, WINDOWS, TIZEN, BLACKBERRY, ANDROID_WEAR, EMBEDDED_OS, OTHER.
	45	N10	otpValue	The OTP value to be send by the issuer to customer.
	46	ANS99	expirationDate	The expiration time for OTP. ex. 2015-05-18T14:40:32.000Z

	47	N2	otpMethodId	01 – SMS 02- Email
	48	ANS99	ID&V method	01 - 'cell_phone': ID&V based on an OTP sent by SMS 02 - 'email': ID&V based on an OTP sent by email 03 - 'bank_app': ID&V managed through the Bank Application 04 - 'outbound_call': ID&V based on an outbound flow, like, for example, weblink 05 - 'customer_service': ID&V based on Cardholder-initiated call to the Bank customer service 06 - 'call': ID&V based on Issuer-initiated voice call to the Cardholder. If we have multiple methods, then it has to be separated with pipe separator ' ' like 01 02.
	49	ANS99	ID&V value	Masked Mobile Number in case ID&V method -01 Masked E-Mail ID in case ID&V method -02 If the methods are multiple, then it has to separate with pipe separator ' '. For example, data should be *****9898 abc*****yz@*****.com
	50	AN19	Replacement PAN	This field is required when the Existing PAN is being replaced with a new PAN.
	51	N4	Replacement Expiry date	This field is required when Card got expired/replaced, it must contain the expiration date for the Existing/new PAN.

UAESWITCH Interface Technical Specifications

	52	N2	PAN Source	This tag, if present, will include one of the following valid values: 01 (Key entered/Manual) 02 (On file) 03 (Mobile banking app) 04 (Camera) 05 (Reader_Mode) 99 (Unknown)
	53	AN15	Card Art Indicator	Unique identifier of the card product associated to the card to digitize.
	54	ANS16	Level Of Trust Standard Version	Version number of standard set applied beginning with 0001.00.
	55	ANS..99	Device Name	Device name that the device owner may use to identify it
	56	ANS3	language	Selected language on the device in ISO 639-3
	57	N1	Tnc Status	T&C acceptance status by end user. Value is "1"(true) if T&C have been accepted, "0"(false) otherwise.
	58	ANS64	Tnc Accepted Date	Date of T&C acceptance by end user in ISO 8601 format YYYY-MM-DDThh:mm:ssTZD Condition: Will be present if 'tncStatus' is true
Field Edits	For any Token based transaction this field should be mandatory. For all other transactions, this field will not be present. For Token based E-Com/SI/SFA transactions, these fields will be received from the acquirer. Same will be forwarded to the issuer only if the issuer is certified to receive token based fields.			
Constraints	None			
Validation	Any additional tags received issuers should ignore the additional tags and process without any format error.			
Compliance	This is mandatory for all Token Based transactions			
Presence	Tag-01 Should be Present in Token Completion notification message Tag-02 Should be Present in Token Completion notification message Tag-04 Should be Present in all Token Based request message except for COF based ECOM/SI transaction. Tag-05 Should be Present in all Token Based request message. Tag-09 Should be Present in all Token Based request message. Tag-10 Should be Present in all Token Based request message except for COF based ECOM/SI transaction. Tag 22 Should be present for all Token LCM messages. Tag 23 Should be present for all Token LCM messages. Tag 24 Should be present for all Token LCM messages. Tag 25 should be present for all SI related token LCM messages Tag 26,27,28 should be present for all card on file LCM messages and authorization messages Tag 50 Should be present for all Token LCM messages.			

	Tag 51 Should be present for all Token LCM messages.
--	--

7.60 DE-115, Additional Trace Data

Type	AN..25
Format	LLVAR
Description	This additional tracing information is provided in outgoing requests and advice at the acquirer's option or by the switch of an acquiring network. The information must be returned unchanged in the related response or advice response, regardless of the number of times its content may change because of the message passing through different networks. This field is not used by issuers. If it is present in a request from an acquirer, its removed t before forwarding the message to the issuer
Field Edits	This remains same for a particular transaction.
Constraints	It is echoed in response.
Validation	This field should be of this format.
Compliance	When present this should be echoed back in a response
Presence	Mandatory-Should be present in the following messages 0100/0110 – Authorization Request/Response 0200/0210 – Financial Request/Response 0400/0401/0410/00420/0421/0430 – Reversal Request/Repeat/Response

7.61 DE-122, Remaining Open to use

Type	AN..25
Format	LLVAR

7.62 DE-123, Address Verification Data

Type	ANS																																
Format	TLV Format (Max 999 bytes)																																
Description	This field description contains Address verification data's which are in TLV format, can have sub-elements. The TLV format is shown below. <table><tr><th>Subfield 1 Length (Byte 2)</th><th>Subfield 2 Verification Data TLV elements (Byte 3-999)</th></tr><tr><td></td><td> Tag Length Value Tag Length Value TLV₁ TLV_N </td></tr></table> <table><tr><th>TAG</th><th>Length</th><th>Value</th><th>Format</th><th>Content of Sub-Element</th></tr><tr><td>C0</td><td>9</td><td>Postal Code</td><td>AN</td><td>A postal/ZIP code, Left-justified. Postal/ZIP codes fewer than 9 alphanumeric characters In length do not require spaces. Numeric-only data is acceptable.</td></tr><tr><td>CF</td><td>40</td><td>Street Address</td><td>AN</td><td>A street address, Left-justified. Street addresses fewer than 40 characters in length Do not require spaces. Alphabetic numbers in street addresses must be converted to numeric equivalents, for Example, "twelve" is 12.</td></tr><tr><td>D0</td><td>14</td><td>Compressed AVS Data</td><td>AN</td><td>This field contains the AVS data for token activation request messages in compressed format based on issuer configuration</td></tr><tr><td>D4</td><td>26</td><td>Cardholder Name</td><td>ANS</td><td>This tag contains the cardholder</td></tr></table>				Subfield 1 Length (Byte 2)	Subfield 2 Verification Data TLV elements (Byte 3-999)		Tag Length Value Tag Length Value TLV₁ TLV_N	TAG	Length	Value	Format	Content of Sub-Element	C0	9	Postal Code	AN	A postal/ZIP code, Left-justified. Postal/ZIP codes fewer than 9 alphanumeric characters In length do not require spaces. Numeric-only data is acceptable.	CF	40	Street Address	AN	A street address, Left-justified. Street addresses fewer than 40 characters in length Do not require spaces. Alphabetic numbers in street addresses must be converted to numeric equivalents, for Example, "twelve" is 12.	D0	14	Compressed AVS Data	AN	This field contains the AVS data for token activation request messages in compressed format based on issuer configuration	D4	26	Cardholder Name	ANS	This tag contains the cardholder
Subfield 1 Length (Byte 2)	Subfield 2 Verification Data TLV elements (Byte 3-999)																																
	Tag Length Value Tag Length Value TLV₁ TLV_N																																
TAG	Length	Value	Format	Content of Sub-Element																													
C0	9	Postal Code	AN	A postal/ZIP code, Left-justified. Postal/ZIP codes fewer than 9 alphanumeric characters In length do not require spaces. Numeric-only data is acceptable.																													
CF	40	Street Address	AN	A street address, Left-justified. Street addresses fewer than 40 characters in length Do not require spaces. Alphabetic numbers in street addresses must be converted to numeric equivalents, for Example, "twelve" is 12.																													
D0	14	Compressed AVS Data	AN	This field contains the AVS data for token activation request messages in compressed format based on issuer configuration																													
D4	26	Cardholder Name	ANS	This tag contains the cardholder																													

					Name.
	01	1	Activation Verification Result	AN	This tag contains one of the following OTP verification result and mobile Banking application code values. 1 = Successfully verified 2 = Verification code expired 3 = Verification code failed 4 = Verification code missing 5 = Verification code retries exceeded
	02	2	Active Account Management Velocity Checking Result	N	This tag contains one of the following AAM Velocity Checking result values. 02 = Time-to-live exceeded 03 = Count exceeded 04 = Amount exceeded
	03	4	Cardholder Verification Methods Identified by Cardholder Device	N, BCD	Contains the following positions in a 4-byte bit map. • Position 1, Unknown • Position 2, None • Position 3, Signature • Position 4, Online PIN • Position 5, Passcode • Position 6, Cardholder device code • Position 7, Fingerprint biometric verified by cardholder device • Position 8, Cardholder device pattern
	04	2	Issuer Special Condition Code	AN	This tag contains an issuer-assigned Value.
	05	1	Card Type Code	AN	C (Credit) D (Debit) P (Prepaid) N (Unknown)

	06	3	Billing Currency Code	AN	Issuer's billing currency code.
	07	1	Billing Currency Code Minor Units	AN	Minor units of the card billing currency.
	08	8	Issuer BID	AN	Recipient issuer business ID.
	09	3	Card Issuer Country Code	AN	Issuer ISO country code.
	10	1	Fast Funds Indicator	N	B (Recipient issuer participates in fast funds for all transactions) C (Reserved for future use) D (Recipient issuer participates in fast funds for domestic transactions only) N (Recipient issuer does not participate in fast funds)
	11	1	Blocked for all OCTs	AN	Y (Issuer is blocked for receiving funds) N (Issuer is not blocked for receiving funds)
	12	1	Online Gambling Block Indicator	AN	Y (Issuer is blocked for receiving gambling payouts) N (Issuer is not blocked for receiving gambling payouts)
	13	1	Geographic Restriction Indicator	AN	Y (Issuer is blocked for receiving cross-border OCTs) N (Issuer is not blocked for receiving cross-border OCTs)
	14	3	Destination Currency Code	AN	Recipient issuer currency code.
	15	1	Destination Currency Code Minor Units	AN	Recipient issuer currency code Minor units.

UAESWITCH Interface Technical Specifications

	16	3	Issuing Institution Country Code	AN	Recipient issuer 3–digit country code.
	17	Reserved for future use			
	18	Reserved for future use			
Field Edits	This remains same for a transaction.				
Constraints	When present this should not be echoed back in a response.				
Validation	This field should be of this format.				
Compliance	NA				
Presence	Mandatory-Should be present in the following messages in case of Address verification service. 0100/0110 – Authorization Request/Response 0200/0210 – Financial Request/Response				

Participants will connect to UAESWITCH system using persistent socket connections. Participant will be responsible to generate the logon message after every successful TCP socket connection.

Size of Length Data	Two bytes A 2-byte header should be prefixed to all messages sent to UAESWITCH. The header is used as an indicator of the length of the TCP/IP stream
Length Inclusive	Yes Above 2-byte header will provide the data length of the ISO message including the 2-byte header. If this option is selected, then a message of 10 bytes and length data of 2 bytes would have a total length of 12 bytes and have the following layout 00 0C 12 34 56 78 90 12 34 56 78 90
Type of connection	UAESWITCH will be SERVER and member bank is CLIENT Member bank will initiate the connection to UAESWITCH System.
Host IP Address	To be defined by the UAESWITCH
Port Number	To be defined by the UAESWITCH and port will be allocated to a bank

For a message of 61 bytes and length data of 2 bytes the total length indicator will be (003F) 63 bytes and have the following layout:

As far as the UAESWITCH is concerned, a session can be considered to exist between the UAESWITCH and a bank if both of the following conditions are satisfied:

- Details of ISO 8583 logon message processing are provided in chapter 4, Transaction Processing.

9. Security Protocol

This chapter describes the security features of the UAESWITCH, which are designed to ensure the security of PIN data passed between banks and the UAESWITCH. This is done by encrypting the PIN entered by the customer prior to transmission through the UAESWITCH network.

Section 6.1, PIN Encryption Scheme, describes how PINs are encrypted/decrypted and maintained within the UAESWITCH network

9.1 PIN ENCRYPTION SCHEME

All PINs passed through the UAESWITCH network will be encrypted in Triple-DES format as follows:

- The PIN entered by the customer will be formed into a PIN block according to ANSI standard X9.8 (which is equivalent to ISO standard DP/9564/1, format 0)
- The PIN block will be encrypted under an encryption key known only to the bank and UAESWITCH.

For each bank, two encryption keys will be used:

- The Issuer Working Key (IWK): used by the UAESWITCH to encrypt the PIN block when sending a transaction to an issuer for authorization
- The Acquirer Working Key (AWK): used by the bank to encrypt the PIN block when sending a transaction to the UAESWITCH for authorization.

Thus, as a transaction passes through the UAESWITCH network, the PIN block must be translated from encryption under the AWK of the acquiring bank to encryption under the IWK of the issuing bank. UAESWITCH will carry out this translation.

As a further security measure, the IWK and AWK for each bank will be changed regularly. The UAESWITCH, without the need for any down time, will do this key change online. All such key changes will be initiated from the UAESWITCH, rather than the Member Banks. In order to secure the new key value as it is transferred from the UAESWITCH to the bank; it is itself encrypted under a further key, known as the Zone Control Master Key (ZCMK). There will be one ZCMK for each Member Bank. The ZCMK will change very rarely, and such a change will require some down time of the link to the Member Bank in question.

9.1.1 ANSI X9.8 PIN Block

The ANSI X9.8 PIN block is a 16 hex digit block containing the result of performing an exclusive OR operation on two blocks of data.

The first block of data is comprised of 16 hex digits, as follows:

C L P P P P F F F F F F F F F F F F

Where:

C	=	A control field (set to zero).
L	=	The length of the PIN (min 4, max 12).
P	=	The PIN digits.
PF	=	PIN digits or hex F filler digits, depending on the PIN length.
F	=	Filler digits, always hex F.

The second block of data is comprised of 16 hex digits, as follows:

0 0 0 0 P1 P2 P3 P4 P5 P6 P7 P8 P9 P10 P11 P12

Where:

0	=	Pad digits. These are always hex 0.
P1-P12	=	the least significant 12 digits of the PAN, not including the check digit.

P12 is the digit before the check digit.

9.1.2 Zone Control Master Keys

There will be one Zone Control Master Key (ZCMK) for each Member Bank. The value of the ZCMK will be chosen by UAESWITCH and notified to the bank.

The method for transmitting the ZCMK from the UAESWITCH to the bank is described below:

- ZCMK component A is randomly generated by the UAESWITCH employee A and sent to Member Bank employee A
- ZCMK component B is randomly generated by the UAESWITCH employee B and sent to Member Bank employee B
- ZCMK component C is randomly generated by the UAESWITCH employee C and sent to Member Bank employee C
- ZCMK components A, B and C are combined at the UAESWITCH to form the ZCMK
- ZCMK components A, B and C are combined at the bank to form the ZCMK.

This method ensures that no one person knows all the information necessary to discover the value of the ZCMK.

9.1.3 Issuer/Acquirer Working Keys

These keys are used to encrypt/decrypt the PIN blocks passed between the UAESWITCH and banks. Each Member Bank will have its own IWKs and AWKs.

These keys will be changed periodically, by exchange of message over the on-line ISO 8583 interface between the bank and the UAESWITCH. UAESWITCH will always initiate this key change. The message flows for these key changes are described in chapter 6, Transaction Processing.

In order to ensure the smooth change over from one IWK (or AWK) to another after a key change, each Member Bank will have three IWKs (AWKs), numbered 1 to 3. At any one time, these can be characterized as:

- The current IWK (AWK), i.e., the one currently in use by UAESWITCH and the bank
- The IWK (AWK) which will be used by UAESWITCH and the bank after the next IWK (AWK) change. The value of this key will have been set up by the previous IWK (AWK) change.
- The IWK (AWK) which will be changed by the next IWK (AWK) change.

In order that the recipient of a message knows which IWK/AWK was used to encrypt the PIN block, field 53, Security Related Control Information, in the message will contain the key sequence number (between 1 and 3). See chapter X, Data Element Descriptions, for further details on use of field 53.

9.1.4 AWK Change Procedure

The procedure for AWK change is as follows. Assume that a bank is currently using AWK N (say 2). AWK N+1 (in this case 3) will already have an agreed value from the previous AWK change. At the next AWK change, UAESWITCH will send a new value for AWK N+2 (in this case 1, since the numbers are cyclic). The new AWK will be generated randomly. At this time, the bank should perform the following operations:

- Validate the new key value
- If validated OK then
 - Store this new value as AWK number N+2 (in this case 1)
 - Make AWK N+1 (in this case 3) the current AWK (i.e., start using AWK 3 in all subsequent transaction requests)
 - Return a zero response code in the 0810 response message
- If not validated OK then
 - Continue to use AWK number N (in this case 2)
 - Return a non-zero response code in the 0810 response message.

9.1.5 IWK Change Procedure

The procedure for IWK change is as follows. Assume that a bank is currently using IWK N (say 2). IWK N+1 (in this case 3) will already have an agreed value from the previous IWK change. At the next IWK change, the UAESWITCH will send a new value for IWK N+2 (in this case 1, since the numbers are cyclic). The new IWK will be generated randomly. At this time, the bank should perform the following operations:

- Validate the new key value
- If validated OK then
 - Store this new value as IWK number N+2 (in this case 1)
 - Make IWK N+1 (in this case 3) the current IWK. (i.e., expect to receive IWK 3 in all subsequent transaction requests) Note that the bank must still accept PINs encrypted under IWK N at this time, since the UAESWITCH may continue to send PINs encrypted under IWK N if, for example, it does not receive the response to key change message.
 - Return a zero response code in the 0810 response message
- If not validated OK then
 - Continue to expect IWK number N (in this case 2)
 - Return a non-zero response code in the 0810 response

9.1.6 IWK/AWK Validation

When a new IWK or AWK is received, the bank should perform the following validation:

- Decrypt the key using the ZCMK
- Check that the clear key value has odd parity. If not, reject the key change with response code 30 (format error)
- Calculate the check digits by encrypting sixteen zeroes with the clear key value. The check digits are the left-most four digits of the result
- Compare the check digits calculated with those received in the key change message. If not equal, then reject the key change with response code 30 (format error).

10. Change of Business Day

The UAESWITCH system is required to calculate the central settlement position between each Member Bank and the UAESWITCH. In order to perform this function, the UAESWITCH will specify the settlement date to be applied to monetary transactions processed through the UAESWITCH network. The UAESWITCH will inform the card issuer of the settlement date that applies to a transaction in field 15 (Date, Settlement) of a request message. Issuer's must return this field in related responses to the acquirer.

Because acquirers and issuers may actually have their customer accounting systems working on different accounting "days", facilities exist for the UAESWITCH to log, for information purposes, an acquirer posting date and an issuer posting date.

UAESWITCH will perform an end-of-day process that extracts transaction data from the UAESWITCH Transaction Log File that banks can use for the following purposes:

- Confirm the transactions received over the on-line link
- Use for reconciling differences detected by the bank itself or as a result of cardholder queries.

In addition to the settlement date contained in field 15, the UAESWITCH system employs the following features:

- A SAF file for forwarding Reversals and Advises, and cutover and reconciliation messages. This is explained in more detail in section 8.3, SAF File, later.
- Settlement (0800 cutover) messages that inform a bank that the UAESWITCH is going to start logging its acquirer transactions to a new UAESWITCH settlement date.
- Delayed sending of reconciliation (05xx) messages to indicate the UAESWITCH totals for approved transactions exchanged during the UAESWITCH settlement date for a bank's "acquirer" traffic and its "issuer" traffic.

Note: The UAESWITCH totals are intended to reflect the totals of the transactions exchanged on-line. The "issuer" totals do not include transactions that have not yet been forwarded to the banks. (These will not be forwarded after the UAESWITCH has cutover to a new settlement date) and the "acquirer" totals do not include reversals for late responses that might still be held in the UAESWITCH SAF file.

10.1 Stand in Authorization

The UAESWITCH does not currently offer stand-in authorization.

10.2 Store and forward (SAF)

The UAESWITCH SAF file is used to store the following transactions:

- All reversals and advices received from member banks. Reversals and advices switched to a bank are always responded "approved" by the UAESWITCH. The UAESWITCH then forwards the reversal/advice to the bank.
- Cutover notification and acquirer/issuer reconciliation total notification. These are always placed in the SAF so that their delivery is guaranteed to a bank in strict chronological order.

Transactions stored in the SAF file will be forwarded to the bank when the link to the bank becomes available. In case the reversal or advice is originated by acquirer and acknowledgement is not received from the issuer within the timeout period, UAESWITCH shall store the advice in SAF and the SAF shall be cleared from the system as and when the other host is online and is ready to accept SAF advices. In case of SAF timing out, it will be retried for 3 times before getting purged and the affect taken into settlement.

Cutover and Reconciliation messages will always be forwarded regardless of whether or not the Date, Settlement value is earlier than the banks UAESWITCH current business day.

10.3 Totaling (For Reconciliation Messages)

The UAESWITCH maintains two sets of "issuer" and "acquirer" business day totals for each bank. These may be thought of as the "current day" and the "next day". Once the UAESWITCH starts to cutover the bank interfaces, the issuer totals for the next day will start to be used in addition to those for the current day. Once all bank interfaces have been cutover, a window of at least five minutes will elapse before the UAESWITCH performs the following operations:

- Sends the "current day's" "issuer" and "acquirer" totals to each bank
- Moves the "next day's" totals into the "current day's" totals
- Sets the "next day's" totals to zero.

Note: If a particular bank interface is down for more than one settlement day it may be possible that when the interface becomes available again the bank may receive transactions for a settlement date greater than its "next day's" totals. In these situations, the bank's processing system should roll its reconciliation totals automatically before processing the transaction. If an acquirer and/or card issuer reconciliation message is subsequently received by the bank for the "old" date, it should be responded to with an "Error" settlement code value of "3" in field 66 of the 0510 or 0512 response.

10.4 Settlement

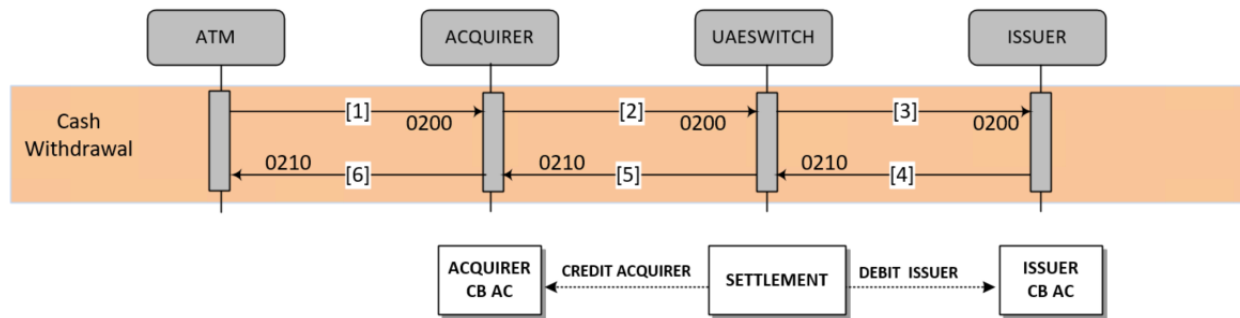
Once all banks have been cutover, UAESWITCH will execute its end-of-day processing programs. These programs:

- Are able to produce an "Extract" file to be sent to Member Banks. This file includes all the transactions involving a particular bank for the business day.
- Report on the settlement position between each Member Bank and the UAESWITCH.

All financial transactions acquired by UAESWITCH member banks ATMS/POS terminals and processed via UAESWITCH contain both authorization and clearing information to be accounted for settlement in a single message format

ATM Transactions Settlement

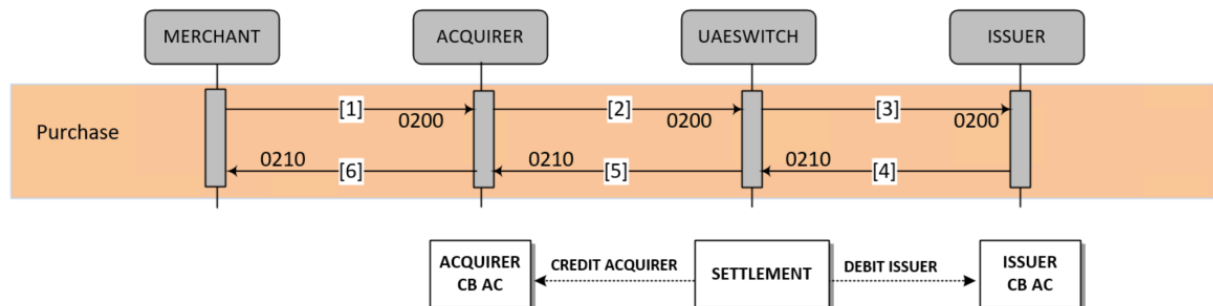
ATM Transactions processed for a business day is accounted for net posting on next CBUAE business day



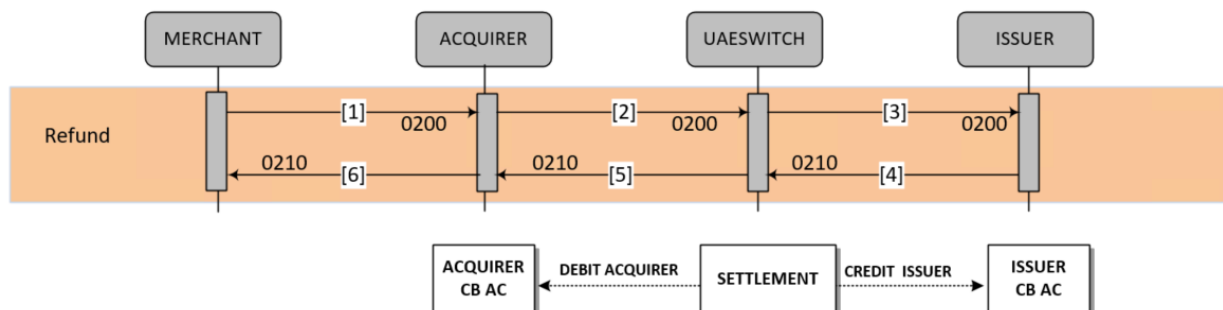
POS Transactions Settlement

POS Transactions processed for a business day is accounted for net posting on next CBUAE business day

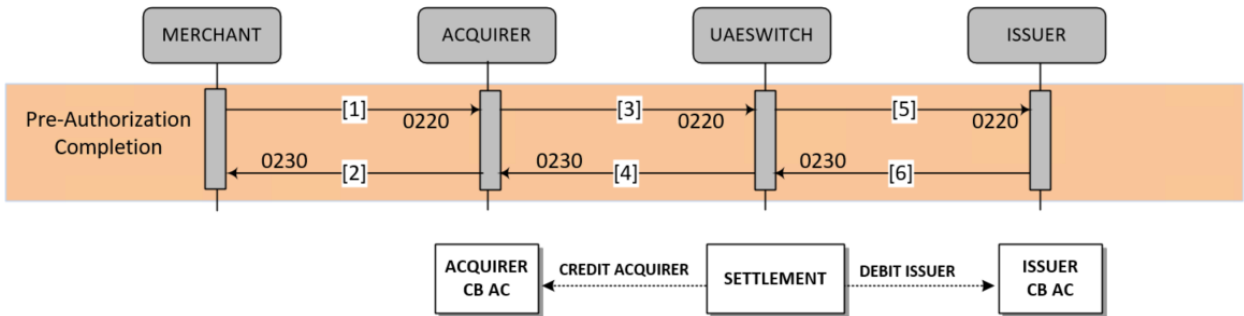
POS Transaction Purchase



POS Transaction: Refund

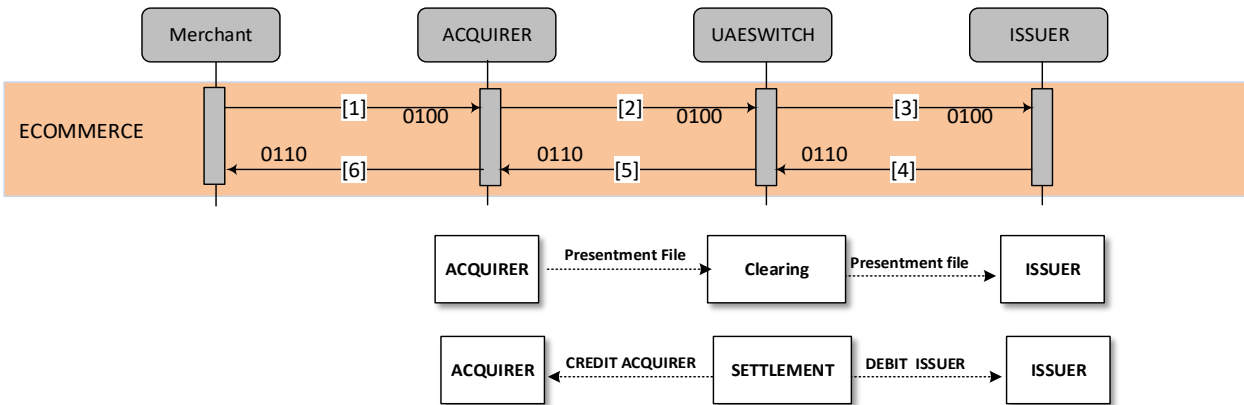


POS Transaction: Pre-Authorization Completion



DMS Transaction

DMS transactions are considered for settlement when the presentment file is submitted by the acquirer for clearing



11. Exceptions Transactions Processing

As part of the online transaction processing between UAESWITCH host and member bank host exceptions can occur such as

- Issuer Response timeouts
- Message format error
- Data Security error
- Communication exceptions
- Terminal operation error

11.1 Rules for exceptions processing

For pre-authorization and financial messages in request messages, the original transactions can be cancelled with reversal advice messages while abnormalities occur. The abnormalities are as follows:

- Participant cannot forward the financial transaction acceptance response to the transaction sender.
- Participant receives reversal advice from the transaction sender.
- Participant receives no response for a request message within the response time frame.
- Participant receives a late acceptance response to the request message.

When Participant cannot send reversal advice correctly, they shall store and forward the advice.

Participant shall match with the original transaction when receiving reversal advice. If the original transaction is matched and successful, the original transaction will be cancelled and a reversal successful response (with response code as "00") is sent. Neither the original transaction nor the reversal advice is involved in settlement. Otherwise, a corresponding reject code will be given according to the specific situation.

Except for network management advice (including sign on/sign off, cutoff start and cutoff end, etc.) and reconciliation advice, UAESWITCH or the Participant shall try to send the advice to the receiver by adopting store-and-forward mechanism.

11.2 Issuer Response timeouts

UAESWITCH will mark a member bank status as not available in the following cases

- The member bank host is unable to acknowledge an echo request initiated by UAESWITCH
- Member bank host interface has exceeded the threshold limits for incorrect message acknowledgement

Once a member bank interface is marked as down, UAESWITCH will reject all request information destined for the Participant as an issuer without any impact on the messages originated from the Participant host

11.3 Message Format Error

If participants sends data which is not marching to the interface standards, the same will be rejected with a 9XXX Series message. The reject message will correspond to the first message grammatical error detected by UAESWITCH

11.4 Data Security Error

Transactions with PIN block translations will be rejected with a response code of 96 by UAESWITCH

11.5 Communication exceptions

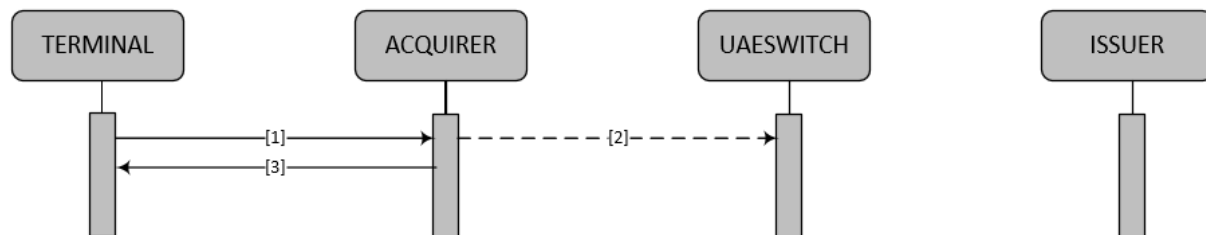
During online transactions processing Participant can encounter communication abnormalities while

- Sending request message fails
- Sending response message to request fails
- No response received after sending request message
- Sending reversal advice message fails
- Sending response message to reversal advice fails
- No response received after sending reversal advice message
- Receiving late response message to request message

When such abnormalities are detected, participants

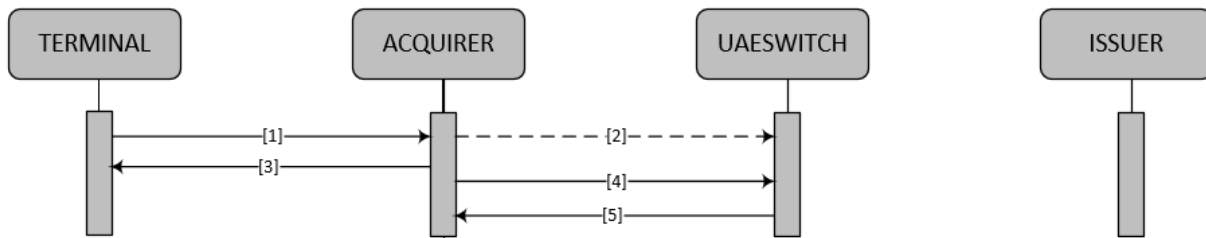
- Should send the echo test message at a certain interval to test if the connection has been restored.
- Shall abandon unsent response message
- For a request message that needs to be forwarded, response with a response code "91" (Issuer or switch center is inoperative) will be sent to the Acquirer.
- Advice messages (022X and 042X) shall be saved in store-and-forward queue and sent after the connection restores.
- While receiving a response to echo test, which means the connection restores, the Participant shall send out the messages in the store-and-forward queue in turn.

11.5.1 Case 1 The Acquirer Cannot Forward Request from the Terminal



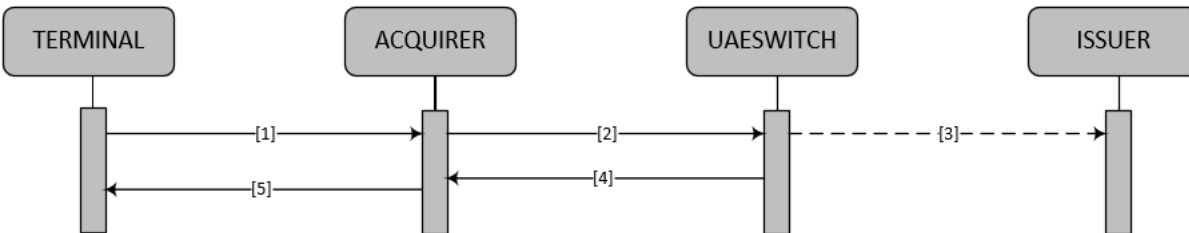
1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER unable to send the request to the UAESWITCH
3. ACQUIRER shall send the reject response to the TERMINAL directly

11.5.2 Case 2 UAESWITCH Cannot Receive Request



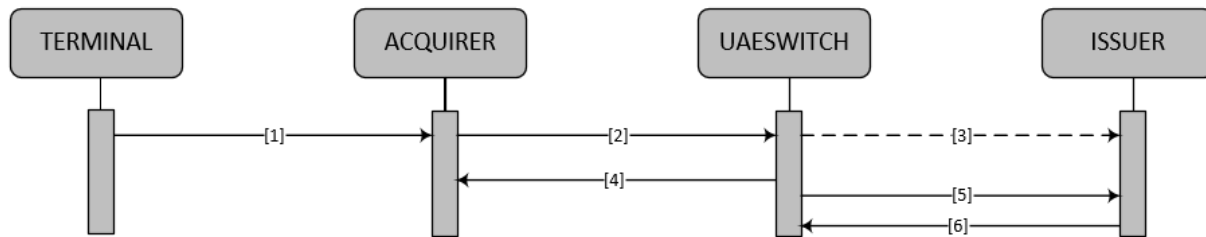
1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH, which is not received by UAESWITCH
3. ACQUIRER shall send the reject response to the TERMINAL directly
4. ACQUIRER sends a timeout reversal to UAESWITCH
5. UAESWITCH acknowledges the timeout reversal to the ACQUIRER

11.5.3 Case 3 UAESWITCH Cannot Forward Request to the Issuer



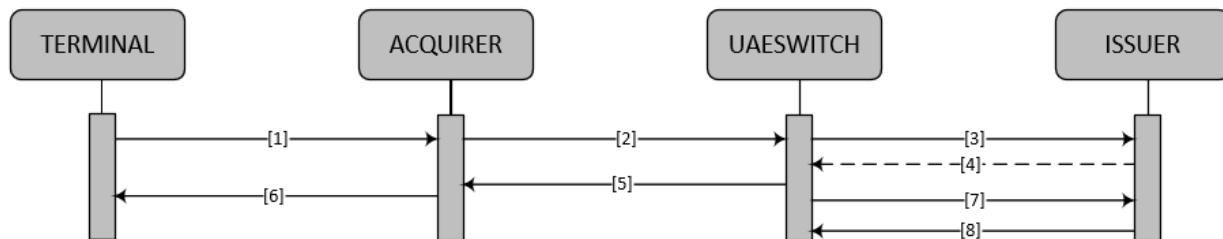
1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH, which is received by UAESWITCH
3. UAESWITCH attempt to submit the request to the ISSUER
4. UAESWITCH acknowledges response with 91 to the ACQUIRER
5. ACQUIRER shall send the reject response to the TERMINAL directly

11.5.4 Case 4 The Issuer Cannot Receive Request



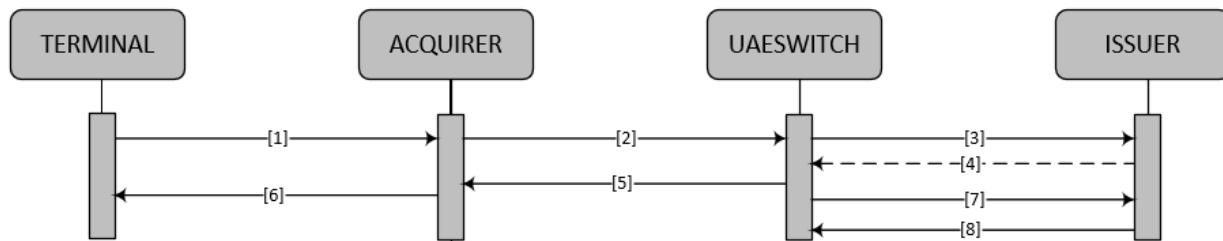
1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH
3. UAESWITCH submit the request to the ISSUER, which is not acknowledged by ISSUER
4. UAESWITCH sends a timeout response to the ACQUIRER
5. UAESWITCH shall send the reversal to the ISSUER, if the transaction is a financial transaction
6. ISSUER acknowledges the timeout reversal to UAESWITCH

11.5.5 Case 5 The Issuer Cannot Send Request Response to UAESWITCH



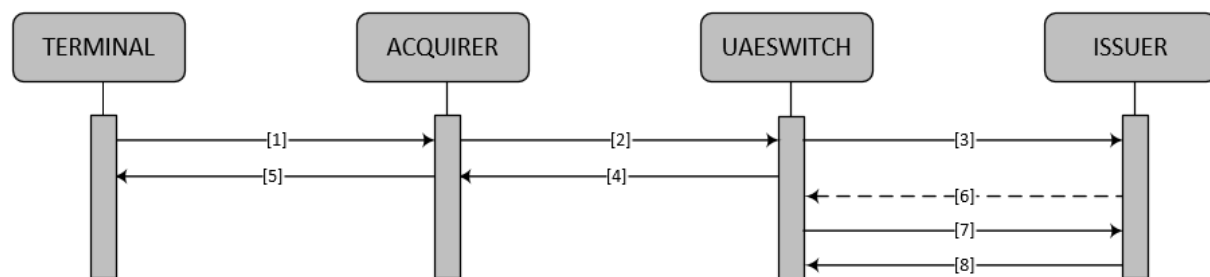
1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH
3. UAESWITCH submit the request to the ISSUER
4. ISSUER unable to acknowledge the request to UAESWITCH
5. UAESWITCH sends a timeout response to the ACQUIRER
6. ACQUIRER shall send the reject response to the TERMINAL directly
7. UAESWITCH shall send the reversal to the ISSUER, if the transaction is a financial transaction
8. ISSUER acknowledges the timeout reversal to UAESWITCH

11.5.6 Case 6 UAESWITCH Cannot Receive Response from the Issuer



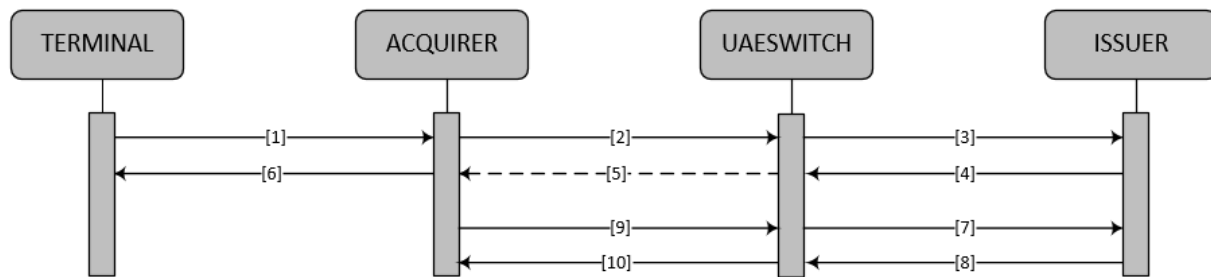
1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH
3. UAESWITCH submit the request to the ISSUER
4. ISSUER acknowledge the request to UAESWITCH, which is not received by UAESWITCH
5. UAESWITCH sends a timeout response to the ACQUIRER
6. ACQUIRER shall send the reject response to the TERMINAL directly
7. UAESWITCH shall send the reversal to the ISSUER, if the transaction is a financial transaction
8. ISSUER acknowledges the timeout reversal to UAESWITCH

11.5.7 Case 7 UAESWITCH Receives Late Response from the Issuer



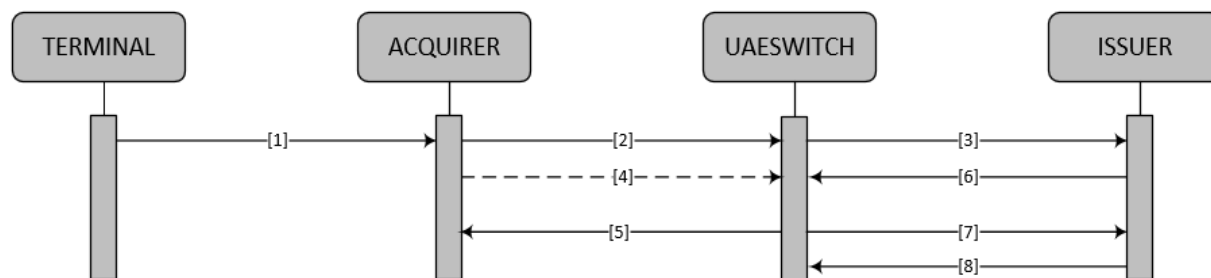
1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH
3. UAESWITCH submit the request to the ISSUER
4. UAESWITCH sends a timeout response to the ACQUIRER
5. ACQUIRER shall send the reject response to the TERMINAL directly
6. UAESWITCH receives the response from the ISSUER after transaction has timeout
7. UAESWITCH shall send the reversal to the ISSUER, if the transaction is a financial transaction
8. ISSUER acknowledges the timeout reversal to UAESWITCH

11.5.8 Case 8 UAESWITCH Cannot Forward Request Response to the Acquirer



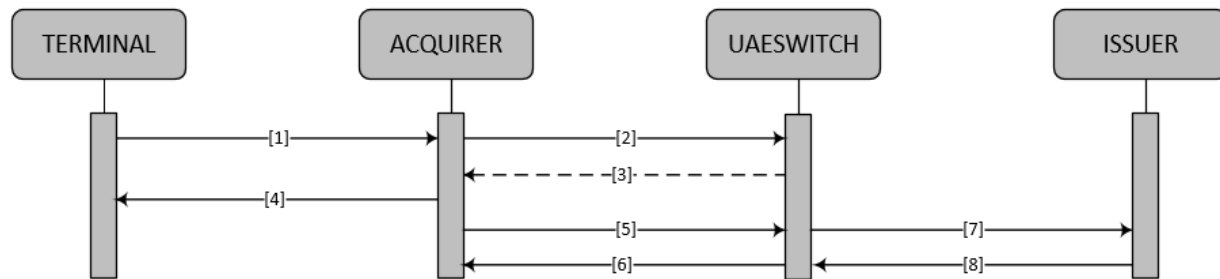
1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH
3. UAESWITCH submit the request to the ISSUER
4. ISSUER acknowledges the response to UAESWITCH
5. UAESWITCH attempts to acknowledge the response to the ACQUIRER
6. ACQUIRER shall send the reject response to the TERMINAL directly
7. UAESWITCH shall send the reversal to the ISSUER, if the transaction is a financial transaction
8. ISSUER acknowledges the timeout reversal to UAESWITCH
9. ACQUIRER sends a timeout reversal to UAESWITCH
10. UAESWITCH acknowledges the timeout reversal to the ACQUIRER

11.5.9 Case 9 UAESWITCH Receives Early Reversal from the Acquirer



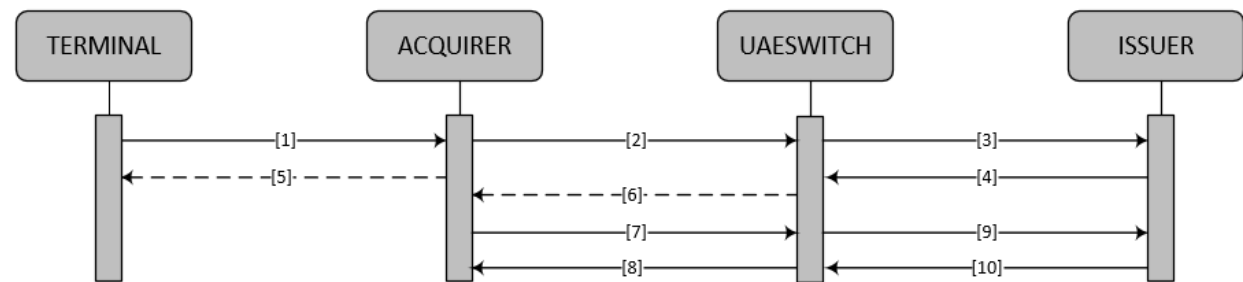
1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH
3. UAESWITCH submit the request to the ISSUER
4. ACQUIRER sends a timeout reversal to UAESWITCH without receiving the issuers response within the response time frame
5. UAESWITCH acknowledge the reversal response to the ACQUIRER
6. UAESWITCH receives the response for the original request from the ISSUER
7. UAESWITCH sends a timeout reversal to ISSUER
8. ISSUER acknowledges the timeout reversal to UAESWITCH

11.5.10 Case 10 The Acquirer Cannot Receive Response from UAESWITCH



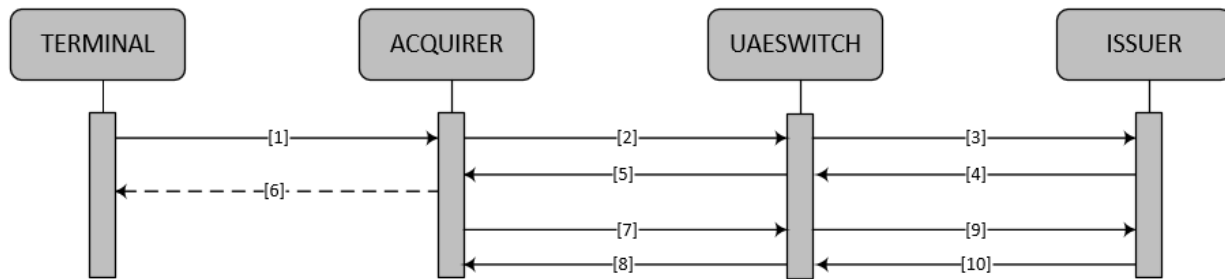
1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH
3. ACQUIRER detects the timeout in the response from UAESWITCH
4. ACQUIRER shall send the reject response to the TERMINAL directly
5. ACQUIRER sends a timeout reversal to UAESWITCH
6. UAESWITCH acknowledge the reversal response to the ACQUIRER
7. UAESWITCH sends a timeout reversal to ISSUER
8. ISSUER acknowledges the timeout reversal to UAESWITCH

11.5.11 Case 11 The Acquirer Receives Late Acceptance Response from UAESWITCH



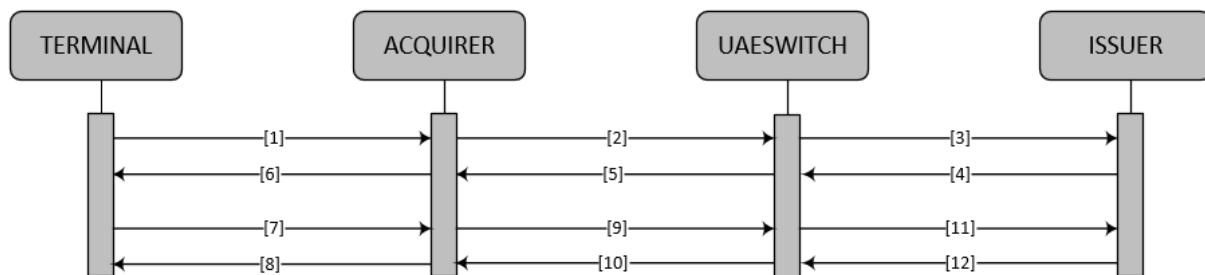
1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH
3. UAESWITCH submits the request to the ISSUER
4. ISSUER acknowledges the response to UAESWITCH
5. ACQUIRER detects the timeout in the response from UAESWITCH and send the reject response to the TERMINAL directly
6. ACQUIRER receives the response form UAESWITCH after the timeout
7. ACQUIRER sends a timeout reversal to UAESWITCH
8. UAESWITCH acknowledge the reversal response to the ACQUIRER
9. UAESWITCH sends a timeout reversal to ISSUER
10. ISSUER acknowledges the timeout reversal to UAESWITCH

11.5.12 Case 12 The Acquirer Cannot Send Terminal Operation Instruction



1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH
3. UAESWITCH submits the request to the ISSUER
4. ISSUER acknowledges the response to UAESWITCH
5. UAESWITCH acknowledge the response to the ACQUIRER
6. ACQUIRER fails to send the response to the TERMINAL
7. ACQUIRER sends a timeout reversal to UAESWITCH if the original payment request has been accepted by the ISSUER
8. UAESWITCH acknowledge the reversal response to the ACQUIRER
9. UAESWITCH sends a timeout reversal to ISSUER
10. ISSUER acknowledges the timeout reversal to UAESWITCH

11.6 Terminal Operations exceptions



1. TERMINAL submits request to the ACQUIRER
2. ACQUIRER submits the request to the UAESWITCH
3. UAESWITCH submits the request to the ISSUER
4. ISSUER acknowledges the response to UAESWITCH
5. UAESWITCH acknowledges the response to the ACQUIRER
6. ACQUIRER sends the response to the TERMINAL
7. TERMINAL sends a timeout reversal to ACQUIRER if the TERMINAL is unable to provide the service
8. ACQUIRER acknowledges the reversal response to the TERMINAL
9. ACQUIRER sends a timeout reversal to UAESWITCH
10. UAESWITCH acknowledges the reversal response to the ACQUIRER
11. UAESWITCH sends a timeout reversal to ISSUER
12. ISSUER acknowledges the timeout reversal to UAESWITCH

12. Compliance

For Bins under UAESWITCH Bin list when accepted on member banks Terminal Devices

12.1 Card/Customer Authentication

All card present transactions performed on Retail POS Terminal must be send online for Card/Customer authentication

12.2 Customer Authentication

Card Acceptance	Authentication
Contact EMV Card Chip Dip	Online PIN
Contactless EMV Card	
Amount less than Terminal CVM Limit	No PIN Issuer can maintain their own threshold limits.
Amount above the terminal CVM limit	Online PIN
EMV Fallback	Online PIN

12.3 General compliance

- Message sent to UAESWITCH must be formatted as per the specification defined in this document.
- Acquirer will take all care for configuring the POS devices correctly i.e., TID, MCC, address, location, date and time setting etc. Country code in POS device should be populated correctly.
- Acquirer has to generate reversal for the transaction for which response is not received within the time-out parameter defined for acquirer
- In a situation wherein UAESWITCH system encounters a format error with the request message sent by acquirer, UAESWITCH will send a format error decline message to acquirer. No reversal needs to be generated by the acquirer for such decline message on account of format error
- Issuer need to verify all authentication related data like PIN, OTP, ECI, ICS DATA 1, CVD1, CVD2, ICS DATA 2, biometric etc.
- Issuer need to respond the request within the issuer time out parameter, failing which UAESWITCH will generate reversal towards issuer and decline response towards acquirer for the transaction.
- Issuer need to populate all the data elements in the response as per the message specification.
- All advice messages need to be acknowledged.
- Customer and device sensitive data like PIN, expiry date, track, POS condition code, POS Entry Mode must not be echoed back in the response
- Issuer may receive reversal up to next 3 cutover. Each cut-over cycle is of 24 hours.
- For all Purchase/Pre-authorization/Refunds transactions Issuer needs to populate DE 38.
- Acquirers and Issuers must support the Q0 response code implementation as outlined in Section 12.9 of the specification.
- Acquirers are required to process transactions in SMS mode for the ATM channel and in DMS mode for eCommerce transactions all the time.
- Currently, UAE Switch ICS debit/prepaid card transactions on POS terminals are processed in SMS mode. However, as part of the Jaywan credit card program, acquirers are required to support DMS

mode for the POS channel. In the future, this requirement will be extended to debit and prepaid cards.

- The POS BIN file includes a field called Issuer Acceptance Capability, which indicates whether transactions on the POS channel should be processed via DMS or SMS.
- The UAE Switch and Jaywan Scheme are enhancing their capabilities to support magnetic stripe transactions, both with and without PIN, as well as manual (keyed-in) transactions. Acquirers and issuers must carefully review the operational guidelines and implement relevant controls to mitigate any possible risks.

12.4 Purchase

The basic service which allows the cardholder to pay for the purchase of goods and services from a card acceptor using their card or digital wallet

Merchant / Acquirer

- Purchase transaction shall contain appropriate indicators in **DE-61, SF 7 as '0'**

Issuer

- After performing the required authorization checks, to acknowledge the response as per the interface standards

12.5 Pre-Authorization & Pre-Authorization Completion

Pre-authorization allows a merchant to reserve funds on a customer's card without taking the funds. When a merchant is ready to charge the customer, merchant can process a Pre-authorization Complete, which finalizes the transaction.

Pre-authorization is useful for ensuring customer has the funds available for an order that is being created prior to actually delivering the product or service. Merchant is also able to change the payment amount before actually charging the customer

For Pre-authorization transactions, the central operator will generate a transaction id to be associated during the end-to-end life cycle of the pre-authorization transaction

Primary Merchant Categories

Hotels enable funds to be held either at the booking stage or during check-in. Pre authorization guarantees that when the time of check out comes, there are funds available to cover additional charges incurred during the guest's stay

Car rental agencies also commonly use pre authorizations with their clients. By placing a hold on funds when the car is rented, agencies can be sure that the car will be returned in good shape, with a full tank of gas. If there is damage to the car or a need for fuel, the hold will cover these charges.

Tour operators and activity providers also utilize pre authorizations. For those lending customers expensive pieces of equipment, the funds protect them from being stuck with the costs associated with loss, damage, or theft.

Merchant / Acquirer

- An Acquirer may support and may optionally offer to its Merchants with pre-authorization Transactions. However, they must comply with the Rules applicable to the pre-authorization.
- Pre-authorization transaction shall contain appropriate indicators in **DE-61, SF 7 as '4'**
- Merchant / Acquirer bank shall maintain the transaction id provided as part of pre-authorization request response
- For incremental authorizations, the transaction id shall be provided in the transaction request by the acquirer
- For incremental authorization, the acquirer shall provide original DE-2 with appropriate incremental preauthorization identifier in **DE-61, SF7 = 6 and DE-63 Tag 02 (original transaction id)**
- The acquirer is expected not to populate any authorization completion after the expiry of guarantee period as indicated in the rule books
- Reversal message must be sent when the Transaction has failed to complete or merchant may initiate the cancellation (as Void) of pre-Auth Transaction.
- The acquirer should set a transaction limit base on the merchant businesses/category.
- The acquirer bank may support the Pre-Auth extension.
- The acquirer bank may support the partial capture or final completion for eCommerce transactions.
- Acquirer can accept or decline preauthorization completion from different terminals
- Acquirer shall validate whether preauthorization completion is submitted on time.
- Preauthorization completion shall contain original card number DE-2, DE-38 and DE-63 Tag 02

Central Operator (UAESWITCH)

- For pre-authorization transactions, the central operator shall generate a transaction id and populate the same in **DE-63, TAG 02**

Issuer

- The issuer must guarantee period for transactions completed and block the pre-authorization amount for the duration as indicated in the rule books. After that, issuer should release it.
- Issuer must inform the cardholder with the amount for which will be blocked or release.
- Issuer shall respond back the transaction id in **DE-63, TAG 02**
- Member bank Issuer shall either accept or decline the incremental preauthorization transaction
- If the member bank issuer supports incremental preauthorization, the issuer shall add the incremental amount to the original authorization amount (as a block on open to buy) and increase pre-authorization expiry date in accordance with the incremental pre-authorization
- If issuer receive a Partial Capture, the remaining held amount should continue the maximum period allowed.
- The held amount should be immediately released back to accountholder's account if the pre-authorization capture was not received during the subject period (expired pre-Auth) or when the pre- authorization Final Capture amount is lower than the pre-authorized Original amount, and the cardholder shall be notified.
- In case of receiving Void, the issuer releases the amount and notify the cardholder showing the amount released.
- If the member bank issuer observes any discrepancy in preauthorization completion amount or expiry of the preauthorization transaction. The member bank issuer shall initiate dispute process.

- Preauthorization completion amount can be less, equal to or greater than the original transaction amount
- Member bank issuer shall maintain the tolerance limit for per authorization completion amount and validate the same as part of preauthorization completion

12.6 Refund Transaction

A POS refund transaction is used to credit a cardholder with applicable funds in consideration for goods returned to the retailer by the cardholder or as a refund for services not rendered.

POS transaction refunds must be supervisor-controlled, i.e., a “supervisor control card” or “supervisor password” is required to be entered to verify each POS refund transaction.

A refund receipt must be printed in duplicate and a copy presented to the cardholder.

Individual acquirers have the choice whether or not to allow this function. However, if they decide to do so, full responsibility for this transaction rests with the acquirer.

This tells us that Refund function is an optional for the acquirer bank, however it is supported by UAESWITCH/GCC Network for both acquirer and issuer considering the following:

1. Reference number for the original transaction should be considered in the refund
2. Refund Transaction to be performed with same currency of the acquirer country which obtained the purchase transaction
3. The refund process should be done within the announced merchants policy which is accepted by the acquirer country
4. To add an indicator field to include the Authentication code of the original purchasing transaction, however it is optional to enter this data
5. The Acquirer is responsible to ensure the merchants’ eligibility for the refund feature and that proper measures are in place to monitor refund activities by merchants with this service active.
6. Switch processing fees for the original purchase will not be refunded, as a result no processing fees will be applied to process the refund transaction.
7. Refund Transaction is considered a new transaction with reference to original purchase transaction in DE38. DE-38 is optional
8. No settlement, interchange, authorization, or MSC fees are levied on a Refund Transaction.
9. The cardholder must receive the paid amount (in transaction currency) without any deducted charges (only for full amount refunds).
10. The Issuer bank to follow internal compliance policy in enabling Refund capability to cardholders by default. The Issuers should monitor this capability through internal risk policies and procedures.
11. The Issuer bank to follow internal compliance policy for verifying the validity of the original purchase transactions prior to responding to the online refund transaction.
12. The Issuer bank to follow internal compliance policy in regards to authorization of a Refund Transaction request if the original transaction was not found.
13. The Issuer bank to follow internal compliance policy in reference to the refund transaction amount velocity thresholds.
14. The time frame of a Refund, being the period between the transaction date and the Refund date is determined by the Merchant according to their internal policies and procedures (and may be

- subject to commercial (licensing) laws and regulation. The refund period that Issuer bank will be able to validate the original transaction online should be 7 days.
15. A refund transaction will always be processed online even when the Card and Terminal are enabled for Offline Authorization.
 16. Following the completion of a Refund Transaction, the Merchant must provide the Cardholder with a (Refund) Transaction receipt.
 17. The refund capability should be disabled on all POS terminals by default. The function should not be activated until:
 - a) The Acquirer has offered, and the Merchant accepts inclusion of the function on their POS service.
 - b) The Acquirer ensures that the Merchant fully understands the duties, responsibilities, related risk, fraud liability, and operating procedures relating to the Refund of Transactions.
 - c) The Merchant has signed the updated MSA (which includes the Refund Policy).

In exceptional circumstances, the Acquirer may elect to decline merchant request to activate the service based on the Acquirer's internal risk policies and procedures, subject to appeal by the Merchant to their local bank. The Acquirer may also disable the Refund function if the Merchant requests.
 18. When a Refund is provided using POS, the issuer must credit the same card account used to make the original POS purchase. The Issuer must validate that the same card has been used for purchase and refund (Exceptions are if the card has been renewed or the PAN had been issued newly).
 19. To authenticate the 'Original Transaction' the Merchant must ask the Cardholder for a transaction receipt or similar documentation as proof of the original purchase transaction; if the original receipt is not available, the Merchant may fall back to their internal policies and procedures in deciding whether to proceed or not, with the refund transaction.
 20. The Switch/Acquirer must monitor Refund Transaction if a merchant exhibits repetitive, unusual or excessive card refunds. The Switch/Acquirer may initiate an investigation at their own discretion, subject to the UAESWITCH Switch Rules, Standards, and Procedures Manual.
 21. In the event where an attempted Refund Transaction is not complete, the Issuer on behalf of the cardholder may raise a claim if the Issuer is satisfied with the authenticity of the concerned transaction and supporting documents.
 22. Merchants must refund the (relevant) proportion of the purchase amount through one single refund transaction or multiple refund transactions; however, the issuer must ensure that the total refund transactions do not exceed the original purchase amount.
 23. A merchant may choose to refund a Cardholder outside the network (i.e., a refund in cash or in kind). In such instances, the merchant accepts full responsibility for the transaction and none of the switch members will have any liability for the transaction. The Merchant may not fall back to the UAESWITCH network for any dispute arising out of such a refund or after the period indicated in point 15 stated above.
 24. Issuers and Acquirers must ensure the capability to perform a refund transaction through NFC for plastic, contact and for contactless.
 25. Refund transactions should be allowed even if the original transaction was performed through a payment instrument that differs than the one used initially (regardless if it was a contact or contactless). For example, an original transaction was performed through plastic in contact mode, the refund should be made available even if it was triggered by Tokenized instrument in NFC mode.
 26. No refund is accepted for POS Advanced Payment.

E-Commerce Refund:-

For refunds initiated by e-commerce merchants, acquirers are required to include the following data elements from the original sale transaction in the refund request:

- Original Transaction ID
- ECI (Electronic Commerce Indicator)
- CAVV (Cardholder Authentication Verification Value)

Issuers are recommended to validate the details received in DE-104 — if present — against the corresponding data from the original sale transaction.

12.7 Partial Authorization

A Partial Authorization occurs when an authorization is attempted for the full amount of the transaction and there are not enough funds available to cover the full amount, so an authorization for the amount available in the account is returned. This allows the cardholder to use the card presented for the amount available and for the merchant to obtain an additional form of payment for the difference.

Merchant

- Partial authorization service is optional and dependent upon merchant policies and device capabilities
- Merchants supporting partial authorization shall initiate the purchase transaction with partial authorization acceptance identifier in **DE-61, SF 2 as '1'**
- Merchant shall initiate void or reversal only of the partial authorized amount

Issuer

- Issuers have the choice to return a partial authorization or reply with a decline the transaction if funds are not available
- Issuers identifies that the merchant supports partial authorization based on **DE-61 , SF2 as '1'**
- Issuers supporting partial authorization acknowledges the response by populating
 - DE-39 with response code '10'
 - DE-4 with partial authorized amount
 - DE-54 with original transaction amount as sent in the payment request

Example

Say the transaction amount is 1000 AED. Issuer would attempt to debit 1000 AED from the customer's account, however, identifies there is no sufficient fund to authorize the transaction. Since the merchant supports partial authorization (DE-61, SF 2 "1"), Issuer shall debit the available amount say 600 AED.

Issuer responds back with the following details.

- DE-39 = 10
- DE-4 = Actual amount debited (600 AED)
- DE-54 = Original Transaction amount (1000 AED)

12.8 Purchase with Cashback

A Purchase with cashback option is a service offered to retail customers whereby an amount is added to the total purchase price of a transaction paid by payment instrument and the customer receives that amount in cash along with the purchase.

Merchant

- Purchase with cashback service is optional and dependent upon merchant policies and device capabilities
- Merchants supporting purchase with cashback shall initiate the transaction with cashback authorization acceptance identifier in **DE-61, SF 7 as '7'**
- Merchants supporting partial authorization shall initiate the purchase cashback transaction
 - DE-3 with '090000'
 - DE-61 SF 7='7'
 - DE-4 shall contain purchase + cashback amount (total amount)
 - DE-54 shall contain cashback amount
- The charge slip to the customer shall clearly specify the purchase and cashback amount
- Void /reversal if any, shall be for the whole amount inclusive of purchase and cashback amount
- Refund, if any shall be allowed only purchase amount

Issuer

- Issuers have the choice to approve or reply with a decline a purchase with cashback transaction
- Issuers identifies that the merchant supports partial authorization based on DE-3 '090000' and validates the presence of DE-54 in the transaction message

12.9 Contactless Transactions no CVM thresholds

For contactless transactions received without a PIN i.e., no CVM was performed, and the issuer requires a PIN due to single transaction limit exceeding the CVM limit OR the contactless cumulative limit is exceeded, the issuer bank will respond in DE39 with value "Q0" to ask for PIN; the POS Acquirer will force the Pin when the Issuer responds with Value (Q0) in DE39

If the Issuer responds with Q0, the following should be considered for the "next transaction"

- The transaction will have a new Transmission Date and Time (DE-7)
- The transaction will have a new Local Transaction Date and Time (DE-12)
- The STAN will be incremented (DE-11)
- The transaction will have a new Retrieval Reference Number (DE-37)
- The POS Condition Code (DE-22) Position 1 (Card data input capability) and Position 7 (Card data input mode) will be "7" i.e., contactless
- The EMV data (DE-55) will be duplicated from the previous transaction request which was declined with Action Code "Q0" and Issuers must accept this as valid and not reject it or any parts of the EMV data e.g., ATC

Note: - Jaywan as a scheme will be introducing merchant discounts at point of sale. In a contactless transaction with a single tap, Jaywan may sent authorization amount lesser from Authorized amount(9f02) as discounts may be applied post customer accepting the offer. Solutions developed by issuers should accommodate this process.

12.10 POS Transaction Displays and Transaction Process Flows

The following table details the minimum level of message prompts and responses that are required to support UAESWITCH POS Transactions

	Pin Pad Display	Action	Terminal Display
Idle Mode	"READY"		
Transaction Initiation	"Please Wait"	a. Transaction Selected b. Card Swiped/DIP c. Amount Entered	"Purchase Enter amount xxxx.xxx"
Customer Advice	"xxxx.xxx (Value) Enter PIN"		"Customer PIN"
Customers Enters PIN	"Please Wait"		
Issuer Response	"Approved" or "Transaction Declined"	Transaction Record is printed	"Approved" or "Transaction Declined"

The UAESWITCH POS Transaction is then complete, and the terminal reverts back to the idle Mode

- It should be noted that if a connection cannot be made to the Issuer Participating Switch, the transaction must be declined, and the terminal display will indicate "ISSUER UNAVAILABLE" This message will also be printed on the transaction record.
- The "Approved" response indicates that the transaction has been approved, and the customers' account has been debited for the transaction.
- The "Transaction Declined" response indicates that the card issuer has declined the transaction, and the cardholder should contact their card issuing bank for clarification.

12.11 POS Transaction Record Receipts

POS device must produce a "Transaction Record" for each transaction in duplicate, irrespective of whether the transaction has been approved or declined. One copy of the Transaction Record must be retained by the Merchant (for possible production within the required document retention period), whilst the other copy of the Transaction Record must be provided to the cardholder.

12.11.1 Approved UAESWITCH POS transactions

For all UAESWITCH issuer-approved/authorized POS transactions, the POS terminal must display the narration "Approved" and a transaction record slip produced in duplicate which contains the following information as a minimum standard:

- Authorization Code (e.g., 012345) Merchant name and location
- Date of transaction
- Time of transaction

- Merchant ID
- Terminal ID
- Transaction Sequence Number
- Card type
- Card number (e.g., 123 456 **** * 7891, in accordance with PCI standards)
- Transaction amount and currency
- Authorization Code
- The receipt may, at the POS acquirer's discretion, additionally contain the cryptogram and the data elements used to calculate the cryptogram

12.11.2 Declined UAESWITCH POS Transactions

Where a POS transaction is attempted, and the transaction is declined by the issuer, the terminal display will show “declined” or “pick up card”, however the corresponding Transaction Record must contain the following information:

- Merchant Name and Location
- Date of transaction
- Time of transaction
- Transaction amount and currency
- Merchant ID
- Terminal ID
- Transaction Sequence Number
- Card type (GCC, Visa, MasterCard etc.)
- Card number (e.g., 123456 **** * 1234)
- “Narration “transaction declined”
- Issuer decline code

12.12 MIT/Recurring Transactions

Merchant-Initiated and Recurring Transactions

- For MIT (Merchant-Initiated Transactions) or recurring transactions, merchants are required to populate the original transaction ID of the previously authenticated transaction.
- For MIT/CIT (Customer-Initiated Transactions), issuers are required to store the original transaction ID for future reference and may validate the original transaction ID and process the transaction accordingly.

Recurring Transactions Overview

Recurring transactions refer to automated payments made at regular intervals for ongoing services or subscriptions. These transactions are typically used in eCommerce platforms, enabling businesses to charge customers for services such as memberships, subscriptions, or installment plans.

Each recurring transaction is linked to an initial transaction, which captures the customer's consent and payment details. Mapping subsequent payments to the original transaction ensures proper authorization and traceability.

Expected Data Elements for Recurring Transactions

- **DE-22** = '10'
- **DE-25** = '58'
- **DE-61.4** = '4'
- **DE-104 Subfield 06** = Original Transaction ID
- **DE-104 Subfield 07** = Token Cryptogram (used for Card-on-File transactions using Jaywan scheme token)
- Additionally, the transaction status information can be sent in the original transaction under **DE-61 Subfield 7**.

12.13 Tokenization

Tokenization Overview

In **tokenization**, the actual **Primary Account Number (FPAN)** is replaced with a **token(DPAN)**, providing enhanced security and preventing misuse of card data. These **tokens** are merchant- or wallet-specific, ensuring that even if compromised, their use is restricted.

Token Provisioning Flow

1. **Initiation from wallet** : The Customer initiates a provisioning request using **OEM Pay wallet (e.g., Apple Pay, Samsung Pay, Google Pay)** to the issuer via the Jaywan TSP.

Issuers to refer the respective OEM Wallet implementation guidelines while implementing the level of Trust.

If the wallet provider has not provided Level of Trust information in the provisioning request, the Jaywan TSP will default the value to '99'. Issuers may either proceed with step-up authentication for the cardholder or choose to decline the provisioning request at their discretion.

2. Issuer Response Mapping

Flow Level	DE-39 Response	Description
GREEN	00	Seamless provisioning
YELLOW	85	ID&V via OTP SMS/email/call center
RED	05	Declined provisioning

Response codes other than '05' are considered issuer-side technical declines during tokenization.

In the case of Merchant Provisioning (COF), issuers will receive DE-105 tag 21 as M4M_PAY.

Issuers are required to validate the COF provisioning request and indicate approval or decline by responding with '00' or '05' respectively, since ID&V is not applicable for this use case.

COF provisioning requires acquirers to send an authentication request for customer validation.

COF provisioning will be allowed only if the transaction is fully authenticated with ECI Value = 05.

3. Authentication Display to Cardholder

OEM Pay displays the appropriate **authentication method** based on the issuer's response. A common **ID&V method** is **OTP (One-Time Password)**, generated by the Jaywan TSM.

4. OTP Flow

The OTP is transmitted to the issuer via the **Jaywan System**. The issuer must send the OTP to the cardholder using the ID&V method selected by the cardholder within the wallet.

5. Token Activation

Upon successful authentication, the Jaywan TSP assigns a **token** from the token range mapped to the issuer's FPAN bin range. The token is now active and ready for use.

6. Tap & Pay Transaction Processing

- Tokenized transactions (e.g., Tap & Pay) are routed through the UAE Switch.
- The UAE Switch initiates a detokenization request using the token PAN.
- The cryptogram (ARQC) is validated by Jaywan TSP and DE55 will not be present while sending it to the issuer.
- Upon successful validation of the token data, the tokenization system retrieves the real PAN and sends the transaction to the issuer with DE-105.
- Issuers will receive the FPAN in DE-2 and Token Pan in DE-35 & DE-105 tag 01.

Key Field Requirements

<i>Use Case</i>	<i>Field</i>	<i>Value</i>	<i>Notes</i>
Token Provisioning Request	DE-25	'51'	Identifies token provisioning
	DE-61.SF7	'9'	Identifies token provisioning
	DE-32	'784200200'	Must be present; else, transaction is declined
	DE-25	'53'	For OTP requests

Track Data

DE-35

DPAN will be
presentIssuer should not validate for any
token based transactions.

12.13.1 Token Life Cycle Management (TLCM)

Jaywan Mono Badged Cards:

Whenever there is change in the card status or renewal (expiry date change), issuers must send token lifecycle message to Jaywan TSP for appropriate action to be taken on token. This is to ensure the card status/expiry date in issuer host system always align with Jaywan token vault and avoid any declines due to the mismatch. In near future Jaywan may introduce minimum approval rates and hence it is critical to submit the updates in a timely manner.

In case of replacement scenarios due to any reason fraud/lost/stolen it is issuers discretion to either delete the existing tokens and customers to provision the new card or issuers can initiate a LCM message to link the existing tokens with a newly issued card(FPAN), in this case issuers should not be sending the LCM to delete the tokens.

In case of replacement due to damaged plastic or any other use case where issuer wanted to keep the existing token active, issuers must use replacement LCM message to link the existing token with the new FPAN. In this case, issuers should not be sending LCM messages to delete the token.

In the case of product transfer, issuers must call the Jaywan Token LCM API to delete the tokens associated with the existing card. Customers will then need to provision the new card to continue using tokenized services.

Jaywan Co-Badged Cards:

Whenever there is a change in the card status, Issuers to send the TLCM to the ICS TSP and Jaywan TSP for token sync-up. OEMs will ensure the token status is updated at Jaywan TSP. Issuers will receive the notification event from Jaywan for the card status update activities.

In case of token deletion from the wallets, Issuers will receive notification from the ICS as well as Jaywan scheme about the activity confirming the deletion of the tokens.

In case of a renewal (expiry date change) scenario for FPAN, issuers must send token lifecycle message to ICS TSP and Jaywan TSP for appropriate action to be taken on the respective tokens. This is to ensure the expiry date in issuer host system always align with Jaywan token vault and avoid any declines due to the mismatch. In near future Jaywan may introduce minimum approval rates and hence it is critical to submit the updates in a timely manner.

In case of replacement scenarios due to any reason fraud/lost/stolen it is issuers discretion to either delete the existing tokens and customers to provision the new card or issuers can initiate a LCM message to link the existing tokens with a newly issued card(FPAN), in this case issuers should not be sending the LCM to delete the tokens.

In case of replacement due to damaged plastic or any other use case where issuer wanted to keep the existing token active, issuers must use replacement LCM message to link the existing token with the new FPAN. In this case, issuers should not be sending LCM messages to delete the token.

Key Field Requirements

<i>Scenario</i>	<i>DE-105 Tag</i>	<i>Required Data</i>
<i>Card Expired</i>	Tag 51	New Expiry Date
<i>Card Replaced</i>	Tag 50	New Card Number (PAN)
	Tag 51	New Expiry Date
	Tag 53	New Card Art Id

*DE 105 tag 50 is mandatory for updating card expiry and PAN details.

1. Card expiry update:

- DE 02 and DE 105 tag 50 should be the same FPAN.

2. New RPAN update:

- DE 02 should contain the old FPAN and DE 105 tag 50 should contain the new FPAN.

12.14 Ecommerce Transaction

For eCommerce transactions, the following values are expected in the transaction request:

- **DE-22** = '81'
- **DE-25** = '58' (MIT) or '59' (CIT)
- **DE-61.4** = '1', '4' or '5'

For 3DS authenticated Transactions, the following values are expected *in addition* to the above:

- **DE-104 Tag 03** = '05' or '06'
- **DE-104 Tag 04** = CAVV data
- **DE 104 Tag 05** = CAVV result code (If the issuer has opted for OBS, it will contain the validation result otherwise the value will be U)

The issuer is required to validate **above data elements** to ensure it is a secure transaction and process the transactions accordingly

For non 3DS Authenticated Transactions, the following values are expected in addition to the above:

- We will receive **ECOM Indicator** = '07' or '08'
- Expiry date/CVV2 may or may not present in the authorization.

If the issuer chooses to support **attempted authentication** (where a CAVV is generated by the Directory Server on behalf of the issuer), the ECI value received will be '**06**'. It is at the issuer's discretion to authorize such transactions.

If the issuer is opted for Jaywan On behalf services for CAVV validation, then issuers are required to validate the CAVV result codes and process the transactions accordingly. If the issuers are not opted for On behalf services, then issuers are required to perform CAVV validation while processing the transaction.

Digital Secure Remote Payments

For token-based eCommerce transactions (Secure Remote Payments), Acquirers are required to include the following mandatory data elements in the transaction message:

- DE-22 = '09'
- DE-25 = '58' or '59'
- DE-104 Tag 03 = '05' or '07'
- DE-104 Tag 04 = CAVV Value (the field will be present, If authentication performed using Issuer ACS)
- DE-104 Tag 07 = Token Cryptogram

These data elements ensure proper authentication and validation of secure, tokenized transactions in a remote payment environment.

If the issuer is opted for Jaywan On behalf services for CAVV validation, then issuers are required to validate the CAVV result codes and process the transactions accordingly. If the issuers are not opted for On behalf services, then issuers are required to perform CAVV validation while processing the transaction.

Card On File Transactions

For card on file transactions, acquirers are required to include the following mandatory data elements in the transaction message:

- DE-22 = '10' or '81'
- DE-25 = '58' (MIT) or '59' (CIT)
- DE-104 Tag 03 = ECI Value (indicates authentication was performed)
- DE-104 Tag 04 = CAVV Value (indicates authentication was performed)
- DE-104 Tag 06 = Original Transaction Id (Optional)
- DE-104 Tag 07 = Token Cryptogram

Issuers

- DE-104 Tag 06 will contain the original transaction id of previously authenticated transactions and issuers may validate while processing the transaction.
- If the issuer is opted for Jaywan On behalf services for CAVV validation, then issuers are required to validate the CAVV result codes and process the transactions accordingly. If the issuers are not opted for On behalf services, then issuers are required to perform CAVV validation while processing the transaction.

- In the authorization request, the CVV2 (DE-104, Tag 01) and expiry date may be optionally included. When provided, issuers are expected to perform validation and include the corresponding CVV2 result code(DE-104, Tag 02) in their response.
- DE-105 Tag 21 as M4M_PAY indicating it is a tokenized COF

12.15 MOTO Transactions

MOTO payments are transactions where customers give their payment card information to businesses over the phone or through mail, rather than in person or online. The acronym stands for “Mail order/Telephone order.”

Businesses use these transactions to process payments when a customer's card is not physically present or there is problem while using card.

In this Manual transaction initiated by merchant by entering card manually on the terminal. Below are the values will receive in transaction data elements

- DE-22 will be '01'
- DE-25 will be '08'
- DE-61.4=2/3 for this transaction.
- DE 61.1 = 2 (For online transaction)
- CVV2 may or may not be present for issuer validation

12.16 Offline Transaction/Financial Transaction Advice

For Offline or Financial transaction advice messaged below are the two key indicators populated in the transaction message by the acquirer and the same will be available to UAE issuers.

- MTI will be '0220'
- DE-25 will be 09(Debit)/10(Credit)
- DE63 SF 04 will contain the relevant function code

Acquirers

- Acquirers must implement appropriate controls before submitting an offline transaction/Financial Transaction Advice message (0220) for debit/credit/refund transactions. Acquirers must evaluate the merchant risk as part of their underwriting process. These controls should include, but not be limited to, mechanisms that will verify the legitimacy of the original transaction and fraud detection protocols that will monitor for unauthorized or erroneous refund requests.
- Acquirers must implement relevant system-level controls, including setting transaction thresholds based on risk appetite, when submitting an advice message (0220) for debit transactions. The assessment may include, but not be limited to, historical fraud data, types of transactions, customer risk profiles and compliance and regulatory requirements. As these transactions will be force-posted to issuers without authorization, liability remains with the acquirers.
- These messages should be used strictly for special offline use cases, which may include specific scenarios such as on-board/transit. "Special offline use cases" should further also be defined as

transactions that occur in environments where connectivity to the processing network is limited or unavailable.

- We strongly recommend acquirers to perform deferred authorization instead of sending as offline advice message.
- This feature must be enabled only for UAE Switch issuers and should not be available to GCC-issued cards.

Issuers

- Issuers must establish relevant checks and controls before posting credit advice messages to card holders. These checks should include, but not be limited to, ensuring the legitimacy of the refund request, and monitoring for unusual patterns that may indicate fraudulent behavior/activities.
- Credit advice messages must be posted to the cardholder's account within 12 hours to avoid customer inconvenience. In case of rejection within this timeframe, issuers must follow the relevant operational rules (refer to the latest version of the operating rules previously communicated). Contingency plans should be documented to address situations where system failures or other disruptions may prevent timely posting of credit advice messages.
- If the EMV data (DE55) is present in the transaction, Issuers must accept this as valid and not reject it or any parts of the EMV data e.g., ATC

12.16.1 On-Board/Transit Use Cases

Acquirer may process a Chip Transaction that takes place at the on-board/transit POS Terminal of a Merchant , if all the following conditions are satisfied:

The POS Terminal has no online capability and does not perform fallback procedures from chip to magnetic stripe.

- Prior to authorization, the merchant must conduct a Mod-10 check digit routine to verify card authenticity and must confirm that the card number is within JAYWAN BIN range.
- If the POS terminal recommends against transaction approval based on its own risk parameters, the transaction must not proceed.
- The card declined the offline authorization request. The acquirer processes such declined transactions at the risk of receiving authorization related chargebacks.
- The merchant is identified with one of the following MCCs:
 - MCC 4111 (Transportation—Suburban and Local Commuter Passenger, including Ferries)
 - MCC 4112 (Passenger Railways)
 - MCC 4411 (Cruise Lines)
 - MCCs 3000 through 3350 and 4511 (Air Carriers, Airlines).

12.16.2 Special Offline Use Cases

Acquirer may process a Chip Transaction that takes place at the Special offline use case Terminal of a Merchant , if all the following conditions are satisfied:

The POS Terminal has online capability and merchant process an offline transaction when network connectivity is not available.

- a. Prior to authorization, the Merchant must conduct a Mod-10 check digit routine to verify Card authenticity and must confirm that the Account number is within JAYWAN BIN range.
- b. An authorization request must not contain a key-entered account number or expiration date.
- c. If the POS Terminal recommends against Transaction approval based on its own risk parameters, the Transaction must not proceed.
- d. The card declined the offline authorization request. The Acquirer processes such declined Transactions at the risk of receiving authorization related chargebacks.
- e. The Acquirer must not submit declined Transaction on terminal should not be sent as advice message.

12.17 Deferred Authorization

Acquirers

Prior to enabling deferred authorization, Acquirers must evaluate the merchant risk as part of their underwriting process.

Acquirers must implement appropriate controls before submitting an deferred authorization message. Acquirers must evaluate the merchant risk as part of their underwriting process. These controls should include, but not be limited to, mechanisms that will verify the legitimacy of the transaction and fraud detection protocols that will monitor for unauthorized or erroneous transaction requests.

Acquirer may process a Chip Transaction that takes place at the offline POS Terminal of a Merchant, if all the following conditions are satisfied:

The POS Terminal has online capability and merchant process an offline transaction when network connectivity is not available.

- a. Prior to authorization, the Merchant must conduct a Mod-10 check digit routine to verify Card authenticity and must confirm that the Account number is within JAYWAN BIN range.
- b. An authorization request must not contain a key-entered account number or expiration date.
- c. Before a terminal can be used to process an offline sale, at least one online transaction must be processed on the terminal.
- d. If the POS Terminal recommends against Transaction approval based on its own risk parameters, the Transaction must not proceed.
- e. The card declined the offline authorization request. The Acquirer processes such declined Transactions at the risk of receiving authorization related chargebacks.
- f. The Acquirer must convert all "refer to card issuer" and "capture card" messages received from Issuers to "decline." (not sure if this can be done)
- g. The Acquirer must not submit declined Transactions into clearing to avoid chargeback liability.
- h. This feature must be enabled only for UAE Switch issuers and should not be available to GCC-issued cards.

Issuers

- a. If the EMV data (DE55) is present in the transaction, Issuers must accept this as valid and not reject it or any parts of the EMV data e.g., ATC

13. Appendix

13.1 Document Revision History

1	1.1	4.1 POS Transaction Purchase Sale: Removed 0100/0110 Refund: Removed 0100/0110 Included Balance Enquiry 0200/0210 4.2.2. Response Timer Control Removed Message Type 0100/0110 for Purchase 4.3.2.1. Purchase Indicate MTID 0200/0210 in Transaction flow 4.3.2.2. Pre-Authorization & Incremental Pre-Authorization Indicate MTID 0100/0110 in transaction flow 4.3.2.4. Refund Indicate MTID 0200/0210 in transaction flow 4.3.2.5. Void Indicate MTID 0200/0210 in Purchase Indicate MTID 0200/0210 in Refund 6.5. Purchase Request / Response Removed MTID 0100/0110 Changed Format for DE-44/DE-62/DE-63 6.6. Pre Authorization Request/Response Changed Format for DE-44/DE-62/DE-63 6.7. Incremental Pre Authorization Request/Response Changed Format for DE-44/DE-62/DE-63 6.8. Pre-authorization Completion Request/Response Changed Format for DE-44/DE-62/DE-63 6.9. Refund Request / Response Removed MTID 0100/0110 DE-38 Mandatory Changed Format for DE-44/DE-62/DE-63 6.10. Void, POS Reversal Transaction Request/Response Changed Format for DE-44/DE-62/DE-63 7.Detailed Description of Data Elements 7.4.DE-6, Amount Cardholder Billing Changed Description 7.12.DE-16, Date, Conversion Changed Description 7.14.DE-18, Merchant Category Code Changed Description 7.22.DE-37, Retrieval Reference Number (RRN) Changed Type to AN12 7.23.DE-38, Authorization Identification Response Removed remarks from Type

		7.24.DE-39, Response Code Introduced Response code for Partial Approval 7.28.DE-44, Additional Data, Response Data Changed Type AN15 and format to Fixed 7.29.DE-47, Additional Data, National Included future change for Key Block support Type to ANS and Format to TLV 7.37.DE-55, ICC System Related Data included MTID 0200/0210 in Table Header Additional TAG 9F6E 7.41.DE-62, Additional Data 2, Private Changed Type to ANS and Format to TLV 7.42.DE-63, Network Data, Private TLV Change Changed Type to ANS and Format to TLV 7.45.DE-74, Credits, Number Changed Type to N and Format to TLV 7.46.DE-75, Credits, Reversals Number Changed Type to N and Format to TLV 7.47.DE-76, Debits, Number Changed Type to N and Format to TLV 7.48.DE-77, Debits, Reversal Number Changed Type to N and Format to TLV 7.49.DE-80, Inquires, Number Changed Type to N and Format to TLV 7.50.DE-86, Credits, Amount Changed Type to N and Format to TLV 7.51.DE-87, Credits, Reversal Amount Changed Type to N and Format to TLV 7.52.DE-88, Debits, Amount Changed Type to N and Format to TLV 7.53.DE-89, Debits, Reversal Amount Changed Type to N and Format to TLV 10.4. Settlement Transaction flows and associated settlement posting Introduced new section in Appendix 13.1. Document Revision History 13.6. Additional Business Use cases To Cover all non-standard business use case flows and Data Element Requirement 13.7.ISO8583 Sample Message Sample ISO8583 Message Sets
2	1.2	4.1. Supported Transactions POS Transaction Updated VOID Message Type indicator 0400/0401,0410

		Updated Reversal Message Type indicator 0420/0421,0430 4.2.2. Response timer Control 4.2.5. Reconciliation Totals 4.2.6. Reversal Processing Included 0420/0430 MTID 4.3.2.1 Purchase 4.3.2.2 Pre-Authorization & Incremental Pre-Authorization 4.3.2.3. Pre-Authorization & Pre-Authorization Completion 4.3.2.4. Refund Included Reference Sections 4.3.2.6. Reversal Update MTID 0420/0430 6.3. ATM & POS Reconciliation Request/ Response Changed Header to include ATM & POS Reflected the changes related to the formats DE-74/DE-75/DE-76/DE-77/DE-80/DE-86/DE-87/DE-88/DE-89 6.4. Network Management Reflected Format level changes for DE-47 6.5. Purchase Request / Response 6.6. Pre Authorization Request / Response 6.7. Incremental Pre Authorization Request / Response 6.8. Pre-authorization Completion 6.9. Refund Request / Response 6.10. Void, POS Reversal Transaction Request / Response Indicated M, C attribute for DE-43/DE-48/DE-60/DE-61/DE-62/DE-63/DE-100/ Removed presence of DE-115 6.9. Refund Request / Response Changed DE-38 in 0200 to be Optional 7.2. DE-3, Processing Code Removed 02 Void 10 Pre-Authorization, AFT 11 Pre-Authorization Completion 7.3. DE-4, Amount Transaction Included compliance for Purchase with cashback transaction, Partial authorization
--	--	--

		Included presence of 0420/0430 for the below data elements 7.1. DE-2 Primary Account Number 7.2. DE-3, Processing Code 7.3. DE-4, Amount Transaction 7.4. DE-6, Amount Cardholder Billing 7.6. DE-10, Conversion Rate, Cardholder Billing 7.8. DE-12, Time, Local Transaction 7.9. DE-13, Date, Local Transaction 7.10. DE-14, Date, Expiration 7.11. DE-15, Date, Settlement 7.13. DE-17, Capture Date 7.14. DE-18, Merchant Category Code 7.15. DE-19, Acquiring Country Code 7.16. DE-22, Point of Service (POS) Entry Mode 7.18. DE-25, Point of Service (POS) Condition Code 7.19. DE-32, Acquiring Institution ID 7.20. DE-33, Forwarding Acquiring Institution ID 7.23. DE-38, Authorization Identification Response 7.24. DE-39, Response Code 7.25. DE-41, Card Acceptor Terminal ID 7.26. DE-42, Card Acceptor Identification Code 7.27. DE-43, Card Acceptor Acquirer Name 7.28. DE-44, Additional Data, Response Data 7.30. DE-48, POS retailer Data 7.31. DE-49, Transaction Currency Code 7.33. DE-51, Currency Code, Cardholder Billing 7.40. DE-61, Point of Service Data, Private 7.41. DE-62, Additional Data 2, Private (For tokenized PI) 7.54. DE-90, Original Data Element 7.58. E-100, Receiving Institution Identification Code 7.59. DE-115, Additional Trace Data 7.2. DE-3, Processing Code Included reference sections 7.3. DE-4, Amount Transaction Included reference sections 7.24. DE-39, Response Code Included reference to Partial Authorization 7.28. DE-44, Additional Data, Response Data Changes in 44.1—Address Verification Result Code (1 Byte) Code R/S/W/X 7.29. DE-47, Additional Data, National
--	--	---

		Removed old format (Variant) 7.34. DE-52, Personal Identification Number (PIN) Data Indicated the presence limited to only requests 7.36. DE-54, Additional Amounts Updated Description Compliance additional info for purchase with cashback/Partial authorization Included references sections 7.37. DE-55, ICC System Related Data TAG 9F19 included 7.39. DE-60, Additional Data Indicated the presence limited to only requests 7.40. DE-61, Point of Service Data, Private Updated Subfield 12 details DE 61, subfield 14 Included references sections 7.41. DE-62, Additional Data 2, Private Amended additional sub fields 7.42. DE-63, Network Data, Private TAG 02 clarification 7.60. DE-122, Remaining Open to use Changes reflected to field edits/constraints 7.61. DE-123, Address Verification Data New Data Element included 13.6.1.1. POS Balance Enquiry Indicated M/C Presence for DE-48/DE-60/DE-61/DE-62/DE-100 Removed presence of DE-62/DE-63/DE-115
3	1.3	4.3.2.2. Pre-Authorization & Incremental Pre-Authorization Changed requirement for DE-38 to be entered in incremental pre-authorization 6.1. ATM Financial Transaction Request/ Response DE-14/DE-18 Indicator in 0210 Response 6.2. ATM Reversal Request/ Response DE-14/DE-18 Indicator in 0410 Response

	6.3. ATM & POS Reconciliation Request/ Response Removed De-2 DE-50 Format Corrected 6.5 Purchase Request/Response DE-48/DE-60 Changed Mandatory for Issuer DE-62/DE-63 Changed Conditional for Issuer DE-32/D-33 Format corrected 6.6. Pre Authorization Request / Response DE-48/DE-60 Changed Mandatory for Issuer DE-62/DE-63 Changed Conditional for Issuer DE-32/D-33 Format corrected 6.7. Incremental Pre Authorization Request / Response Indicated Values to be mirrored from original pre-authorization in the incremental pre-authorization requests DE-48/DE-60 Changed Mandatory for Issuer DE-62/DE-63 Changed Conditional for Issuer DE-32/D-33 Format corrected 6.8. Pre-authorization Completion DE-48/DE-60 Changed Mandatory for Issuer DE-62/DE-63 Changed Conditional for Issuer DE-32/D-33 Format corrected 6.9. Refund Request / Response DE-48/DE-60 Changed Mandatory for Issuer DE-62/DE-63 Changed Conditional for Issuer DE-32/D-33 Format corrected 6.10. Void, POS Reversal Transaction Request / Response DE-35/ DE-52/DE-53/DE-55/DE-57 indicators updated Updated requirement for DE-38
--	---

		DE-32/D-33 Format corrected 7.22. DE-37, Retrieval Reference Number (RRN) Changed Format to Fixed Changed Description 7.30. DE-48, POS retailer Data Changed Format to LLVAR 7.37. DE-55, ICC System Related Data Constraints related to 0220/0230 7.38. DE-57, EMV System Related Data Format Corrected 7.39. DE-60, Additional Data Changed Format to LLVAR 12.5. Pre-Authorization & Pre-Authorization Completion Updated requirement for Data Elements contents form Original Pre-Auth in incremental Pre-Authorization requests 12.5. Refund Transaction Removed 8. No settlement, interchange, authorization, or MSC fees are levied on a Refund Transaction. Sequence 9/10/11/12 updated to reflect issuer bank compliance policy 13.7.1.3. Key Exchange TLV format Key Block TR-31 Key Block Sample
4	1.4	7.10. DE-14, Date, Expiration Field Edits Corrected 7.14. DE-18, Merchant Category Code Constraints for ATM / POS Transactions indicated 7.30. DE-48, POS retailer Data Constraints Corrected 7.37. DE-55, ICC System Related Data

		0110/0210 Tag indicator presence 0400 Tag indicator Presence 9F6E - Length Indicator 7.39. DE-60, Additional Data Constraints Corrected
5	1.5	Added below transactions 2.8 Ecommerce transaction added 3.5 File update Message added 3.6 Administrative message Included 4.1 Below transaction added in supported Transaction section - E-commerce - Account Verification Inquiry for Token transaction - Recurring Transaction 4.2.6 Response code updated 4.3.2.1 Diagram added for DMS transaction 4.3.2.4 Diagram for Refund transaction added 4.3.2.5 Diagram changes for DMS functionality 4.3.2.6 Diagram changes for DMS functionality 4.3.2.7 Diagram added for E-commerce transaction 5.2 Added Administrative and file update message 6.1 Added DE-6 and DE-51 and Token data 6.5 Added Token data and removed DE-62 6.6. Added Token data in preauthorization 6.7 Added Token data and removed DE-62 6.8 Added Token data and removed DE-62 6.9 Ecommerce transaction Added

		6.10 MOTO transaction Added 6.11 Added Token data and removed DE-62 6.13 Added Account Verification for Token transaction 6.14 Added Life cycle management message for Jaywan TSP 6.15 Added Life cycle Management message as Issuer Update 6.16 Added message for Send OTP 6.17 Added message Onus transaction detokenization 7.28 Removed CAVV and CVV2 from DE-44 7.41 Removed DE-62 7.58 Added DE-104 for CVV2 and CAVV 7.59 Added DE-105 for Tokenization 10.4 Added diagram for DMS settlement 12.12 Added compliance section for Recurring 12.13 Added compliance section for Tokenize transaction 12.14 Added compliance section for Ecommerce transaction 12.15 Added compliance for MOTO transactions.
6	1.6	4.2.2 Updated Response timer Control 4.2.6 Added Value 00 = Approved in Acquirer Reversal Processing 4.6.1.2 Added Jaywan Mono Badge Card - Token Provisioning flow 4.6.2.1 Changed tittle to Jaywan Mono Badge Card - Life cycle Management from Issuer 4.6.2.2 Changed tittle to Jaywan Mono Badge Card - Life cycle Management from TR 4.6.2.3 Added Jaywan Co-Badge Card - Life Cycle Management from Issuer flow

	4.6.2.4 Added Jaywan Co-Badge Card - Life Cycle Management from TR flow 6.1 Updated DE 105 tag details 6.2 Added DE 105 tag details in ATM Reversal Request and Response table 6.3 Updated field 99 name in ATM & POS Reconciliation Request and Response table 6.4 Added field 48 and 105 tag details in Purchase transaction request and response table 6.5 Added fields in Pre Authorization request and response table 6.6 Added fields in Incremental Pre-authorization request and response table 6.7 Added Acquirer action in Pre-authorization Completion 6.8 Added fields in Preauthorization Completion request and response table 6.9 Added fields in Ecommerce request and response table 6.10 Added fields in MOTO Transaction Request and Response table 6.11 Added fields in Recurring Transaction Request and Response table 6.12 Added fields in Refund Request and Response table 6.13 Added fields in Void/Cancel/Reversal Transaction Request and Response table 6.14 Added fields in Account Verification request and response table 6.15 Added fields in Token Provisioning Request and Response table 6.16 Added fields in Send OTP Request and Response table 6.17.1 Added fields in Life Cycle Management – Token Request and Response table 6.17.2 Added fields in Life Cycle Management- (Issuer request and response) table 6.18 Added fields in Onus Transaction request and response for detokenize card table
--	--

	6.19 Added Offline Transactions/Financial Transaction Advice (Debit/Credit) 7.3 Added changes for international acceptance and for international acceptance 7.4 Added changes in compliance rules for DE-49 7.10 Added validation details 7.14 Updated message types for DE-18 7.16 Added DE-63, DE-104 in compliance rule checks 7.18 Added 09,10 values in description for DE-25 7.21 Updated compliance rule for DE-35 7.24 Added few reason codes 7.26 Added compliance rule for Card-on-File (CoF) provisioning 7.27 Added compliance rule for Card-on-File (CoF) provisioning 7.28 Updated type to AN15 for DE-44 7.31 Added compliance rules for DE-49 7.34 Added changes in field edits and presence 7.36 Added formats for purchase with cashback and For Partial Auth in description for DE-54 7.37 Added changes in constraints for Remote Pay transactions 7.38 Added changes in EMV tag sample table for tag 05 7.40 Updated the data element length to AN.255 (LLVAR) Added changes in Subfield 7 (POS Transaction Status) 7.41 Updated the data element length to ANS..255(LLVAR) Added Tag changes for tag 03,04 for DE-63 7.58 Added additional tags for DE-104 7.59 Added tag changes
--	--

		7.62 Updated data element tittle from Account to Address for DE-123 12.3 Added details in General compliance 12.12 Added MIT/Recurring Transactions 12.13 Added Tokenization details 12.14 Added details for Ecommerce Transaction, Digital Secure Remote Payments and Card On File Transactions 12.15 Added details in MOTO Transactions 12.16 Added details for Offline Transaction/Financial Transaction Advice 12.17 Added details for Deferred Authorization
7	1.6.1	<u>Updated the below sections for Co-Badging Support</u> 4.6.1.2 Jaywan Co-Badge Card - Token Provisioning Updated the flow 4.6.2.3 Jaywan Co-Badge Card - Life Cycle Management from Issuer Updated the flow 4.6.2.4 Jaywan Co-Badge Card - Life Cycle Management from TR Updated the flow 12.13.1 Token Life Cycle Management (LCM) Updated the flow <u>Updated the below sections for Card On File Support.</u> 6.17 COF Provisioning Request / Response - Added COF Provisioning Request/Response flow 6.18.1 Life Cycle Management – Token Completion/Event Notification (Request and Response) 12.13 Tokenization Updated Issuer response mapping In the case of Merchant Provisioning (COF), issuers will receive DE-105 tag 21 as M4M_PAY. Updated the section 6.7,6.9,6.11,6.12,6.13,6.18.1,6.20 for the below data elements, DE-105 tag 04 & 10 changed to conditional to support COF Added DE-105 tag 26,27 & 28

Minor changes on the data layout

6.1 ATM Financial Transaction Request/ Response

DE-18 Issuer Response made O – Optional as per the current processing for ATM transactions

6.2 ATM Reversal Request/ Response

DE-14 Issuer Response made O – Optional as per the current processing for ATM transactions

DE-43 Issuer Response made O – Optional as per the current processing for ATM transactions

6.5 POS Purchase Request / Response

Added DE-63 Tag 02 Transaction Identifier for DMS transaction support

DE-63 Tag 03 Updated the tag response flow from switch to acquirer

6.6 POS Pre-authorization Request / Response

Removed DE-54 Additional Amounts

DE-63 Tag 03 Updated the tag response flow from switch to acquirer

Removed DE-104

DE-105 Tag 06,07,08 & 09 changed to mandatory

6.7 Incremental Pre Authorization Request/Response

Removed DE-54 Additional Amounts

DE-63 Tag 03 Updated the tag flow from switch to acquirer

Removed Switch Response (C104) for DE-104 Tag 07

DE-105 Tag 06,07,08 changed to mandatory

6.8 Pre-authorization Completion

Removed DE-54 Additional Amounts

DE-63 Tag 03 Updated the tag flow from switch to acquirer

6.9 Ecommerce Request/Response

DE-63 Tag 03 Updated the tag flow from switch to acquirer

Removed Switch Response (C104) for DE-104 Tag 07

6.11 Recurring Transaction Request/Response

DE-63 Tag 03 Updated the tag flow from switch to acquirer

Removed Switch Response (C104) for DE-104 Tag 07

DE-104 tag 06 changed to conditional

6.12 Refund Request/Response

Removed DE-54 Additional Amounts

DE-63 Tag 02 Added C063 from Acquirer

DE-63 Tag 03 Updated the tag flow from switch to acquirer

	Added DE-104 tags 03,04,05 & 06 Removed Switch Response (C104) for DE-104 Tag 07 6.13 Void/Cancel/Reversal Transaction Request/Response Removed DE-104 tag 07 Token Cryptogram Removed DE-105 from Issuer response 6.14 Account Verification DE-63 Tag 03 Updated the tag flow from switch to acquirer 6.15 Wallet Based Token Provisioning Request / Response DE-105 Tag 19 Switch and Issuer response made optional 6.16 Send OTP Added DE-33 Forwarding Institution ID Added DE-100 Receiving Institution ID 6.19 Onus transaction Detokenization Added DE-14 Date, Expiration DE-18 Acquirer response made optional Added DE-105 tag 21 Wallet Provider ID 6.20 Offline Transactions/Financial Transaction Advice (Debit/Credit) Removed DE-54 Additional Amounts DE-63 Tag 03 Updated the tag flow from switch to acquirer 6.21 POS Balance Enquiry Added POS Balance Enquiry 7.21 DE-35, Track II Data Updated Compliance Rule for tokenized transaction 7.24 DE-39, Response Code Contactless Transactions no CVM thresholds Deleted Condition - The acquirer should populate DE-57 Position 5 with the value 3 7.27 DE-43, Card Acceptor Acquirer Name Updated constraints - In the case of transactions originating from aggregator merchants, this field must contain the actual merchant's name 7.28 DE-44, Additional Data, Response Data Changed Presence - Optional. Reserved for Future Use 7.36 DE-54, Additional Amounts Updated presence details
--	---

	7.37 DE-55, ICC System Related Data EMV Tag 9F33 Updated to Conditional and updated usage condition EMV Tag 9F6E - Updated Usage Condition Added EMV Tag 9F25 – FPAN Suffix Updated Constraints 7.38 DE-57, EMV System Related Data Deleted Position 5 value 3 Updated Format - Fixed (EBCDIC) 7.58 DE-104, Additional data – Payment Services The format type corrected. 7.59 DE-105, Token Data Updated comments for Tags 03,04,09,10,31,33,34,36,52 Updated DE-105 presence details Updated tag 48 length to ANS99 Updated tag 34 length to AN2 7.61 DE-122, Remaining Open to use Updated Presence details 12.6 Refund Transaction Updated under compliance rules for ECom Refund. 12.14 Ecommerce Transaction For 3DS authenticated Transactions – Updated DE 104 Tag 05 = CAVV result code (If the issuer has opted for OBS, it will contain the validation result otherwise the value will be U) Card On File Transactions – Deleted DE 105 Tag 21 = M4M_PAY for acquirers (if COF token is used) For Issuers – Added DE-105 Tag 21 as M4M_PAY indicating it is a tokenized COF 12.16 Offline Transaction/Financial Transaction Advice Added Compliance rule for Acquirers - This feature must be enabled only for UAE Switch issuers and should not be available to GCC-issued cards. Added Compliance rules for Issuer 12.16.2 Special Offline Use Cases Moved Compliance rules for Issuer to 12.16 section 12.17 Deferred Authorization Added Compliance rule for Issuer 13.3 Data Formats & Data Encoding Standards
--	---

	Updated length format examples for LLVAR and LLLVAR
	13.6 Additional Business Use cases Added details for the additional business use cases for the below, Pre-Authorization Services Refund (0200/0210) Cancellation/Void Account Status Inquiry No Show Remote Payments Resubmissions/Reauthorizations Time based payment authorization request or Subscriptions or Installments/Recurring Payment Related/Delayed Charges Un Schedule Transactions COF (CIT/MIT) Partial Shipment Onus Detokenization

13.2 Abbreviations in Data Element / Message format

AQ	Acquirer
SW	UAESWITCH
ISS	Issuer
M	Field, Mandatory
CX	Field, Conditional (Appendix 13.4)
->	Field, Forwarded and unchanged
DE	Data Element
A	Alphabetic characters
N	Numeric characters in the ASCII/EBCDIC text range
S	Special Characters
An	Alphanumeric (alphabetic and numeric characters)
as	Alphabetic and special characters
ns	Numeric and special characters
ANS	Alphabetic, numeric, and special characters
VAR	Variable length field
3	Fixed length of three characters
B	Binary representation data

BCD	Binary Coded Decimal: Binary representation of each digit by 4 bits, which in general represent the values/digits/characters 0-9.
HB	Hex Binary representation of data
MM	Month
DD	Day
YY	Year
HH	Hour
Mm	Minute
SS	Second
LL,LLL	length of variable field that follows Length of variable field that follows. 'LL' - Two-digit length indicator (1 byte BCD); LLL Three-digit length indicator (2 bytes BCD); LLLL-Four-digit length indicator (3 bytes BCD)
VAR	variable length field
3	fixed length of three characters
..17	Variable length up to maximum 17 characters. All variable length fields will in addition contain two to three positions at the beginning of the field to identify the number of positions following to the end of that field.
...17	Variable field of up to 17. The '...' is a Three-digit length indicator (2-byte BCD) specifying the number of digits defining the length of the variable data to follow.
X	"C" for credit, "D" for debit and must always be associated with a numeric amount data element, i.e., x + n16 in amount, net settlement means prefix "C" or "D" and 16 digits of amount, net settlement. An amount of zero should be prefixed with a "C"
Z	Tracks 2 and 3 code set as defined in ISO 7811 and ISO 7813.
P2PE	Point to Point Encryption
TDES	Triple DES

13.3 Data Formats & Data Encoding Standards

Numeric Data	Fields with logical representations containing only type "n" data will be formatted in Binary Coded Decimal (BCD). All such fields must be sent as an integer number of bytes, right justified and padded with leading zeroes where necessary.
Non-Numeric Data	Fields with logical representations containing type "a", "s" or "x" data will be formatted in EBCDIC. All such fields must be sent as an integer number of bytes, left justified and padded with trailing spaces where necessary.

Track 2 Data	Track 2 data (field 35) must be formatted in Binary Coded Hexadecimal (BCH), right justified with leading zeroes. The field separator character must be formatted as hexadecimal 'D'.
Variable Length Data	Variable length fields must have the LL or LLL length component formatted as a single hexadecimal byte, preceding the main data component of the field. The data component of variable length fields must be formatted according to the rules defined above for Numeric, Non-numeric and Track 2 Data.
“LLVAR”	“LL” indicates the number of positions in the VLI, and the value in the VLI shows the length of the variable-length data subfield that follows. The length may be 01 to 99 “VAR” is the variable length data subfield Example: A 27-byte field with “LLVAR” indicates a VLI of 2 digits (1 bytes) with a maximum length of 25 bytes of variable data.
“LLLVAR”	“LLL” indicates the number of positions in the variable-length data subfield that follows. Length may be 001 to 999 Example: A 503-byte field with “LLLVAR” indicates a VLI of 3 digits (2 bytes) with a maximum length of 500 Bytes of variable data.
Bit Maps	Each bit map must be sent as a set of four consecutive binary two-byte blocks in ascending order by field position i.e., fields 1 to 16 in the first two-byte block, fields 17 to 32 in the second two-byte block, fields 33 to 48 in the third two-byte block and fields 49 to 64 in the Fourth two-byte block.
TLV	Tag Length Value

13.4 Conditional Data Element in message field

Abbr. of Condition	Explanation
C5	Settlement Amount
C6	Cross Border Transaction Set by Switch
C14	DE14 may not be present in the Manual, Moto and Merchant Initiated Transactions(MIT)
C15	Required if DE-70 is set as '201' (cutover) in 0800
C16	Cross Border Transaction Set by Switch If present in original transaction, same to echoed in advice/reversal messages
C23	Required for EMV Transaction Transporting CHIP data DE2-22, DE-23, DE-55, DE-57 Related. (if tag 5F34 can be present in the contact/contactless card)
C35	For chip-based transactions Data element "Track 2 equivalent data" identified by tag '57', excluding pad characters, when present.
C38	Required for Purchase/Pre-authorization/Pre-Auth completion/Refund/ authorization Required for Successful authorization
C44	Optional. To be populated by Issuer Future Use case
C47	Required if DE-70 is set as '101' (Key Exchange) in 0800
C50	Settlement Currency Code
C51	For Cross-Border transactions. Set by Switch If present in original transaction, same to echoed in advice/reversal messages
C52	Required for Pin Based transaction
C53	Required for Pin Based transaction
C54	Present for cashback transaction/partial authorization If present in original transaction, same to echoed in advice/reversal messages
C55	Required For chip-based transactions and wallet based transactions.
C57	Required For chip-based transactions
C62	Tokenized Instrument example OEM Wallet (Apple Pay/Samsung Pay/Google Pay) If present in original transaction, same to echoed in advice/reversal messages
C63	POS Pre-authorization request Processing Conditions If present in original transaction, same to echoed in advice/reversal messages C063 Transaction identifier will be available for all DMS transactions
C66	If DE66 is '2' or '3' then the following Data Elements to be populated DE-74/ DE-75/DE-76/DE-77/DE-80/DE-86/DE087/DE-88/DE-89
C95	Will be present when the reversal transaction is for an amount other than the original transaction amount (DE-4).

	Not present in Full reversal
C104	This Data element is present in ECOM Purchase/Pre-Auth, Token provisioning and MOTO transactions. On the basis of transaction, this data element populates value of CVV2, ECOM indicator and CAVV related data.
C105	Tokenization related data is present in this field. This field will be present in all tokenized transaction.
C122	Required for 0210 approval responses to both balance inquiry requests and cash withdrawal requests. It is also mandatory in declined cash withdrawal requests where DE-39 (Response Code) is 51 or 61.

13.5 Envisaged Services

Service Name	Description	Support
Funds Request for Top-up	A service requesting funds for loading of a prepaid mobile top-up account. The top-up of the account itself is not directly addressed. In contrast to a Payment transaction for Services, this service transports additionally mobile phone data.	An Authorization with a specific Processing Code and Card Acceptor Business Code using Authorization Request and Authorization Request Response. Additional mobile phone information e.g., for supporting dispute handling is transported as private data.
Payment with Cashback	A service which allows the cardholder to obtain cash from the card acceptor in conjunction with a payment. Also called a Cashback transaction. The cardholder receives the extra amount in cash along with the goods/services.	Authorization of an accurate amount with a specific Processing Code and an additional amount field using Authorization Request and Authorization Request Response. An issuer has the possibility to approve the Payment amount but decline the Cashback amount. Partial Reversals are not supported for Payment with Cashback

13.6 Additional Business Use cases

Service Name	Description	Support
Pre-Authorization Services	A service composed of the 3 steps Pre-Authorization, Update Pre-Authorization (optional and potentially with several occurrences), and Payment Completion A Pre-Authorization allows the card acceptor to reserve an amount for a specified period of time to ensure that sufficient funds are available to complete a subsequent payment. The Pre-Authorization is used only to reserve the amount since neither the final amount nor the final date and time of the actual payment are known (e.g., car rental, hotel, video rental, etc.). Pre-Authorization is also called "Reservation". The Update Pre-Authorization allows the card acceptor to update the estimated amount and/or the validity period of the previous Pre-Authorization or the previous Update Pre-Authorization. Also called a supplementary authorization The Payment Completion allows the card acceptor to finalize a payment following a Pre-Authorization or Update Preauthorization Request.	First step (Pre-Authorization) and optional subsequent steps (Update Pre-Authorization): Authorization of an estimated amount valid for a specified period of time, using Pre-Authorization Request (first step), optionally Update Pre-Authorization Request (Subsequent steps), and Authorization Request Response. At any time before the validity period expires an acquirer may generate an Update Pre-Authorization Request which, if approved, supersedes the most recent (Update) Pre-Authorization. Final step (Payment Completion): There are two options for the acquirer gateway to perform the final step: Partial Reversal if the final amount is less than the most recently authorized amount, using Reversal Advice, Reversal Advice Repeat, and Reversal Advice Response Confirmation of the final amount, using Completion Advice, Completion Advice Repeat, and Authorization Advice Response The issuer gateway must support both options.

UAESWITCH Interface Technical Specifications

Refund (0200/0210)	A service which allows the card acceptor to reimburse the cardholder partially or totally. Unlike Cancellation, Refund is not necessarily linked to any previous transaction.	Authorization with a specific Processing Code using Authorization Request and Authorization Request Response.
Cancellation/Void	A service which allows the card acceptor to cancel a previously approved transaction. Cancellation should only occur before the transaction is cleared to the issuer. It is sometimes called "Manual Reversal".	Full Reversal with a specific Message Reason Code using Reversal Advice, Reversal Advice Repeat, and Reversal Advice Response.
Account Status Inquiry	A service that allows the validity of the card to be checked. This transaction is only for information and has no financial impact on the card account. It is sometimes called "Information request" Merchants/Acquirers can make use of this services for Card On File tokenization.	Authorization with request containing specific attributes in DE-22, DE-25, DE 61 SF7 and optionally DE-104
No Show	A service which allows the card acceptor to charge the cardholder's account due to the fact that the cardholder has not arrived within the specified time and has not cancelled the guaranteed reservation within the specified period. It is used e.g., for hotel trade.	No Show may be performed without an online authorization. If there was a Pre-Authorization, No Show may be performed as the final step of the Pre-Authorization Services (two options). If there was an authorization of a Payment, No Show may be performed as a partial Reversal, if the amount to be charged is less than the authorized amount.
Remote Payments	A Remote Payment is a transaction where a customer uses the wallets to perform transactions from Merchants website/app	Authorization with transaction Request containing Specific attributes in DE-22 and containing a DE-105.
Resubmissions/Reauthorizations	A cardholder's monthly subscription fails due to insufficient funds. The merchant retries the	MIT Authorization that is re-attempted after a previous authorization request was declined, where the issuer's response does

	transaction again to recover the money.	not restrict the merchant from trying again. Authorization with request containing specific attributes in DE-22, DE-25, DE 61 SF7 and optionally DE-104
Time based payment authorization request or Subscriptions or Installments/ Recurring Payment	A service where a cardholder enrolls for a service and agrees with the merchants to have them paid in intervals as fixed or variable amount.	A transaction that is part of a series, made under an agreement between a cardholder and a merchant, where the cardholder authorizes the merchant to store their account details and initiate one or more future transactions of a fixed or variable amount over a specified time period. The transaction series is based on a single purchase. Every recurring transaction shall use the same Transaction id (DE63.02) used in the original authorization. The original authorization should be securely authenticated. Authorization with request containing specific attributes in DE-22, DE-25, DE 61 SF7 and optionally DE-104
Related/Delayed Charges	A service where a merchant like car rental company may charge for fuel or toll fees after the vehicle has been returned by the cardholder.	A subsequent charge applied to the account after the original transaction has been completed and services rendered. Original transaction id(DE63 tag02) should be sent in DE104 tag06. Authorization with request containing specific attributes in DE-22, DE-25, DE 61 SF7 and optionally DE-104
Un Schedule Transactions COF (CIT/MIT)	Service where the consumer agrees to allow the merchant like utility provider to initiate a charge whenever the postpaid electricity bill is generated, based on usage. Since billing amounts and dates may vary, the charges are initiated as unscheduled transactions.	A transaction made under an agreement between a cardholder and a merchant, where the cardholder authorizes the merchant to store and use the cardholder's account information to initiate one or more future transactions. These transactions may be for a fixed or

UAESWITCH Interface Technical Specifications

		variable amount but occur irregularly, without a fixed schedule. Authorization with request containing specific attributes in DE-22, DE-25, DE 61 SF7 and optionally DE-104
Partial Shipment	When a merchant is not able to process the full quantity of goods ordered via e-commerce at the time of purchase. As a result, the items are shipped separately, and each shipment is processed as an individual transaction	Authorization with request containing specific attributes in DE-22, DE-25, DE 61 SF7 and optionally DE-104
Onus Detokenization	A service that allows to convert a tokenized PAN into the actual PAN for processing of On-us transactions.	Authorization to be sent with specific processing code In Request DPAN will be present in DE-2 In Response FPAN will be present in DE-2 and DPAN will be present in DE-105 tag 01

13.7 ISO8583 Sample Layout for Specific Data Element

13.7.1 Key Exchange Data Layout

13.7.2 Key Exchange Fixed 41 Digits

MTID	0800	
Key Sample	BFDDDEFAD7775D5892BFD7041FB6C4E43D6B1E101	Length 41
New Key Value	BFDDDEFAD7775D5892BFD7041FB6C4E4	Length 32
Check Digit Value	3D6B1E	Length 06
Acq Working Key	1	Length 01
Sequence	01	Length 02

13.7.3 Key Exchange TLV format Variant

MTID	0800	
Key Sample	01032BFDDDEFAD7775D5892BFD7041FB6C4E4020063D6B1E0300110400201	
Tag	01	
Length	032	
New Key Value	BFDDDEFAD7775D5892BFD7041FB6C4E4	Length 32
Tag	02	
Length	006	
Check Digit Value	3D6B1E	Length 06
Tag	03	
Length	001	
Acq Working Key	1	Length 01
Tag	04	
Length	002	
Sequence	01	Length 02

13.7.4 Key Exchange TLV format Key Block

MTID	0800	
Key Sample	01073RA0072P0TN00N00000E847ADFF1404E3C75843F9D6033FCF6D4DDAFC2C377CE5239F25189020063D6B1E0300110400201	
Tag	01	
Length	073	
New Key Value	RA0072P0TN00N00000E847ADFF1404E3C75843F9D6033FCF6D4DDAFC2C377CE5239F25189	Length 73
Tag	02	
Length	006	
Check Digit Value	3D6B1E	Length 06
Tag	03	
Length	001	
Acq Working Key	1	Length 01
Tag	04	
Length	002	
Sequence	01	Length 02

13.7.5 Reconciliation Data Layout

13.7.6 TLV Format DE-74,DE-75,DE-76,DE-77,DE-80

MTID	0500,502	
Key Sample	01101111111111110210222222222203103333333333	
Tag	01	
Length	10	
New Key Value	1111111111	Length 10
Tag	02	
Length	10	
Check Digit Value	2222222222	Length 10
Tag	03	
Length	10	
Acq Working Key	3333333333	Length 10

13.7.7 TLV Format DE-86,DE-87,DE-88,DE-89

MTID	0500,502	
Key Sample	01161111111111111111021622222222222222220316333333333333333333333333	
Tag	01	
Length	16	
New Key Value	1111111111111111	Length 16
Tag	02	
Length	16	
Check Digit Value	2222222222222222	Length 16
Tag	03	
Length	10	
Acq Working Key	3333333333333333	Length 16