Oman National ATM/POS Switch Network

OmanNet Operating Rules

Technical Book 1 - Terminal & Card Specifications

Version 2.0 – February 2014

Table of Contents

Table of Figures

Table of tables

Change Control

Document Amendment Record			
Change No.	**Date**	**Prepared by**	**Brief Explanation**
Version 1	December 2010	CBO PSD	Initial Version
Version 1.1	January 2014	CBO PSD	Revision for EMV and Additional Switch Functionality Section 1: Revised for ATM and POS chip requirement and transaction flow Section 2: Revised for chip specifications, personalization requirements, and PIN management
Version 1.2	February 2014	CBO PSD	Revision based on first feedback Section 1: Addition of Account to Account Transfer flow Section 2: Content revised Document formatting
Version 2.0	February 2014	CBO PSD	Section 1: (1.2.4) Automatic reversal generation on late response. (1.2.6.3) Wrong PIN statement removed. (1.2.6.5) RRN replaced with STAN for refund Second Release

1 Terminal Specifications

1.1 ATM Terminal Specifications

1.1.1 ATM Physical and Protocol Requirements

1.1.1.1 Display Requirements

- ATMs participating in the OmanNet network should preferably present a full screen graphical interface; single line interfaces are acceptable as well.

1.1.1.2 Magnetic Stripe Reader

- The Magnetic stripe reader should be capable of reading Track-2 encoded data from ISO/IEC 7813:2001 compliant payment cards.

1.1.1.3 Chip Card Reader

- The Chip Card reader should be capable of reading chip personalized with data from ISO/IEC 7816:2001 compliant smart cards
- The Chip Card reader must be compliant with the mechanical and electrical requirements as specified by EMVCo and EMVCo type approved[1]
- The Chip Card reader must be integrated with the Magnetic Stripe reader

1.1.1.4 Receipt Printer

- All ATMs must provide a transaction receipt. No transactions should be initiated when the receipt printer is not available, or is out of paper.

1.1.1.5 Audit Trail

- All ATMs must have Audit Trail capability in the form of either a Journal Printer or Electronic Journal
- The Audit Trail functionality should capture transaction logs, terminal events and device status

1. EMVCo Type Approval testing is divided into two levels. The Level 1 Type Approval process tests compliance with electromechanical characteristics, logical interface, and transmission protocol requirements defined in part 1 of the EMV specifications. Level 2 Type Approval tests compliance with debit/credit application requirements defined in the remainder of the EMV specifications (refer to the EMVCo website for details – http://www.emvco.com).

1.1.1.6 PIN Entry Device (PIN Pad)

- The PIN Pad should be compliant with the requirements as specified in ISO 9564-1:2002
- The PIN Pad must be PCI/PED certified
- The PIN Pad should be configured to accept PIN values up to the maximum of 12 digits. PIN Pad keys must be identified both in Arabic and English. Support of alphanumeric PIN values is not a requirement.

1.1.1.7 Communications Interface

There is no requirement for an interoperable communication infrastructure between the ATM and the Acquirer host system, as it is beyond the scope of OmanNet specifications.

However OmanNet recommends the following to be implemented at the Acquirer system level:

- Synchronization of Date/Time between the ATM and the Acquirer host system. Additionally the host system should also synchronize the clock with a date/time server
- Remote Key Loading at the ATM for PIN Encipherment
- Secure Messaging through MAC for all transactional messages between ATM and the Acquirer system

1.1.2 Magnetic Stripe / Chip Selection Requirements

The ATMs capability of reading Chip card technology shall be the primary method of reading payment cards. The magnetic stripe method shall be utilized under the following conditions:

- ICC not present on the card and the service code on the magnetic stripe should indicate that it is a magnetic stripe card
- ICC cannot be read due to ICC failure or ICC reader failure (fall back indicator must be present)

The magnetic stripe technology shall be supported by the ATMs, mainly, to process magnetic stripe only cards or fallback due to dirty or damaged ICC. However, at no time shall the ATM use magnetic stripe processing when:

- No usable application on the ICC, AIDs do not match between ICC and the ATM
- Smart card not usable, i.e. ICC is blocked

1.1.3 PIN Security Requirements

Acquirer Banks are required to comply with PCI PIN Security Requirements for the secure management, processing and transmission of Personal Identification Number (PIN) data during transaction processing at the ATMs (refer to PCI website for details http://www.pcisecuritystandards.org).

1.1.4 Transaction Set Support

The following sets of ATM transactions are required to be supported for OmanNet card:

Transaction	Description
Cash Withdrawal	A cash disbursement obtained at an ATM. Note: It is recommended that terminal do not support partial dispense.
Cash Withdrawal Reversal	A cash withdrawal reversal can be caused by multiple reasons, ATM hardware malfunction, EMV cryptogram error, and card holder not taking the card on time. Reversals for ATM cash withdrawal transaction could be for the full amount (full reversals) or part of the amount (partial reversals).
Balance Inquiry	This is an online inquiry for the balance of a specific cardholder's account. This service displays and prints the account balance for the primary account belonging to the cardholder.
Mini Statement	Mini-statements can list previously initiated transactions including deposits, credits and debits. They are printed on standard receipts when cardholders select the mini-statement option. Available only to OmanNet local debit cards.
Cardholder Account Transfer	This transaction enables the cardholder to transfer from his card's account to another account belongs to same cardholder. Available only to OmanNet local debit cards.

Account to Account Transfer **(Inter Bank Funds Transfer)**	Account to Account Transfer is a service available on on-us ATM to OmanNet debit cards. This service permits the cardholder to transfer funds to another OmanNet member bank debit card. The implementation of the sender service is optional to the bank

Table 1 – ATM Transaction Set

1.1.5 General Acceptance at ATM

The following provides an overview of the general transaction acceptance requirement and best practices that apply to Magnetic Stripe and Chip card.

1.1.5.1 Primary Account Number (PAN)

- ATM accepting OmanNet cards must accept Primary Account Number (PAN) up to 19 digits that contain a valid IIN registered with OmanNet.

1.1.5.2 Expiration Date

- ATM accepting OmanNet cards should not decline a transaction based on the expiration date on the card. The ATM must accept the transaction even if the card has expired and route it online for issuer authorisation.

1.1.5.3 Account Selection

ATM accepting OmanNet cards should allow the cardholders to select accounts of the following types:

- Default Account
- Checking or Current Account
- Savings Account

1.1.5.4 Language Selection

- ATM accepting OmanNet cards should prompt the cardholder with a screen allowing for the selection of the language

- at least, English and Arabic languages should be supported, other languages are optional

1.1.6 Magnetic Stripe Transaction Flow

The following subsections illustrate how an Acquirer could implement the requirements; Acquirers may implement other methods as long as they are compliant with the underlying specifications and satisfy the overall requirements.

- ATM transactions shall be processed in online processing mode only. OmanNet requires all authorizations to be done online; this includes online card authentication

- A transaction is initiated once a card is inserted into the magnetic stripe reader of the ATM

1.1.6.1 Withdrawal

The Withdrawal transaction is a financial transaction that offers cash disbursement facility to the cardholder.

1. **Welcome screen**

   - The first screen displayed to the OmanNet cardholder should show a welcome screen with the message "Welcome to OmanNet Services"
   - The Acquirer can choose to integrate the welcome screen with the language selection screen as well

2. **Language Selection**

   - The ATM presents the cardholder with a screen allowing for the selection of the language
   - As a minimum requirement, ATMs must offer language support for English and Arabic; other languages are optional

   Note: This step is not repeated if the Language was already selected for another transaction

3. **PIN Entry**

   - The cardholder enters his PIN code
   - ATMs must allow for entering 4 to 12 digits PIN length values

   Note: This step is not repeated if a valid PIN was entered for a previous approved transaction

4. **Transaction Selection**

   - The ATM allows for prompts selection of available transactions
   - Only transactions supported for the card are presented to the cardholder
   - The cardholder must select "Cash Withdrawal"

5. Account Selection

The ATM presents the cardholder to select an account from the following:

- Default Account
- Checking or Current Account
- Savings Account

6. Amount Selection

- The ATM presents the cardholder with a set of pre-defined amounts or allow the cardholder enter a different amount
- The ATM should only present amounts it can dispense
- For cardholder's selected amounts, the ATM should reject amounts it cannot dispense or that exceed the maximum limit per transaction

7. Online Processing

- The ATM generates an authorization request (or its local equivalent) containing all the data relevant to transaction routing and processing
- The Issuer will respond with one of the following (but not limited to that, for the list of valid response code, refer to Member Bank Interface Specifications):
    - Transaction Authorized
    - Transaction Declined, Not Sufficient Funds
    - Transaction Declined, Wrong PIN
    - Transaction Declined, Exceeds Withdrawal Limit
- If the Issuer could not be reached, an Error response is returned to the Acquirer

8. Transaction Completion

- For approved transactions, the ATM will collect the money from the appropriate cassettes. If an error was encountered during this process or the approved amount cannot be dispensed, the transaction is cancelled and reversed
- The ATM prints the receipt, displays the message "REMOVE CARD" to notify the cardholder that the card may now be removed
- Once the card is removed, the ATM dispenses the Cash

- If the transaction is declined because of entering "Wrong PIN" and more PIN entering trials are still available, the ATM should display the error message and return to the processing step where the PIN entry is requested

- If the transaction is declined because of a business reason (not sufficient funds, exceed withdrawal limit …) or for a technical reason, the ATM will display the appropriate error message, eject the card and end the transaction

- If the transaction is declined by the issuer, and the issuer indicates to retain the card, then the ATM should be able to retain the card and inform the cardholder accordingly

- ATM terminals need to log and print all transactions in their transaction journal for auditing purposes before ejecting the card and getting ready to accept another transaction

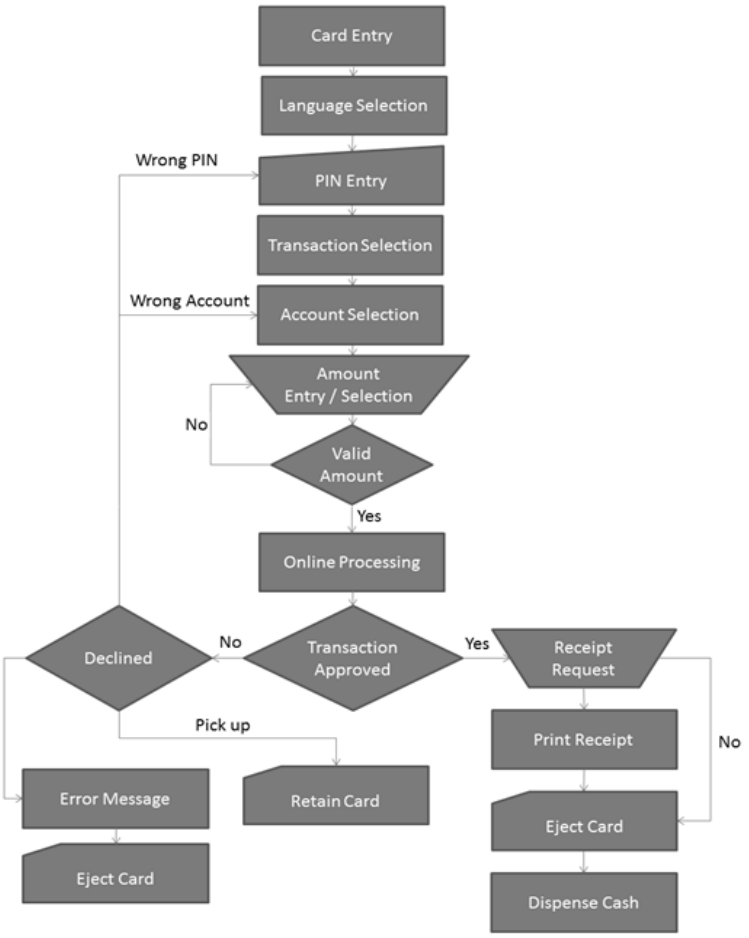

Figure 1 – Cash Withdrawal Transaction Flow

1.1.6.2 Balance Inquiry

A balance inquiry is available for the convenience of the cardholder. This transaction is informative and only provides a display and print out of the cardholder's account balances (refer to Member Bank Interface Specifications, data element 54 for details).

1. **Welcome screen**

   - The first screen displayed to the OmanNet cardholder should show a welcome screen with the message "Welcome to OmanNet Services"
   - The Acquirer can choose to integrate the welcome screen with the language selection screen as well

2. **Language Selection**

   - The ATM presents the cardholder with a screen allowing for the selection of the language
   - As a minimum, ATMs must offer language support for English and Arabic; other languages are optional

   Note: This step is not repeated if the Language was already selected for another transaction

3. **PIN Entry**

   - The cardholder enters his PIN code
   - ATMs must allow for entering 4 to 12 digits PIN length values

   Note: This step is not repeated if a valid PIN was entered for a previous Issuer approved transaction

4. **Transaction Selection**

   - The ATM allows for prompts selection of available transactions
   - Only transactions supported for the card are presented to the cardholder
   - The cardholder must select "Balance Inquiry"

5. Account Selection

The ATM presents the cardholder to select an account from the following:

- Default Account
- Checking or Current Account
- Savings Account

6. Online Processing

- The ATM generates an authorization request (or its local equivalent), containing all the data relevant to the transaction routing and processing
- The Issuer will respond with one of the following (but not limited to that, for the list of valid response code, refer to Member Bank Interface Specifications):
  - Transaction Authorized – Balance included with response
  - Transaction Declined, Wrong PIN
- If the Issuer could not be reached, an Error response is returned to the Acquirer

7. Transaction Completion

- For approved transactions, the ATM will display the balance returned by the Issuer. The terminal should timeout the details display within a predefined time (value will come from Acquirer). However, an option must also be provided to the cardholder to clear the screen and proceed to the next screen display prior to the display timeout
- The cardholder should also be given the possibility to request a receipt. The ATM then returns to the transaction selection screen allowing for a new transaction to be selected or to cancel the operation
- If the transaction is declined because of entering “Wrong PIN” and more PIN entering trials are still available, the ATM should display the error message and return to the processing step where the PIN entry is requested
- If the transaction is declined because of a technical reason, the ATM will display the appropriate error message, eject the card and end the transaction

- If the transaction is declined by the issuer, and the issuer indicates to retain the card, then the ATM should be able to retain the card and inform the cardholder accordingly

- Terminal receipts shall contain the following details:

  - Transaction date and time
  - Terminal ID
  - Truncated Card Number
  - Transaction Sequence/Receipt Number
  - Transaction-Specific Details: Amount, account details, available balances
  - Authorization Response Code
  - ATM Location

- ATM terminals need to log and print all transactions in their transaction journal for auditing purposes before ejecting the card or getting ready to accept another transaction

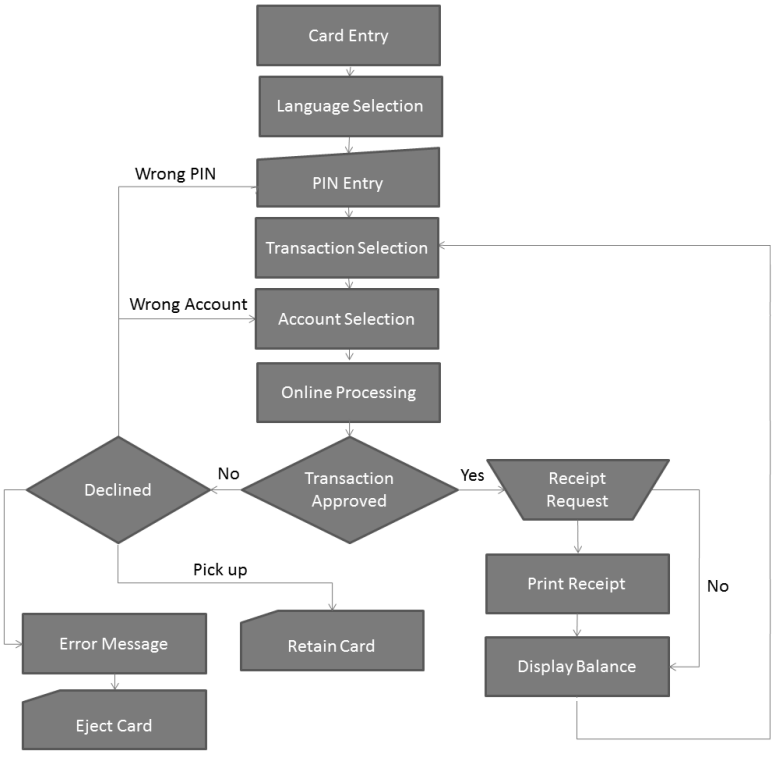

Figure 2 – Balance Enquiry Transaction Flow

1.1.6.3 Mini-Statement

A Mini-Statement is a non-financial and non-payment transaction available for the convenience of the cardholder. This transaction is informative and provides only a print-out of summary details corresponding to recent activities on his account.

Mini- Statement transaction processing takes place in a similar way as Balance Inquiry. The maximum number of mini- statement details line is 6. Details will be printed on a receipt; and no other details will be displayed on the ATM screen.

1. **Welcome screen**

   - The first screen displayed to the OmanNet cardholder should show a welcome screen with the message "Welcome to OmanNet Services"
   - The Acquirer can choose to integrate the welcome screen with the language selection screen as well

2. **Language Selection**

   - The ATM presents the cardholder with a screen allowing for the selection of the language
   - As a minimum, ATMs must offer language support for English and Arabic; other languages are optional

   Note: This step is not repeated if the Language was already selected for another transaction

3. **PIN Entry**

   - The cardholder enters his PIN code
   - ATMs must allow for entering 4 to 12 digits PIN length values

   Note: This step is not repeated if a valid PIN was entered for a previous Issuer approved transaction

4. **Transaction Selection**

   - The ATM allows for prompts selection of available transactions
   - Only transactions supported for the card are presented to the cardholder
   - The cardholder must select "Mini- Statements"

5. Account Selection

The ATM presents the cardholder to select an account from the following:

- Default Account
- Checking or Current Account
- Savings Account

6. Online Processing

- The ATM generates an authorization request (or its local equivalent) containing all the data relevant for transaction routing and processing
- The Issuer will respond with one of the following (but not limited to that, for the list of valid response code, refer to Member Bank Interface Specifications):
  - Transaction Authorized – Statement Information included with response
  - Transaction Declined, Wrong PIN
- If the Issuer could not be reached, an Error response is returned to the Acquirer

7. Transaction Completion

- For approved transactions, the ATM will print the statement and proceed to the transaction selection screen, allowing for a new transaction to be selected or to cancel operation
- If the transaction is declined because of entering “Wrong PIN” and more PIN entering trials are still available, the ATM should display the error message and return to the processing step where the PIN entry is requested
- If the transaction is declined because of a technical reason, the ATM will display the appropriate error message, eject the card and end the transaction
- If the transaction is declined by the issuer, and the issuer indicates to retain the card, then the ATM should be able to retain the card and inform the cardholder accordingly
- ATM terminals need to print all transactions log in the transaction journal for auditing purposes before ejecting the card or getting ready to accept another transaction

- Terminal receipts should contain the following details:
    - Transaction date and time
    - Terminal ID
    - Truncated Card Number
    - Transaction Sequence/Receipt Number
    - Transaction-Specific Details: Amount, account details, available balances, mini-statement details
    - Authorization Response Code
    - ATM Location

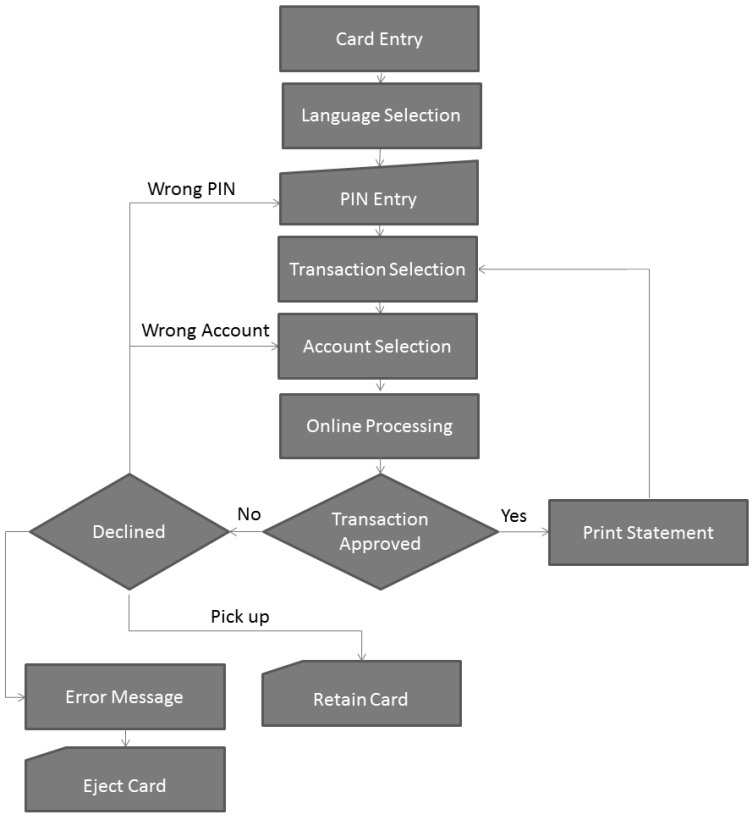

Figure 3 – Mini-Statement Transaction Flow

1.1.6.4 Cardholder Account Transfer

Cardholder Account Transfer is a financial transaction available for the convenience of the cardholder. This transaction provides transfer of funds between two linked accounts on the same card.

1. **Welcome screen**

   - The first screen displayed to the OmanNet cardholder should show a welcome screen with the message "Welcome to OmanNet Services"
   - The Acquirer can choose to integrate the welcome screen with the language selection screen as well

2. **Language Selection**

   - The ATM presents the cardholder with a screen allowing for the selection of the language
   - As a minimum, ATMs must offer language support for English and Arabic; other languages are optional

   Note: This step is not repeated if the Language was already selected for another transaction

3. **PIN Entry**

   - The cardholder enters his PIN code
   - ATMs must allow for entering 4 to 12 digits PIN length values

   Note: This step is not repeated if a valid PIN was entered for a previous Issuer approved transaction

4. **Transaction Selection**

   - The ATM allows for prompts selection of available transactions
   - Only transactions supported for the card are presented to the cardholder
   - The cardholder must select "Account Transfer"

5. Account Selection

The ATM presents the cardholder to select an account from the following:

- Default Account
- Checking or Current Account
- Savings Account

6. Amount Entry

- The ATM prompt the cardholder to enter the amount to be transferred

7. Terminal Online Processing

- The ATM generates an authorization request (or its local equivalent) containing all the data relevant to transaction routing and processing
- The Issuer will respond with one of the following (but not limited to that, for the list of valid response code, refer to Member Bank Interface Specifications):
  - Transaction Authorized
  - Transaction Declined, Wrong PIN
- If the Issuer could not be reached, an Error response is returned to the Acquirer

8. Transaction Completion

- For approved transactions, the ATM will print the receipt that indicates the account transfer approval, and proceed to the transaction selection screen, allowing for a new transaction to be selected or to cancel the operation
- If the transaction is declined because of entering "Wrong PIN" and more PIN entering trials are still available, the ATM should display the error message and return to the processing step where the PIN entry is requested
- If the transaction is declined because of a business or a technical reason, the ATM will display the appropriate error message, eject the card and end the transaction
- If the transaction is declined by the issuer, and the issuer indicates to retain the card, then the ATM should be able to retain the card and inform the cardholder accordingly

- ATM terminals need to print all transactions log in the transaction journal for auditing purposes before ejecting the card or getting ready to accept another transaction

- Terminal receipts shall contain the following details:

  - Transaction date and time
  - Terminal ID
  - Truncated Card Number
  - Transaction Sequence/Receipt Number
  - Transaction-Specific Details: Amount, account details,
  - Authorization Response Code
  - ATM Location

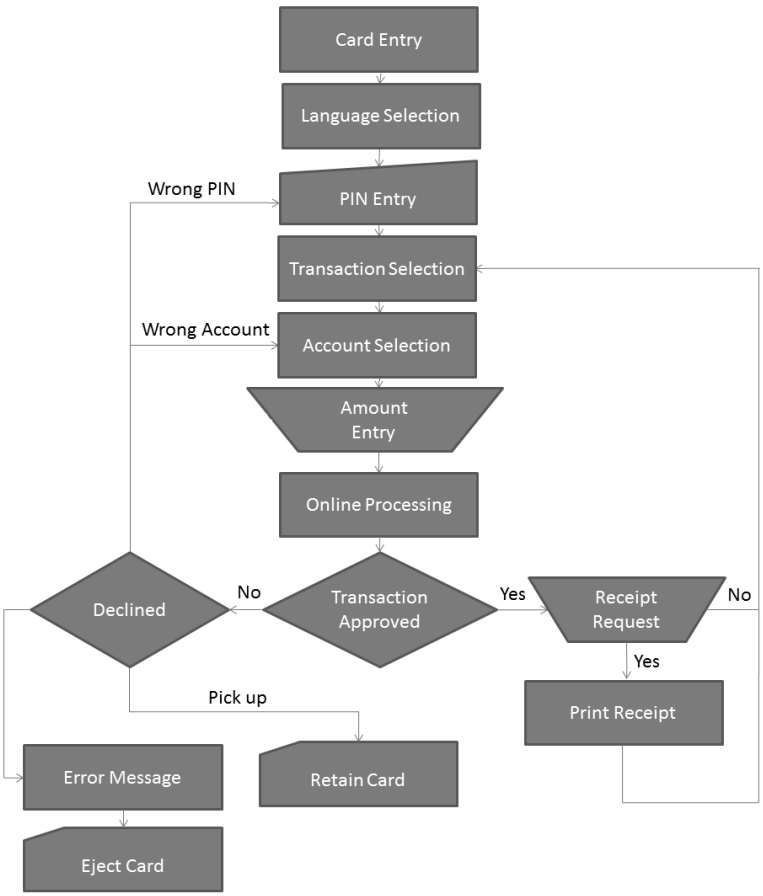

Figure 4 – Cardholder Account Transfer Transaction Flow

1.1.6.5 Account to Account Transfer

Account-to-Account Transfer is a financial transaction available as a value added service for the cardholder. This transaction provides transfer of funds from cardholder account to another cardholder account of another member bank on OmanNet. This service is only available on (on-us) ATM of the cardholder, i.e. the cardholder can make use this service through their bank's own ATM.

1. **Welcome Screen**

   - The cardholder should see the on-us welcome screen of the bank

2. **Language Selection**

   - The cardholder should see the on-us language selection screen of the bank
   - As a minimum, ATMs must offer language support for English and Arabic; other languages are optional

   Note: This step is not repeated if the Language was already selected for another transaction.

3. **PIN Entry**

   - The cardholder enters his PIN code
   - ATMs must allow for entering 4 to 12 digits PIN length values

   Note: This step is not repeated if a valid PIN was entered for a previous Issuer approved transaction

4. **Transaction Selection**

   - The option to select "Account to Account Transfer" should be present for the cardholder to select the transaction. The "Account to Account Transfer" can be on the main menu or a sub-menu, the decision is left to the bank's own discretion
   - The cardholder must select "Account to Account Transfer"

5. **Account Entry Screen**

   - The ATM should allow the cardholder to enter the Beneficiary - Personal Account Number (PAN)

6. From Account Selection

The ATM presents the cardholder to select an account from the following:

- Default Account
- Checking or Current Account
- Savings Account

7. Amount Entry

- The ATM prompts the cardholder to enter the amount to be transferred

8. To Account Selection

The ATM should prompt the cardholder to select the account type of the destination account:

- Default Account
- Checking or Current Account
- Savings Account

9. 1st Terminal Online Processing

- The ATM generates an account inquiry request containing all the data relevant to transaction routing and processing
- The Recipient bank will respond with one of the following (but not limited to that, for the list of valid response code, refer to Member Bank Interface Specifications):
  - Transaction Authorized
  - Transaction Declined, Invalid Account
- If the Recipient could not be reached, an Error response is returned to the Acquirer

10. Account Confirmation Screen

- The ATM should display the Beneficiary Name on the confirmation screen for the cardholder to commit funds transfer or cancel further processing
- If cardholder proceeds with transfer, the 2nd terminal processing occurs for actual transfer

11. 2nd Terminal Online Processing

- The ATM generates a funds transfer request (or its local equivalent) containing all the data relevant to transaction routing and processing
- The Sender bank will respond with one of the following (but not limited to that, for the list of valid response code, refer to Member Bank Interface Specifications):
  - Transaction Authorized
  - Transaction Declined, Insufficient funds
- If the Issuer could not be reached, an Error response is returned to the Acquirer

12. Transaction Completion

- For approved transactions, the ATM will print the receipt that indicates the account transfer approval, and proceed to the transaction selection screen, allowing for a new transaction to be selected or to cancel the operation
- If the transaction is declined because of entering "Wrong PIN" and more PIN entering trials are still available, the ATM should display the error message and return to the processing step where the PIN entry is requested
- If the transaction is declined because of a business or a technical reason, the ATM will display the appropriate error message, eject the card and end the transaction
- If the transaction is declined by the issuer, and the issuer indicates to retain the card, then the ATM should be able to retain the card and inform the cardholder accordingly
- ATM terminals need to print all transactions log in the transaction journal for auditing purposes before ejecting the card or getting ready to accept another transaction
- Terminal receipts shall contain the following details:
  - Transaction date and time
  - Terminal ID
  - Truncated Card Number
  - Transaction Sequence/Receipt Number
  - Transaction-Specific Details: Amount, account details,
  - Authorization Response Code
  - ATM Location

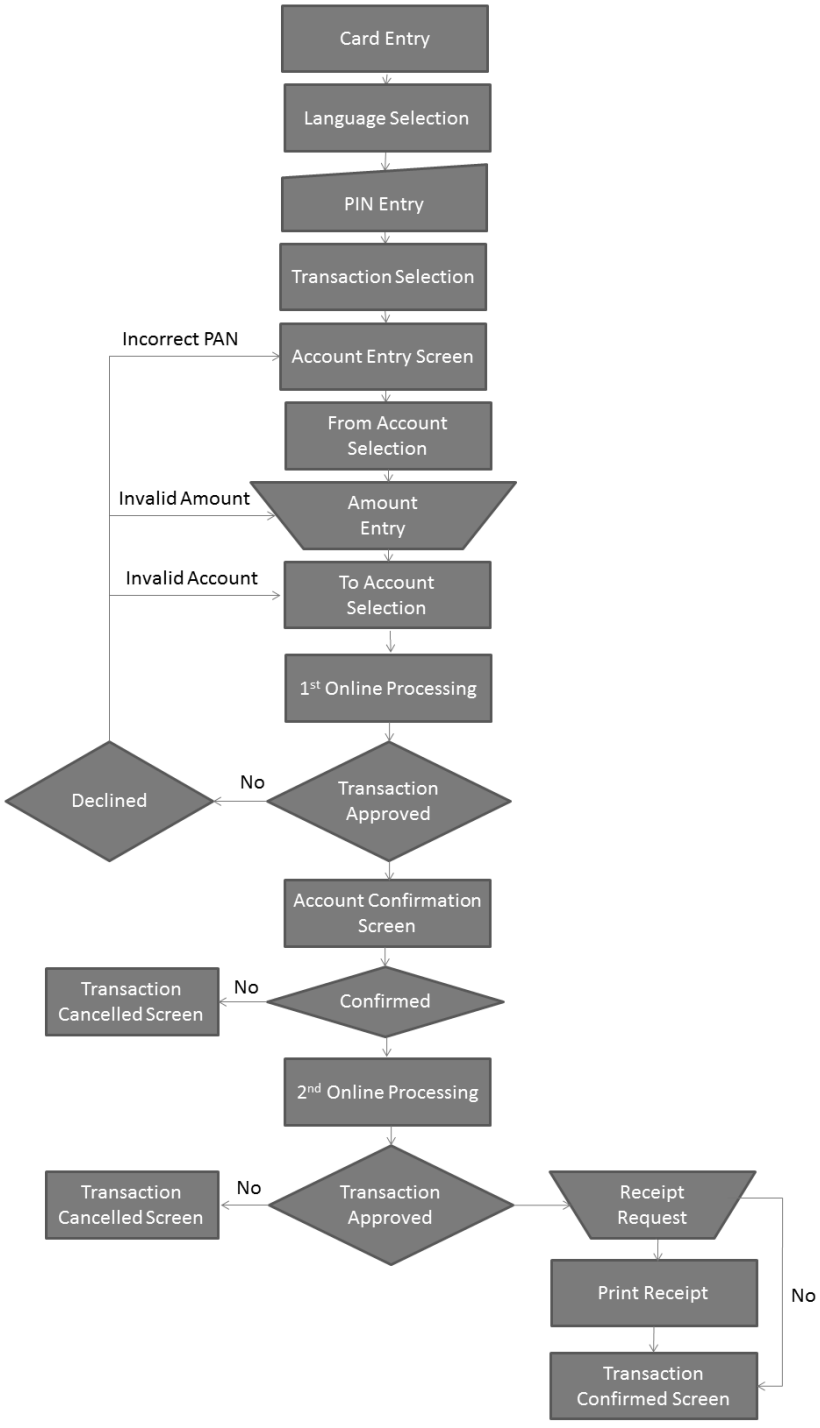

Figure 5 – Account to Account Transfer Transaction Flow

1.1.7 Chip Card Transaction Handling

For the Chip card transaction the Acquirer are required to implement the EMV function requirement. The following subsections illustrate how an Acquirer could implement the EMV requirements.

Acquirers may implement other methods as far as they are compliant with the underlying specifications and satisfy the overall requirements.

A transaction is initiated once a card is inserted into the Chip card reader of the ATM. To complete a Chip card transaction, the ATM should follow the standard EMV Contact Transaction processing steps:

1. Application selection
2. Initiate application processing
3. Read application data
4. Processing restrictions
5. Offline data authentication
6. Cardholder verification
7. Terminal risk management
8. Terminal action analysis
9. Card action analysis
10. Online processing
11. Completion and script processing

ATMs will always go online for transaction authorizations. For this reason, many EMV functions used to support offline functionality are not needed for ATMs.

1.1.7.1 Basic EMV Requirements for ATM

The following Application Identifiers (AIDs) are to be accepted at the ATM

Application Name	AID
Visa Credit/Debit	A0000000031010
Visa Electron	A0000000032010
Visa Plus	A0000000038010
MasterCard Credit/Debit	A0000000041010
MCI Electronic / Maestro	A0000000043060
MasterCard Cirrus	A0000000046000

- The terminal floor limit for ATM transactions must be set to zero
- All ATM transactions will go online; therefore they are not required to perform Offline Data Authentication (SDA/DDA/CDA)
- The Cardholder Verification Method (CVM) will always be Online PIN; no other CVM should be supported by the ATM

- The ATM must perform the Online Processing - Card Authentication Method (CAM) where a cryptogram (Authorization Request Cryptogram – ARQC) is generated by the chip and validated by the issuer as part of authorization processing

- The issuer may optionally send another cryptogram in the response message (Authorization Response Cryptogram – ARPC), which is validated by the chip

- Lastly, the ATM must be able pass issuer script to the chip if the issuer has sent them

1.1.7.2 EMV Flow on ATM

The ATM flow can be modified to address the requirements for EMV transactions. The EMV functions relevant to the ATM are briefly described below:

1. **Card Entry**

    - The ATM should check the magnetic stripe track data for the service code value (2xx/6xx) indicating that an EMV chip is on the card. Consequently, the ATM may attempt to read the ICC directly

2. **Application Selection**

    - As defined by EMV, the ATM prepares a list of candidate applications shared between the card and the ATM and present the list to the cardholder, or selects the application if only one application is present

    - Most cards carry Payment Systems Environment (PSE) that is a list of application on the card, and it is recommended that the ATM use the PSE selection method to be more efficient

3. **Application Initiation and Read Application Data**

    - Once the application has been identified and selected for use, the ATM will attempt to retrieve the appropriate data from the ICC

4. **Processing Restrictions**

    - The ICC may be personalized to prevent use at the ATM. in that case, the appropriate message should be displayed, such as “This card does not permit ATM usage”

5. **Offline Data Authentication**

    - The ATM will not perform Offline data authentication

6. Cardholder Verification

- The only Cardholder Verification Method (CVM) permitted at the ATM is Online PIN. All other CVMs, such as Offline PIN or signature are not allowed
- The authorization request message that is forwarded to the issuer for verification should include the encrypted Online PIN

7. Terminal Risk Management

- The ATM will not perform Terminal Risk Management

8. Terminal Action Analysis

- The ATM always goes online for an authorization, and efficiency during this step can be accomplished by taking advantage of Terminal Action Analysis, ATM may:
  - Perform both IAC/TAC-Denial processing
  - Skip IAC/TAC-Online processing, and go online after requesting an ARQC
  - If unable to go online, request an AAC, and terminate the transaction with an appropriate message without performing the IAC/TAC-Default processing

9. Online Processing

- During Online Processing, the ATM will attempt to go online with the Authorization Request Cryptogram (ARQC) always included with other chip data in the authorization message
- The Issuer host validates the ARQC to prove that card is valid and can use the results in its authorization decision
- Issuer may generate an Authorization Response Cryptogram (ARPC) as part of the response message

Completion and Issuer Script Processing

- If the online authorization response contains an ARPC, the ATM must pass the cryptogram on to the card to be validated
- When the online authorization is completed, the ATM request the chip a final cryptogram based on issuer response
  - An approval would result in a request for a Transaction Certificate (TC)
  - A decline would result in a request for an Application Authentication Cryptogram (AAC)

- If the Issuer has approved the transaction but the card declines the transaction (the ATM requests a final cryptogram of a TC but the card returns an AAC), the ATM must generate a reversal

- Issuers can update parameters on the ICC by the application of issuer scripts. ATMs must support issuer script handling and be able to pass the script to the card ICC for processing

- The ATM receipt shall contain the following details

  - Transaction date and time
  - Terminal ID
  - Truncated Card Number
  - Transaction Sequence/Receipt Number
  - Transaction-Specific Details: Amount, account details, available balances
  - Authorization Response Code
  - ATM Location
  - Application Label / Application Preferred Name (ICC transaction only)
  - Application Identifier (ICC transaction only)
  - Application Cryptogram (ICC transaction only)

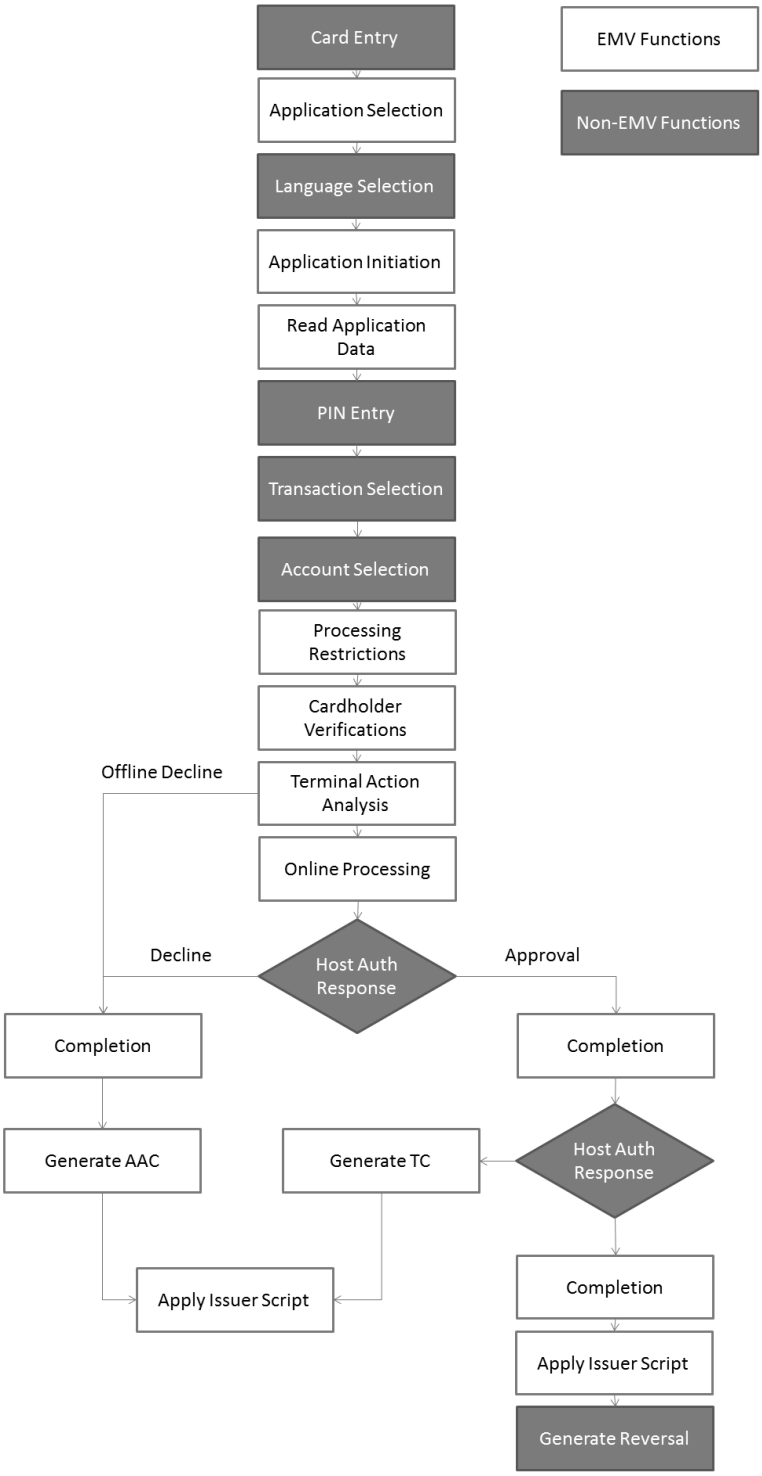

Figure 6 – ATM EMV Transaction Flow

1.2 POS Terminal Specifications

1.2.1 POS Physical and Protocol Requirements

1.2.1.1 POS Display Requirements

- The POS display is the terminal's screen through which messages presented to the user. These messages can contain information on the progress of the current transaction and/ or messages in response to specific actions of the user
- As a minimum, the Merchant Display must be capable of displaying 2 lines of 16 characters each
- The screen resolution must be sufficient to read textual messages in Arabic, English or a combination of the two when the terminal is installed in a live merchant environment

1.2.1.2 Magnetic Stripe Reader

- The Magnetic stripe reader must be capable of reading Track-2 encoded data from ISO/IEC 7813:2001 compliant payment cards swiped through the reader

1.2.1.3 Chip Card Reader

- The Chip card reader should be capable of reading chip personalized with data from ISO/IEC 7816:2001 compliant smart cards
- The Chip card reader must be compliant with the mechanical and electrical requirements as specified by EMVCo and EMVCo type approved

1.2.1.4 Keyboard

- The Keyboard of the POS terminal is used by the merchant staff to enter transaction's related data (transaction amount …etc.), to select between transaction types and choose functions that related to the management of the terminal
- Transactions are selectable at the device by the merchant via a function or transaction key
- All function keys must be labeled or identified properly to avoid mistakes
- Besides the above function keys, the terminal must be fitted with a numeric keyboard allowing the merchant to enter transaction related amounts

1.2.1.5 Transaction Receipt printer

- The POS should be equipped with a printing device used to print the cardholder transaction receipt and may be used to print a hard copy of the terminal activity log, audit traces, transaction status, and other types of reports
- The printer must be able to print information in Arabic, English and a combination of both character sets. The main receipt language is dynamically chosen based on the language indicator read from the card with the summary receipt language chosen based on the merchant language

1.2.1.6 PIN Entry Device (PIN Pad)

- The PIN Pad must be compliant with the requirements specified in ISO 9564-1:2002
- PIN Pad must be PCI/PED certified
- The PIN Pad must be configured to accept PIN values up to the maximum of 12 digits
- Support for alphanumeric PIN values is not a requirement
- PIN Pad keys must be labeled or identified both in Arabic and in English
- The PIN Pad must contain a screen to display messages to the cardholder. As a minimum, the screen must be able to display one line of 16 characters; the resolution should be clear enough that both Arabic and English responses are shown to the cardholder
- Messages can be displayed in either Arabic or English
- The language first displayed on the PIN pad is chosen based on the language indicator contained on the cardholder's card (magnetic stripe or chip) or the default language for the terminal
- The PIN pad presents a method for changing the language displayed on the PIN pad at any time though a LANGUAGE key

1.2.1.7 Electrical Connections/ Power supply

- Terminals should be equipped with an additional power supply to the main power supply (UPS, rechargeable battery, etc…) designed in a way that a power cut down during a transaction allows the terminal to complete the transaction; the transaction/ terminal must not be left in an undefined state
- The POS terminal must be designed such that the terminal application software, the terminal initialization data, security keys and stored transaction details are not lost in case of a power failure

1.2.2 Magnetic Stripe / Chip Selection Requirements

Terminals capability of reading Chip card technology shall be the primary method of reading payment cards. The magnetic stripe method shall be utilized under the following conditions:

- ICC not present on the card, the service code on the magnetic stripe should indicate that it is a magnetic stripe card

Terminal with separate ICC and magnetic stripe reader shall prompt the user to insert the card first on the ICC reader with a message “Use Chip Reader” in case the user tried to swipe (use the magnetic stripe of the card) initially.

Whenever a card is swiped, terminals must read the service code on the magnetic stripe of card in order to determine if an ICC is present or not. A service code beginning with ‘2’ or ‘6’ indicates that an ICC is present on the card, and the terminal should process the card using ICC based processing or prompt the merchant to insert the card in the ICC reader.

As soon as the card has been inserted into the reader, the message “Please Wait” shall be displayed in order to reassure the cardholder or attendant that the transaction is being processed.

Terminals must always abort a transaction and display the message “Processing Error” if the card is removed from the terminal prior to the completion of the transaction.

1.2.3 POS Terminal Security

1.2.3.1 PIN Security Requirements

- Acquirer Banks are required to comply with PCI PIN security requirements for the secure management, processing and transmission of PIN data during transaction processing at the ATMs

- Refer to PCI website for details http://www.pcisecuritystandards.org for more information

1.2.3.2 Network Security

- All transaction messages, with the exception of the initial 18xx Network Management Messages, are protected against data alteration by a message authentication code (MAC)

- The MAC algorithm used in the OmanNet scheme is ISO/IEC 9797-1 Algorithm 3

- Full message authentication mechanism is applied; this means that all data elements will be used to calculate the MAC

1.2.3.3 EMV Public Key Infrastructure Requirements

The terminal should be able to apply the following principles whenever it receives a new Certificate Authority Public Key (CAPK) from the card scheme:

- Verify that it received the CAPK and its related data error-free
- Terminals must be able to store at least six (6) CAPK per Registered Application Provider Identifier (RID)
- Usage of CAPK

1.2.3.4 Offline Data Authentication Method (ICC Only)

The terminal performs data authentication using a digital signature scheme based on public key techniques to confirm the legitimacy of critical ICC resident data and authenticate the ICC.

Card Authentication Methods provide support for Offline Data Authentication as specified by EMV, available CAM options are:

- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)
- Combined DDA / Generate Application Cryptogram (CDA)

The terminals must support at least SDA, and DDA for offline data authentication as a basic requirement, support for CDA is optional and encouraged.

1.2.4 Transaction Set Support

The following sets of POS transactions are required to be supported for OmanNet card:

Transaction	Description
Purchase	A data capture transaction that debits a cardholder's account in exchange for goods or services.
Purchase with Cashback	A purchase transaction where the amount of the transaction represent both the value of the goods (or service) and of a cash amount request by the cardholder. The amount of the cash portion is identified in the transaction as a separate item (refer to Member Bank Specifications, section 5.43 P)
Purchase with TIP (gratuity)	A purchase transaction where the amount of the transaction represent both the value of the goods (or service) and of a TIP (gratuity) amount request by the cardholder. The amount of the TIP (gratuity) portion is identified in the transaction as a separate item (refer to Member Bank Specifications, section 5.43 P)
Reversal	Reversals are generated: • When initiated by the merchant as a cancel transaction to reverse the previous purchase transaction • Automatically on a late successful response to a transaction
Refund Transaction	A data capture transaction initiated by the merchant to credit the cardholder for a refund of goods or services, and to debit the merchant's account accordingly. It requires the merchant's supervisor password and the merchant's signature.
Pre-Authorization and Pre-Authorization	Online check of a cardholder's account before a purchase is made. The transaction is entered with an amount that is equal to that of the purchase or that is predetermined by the merchant If approved, this transaction assumes a pre-authorization purchase

Completion	completion will follow to finalize the purchase The pre-authorized amount can optionally be held against the account until a pre-authorization completion occurs or the hold time expires Follow-up to an approved pre-authorization purchase transaction is initiated after the cardholder receives the purchased goods or services with a Pre-Authorization Completion. The amount entered in this transaction supersedes that entered in the pre-authorization purchase.

Table 2 – POS Transaction Set

1.2.5 General Acceptance at POS

The following provides an overview of the general transaction acceptance requirement and best practices that apply to Magnetic Stripe and Chip card.

1.2.5.1 Primary Account Number (PAN)

The POS terminal should validate the modulus-10 check digit in the PAN for key-entered transactions. Acquirers are encouraged to have POS devices that support PAN verification to aid in detecting counterfeit cards.

In addition, these devices read the PAN from the magnetic stripe and compare the last four digits of the PAN to the key-entered last four digits of the embossed or printed PAN.

1.2.5.2 Multiple Language Support

One significant element of terminal operation is dual language (Arabic/English) support capability; Wherever possible, language selection must be automated, but at the same time "switchable".

The dual language support must operate for both the merchant interface (terminal display) and the cardholder interface (PIN pad), and the selection of language for each must be independent from the other.

All OmanNet terminals must provide support for communication with the merchant and the cardholder in both Arabic and in English.

Communication with the merchant will take place in the ‘default’ language but can be swapped to the other language by pressing the <LANGUAGE> key on the merchant/POS keypad.

Communication with the cardholder will occur in the cardholder’s preferred language but this may be swapped for the other language.

1.2.5.3 Terminal Transaction Processing Description

Whenever terminals have to execute a process that may take a while, it must display a message, i.e. “Please Wait”, so as to inform the user that the terminal is busy performing a task and that it has not stopped responding.

1.2.5.4 Transaction Session Management

The terminal shall maintain transaction session management, the terminal should not allow for a second transaction to be initiated until the response of the first transaction has been received or the first transaction has been timed-out.

1.2.5.5 Manual PAN Entry (Key Entry)

Terminals located at selected merchants may offer the possibility to enter manually the cardholder PAN and expiry date.

This method of obtaining the card identification data is subject to the terms and conditions for the specific card product from the issuer bank provided that the issuer bank support manual key entry transactions (MO/TO).

Key entry of card data will be enabled / disabled by the terminal configuration data.

Transaction handling where the card details cannot be read from the chip or from the magnetic stripe is similar to transaction handling when the data is read from the magnetic stripe.

Transaction handling flows for magnetic stripe read transactions will therefore include the manual data capture alternative – if relevant.

1.2.5.6 Void/User Cancellation (Manual Reversal)

Terminals are required to provide a mechanism by which the user is allowed to cancel a completed approved transaction.

Cancelling an approved transaction is called a Transaction Void. This transaction can be performed, either offline or online.

It is important to note, however, that transaction voiding is allowed only within the same business day. Transaction cancellation beyond this time setting shall be made using the refund functionality.

1.2.5.7 Transaction Receipts Requirements

Transaction receipts must be printed when requested by the cardholder. No transaction should be initiated when the terminal detects an “out of paper” condition. However, running out of paper during the processing of a transaction is not a reason as such to cancel the transaction.

The POS terminal must provide the capability to print a duplicate receipt. A duplicate receipt can only be printed for the last completed transaction. The duplicate receipt is clearly marked as such with “DUPLICATE COPY” printed on the receipt.

If the duplicate receipt is printed because the printer failed to produce a proper receipt (for example due to paper jam), the duplicate must be signed. In this case, the duplicate may need to stand for the original receipt. The failed original receipt must be attached to the copy of the duplicate that has been signed and will be retained by the Merchant.

A duplicate receipt is distributed the same as a normal receipt.

The POS transactions receipt should have the following data (at least) printed in reasonable layout:

- Duplicate / Claim copy indicator

- Merchant name and address
- Transaction type (Purchase, Refund, Reversal, Authorization)
- Transaction date and time
- Application Label / Application Preferred Name (ICC transaction only)
- Application Identifier (ICC transaction only)
- Application Cryptogram (ICC transaction only)
- Terminal ID
- Merchant ID
- Retrieval Reference number
- Truncated Card Number (only the value of the last four digits are shown, preceding digits are replaced by an asterisk '*')
- PAN Expiry date
- Transaction amount
- Authorization code (for approved transactions only)
- Transaction result (Approved, Declined, Transaction Void, Cancelled)
- Cardholder signature box (only for transactions that requires cardholder signature).
- Refund Policy (optional)

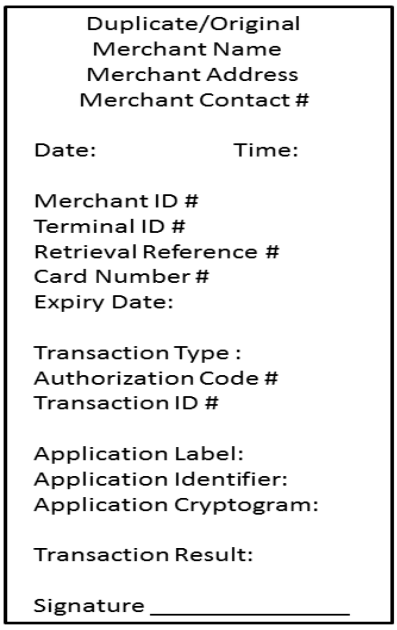

Figure 7 – Sample Receipt Format

1.2.6 Magnetic Stripe Transaction Flow

The following sections describe the suggested magnetic stripe transactions flow for the POS acquirers.

1.2.6.1 Purchase

The Purchase transaction is a financial transaction that offers goods and services facility to the cardholder. The POS transaction will be processed in online processing mode for OmanNet cards.

1. **Language Selection**

   - The POS should allow for language selection to the merchant
   - As a minimum, POS must offer language support for English and Arabic; other languages are optional

2. **Transaction Selection**

   - The POS should allow for the selection of the transaction
   - The merchant must select “Purchase”

3. **Card Swipe**

   - The merchant swipes the card through the magnetic stripe reader

4. **Identify Card**

   - The POS should perform basic risk management based on the service code of the card, a card service code indicates if it is allowed for POS, and whether a PIN is required

5. **Amount Entry**

   - The merchant key-in the transaction amount for which the purchase needs to be processed

6. **PIN Entry**

   - Based on the service code of the card, the POS prompts for PIN entry to the cardholder. The merchant should provide the pin pad to the cardholder to enter the PIN
   - POS must allow for entering 4 to 12 digits PIN length values

7. Online Processing

- The POS generates an authorization request (or its local equivalent) containing all the data relevant to transaction routing and processing
- The Issuer will respond with one of the following (but not limited to that, for the list of valid response code, refer to Member Bank Interface Specifications):
  - Transaction Authorized
  - Transaction Declined, Not Sufficient Funds
  - Transaction Declined, Wrong PIN
- If the issuer could not be reached, an Error response is returned to the Acquirer.

8. Transaction Completion

- For approved transactions, the POS will display “APPROVED” and the Authorization Code on the terminal display
- Declined transactions (due to time-out, unable to connect to acquirer) should be informed with a “DECLINED” message at the terminal display
- If the transaction is declined because of entering “Wrong PIN” and more PIN entering trials are still available, the POS should display the error message and return to the processing step where the PIN entry is requested
- When the transaction is declined, a decline receipt should also be printed for reference in case the transaction was not completed successfully
- If the transaction was approved, the appropriate receipt for the result of the transaction should be printed. The receipt should contain the authorization code which is also displayed at the POS terminal screen

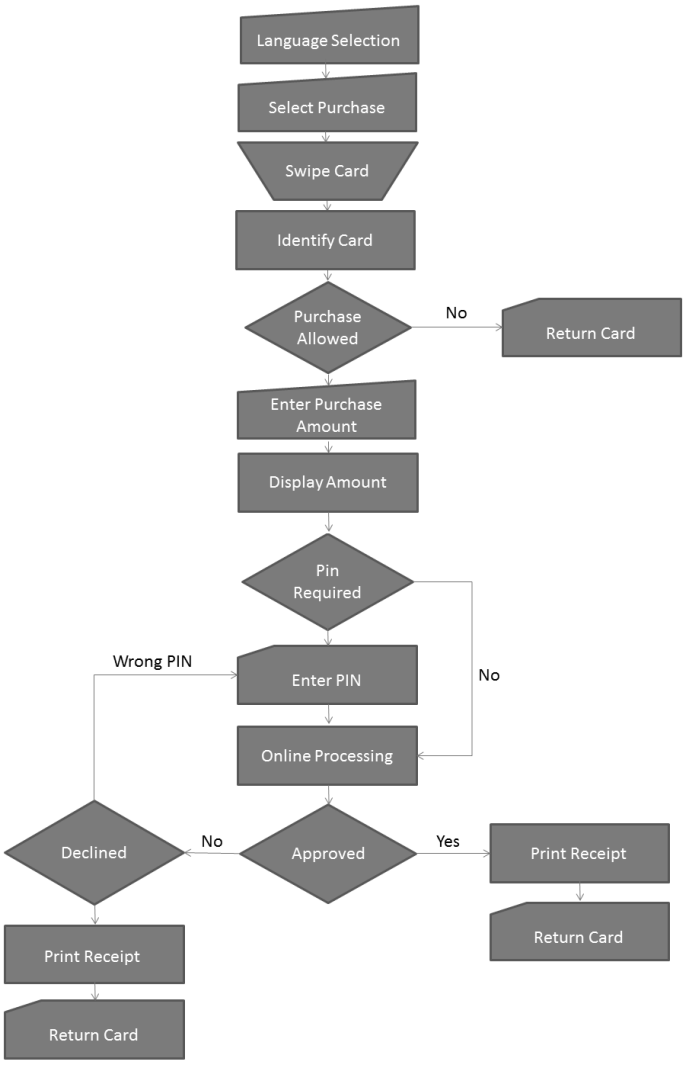

Figure 8 – Purchase Transaction Flow

1.2.6.2 Pre-Authorization

Pre-authorization is the transaction used to validate a cardholder and a sufficiency of funds associated with the card account to cover a future purchase of goods or obtaining of services.

1. **Language Selection**

   - The POS should allow for language selection to the merchant
   - As a minimum, POS must offer language support for English and Arabic; other languages are optional

2. **Transaction Selection**

   - The POS allows for the selection of the transaction. The merchant must select "Authorization"

3. **Card Swipe**

   - The merchant swipes the card through the magnetic stripe reader

4. **Identify Card**

   - The POS should perform basic risk management based on the service code of the card, a card service code indicates if it is allowed for POS, and whether a PIN is required

5. **Amount Entry**

   - The merchant key-in the transaction amount for which the authorization is requested

6. **PIN Entry**

   - Based on the service code of the card, the POS prompts for PIN entry to the cardholder. The merchant should present the PIN pad to the cardholder to enter the PIN
   - POS must allow for entering 4 to 12 digits PIN length values

7. Online Processing

- The POS generates an authorization request (or its local equivalent) containing all the data relevant to transaction routing and processing
- The Issuer will respond with one of the following (but not limited to that, for the list of valid response code, refer to Member Bank Interface Specifications):
  - Transaction Authorized
  - Transaction Declined, Not Sufficient Funds
  - Transaction Declined, Wrong PIN
- If the Issuer could not be reached, an Error response is returned to the Acquirer

8. Transaction Completion

- For approved transactions, the POS will display “APPROVED” and the Authorization Code on the terminal display
- Declined transactions (due to time-out, unable to connect to acquirer) should display a “DECLINED” message on the terminal screen
- If the transaction is declined because of entering “Wrong PIN” and more PIN entering trials are still available, the POS should display the error message and return to the processing step where the PIN entry is requested
- If the transaction was declined, a declined transaction receipt should be printed for reference
- If the transaction was approved, the appropriate receipt for the result of the transaction is printed. The receipt should contain the authorization code and also displayed at the POS terminal screen.
- The Pre-Authorization approval receipt must be retained by the merchant, for obtaining the completion of the pre-authorization

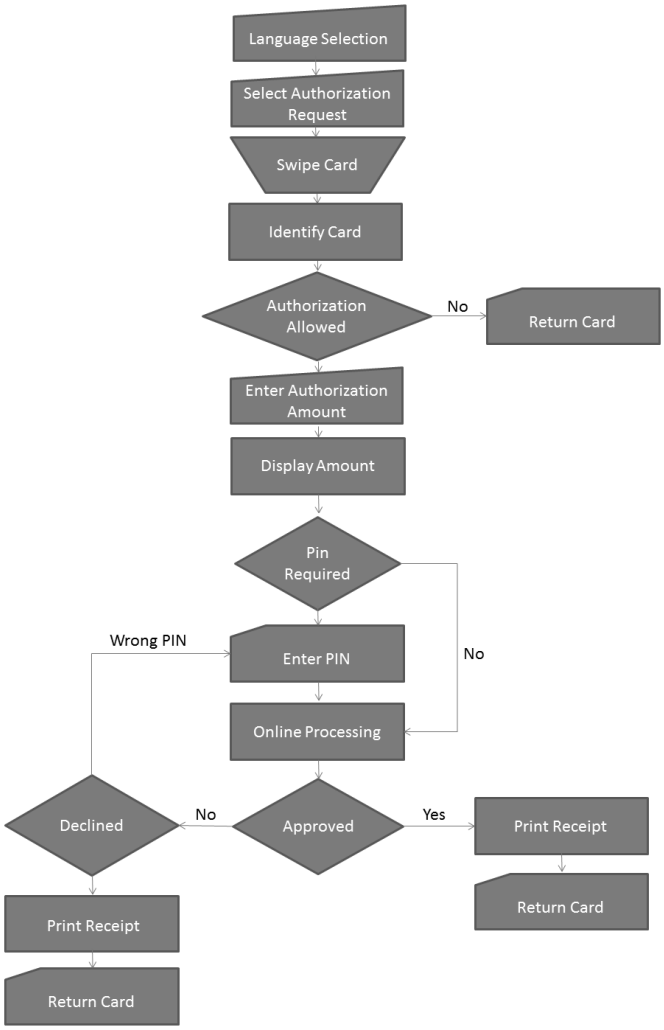

Figure 9 – Pre-Authorization Transaction Flow

1.2.6.3 Pre-Authorization Completion

After Pre-Authorization of a transaction, the Pre-Authorization Completion employed to process the transaction in the same fashion as purchase transaction.

The authorization code received during the pre-authorization of the purchase (if any) is entered as part of the completion transaction. Following is the Pre-Authorization Completion transaction flow:

1. **Language Selection**

   - The POS should allow for language selection to the merchant
   - As a minimum, POS must offer language support for English and Arabic; other languages are optional

2. **Transaction Selection**

   - The POS allows for the selection of the transaction
   - The merchant must select “Authorization Completion”

3. **Card Swipe / Key-in card data**

   - The merchant swipes the card through the magnetic stripe reader, if the card and the cardholder are present. Otherwise, the merchant key-in the card holder data from the authorization receipt

4. **Amount Entry**

   - The merchant key-in the transaction amount for which the completion is requested

5. **Authorization Code Entry**

   - The merchant key-in the authorization code of the Pre-Authorization transaction for which the completion is requested

6. **Online Processing**

   - The POS generates an authorization advice (or its local equivalent) containing all the data relevant to transaction routing and processing

7. **Transaction Completion**

- For approved transactions, the POS will display “APPROVED” and the Authorization Code on the terminal display
- Declined transactions (due to time-out, unable to connect to acquirer) should be presented with a “DECLINED” message at the terminal display

- If the transaction was declined, a decline receipt should be printed for reference
- If the transaction was approved, the appropriate receipt for the result of the transaction is printed. If the pre-authorization was approved, the receipt should contain the authorization code displayed at the POS terminal screen.
- The merchant should retain all receipts of obtained completions of pre-authorizations

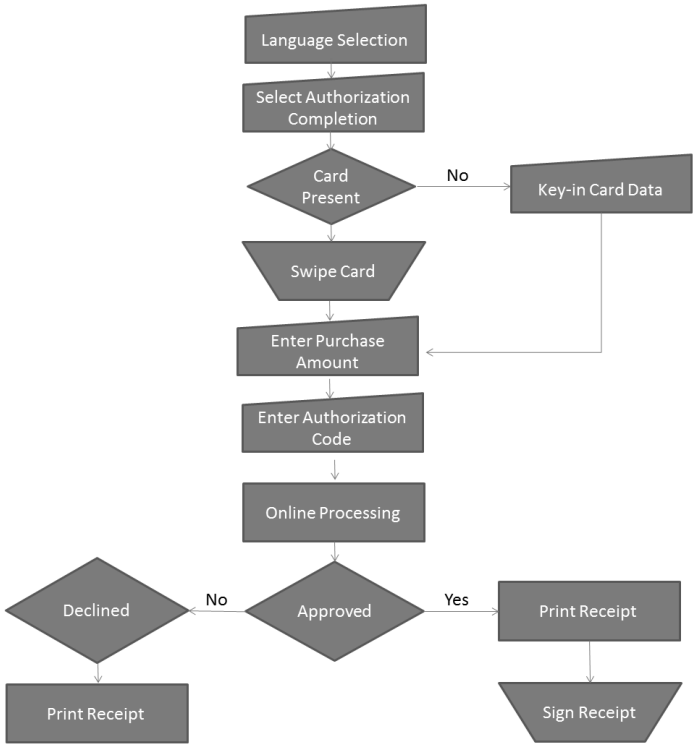

Figure 10 – Pre-Authorization Completion Transaction Flow

1.2.6.4 Reversal Transaction

A reversal is used to cancel the most recent transaction completed at the terminal. This function operates only for the last completed purchase or refund transaction.

If the transaction was approved and the reversal is initiated within the same business day after transaction completion, a receipt is printed out (note that this is only a recommendation, and still the acquiring banks could develop their own rules for reversal flow).

On receipt of the reversal from Acquirer, OmanNet will be responsible for forwarding the reversal message to the issuer; accordingly, the reversal transaction format must be according to the Member Bank Interface Specification.

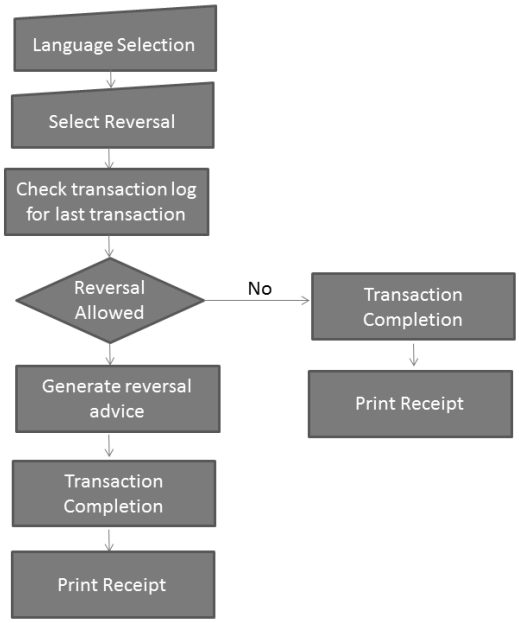

Figure 11 – Reversal Transaction Flow

1.2.6.5 Refund Transaction

A refund transaction is initiated when a customer returns merchandise purchased with a payment card and the credit is being made to the account that was debited for the purchase.

It is assumed that the customer is present when the refund transaction is processed, and in order to initiate a transaction refund, the terminal might prompt the user for a supervisor password (this option should be configurable).

The refund transaction is used to electronically capture the payment details to issue a financial transaction from merchant to refund a cardholder account.

As the actual transfer of funds flows from the merchant's account to the cardholder's account, the merchant supervisor signs the receipt as proof that the merchant initiated the refund at the point of sale.

Each completed POS transaction is given a systems trace audit number (STAN), when the merchant cashier enters a refund and the systems trace audit number of the corresponding purchase may be entered if needed.

The merchant cashier can find the systems trace audit number (STAN) printed on the original purchase receipt. The messages on the merchant display guide the merchant cashier through the steps for keying in the STAN at the appropriate time in processing the transaction.

The refunds should be made on the same cardholder account with which the original transaction was performed. Thus, Purchase refunds assume the same card is used for the refund and for making the original purchase; this is, however, not a system imposed requirement.

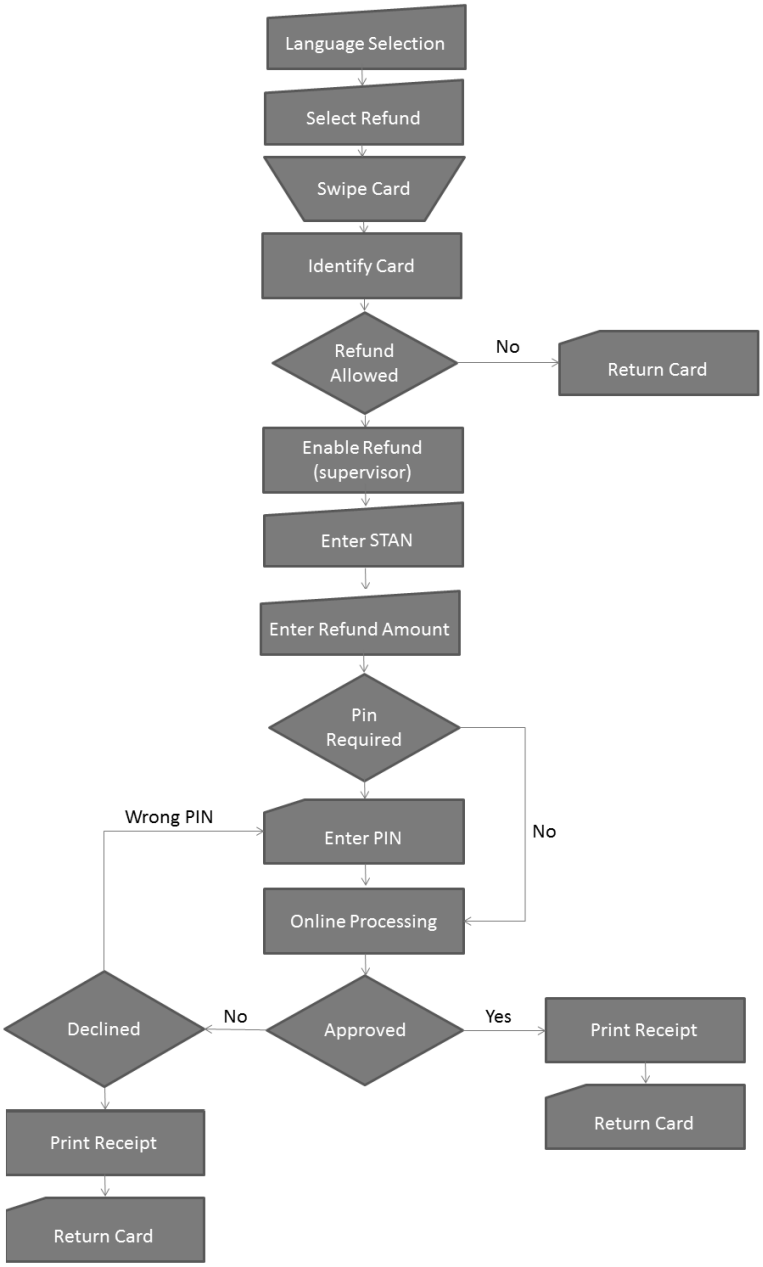

Figure 12 – Refund Transaction Flow

1.2.7 Chip Card Transaction Handling

For Chip card transactions, the Acquirers are required to implement the EMV function requirement.

The transaction flow for Chip card will be similar to that of the Magnetic Stripe. Acquirers may implement other methods as far as they are compliant with the underlying specifications and satisfy the overall requirements.

To complete a Chip card transaction, the POS should follow the standard EMV Contact Transaction processing steps:

1. Application selection
2. Initiate application processing
3. Read application data
4. Processing restrictions
5. Offline data authentication
6. Cardholder verification
7. Terminal risk management
8. Terminal action analysis
9. Card action analysis
10. Online processing
11. Completion and script processing

1.2.7.1 Card Insertion

To initiate a Chip card transaction, the POS terminal should be able to accept a chip card through one of the following methods:

- Dip (and leave in)
- Insertion (for motorized readers)
- Swipe and park[3]

3. Swipe and park consists of a magnetic-stripe swipe reader that guides the card into a chip-reading station at the end of the swipe. Generally, there is a mechanism to hold the card stable in the chip-reading station.

1.2.7.2 EMV Flow at the POS

The following flow describe a sample EMV transaction at the POS, the flow can be modified to address transactions requirements. The EMV functions relevant to the POS are briefly described below:

1. **Application Selection**

   - The POS terminal should allow cardholder to select one of the mutually supported applications during the application selection stage for multi-application chip cards
   - If no application can be selected, the device should display a "Card Type Not Supported", or an appropriate message and fall back to magnetic stripe where permitted
   - The POS terminal should display either the Application Label or Application Preferred Name (or both) in an informative message

2. **Application Initiation and Read Application Data**

   - Once the application has been identified and selected for use, the appropriate data is retrieved from the ICC at this step by the POS

3. **Processing Restrictions**

   - The POS terminal must perform the processing restrictions check based on the data provided by the chip to determine whether the transaction is allowed
   - The POS terminal must check whether the effective date (if present) or the expiration date for the card has been reached; these conditions are later evaluated based on card and device settings to determine the transaction outcome
   - The Application Usage Control (AUC) field may be set by an issuer to limit or enable card's use for certain transaction, for example, goods or service, or cashback. The terminal checks the Application Usage Control received from the card to see if the transaction is allowed

4. **Offline Data Authentication**

   - Offline data authentication enables authentication of a payment application for offline transactions. The three types of offline authentication are:
     - Static Data Authentication (SDA)
     - Dynamic Data Authentication (DDA)
     - Combined DDA / Generate Application Cryptogram (CDA)
   - The terminals must support at least SDA, and DDA for offline data authentication as a basic requirement, supporting CDA is optional and encouraged

5. Cardholder Verification

- The following Cardholder Verification Methods that may be supported by a contact chip device for a chip transaction are:
  - Online PIN
  - Offline PIN
    - Plain Text PIN
    - Enciphered PIN
  - Signature

- When the POS terminal determines that an offline PIN is to be entered, the terminal should determine the retries remaining and display an appropriate message, "Last PIN try", if the PIN try counter contains a value of 1 indicating one remaining PIN try

6. Terminal Risk Management

- The OmanNet debit cards are online only, and POS terminal are not required to perform terminal risk management

7. Terminal Action Analysis

- The POS terminals will always goes online for OmanNet debit cards for an authorization, and efficiency during this step can be accomplished by taking advantage of Terminal Action Analysis; thus, the POS may:
  - Perform both IAC/TAC-Denial processing
  - Skip IAC/TAC-Online processing, and go online after requesting an ARQC

- If the POS was unable to go online, the POS should request an AAC, and terminate the transaction with the appropriate message instead of performing the IAC/TAC-Default processing

8. Online Processing

- During Online Processing, the POS terminal will attempt to go online with the Authorization Request Cryptogram (ARQC) always included with other chip data in the authorization message. The Issuer host validates the ARQC to prove that card is valid and can use the results in its authorization decision

- Issuer may generate an Authorization Response Cryptogram (ARPC) as part of the response message

9. Completion and Issuer Script Processing

- If the online authorization response contains an ARPC, the POS terminal must pass the cryptogram on to the card to be validated.

  When the online authorization is completed, the POS terminal request a final cryptogram based on issuer response, an approval would result in a request for a Transaction Certificate (TC); a decline in a request for an Application Authentication Cryptogram (AAC).

If the Issuer has approved the transaction but the card declines the transaction (the POS terminal requests a final cryptogram of a TC but the card returns an AAC), the POS terminal must generate a reversal

- Issuers can update parameters on the ICC by the application of EMV issuer scripts. POS terminal must support issuer script handling and pass the script to the card for processing

- The POS terminal receipt shall in addition contain the following EMV details:
  - Application Label / Application Preferred Name
  - Application Identifier
  - Transaction Certificate (optional)

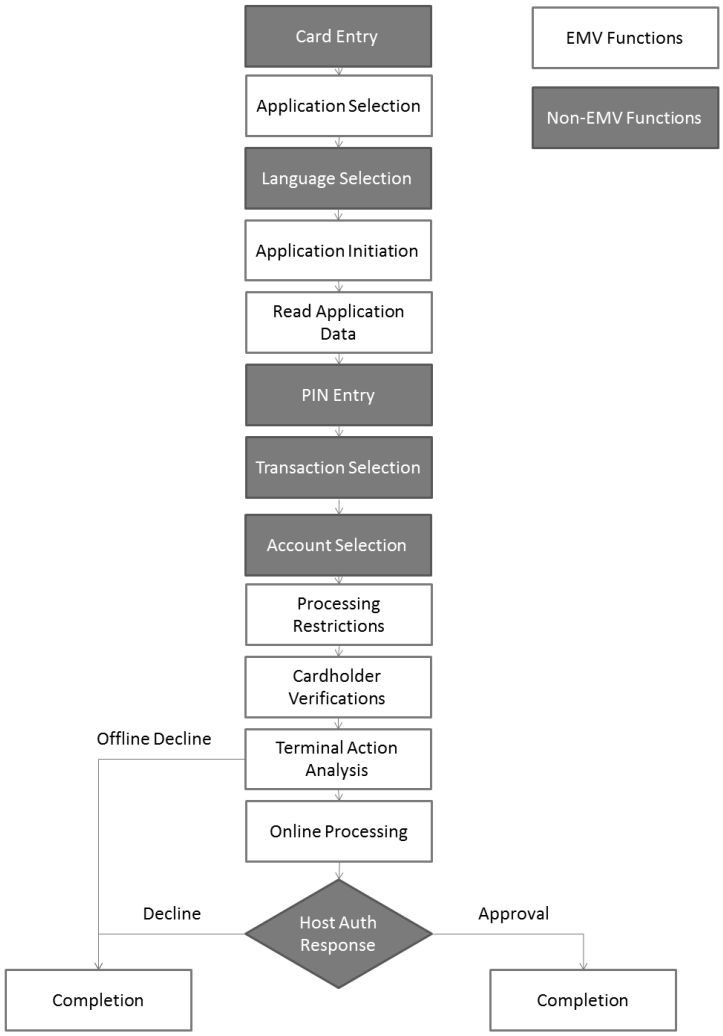

Figure 13 – POS EMV Transaction Flow

2 Cards Specifications

2.1 Magnetic Stripe Card Specifications

2.1.1 General

2.1.1.1 Card Specifications

- The physical characteristics for all cards shall conform to those specified for an ID-1 type card, to "ISO 7810-Identification Cards: Physical Characteristics"
- It is recommended that the magnetic stripe be of the high magnetization coefficient (Hi-Co)

2.1.1.2 Card Manufacturing

- Issuers should use only those card manufacturers that are approved by one of the leading international Networks
- The critical requirements are those related to security of manufacturing and transportation of the blank cards

2.1.2 Primary Account Numbering

The number shown on the card shall be the Primary Account Number (PAN) which consists of 3 components totaling a maximum of 19 digits as follows:

Issuer Identification Number (IIN)	Individual Client Identification	Check Digit
xxxxxx	xxxxxxxxxxxx	x
6 digits	up to 12 digits	1 digit

1. **Issuer Identification Numbering**

- An IIN comprising the first 6 digits of the PAN shall be assigned directly to the Issuer by Visa, MasterCard or ISO

2. **Individual Client Identification**

- Assigned by the member bank, the Individual Client Identification is up to 12 digits in length and must be unique for every individual's own card

3. **Check Digit**

- The value of the Check Digit is computed according to the Luhn formula for Modulus Ten (ISO 7812/1—Identification Cards: Issuer Numbering System)

2.1.3 Card Design

2.1.3.1 Front

The front side of the card shall contain the following:

1. Mandatory Information

- The card shall show clearly the name and logo of the Member
- The card shall show the PAN in Arabic numerals (e.g. 123456 1234567890121)
- The cardholder's name may be in either Arabic or Latin characters
- The card's expiration date

2. Optional Information

- All other information on the front of the card are optional; yet, these embossed information(other than the PAN) should conform to ISO 7811/3 - Identification Cards - Recording

2.1.3.2 Back

The backside of the card should contain the following:

- A magnetic strip of at least two track widths, the member bank may use a 3-track stripe
    - The location and physical characteristics of the magnetic strip should comply with "ISO 7811/4 Identification Card- Recording Techniques Part 4. Location of read only Track 1&2"
- Signature block with a water mark of the Network name or a logo of the member's bank
- Blank area left for the member bank discretionary information
- OmanNet logo

- The following figure shows the dimensions and standards for the OmanNet Logo:

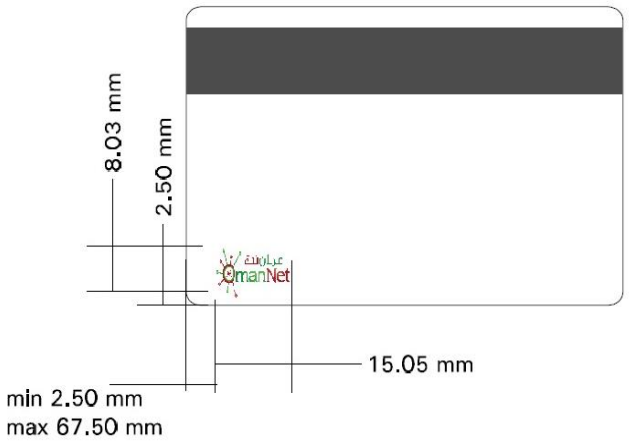

Figure 14 – Dimensions and Standards for the OmanNet Logo

2.1.4 Embossing

Embossed cards shall comply with "ISO 7811/3 ID Cards: Part 3 Location of Embossed Characters"

2.1.5 Encoding

2.1.5.1 Magnetic Stripe Physical Characteristics

The physical characteristics of the magnetic strip shall be as specified in ISO 7811/2. EBC recommending the magnetic material used to be of the high coefficient type to reduce the chance of data accidental erasure.

2.1.5.2 Magnetic Stripe Location

The location of the magnetic strip shall conform to the "International Standard ISO 7811/4 Identification Cards Part 4: Location of Read Only Magnetic Tracks 1& 2."

Track 1

- ISO standard 7813 provides more detailed explanation of Track 1 structure and field definitions

Track 2

- ISO standard 7813 provides more detailed explanation of Track 2 structure and field definitions

Track 3 Optional

- ISO standard 4909 provides more detailed information on the structure of Track 3

2.1.6 Track Layout

2.1.6.1 Service Code

The service code is part of the discretionary data of track 2. It is a three digit value defining various services attribute differentiating cards used in international or national interchange and designating PIN requirements and identifies card restrictions.

OmanNet recommends that the Issuer set the service code to PIN required value for the debit cards to enforce PIN entry at terminals.' For more information about the service code and its structure, please refer to Visa - Payment Technology Standards Manual.

2.2 Chip Card Specifications

2.2.1 General

2.2.1.1 Card Application

To ensure interoperability between cards and terminals, issuers are required to follow the card application standards and restrictions imposed by the card scheme to use on their chip cards.

2.2.1.2 Card Personalization Validation

Card Personalization Validation is a service offered by the card scheme, this service validates the personalization values of an issuer's card with the reference profile.

A chip card compliant with these values and certified by the card scheme will be considered as compatible with OmanNet specification, and will be accepted through OmanNet network.

2.2.2 Personalization Requirements

The following chip personalization requirements are based on the industry standards and are required to be part of the OmanNet card personalization specifications.

2.2.2.1 Zero Length Tags

Cards should not be personalized with any tag that is read by the terminal during a transaction that has a length of zero and no associated data.

2.2.2.2 PAN Sequence Number

Issuers are encouraged to make use of the PAN sequence number to differentiate between cards that have the same PAN, for example:

- Card that have been renewed due to expiry
- Multiple cards corresponding to the same account

2.2.2.3 CVV/CVC Values in ICC

Issuers must ensure that all cards support an ICC CVV/CVC derived in a different way from the magnetic stripe CVV/CVC.

2.2.2.4 Card Online CAM Requirements

Online CAM is the process that enables ICC Issuers to authenticate their card during an online transaction. All OmanNet cards must support online CAM.

2.2.2.5 Card Offline CAM Requirements

To reduce the risk of counterfeit fraud, the cards should support Offline CAM, that might lead to Offline decline of transactions only, Offline approvals on POS is not allowed, all transactions should be processed/authorized online.

- Support of SDA is **not recommend**
- Support of DDA is **recommended**
- Support of CDA provides additional security benefit as compared to DDA, however not all offline-capable terminal support this functionality.

2.2.2.6 Public Key Requirements for Offline CAM Support

Issuers must ensure that they follow the required Public key length recommended by the card scheme for the use of Offline CAM and/or offline enciphered PIN.

The card schemes are responsible for the generation, renewal, and revocation of the key certificate.

2.2.2.7 Card CVM Requirements

Issuer must ensure that they follow CHIP and PIN approach for the debit cards. The following list of CVM is supported for the OmanNet debit cards:

- Online PIN
- Offline plaintext PIN
- Offline enciphered PIN

2.2.3 Authorization Requirements

There are certain requirements that OmanNet recommends for authorization of the transaction made with Chip cards to ensure that highest level of security is established during the transaction.

2.2.3.1 Usage of Application Cryptogram

The Application Cryptogram (AC) allows the Issuer to confirm that the card is genuine, by verifying the Application Request Cryptogram (ARQC) received in the transaction is correct.

An incorrect ARQC may be the case of a counterfeit card, and Issuers are recommended to take caution in authorizing such transaction.

2.2.3.2 Cardholder Verification

The Issuers are advised to use the data present in the EMV transaction.

- Terminal Verification Results (TVR)
- Cardholder Verification Result (CVR)
- Cardholder Verification Method Results (if present)

This data is used to identify that the correct calculations are made and the results from the Terminal and the Card are consistent, i.e. there was no attempt of a wedge attack (also known as the Cambridge Attack).

2.2.3.3 Application Transaction Counter Monitoring

The Application Transaction Counter (ATC) provides a unique number for every cryptogram generated by the ICC.

The ATC is incremented for each transaction, and the Issuers are recommended to keep a record of the last approved transaction ATC. Subsequent transaction received from the card can be matched against the last record for consistency.

Issuers should put in place a mechanism to detect duplicate ATC, decline the transaction and investigate the reason of occurrence.

2.2.3.4 ICC CVV/CVC Validation

The CVV/CVC provides a static form of card authentication that can reduce the counterfeit fraud. However, the validation of the online application cryptogram provides a stronger card authentication method.

2.2.3.5 Issuer Script Requirements

Issuer scripts are commands send to the ICC by the Issuer in a transaction response to update the ICC data.

- Issuers are advised to support at least the APPLICATION BLOCK script
- Issuers must restrict the issuer scripts to one template per, 71 (pre-issuer script) and 72 (post-issuer script)
- The total length of all issuer scripts should not exceed 128 bytes, including the tag and length information
- Script must be protected by secure messaging

2.2.4 PIN Management

Issuers supporting Offline PIN are required to synchronize the Online PIN with the Offline PIN, so they appear as one for the cardholder.

The use of PIN change protocol should support synchronization of the Offline PIN and Online PIN, and handling exceptional conditions, such as time-outs.

Unless both the Offline and Online PIN have been changed successfully, the Offline PIN value should roll back to the original value. In situations where the Online PIN gets updated and the Offline PIN has not been changed, the Issuers should implement procedures to identify such a condition and provide appropriate instructions to the cardholder.

3 Appendix – Terms & Definition

Key terms used within this document are defined below.

Term	Definition
ATM	Automated Teller Machine
EMVCo	Europay, MasterCard, Visa Company (founders of chip cards specification)
HSM	Host Security Module
PAN	Primary Account Number
PIN	Personal Identification Number
POS	Point Of Sale

Table 3 - Terms Definition