

MICRO-ATM STANDARDS

Version 1.4
December 2011



Indian Banks' Association

World Trade Centre, Centre 1, 6th Floor,
Cuffe Parade, Mumbai 400 005



Unique Identification Authority of India

**Planning Commission, Govt. of India,
3rd Floor, Tower 2, Jeevan Bharati Bldg.,
New Delhi 110 001**

Table of Contents

TABLE OF CONTENTS	2
1 EXECUTIVE SUMMARY	3
1.1 REFERENCES	4
2 LIST OF ABBREVIATIONS	5
3 INTRODUCTION AND SCOPE	6
3.1 SCOPE.....	6
3.2 OVERVIEW OF MICROATM DEVICE.....	6
3.3 ONLINE AND OFFLINE ACCESS.....	6
3.4 OBJECTIVES OF MICROATM STANDARDS	7
3.5 WHAT IS INCLUDED IN THE MICROATM STANDARDS	8
4 SYSTEM ARCHITECTURE.....	9
4.1 USE OF BANK IDENTIFICATION NUMBER (BIN) FOR ROUTING OF TRANSACTIONS	10
4.2 THE ROLES OF VARIOUS PARTICIPANTS	11
5 FUNCTIONAL REQUIREMENTS.....	13
5.1 CUSTOMER EXPERIENCE	13
5.1.1 <i>Withdrawal</i>	13
5.1.2 <i>Deposit</i>	13
5.1.3 <i>Funds Transfer (debit only, no cash)</i>	14
5.1.4 <i>Balance Enquiry</i>	14
5.2 FUNCTIONAL DEVICE REQUIREMENTS	15
5.2.1 <i>Processing Speed</i>	15
5.2.2 <i>Role based access</i>	15
5.2.3 <i>Unique device number</i>	15
5.2.4 <i>Unique transaction number</i>	15
5.2.5 <i>Information stored on device</i>	15
5.2.6 <i>Reporting</i>	15
5.2.7 <i>Security</i>	16
5.2.8 <i>Centralized MicroATM Management System (CMMS)</i>	16
5.2.9 <i>Performance requirements</i>	16
5.2.10 <i>Dispute resolution</i>	16
5.2.11 <i>Reversals</i>	17
5.2.12 <i>UIDAI standards for biometrics and authentication</i>	17
5.3 CHARGE SLIP CONTENTS.....	17
6 HARDWARE REQUIREMENTS.....	19
6.1 TERMINAL SPECIFICATIONS	19
6.2 BIOMETRIC SPECIFICATIONS	20
6.3 MAGSTRIPE READER SPECIFICATIONS	20
7 MESSAGE FLOWS	21
7.1 SEQUENCE DIAGRAMS FOR ALL TRANSACTIONS	21
8 CONCLUSION AND SUMMARY	24

1 Executive Summary

The microATM device was originally described at a high level in a vision document by UIDAI titled *“From Exclusion to Inclusion with Micropayments”*. It is meant to be a device that is used by a million Business Correspondents to deliver basic banking services at the last mile. A committee consisting of IBA, UIDAI, NPCI, IDRBT, RBI and various banks was created to define the specifications and use cases of this device, which are presented here.

The costs of not standardizing a device like the microATM are quite high; large sections of Indian society will continue to be left out of the country’s financial system. The telecom industry is widely regarded for relentlessly driving down costs and bringing coverage to large parts of the Indian population. Similar success is possible in the payments industry. The microATM is a first step towards providing an online, interoperable, low-cost payments platform to everyone in the country.

The microATM device design and system architecture are influenced by the design of debit/credit card processing on point-of-service (POS) terminals, combined with authentication services that UIDAI will provide. The microATM is deployed by banks either directly, or through service providers. It is operated by individuals who are business correspondents themselves (individual BCs), or are sub-agents of a corporate BC.

The microATM standards are broad-based, standards-based, and generic. They are based on a bank-led model for financial inclusion, where the AADHAAR infrastructure is an overlay on the existing banking infrastructure.

The basic transaction types that the microATM will support are:

1. Deposit
2. Withdrawal
3. Funds transfer
4. Balance enquiry and mini-statement

The objectives of these specifications are to:

1. Bring down transaction costs
2. Ensure interoperability
3. Ensure security and transparency of transactions
4. Bring down the cost by being compatible with existing systems
5. Provide a uniform customer experience
6. Reduce agent training needs

This document describes the following, to achieve the stated objectives:

1. High-level system architecture for microATM transactions
2. Roles of various participants
3. Supported transaction types
4. Functional requirements for microATMs

5. Minimal hardware requirements
6. Interoperability requirements

Although this document standardizes a specific set of transactions, the device is expected to be deployed by service providers who may provide a variety of other financial and value added services. These additional services will generate increased cash-flows for microATM agents and thus create a strong and self-sustaining ecosystem in the long run.

This document will be updated with learnings from technical and field proof-of-concepts.

1.1 References

Several microATM design decisions are based on recommendations made in these other documents:

1. From Exclusion to Inclusion with micro-payments, UIDAI, Jan 2010
2. Biometric Design Standards for UID Applications (version 1.0), UIDAI, Dec 2009
3. AADHAAR Authentication API Specifications, UIDAI, (Version 1.0)
4. Interface specification for interoperable UID Based Financial Inclusion Architecture (Version 2.0), NPCI
5. Report of the RBI working group on regulatory issues
6. Report of the RBI appointed working group on issues/implications related to cash
7. Mobile Banking transactions in India - Operative Guidelines for Banks - Technology and Security Standards, RBI, Oct 2008
8. Open Standards on Smart Card based solution for financial inclusion, IBA and IDRBT Technical Committee Report, Jan 2010.
9. Interoperability Standards for Mobile Payments, MPFI, Sep 2008

2 List of Abbreviations

BIN	Bank Identification Number
CBS	Core Banking System
CIDR	Central ID Data Repository
CIPP	Central Interoperable Payment Platform
CMMS	Central MicroATM Management System
FI	Financial Inclusion
IBA	Indian Banking Association
IDRBT	Institution for Development and Research in Banking Technology
ISO	International Standards Organization
IT	Information Technology
MPFI	Mobile Payment Forum of India
NPCI	National Payments Corporation of India
ON-US	Intra-bank transactions
OFF-US	Inter-bank transactions
RBI	Reserve Bank of India
UID	Unique Identification Number
UIDAI	Unique Identification Authority of India

3 Introduction and Scope

Tremendous progress has already been made by banks towards financial inclusion. However, it is estimated that a large number of urban and rural poor still lack access to a basic bank account which is an important first step towards financial inclusion.

It has now become a national priority to rapidly accelerate progress toward financial inclusion and ensure safe, secure, sound, efficient access to basic financial services for all residents. Towards this end, a UID-enabled micropayments system is being conceived, which will be based on networks of agents managed by banks. These agents will perform financial transactions using microATMs.

A variety of financial services can be offered once a UID-enabled micropayments platform is available throughout the country. Several last mile collection problems can be solved with the micropayment device; for example, interest payments for micro-finance loans, premiums for micro-insurance policies, contributions to micro-pensions accounts, investments in micro-mutual funds. Likewise, payouts can be made through the same infrastructure as well.

3.1 Scope

This document describes the technological specifications of the microATM device, as applicable to the four basic banking transactions: deposit, withdrawal, funds transfer and balance query. Issues related to connectivity, interoperability, and regulation are outside the scope of this document.

3.2 Overview of microATM device

MicroATMs will allow customers to perform basic financial transactions using only their AADHAAR number and their fingerprint as identity proof (along with a Bank Identification Number for inter-bank transactions). Unlike an ATM, the cash-in / cash-out functions of the microATM will be performed by an operator, thus bringing down the cost of the device and the cost of servicing the customer. The microATM will support the following financial transactions:

- Deposit
- Withdrawal
- Funds transfer
- Balance enquiry

3.3 Online and offline access

Today, both offline and online solutions for financial inclusion (FI) are implemented by banks through FI vendors. In offline solutions, transactions are processed locally and transaction information is stored on smartcards and POS devices for later upload to a Core Bank-

ing System (CBS). In online solutions, all transactions are processed via real-time communication with a CBS.

The “*Interoperability Standards for Mobile Payments*” were published by the Mobile Payment Forum of India (MPFI) in September 2008 [9]. These standards describe mobile to mobile payments. In contrast, the microATM standards are for devices used by BCs to provide basic banking services at the last mile.

Several offline smart-card based solutions are successfully deployed today. IBA and IDRBT have released a standard for smart-card based offline solutions – “*Open Standards for Smart Card based solution for financial inclusion (version 1.2)*”[8].

Offline solutions may be required for many areas of the country for the foreseeable future. However, given the current levels of connectivity and the rapid growth in telecom coverage, this specification focuses only on the online solution (with no offline mode), in order to keep the microATM solution simple. However, this document recognizes the fact that banks and FI vendors may deploy either technology or a combination thereof based on ground reality. Banks have already made investments for financial inclusion, and are in the process of scaling up their investments. These standards make it possible for banks to acquire new devices that meet their existing requirements while complying with microATM standards.

3.4 Objectives of microATM standards

These microATM standards have been developed to:

- 1. Bring down the cost of integrating microATMs into banks’ networks**

Integrating different devices into a bank’s IT system can be a long and arduous process. These standards seek to ensure that banks need only set up a single backend IT system or use their existing systems.

- 2. Maximum compatibility with existing banking systems**

Wherever possible, the messaging protocols and transaction and settlement mechanisms of the microATM have been based on processes in use in the banking industry today. ON-US transactions can be processed internally within a bank, whereas OFF-US transactions will be routed through a multilateral switch for payment and settlement. The UID will be used only for identification and authentication.

- 3. Ensure secure and transparent transactions**

Agents operating from outside a bank branch are not subject to the same level of scrutiny as bank tellers and thus increased attention must be paid to ensure that transactions conducted by branchless banking agents are secure and easy to monitor. The microATM standards ensure that transaction information is appropriately encrypted at the application layer (for storage and transmission). Transactions can be traced for purposes of monitoring fraud and dispute resolution.

4. Ensure a more uniform customer experience

Customer trust and acceptance of microATMs will be key to the success of the micro-payments platform. These standards ensure a consistent customer experience across end devices thus helping to build this trust.

5. Reduce agent training needs

A standardized end device will allow banks to develop a common set of training materials for all agents regardless of what type of end device the agent uses.

3.5 What is included in the microATM standards

The microATM standards include:

- **Basic Functional Requirements:** The basic functions that the microATM should support and the basic performance levels that the microATM should achieve are described. This list of functions that the microATM supports is not intended to be comprehensive: device manufacturers may build in additional functionality to the microATMs.
- **Basic Hardware:** Some basic elements of the microATM hardware have been standardized to ensure that the microATM is capable of capturing fingerprints according to UIDAI specifications, connecting to banks' back-ends, and providing customers with a basic receipt and voice confirmation of their transaction.
- **Messaging:** The sequence diagrams for all message types are shown for illustration purposes. This is largely to clarify the system architecture. Detailed message formats will be described in the report of the RBI appointed working group on connectivity issues [4].

The microATM standards do *not* include detailed requirements for the hardware or the choice of connectivity (e.g. – GPRS, PSTN, CDMA, Ethernet etc.).

4 System Architecture

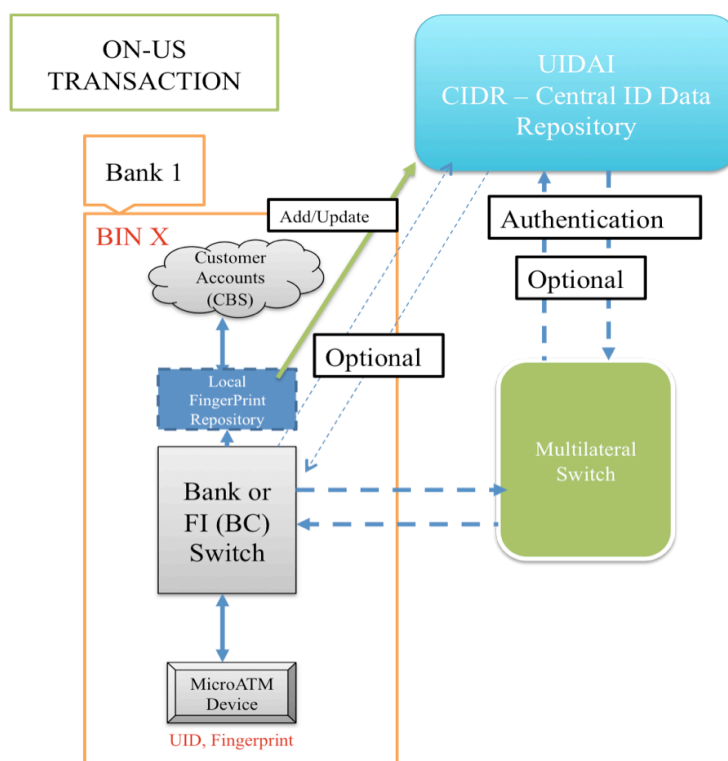


Figure 1: ON-US transactions

The backend transaction flow for ON-US (intra-bank) and OFF-US (inter-bank) transactions originating at microATMs is depicted in the diagrams in this section. In the case of ON-US transactions, transactions can be fully processed within the acquiring bank, which is also the issuing bank.

Authentication policies for AADHAAR authentication must be observed at all times as set forward by UIDAI.

The communication between the different entities involved in processing microATM transactions is described below:

1. MicroATM to Acquiring Bank:

The message formats for this leg of the transaction are not standardized, but they must be aligned with the need for processing OFF-US transactions[4]. The acquiring bank has the freedom to bring the messages to their switches using message formats and connectivity methods of their own choice. The acquiring bank may operate the microATM switch by itself, or outsource the operation to a service provider.

2. Multilateral switch to acquiring and issuing banks

The message formats for this leg will be standardized by the RBI appointed working group on connectivity issues for UID-based financial inclusion[4]. All participating banks will need to conform to these standards.

3. AADHAAR authentication

Any party sending authentication requests to UIDAI will need to conform to message formats[3] and device specifications as specified by UIDAI.

The system architecture described here is for basic customer-facing banking transactions. The system architecture for Electronic Benefit Transfers (EBTs) is not discussed here. However, this document recognizes the fact that EBTs will be delivered to beneficiaries using their UID. The beneficiary will use the microATM to operate the account where these funds are deposited. Over and above the basic transactions described here, banks may also provide other services and products to their customers using the microATM.

4.1 Use of Bank Identification Number (BIN) for routing of transactions

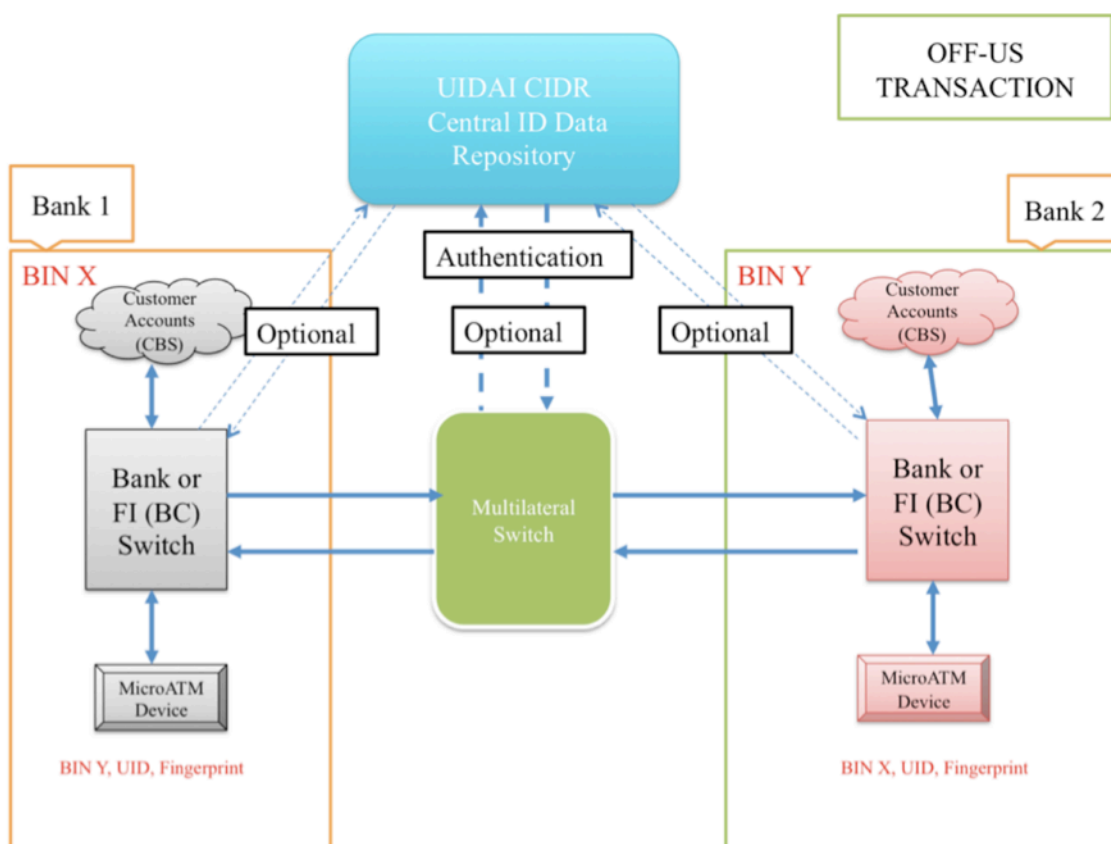


Figure 2: OFF-US transactions

In the case of OFF-US transactions in which a customer conducts a transaction at an agent attached to a bank other than the customer's own bank, the customer's AADHAAR number will not be sufficient for the transaction to be processed correctly. The acquiring bank must also know which bank the customer's account is with so that the transaction request may be forwarded appropriately. For this reason, all customers will be provided a BIN, which will prefix the AADHAAR number for all OFF-US transactions.

The BIN should be an international ISO BIN, which is 6 digits long.

4.2 The roles of various participants

The roles of various participants in the deployment of a microATM network are as follows:

Issuing bank

The issuing bank is the bank that owns the customer relationship, and stores account details in a Core Banking System (CBS). The customer banks with the issuing bank, interacts with the bank for any queries, and the issuing bank serves as the touch point for dispute resolution. It authorizes transactions and carries out all the four transactions that the customer initiates.

Acquiring bank

The acquiring bank is the bank that owns the BC relationship at the transaction point.

Business Correspondent (BC)

A Business Correspondent is appointed by the bank, and provides access to basic banking services using the microATM. These include the ability to take deposits, dispense cash for withdrawals, process funds transfers, or answer balance enquiries.

Multilateral switch (or Central Interoperable Payment Platform)

The multilateral switch is used in the case of OFF-US transactions to provide interoperability. It routes transactions from the acquiring bank to the issuing bank, and routes the authorization, settlement and reconciliation messages. An OFF-US transaction in the case of funds transfer may end up involving multiple banks: the acquiring bank, the issuing bank, and the recipient's bank. This multilateral switch may be operated by NPCI and other interbank switch vendors.

UIDAI

UIDAI will issue unique identity numbers to all residents in the country, and provide means to securely authenticate them. The AADHAAR platform will support the micropayments platform in the following ways:

1. UIDAI will provide methods for secure authentication of an individual, using the AADHAAR number and fingerprint.
2. Secure authentication provided by the UIDAI will facilitate interoperability among microATM devices operated by different banks, much like the existing ATM network.

3. The AADHAAR is a unique number that an individual has for life. It is globally addressable, much like email and mobile numbers. Unlike mobile numbers and email though, a person's AADHAAR number will not change over time. Thus it is natural to use AADHAAR as an identifying and addressing mechanism for all microATM transactions, specifically funds transfer where the AADHAAR of the sender, receiver and BC are involved in a transaction.

IBA, IDRBT, NPCI, and UIDAI

IBA, IDRBT, NPCI, and UIDAI are the custodians of the microATM standards.

RBI

RBI is the regulator of payment systems, and will regulate the microATM payments platform as well.

5 Functional requirements

5.1 Customer experience

The generic process flows for how withdrawal, deposit, funds transfer, and balance enquiry transactions must be conducted by microATMs, are described below. The operator must log in using either PIN or biometric authentication (if s/he is not already) before conducting any transaction. These flows do not include the activity on the network or the backend.

5.1.1 Withdrawal

1. Operator enters customer BIN+AADHAAR and transaction amount. (Micro-ATM may allow customer AADHAAR number to be automatically read from a card via a device such as a card reader or barcode scanner but manual entry of customer BIN+AADHAAR number by operator must also be supported.)
2. Device displays transaction details and prompts for confirmation.
3. Customer indicates confirmation by supplying fingerprint.
4. Success or failure of transaction is displayed on microATM screen. (Device may also notify operator and customer of the success or failure of transaction through other methods such as voice message or SMS but display and paper receipt is required).
5. If transaction has been successfully processed, operator dispenses cash.
6. Customer's account is debited, and the operator's account is credited.
7. Receipt is printed and handed over to the customer.

5.1.2 Deposit

1. Customer hands over cash to operator.
2. Operator enters customer BIN+AADHAAR and transaction amount. (MicroATM may allow customer BIN+AADHAAR number to be automatically read from a card via a device such as a card reader or barcode scanner but manual entry of customer AADHAAR number by operator must also be supported.)
3. Device displays transaction details and prompts for confirmation.
4. Customer indicates confirmation by supplying fingerprint.
5. Success or failure of transaction is displayed on microATM screen. (Device may also notify operator and customer of the success or failure of transaction through other methods such as voice message or SMS).
6. In case of rejection, operator returns cash to customer.
7. In case of success, customer account is credited, and the operator's account is debited.
8. Receipt is printed and handed over to the customer.

5.1.3 Funds Transfer (debit only, no cash)

1. Operator enters customer BIN+UID, recipient identifier (BIN+UID, IFSC+Account number, or BIN+mobile number), and transaction amount. (MicroATM may allow customer BIN+AADHAAR number to be automatically read from a card via a device such as a card reader or barcode scanner but manual entry of customer AADHAAR number by operator must also be supported.)
2. Device displays transaction details and prompts for confirmation.
3. Customer indicates confirmation by supplying fingerprint.
4. Success or failure of transaction is displayed on microATM screen. (Device may also notify operator, customer, and recipient of the success or failure of transaction through other methods such as voice message or SMS).
5. In case of success, customer account is debited, operator account is credited with the commission, and the recipient account is credited with the rest of the amount.
6. Receipt is printed and handed over to the customer.

5.1.4 Balance Enquiry

1. Operator enters customer BIN+UID. (MicroATM may allow customer BIN+AADHAAR number to be automatically read from a card via a device such as a card reader or barcode scanner but manual entry of customer BIN+AADHAAR number by operator must also be supported.)
2. Device displays that customer seeks to perform a balance enquiry.
3. Customer indicates confirmation by supplying fingerprint.
4. Balance printed on paper receipt only. The printout should include the last ten transactions. (In the case of balance enquiries, MicroATM should not send information regarding customer balance via other methods such as voice message or SMS.)

5.2 Functional device requirements

The minimal functional device requirements for the microATM are listed below. Banks and service providers may provide additional functionality depending on their business requirements and security needs.

5.2.1 Processing Speed

R[1] The microATM must be able to perform all internal activities related to processing of transactions promptly. Internal operations do not include data entry or back-end processing of transaction instructions, but do include operations such as encryption and decryption of messages, preparing packets for transfer on the network, accounting, etc.

5.2.2 Role based access

R[2] The microATM must provide different logins for operators, service agents, and super-users. These may be authenticated using AADHAAR authentication[3] as well.

R[3] No transactions may be performed on the microATM without the operator logging in.

5.2.3 Unique device number

R[4] Each microATM will have a unique terminal ID. This number must be transmitted with each transaction. The unique device number will include an institution code, followed by the contents of data elements in fields 41, 42 and 43 from the ISO 8583 protocol. The report of the RBI appointed working group on connectivity issues[4] will provide further details on the structure of these numbers.

5.2.4 Unique transaction number

R[5] A systems trace audit number (STAN) is generated automatically by the terminal. It is incremented for each transaction processed. Although the STAN itself may not be unique across devices, it must be unique after combining the generated STAN with the unique terminal ID.

5.2.5 Information stored on device

R[6] The microATM must maintain certain details of recent transactions (for a prescribed period of time and/or number of transactions). Details on what AADHAAR data may be stored on the device will be provided by UIDAI. All stored data on the device must be stored in an encrypted format.

5.2.6 Reporting

R[7] The microATM must allow operators to generate end of day reports including the total cash flow for the day and a log of all transactions for the day.

5.2.7 Security

- R[8] The microATM must not transmit any confidential data unencrypted on the network.
- R[9] Security requirements specified by UIDAI for AADHAAR data must be followed to secure the biometric and other AADHAAR authentication data.
- R[10] The microATM must automatically log out the operator and lock itself after a period of inactivity.

5.2.8 Centralized MicroATM Management System (CMMS)

- R[11] The Centralized microATM Management System (CMMS) will provide a dashboard and control board functionality at the deploying bank or BC, and have the ability to control every microATM remotely.
- R[12] All incoming and outgoing messages are recorded for validation, verification and audit trail, as specified by the regulator. Each message is stored sequentially as received.
- R[13] The CMMS should be able to configure and update the software remotely.
- R[14] The microATM will have periodic keep-alive messaging capability built into it. The period for keep-alive must be configurable.
- R[15] CMMS should record and save Terminal ID as and when microATM successfully downloads the application parameters
- R[16] CMMS should be able to generate MIS of various actions such as: Download History (History of TIDs of the terminals initialized with date and time), microATM Profile (Profiles of the TIDs loaded on CMMS with details like operator/Merchant name, location, operator UID/TID, transaction types supported/unsupported, communication parameters, etc.)

5.2.9 Performance requirements

- R[17] All transactions once entered on the microATM must have an end-to-end latency of less than 45 seconds for approval or decline. After this period, a transaction must timeout.

5.2.10 Dispute resolution

- R[18] The unique terminal ID, combined with the STAN uniquely identifies every transaction in the system. A Retrieval Reference Number (ISO 8583, data element 37) must be generated. The report of the RBI appointed working group on connectivity issues[4] will provide further details on the RRN.
- R[19] The dispute resolution process will involve all related parties – Issuer, acquirer, multilateral switch and UIDAI.

5.2.11 Reversals

R[20] An online reversal must occur when there is a timeout, no response, a power down, or inability to print receipt. Further details on reversal will be provided by the report of the RBI appointed working group on connectivity issues[4]. These may be revised after a proof-of-concept in the field.

R[21] The issuer is responsible to decline multiple reversals for the same transaction. Issuer is also responsible for reversal matching logic

5.2.12 UIDAI standards for biometrics and authentication

R[22] Biometric hardware must meet minimal standards as described in this document in the hardware requirements section

R[23] The terminal must be capable of following UIDAI authentication as described in the “AADHAAR Authentication API Specification”[3] released by UIDAI.

R[24] The authentication process must comply with authentication policies of UIDAI.

5.3 Charge slip contents

Each charge slip for deposit, withdrawal, and balance enquiry transactions should contain the following items:


1. Bank name
2. BC name
3. Operator location
4. Operator identifier
5. Terminal ID (see functional requirement R4)
6. Systems trace audit number (see functional requirement R5)
7. Customer name
8. Retrieval reference number
9. Last 6 digits of customer's AADHAAR (First 6 digits of customer's AADHAAR should never be printed on charge slip)
10. Transaction date and time
11. Transaction type (e.g. – deposit, withdrawal, balance enquiry, funds transfer)
12. Amount
13. Balance (optional)

Charge slips issues for balance enquiry transactions should include the following items:

Bank Name and Logo

Service Name

1. Transaction Date and Time
2. BC Name
3. Agent Id (if applicable)
4. BC Location
5. Terminal Id

- 
6. Customer UID
 7. Customer Name
 8. STAN
 9. Retrieval reference no. (RRN)
 10. Transaction Status
 11. Transaction Amount (In case of Cash Withdrawal/deposit/Funds Transfer)
 12. A/C Balance (for all the transactions including Funds Transfer)

6 Hardware requirements

The following table specifies minimal hardware requirements. Banks and service providers must use a device that is appropriate for local operating conditions, with specifications that meet or exceed the requirements specified below.

These specifications have been intentionally kept to a minimum to allow a variety of form factors (including mobile phones) and innovation.

6.1 Terminal specifications

Component	Minimum Requirement
Biometric scanner	As per specifications in section 6.2
Connectivity	The device must provide for at least two channels (of service provider's choice) of connecting to the network.
Encryption and encoding	1024-bit PKI, 128-bit AES, Base64 for full compliance with AADHAAR Authentication API specifications[3].
Storage (non-volatile)	Must be capable of storing at least 1000 transactions, or one full day's transactions, whichever is larger.
Display	Must be capable of displaying last 10 transactions without scrolling horizontally. Each transaction must display at least the date, type, and amount.
Magstripe reader (Optional)	As per specifications in section 6.3
Printer	Must be able to print out transaction status and a mini-statement of at least the last 10 transactions. Receipts and other printed items must be legible for at least two months from the date of printing. ¹
Key pad	16 key pad or better
Speaker (Optional)	A facility may be provided for voice confirmation of the transaction
Battery life	Minimum 4 hours
Power Adaptor	AC/DC Adaptor with surge protection.
Certification	CE mark compliance for EMI, EMC
Environment	Operating temp: 0°C to 50°C Storage not including battery: (0°C to 55°C)

¹ In the case that a thermal printer is used, the paper should be of sufficient quality for this requirement to be met.

6.2 Biometric specifications

All MicroATM devices should be certified by STQC to meet the technical specifications as defined by UIDAI. Detailed guidelines on the STQC certification process are available on the STQC website:

<http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification>

6.3 Magstripe specifications

Component	Specifications
Magstripe card reader	ISO triple-track 1/2/3, bi-directional, high-coercivity
Security	SSL v3.0, 3DES encryption, master/session or DUKPT key management
SAM	2
PCI-PED	1.3

7 Message flows

In order to provide some context for the communication between the microATM and the microATM switch, the suggested flow of messages between the various entities involved in processing micropayments transactions is described below.

7.1 Sequence diagrams for all transactions

This section describes sequence diagrams for the different transaction types. Not all the possible cases are shown. These are meant to be illustrative. For example, authentication with UIDAI may be performed at various different points in the transaction flow depending on the type of transaction, and the number of parties involved. Today, many FI transactions are stored in an intermediate system and reconciled once a day in the bank's CBS, consistent with RBI guidelines, For such cases, in the sequence diagrams below, updates to a CBS may actually be updates to an intermediate system. It is not possible to capture all these cases in a concise manner, which is why only specific instances are provided.

Figure 3 shows a sequence diagram for the case of a deposit. It shows the messages between various IT systems involved in a deposit transaction.

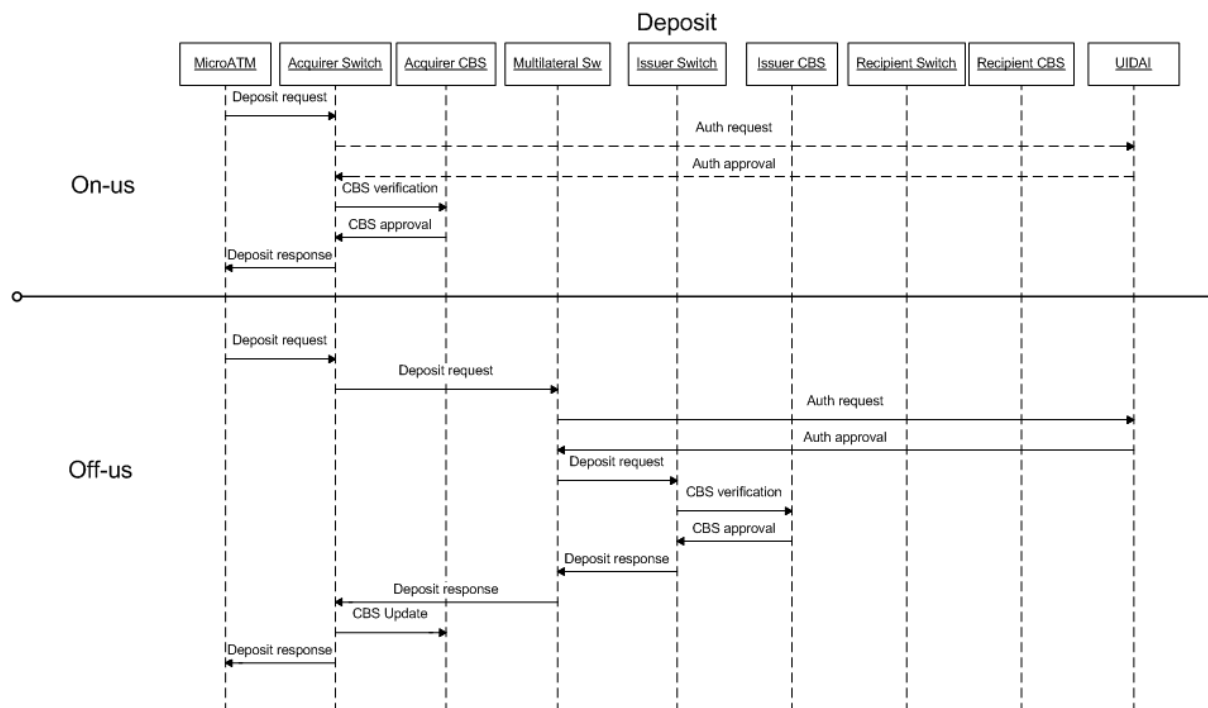


Figure 3: Sequence diagrams for deposits

Figure 4 shows a sequence diagram for the case of a withdrawal. It shows the messages between various IT systems involved in a withdrawal transaction.

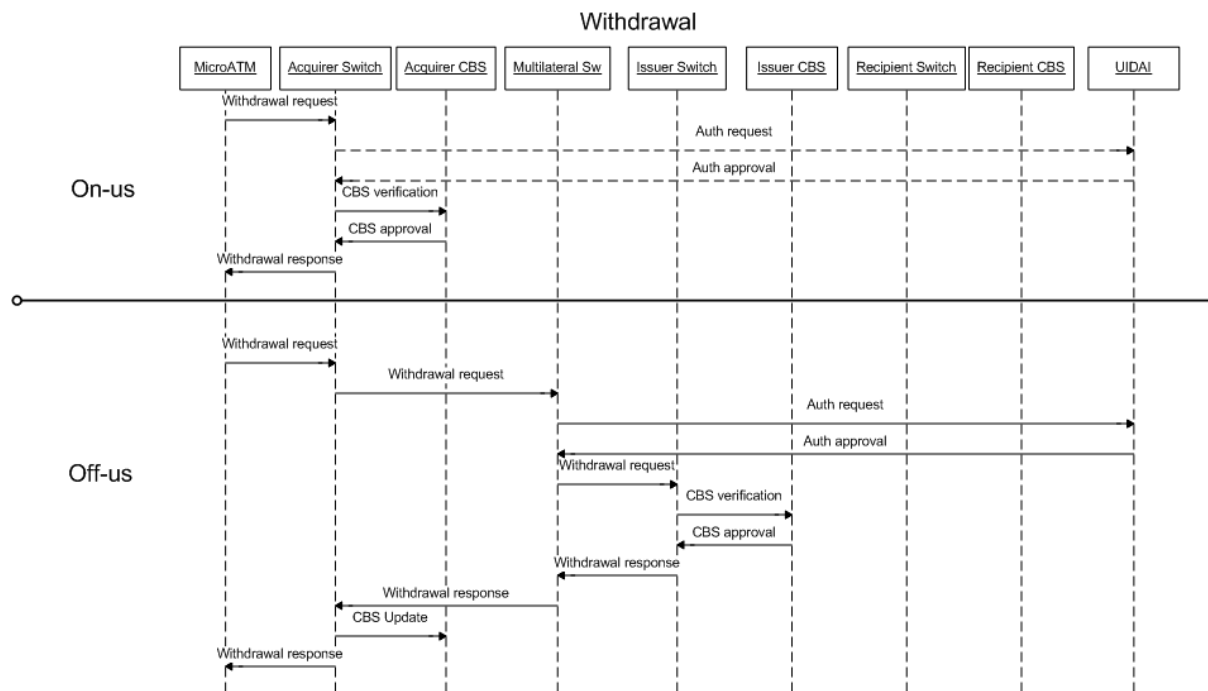


Figure 4: Sequence diagram for withdrawals

Figure 5 shows a sequence diagram for the case of a balance enquiry. It shows the messages between various IT systems involved in a balance query transaction.

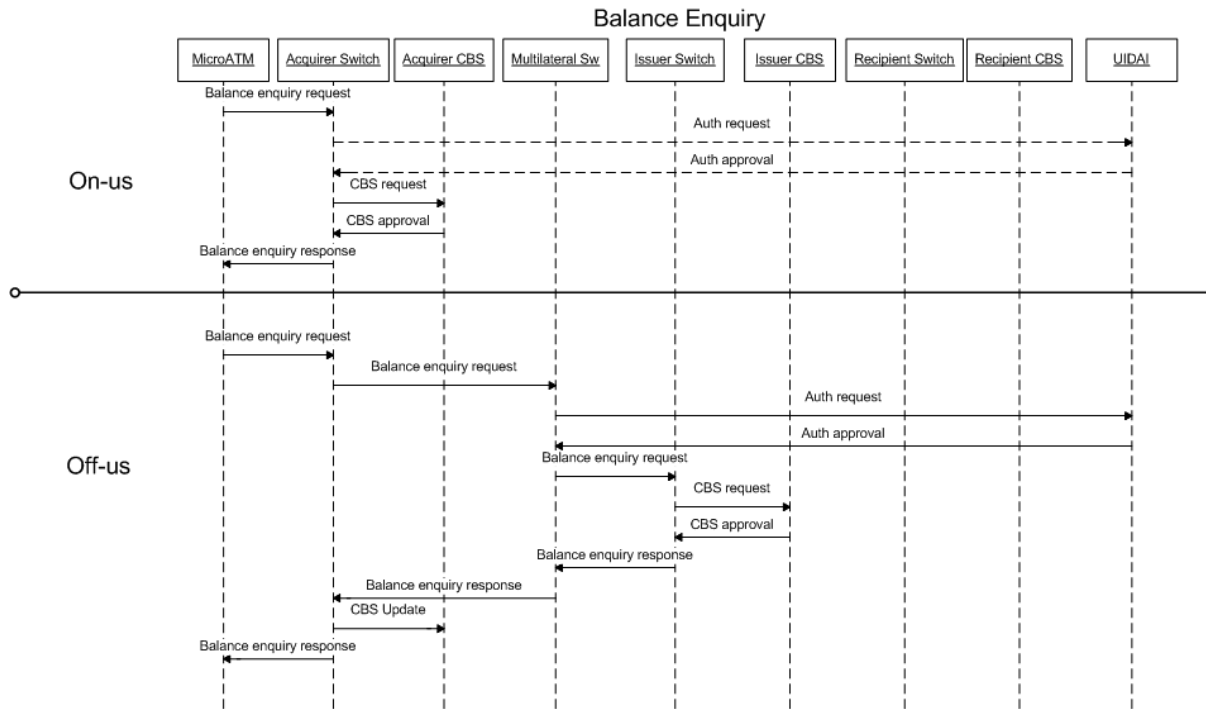


Figure 5: Sequence diagram for balance query

Figure 6 shows a sequence diagram for the case of a funds transfer. It shows the messages between various IT systems involved in a funds transfer transaction. In this case, due to the number of banks involved and possibilities, only the most general case is shown.

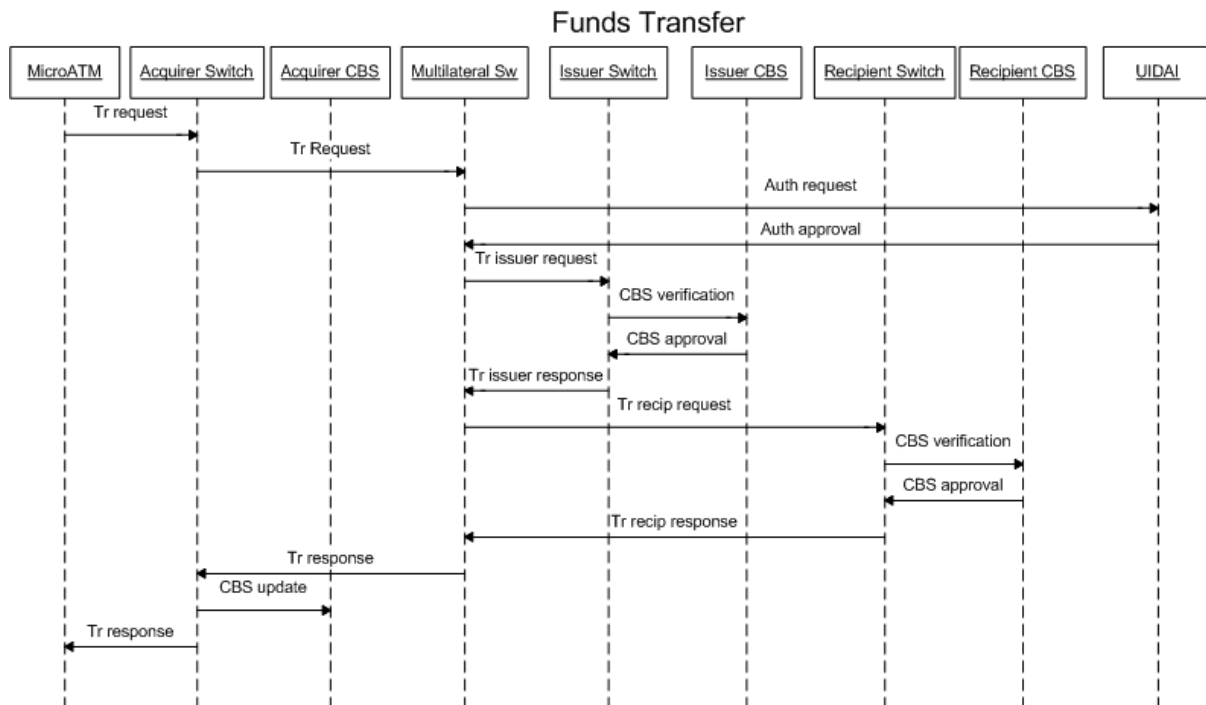


Figure 6: Sequence diagram for funds transfer

8 Conclusion and summary

This document defines standards for the microATM device. These standards are broad-based, standards-based and generic. The goal is to leverage UIDAI's online fingerprint authentication for banking transactions, without requiring a major change to the already existing banking infrastructure.

This device will be deployed by Business Correspondents to implement branch-less banking; provide banking services where bank branches are not present. The microATM standards only provide for basic banking transactions: deposit, withdrawal, funds transfer, and balance query.

The microATM functionality has been restricted to a small set of transactions, so that the device can be robust and simple, but can be scaled for ubiquitous country-wide deployment. Interoperability is a key feature of the microATM, where customers can visit any BC in the country and operate their account.

It is expected that these microATM standards, along with the recommendations for connectivity, and regulatory issues will accelerate the process of financial inclusion in the country, and help achieve the nation's goal of inclusive growth.