MICRO-ATM STANDARDS

Version 1.5.1
March 2013

Indian Banks' Association

Unique Identification Authority of India

Institute for Development and Research in Banking Technology

National Payments Corporation of India

Table of Contents

Executive summary

The Reserve Bank of India held a meeting with UIDAI, IBA, NPCI, IDRBT, NABARD, India Post, and a number of Banks on Aadhaar based financial inclusion on December 11, 2009. Two Working Groups were created to address technology and connectivity issues vide DBOD.BL.No. 12497 /22.01.001/2009-10, dated January 15, 2010 (Annexure I):

> *"7. (b) Working Group on technology issues*
>
> *i. This group may be chaired and convened by Shri M.V.Nair, CMD, Union Bank of India and Chairman, IBA, and have representatives from IDRBT, NPCI, a few banks and RBI (DIT and DPSS) and UIDAI.*
> *ii. The group may look into all technology issues including specifying parameters for micro-ATMs and coordinate with the UIDAI.*
>
> *7. (c) Working Group on connectivity issues*
>
> *i. This group to be chaired and convened by NPCI and may comprise of representatives from NPCI, IDRBT, IBA and RBI (DIT and DPSS).*
> *ii. The group may look into all issues relating to connectivity including central infrastructure, settlement network platform etc."*

The Working Group on technology issues and the Working Group on connectivity issues have jointly prepared these microATM standards.

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. MicroATMs will be deployed by banks either directly, or through service providers and operated by individuals who are BCs themselves (individual BCs), or are sub-agents of a corporate BC.

The microATM device design and system architecture has leveraged the following:

1. Existing investment in point-of-service (POS) devices used by Business Correspondents (BCs) for financial inclusion as well as debit and credit card processing;
2. BC interoperability guidelines issued by RBI (1);
3. The *Report of the Working Group on Securing Card Present Transactions, RBI* (2);
4. The *Revised Scheme for Issue of Kisan Credit Card, RBI* (3);
5. *Mobile Banking transactions in India - Operative Guidelines for Banks*, RBI (4);
6. *Interoperability Standards for Mobile Payments*, MPFI (5);
7. *Open Standards for Smart Card based solution for financial inclusion,* IDRBT (6)*;*
8. *Procedural Guidelines for Aadhaar-enabled Payments System,* NPCI (7);

9. *Aadhaar-enabled Payments System interface specifications*, NPCI (8); and
10. Aadhaar authentication services, UIDAI (9).

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 and payments infrastructure.

The basic interoperable transaction types that the microATM will support are:

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

The microATM will support the following means of authentication for interoperable transactions:

1. Aadhaar + Biometric
2. Aadhaar + OTP
3. Magstripe card + Biometric
4. Magstripe card + OTP
5. Magstripe card + Bank PIN

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; and
6. Reduce agent training needs.

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.

List of abbreviations

API	Application Programming Interface
ASA	Authentication Service Agency
AUA	Authentication User Agency
BC	Business Correspondent
BFD	Best Finger Detection
BIN	Bank Identification Number
CBS	Core Banking System
CIDR	Central ID Data Repository
CMMS	Central MicroATM Management System
FI	Financial Inclusion
IBA	Indian Banks' 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
STAN	Systems Trace Audit Number
TID	Terminal or device Identifier
UID	Unique Identification Number
UIDAI	Unique Identification Authority of India
UKPT/DUKPT	Unique Key per Terminal / Derived Unique Key per Transaction

1 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, an Aadhaar-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 an Aadhaar-enabled micropayments platform is available throughout the country as described in a document from UIDAI titled *From Exclusion to Inclusion with Micropayments* (10). 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.

1.1 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.

1.2 Overview of microATM device

MicroATMs will allow customers to perform basic financial transactions using only their Aadhaar number and their biometric/OTP 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:

1. Deposit
2. Withdrawal
3. Funds transfer
4. Balance enquiry

1.3 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 trans-

action information is stored on smartcards and POS devices for later upload to a Core Banking 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 (5). 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)* (6).

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.

1.4 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 Aadhaar 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.

1.5 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 biometrics 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 are described in the report of the RBI appointed working group on connectivity issues (8).

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

2 System architecture

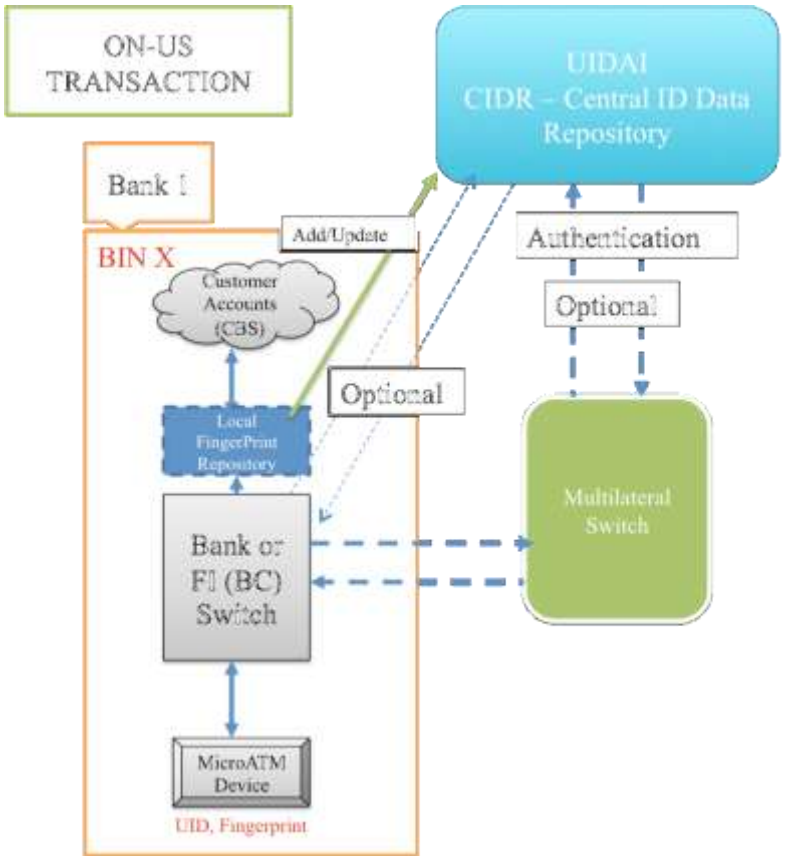


Figure 1: ON-US transactions

Interoperable BC transactions are now permitted by RBI, and thus must follow the guidelines issued by RBI (1). 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, and is consistent with the RBI guidelines on interoperability. ON-US transactions can be fully processed within the acquiring bank, which is also the issuing bank. For ON-US transactions, banks may use their own authentication if biometrics are available with the bank, or use Aadhaar authentication as a fallback. In the case of OFF-US transactions, a standardized authentication method is necessary, which is provided by Aadhaar.

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

- **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 (8). 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.

- **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 Aadhaar-based financial inclusion (8). All participating banks will need to conform to these standards and the relevant procedural guidelines (7).

- **Aadhaar authentication**
  Any party sending authentication requests to UIDAI will need to conform to message formats (9) 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 Aadhaar Number. 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.

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

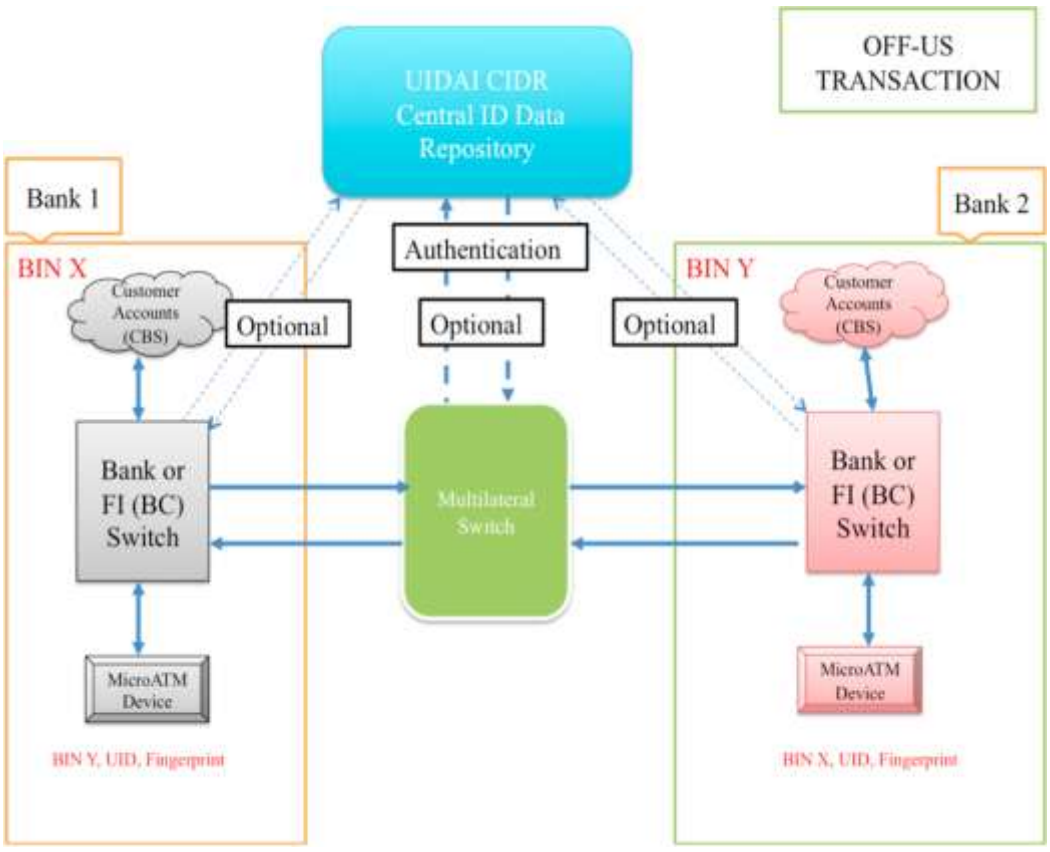


Figure 2: OFF-US transactions

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.

2.2 The roles of various participants

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

1. **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.

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

3. **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. Banks may either appoint an individual BC or a corporate BC who further appoints sub-agents.

4. **Technology Service Provider (TSP)**
   The Technology Service Provider provides technology to the Acquiring Bank to support BC operations.

5. **Multilateral switch**
   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.

6. **UIDAI**
   UIDAI issues unique Aadhaar 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:

a) UIDAI provides methods for secure authentication of an individual, using the Aadhaar number and demographic data, biometrics, OTP, etc.;
b) Secure authentication provided by the UIDAI facilitates interoperability among microATM devices operated by different banks, much like the existing ATM network; and
c) Aadhaar number is a unique number that an individual has for life. It is globally addressable (11), 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 number as an identifying and addressing mechanism for all microATM transactions, specifically funds transfer where the Aadhaar number of the sender, receiver and BC are involved in a transaction.

7. IBA, IDRBT, NPCI, UIDAI

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

8. RBI

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

3 Functional Requirements

3.1 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 before conducting any transaction. These flows do not include the activity on the network or the backend.

3.1.1 Withdrawal

1. Operator enters customer BIN+Aadhaar number 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 biometric authentication by default, or other methods such as OTP as a fallback (9).
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.

3.1.2 Deposit

1. Customer hands over cash to operator.
2. Operator enters customer BIN+Aadhaar number and transaction amount. (Micro-ATM 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 biometric authentication by default, or other methods such as OTP as a fallback (9).
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.

3.1.3 Funds transfer (debit only, no cash)

1. Operator enters customer BIN+Aadhaar number, recipient identifier (BIN+Aadhaar number, 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 biometric authentication by default, or other methods such as OTP as a fallback (9).
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.

3.1.4 Balance enquiry

1. Operator enters customer BIN+Aadhaar number. (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 biometric authentication by default, or other methods such as OTP as a fallback (9).

Balance should be printed on paper receipt. The printout should include the last ten transactions.

3.2 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.

3.2.1 Processing speed

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.

3.2.2 Role based access

2. The microATM must provide different logins for operators, service agents, and super-users. These may be authenticated using Bank's own authentication or Aadhaar authentication (9).
3. No transactions may be performed on the microATM without the operator logging in.

3.2.3 Unique device number

4. Each microATM will have a unique device 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 (8) will provide further details on the structure of these numbers.

3.2.4 Unique transaction number

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 device ID.

3.2.5 Version control and provisioning

6. Device must support version control feature in order remotely monitor and provision application and system software. Remote device management feature must be provisioned as a part of the device deployment.

3.2.6 Information stored on device

7. The microATM must maintain certain details of recent transactions (for a prescribed period of time and/or number of transactions) excluding biometrics. Details on what Aadhaar data may be stored on the device are provided by UIDAI. All stored data on the device must be stored in an encrypted format.

3.2.7 Reporting

8. 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.

3.2.8 Security

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

3.2.9 Centralized MicroATM Management System (CMMS)

12. 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.
13. 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.
14. The CMMS should be able to configure and update the software remotely.
15. The microATM will have periodic keep-alive messaging capability built into it. The period for keep-alive must be configurable.
16. CMMS should record and save Device ID as and when microATM successfully downloads the application parameters
17. CMMS should be able to generate MIS of various actions such as: Download History (History of TIDs of the devices initialized with date and time), microATM Profile (Profiles of the TIDs loaded on CMMS with details like operator/Merchant name, location, operator Aadhaar number/TID, transaction types supported/unsupported, communication parameters, etc.)

3.2.10 Performance requirements

18. 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.

3.2.11 Dispute resolution

19. The unique device 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 has provided further details on the RRN (8).
20. The dispute resolution process will involve all related parties – Issuer, acquirer, multilateral switch and UIDAI.

3.2.12 Reversals

21. 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. These may be revised after a proof-of-concept in the field.
22. The issuer is responsible to decline multiple reversals for the same transaction. Issuer is also responsible for reversal matching logic

3.2.13 UIDAI standards for biometrics and authentication

23. The device must be certified for Aadhaar authentication as per the certification requirements laid down by UIDAI (12).
24. Upon entry of the number, the check digit in the Aadhaar number should be verified by the device as described in the UID numbering scheme (11).
25. The device must be capable of following UIDAI authentication as described in the “Aadhaar Authentication API Specification” (9) released by UIDAI.
26. Device must support “Best Finger Detection” software as per Aadhaar Best Finger Detection API (13) released by UIDAI.
27. Device’s best finger detection software must be in accordance with resident authentication on-boarding document released by UIDAI.
28. The device must be capable of conducting two finger authentication transactions in the same session as laid out on the authentication process documents.
29. As a fallback to biometric authentication, the device must implement the OTP API and OTP authentication capability (14).
30. The device must implement the Aadhaar mobile number update API (15).

3.3 Charge slip contents

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

1. Bank name and logo
2. Service name
3. BC name
4. Operator location
5. Operator identifier
6. Device identifier (TID - see functional requirement R4 (8))
7. Systems Trace Audit Number (STAN - see functional requirement R5 (8))
8. Customer name
9. Retrieval reference number (RRN)
10. Last 6 digits of customer's Aadhaar number (First 6 digits of customer's Aadhaar number should never be printed on charge slip)
11. Transaction date and time
12. Transaction type (e.g. – deposit, withdrawal, balance enquiry, funds transfer)
13. Transaction amount
14. Account balance

4 Hardware requirements

4.1 Device specifications

MicroATMs may be all-in-one integrated devices, or mobiles / PCs / tablets with accessories. Banks procuring microATMs may choose to award higher technical scores for particular form factors, or optional features, which meet their own business requirements.

Component	Minimum Requirement
Biometric scanner	As per specifications in section 4.2.
Connectivity	The device must provide for two channels (of service provider's choice) of network connectivity.
Security	2048-bit PKI, 256-bit AES, Base64, SHA-256 for full compliance with Aadhaar Authentication API specifications (9).
Non-volatile storage	Must be capable of storing audit trails of at least 1000 transactions.
Display	Must be capable of displaying last 10 transactions without scrolling horizontally. Each transaction must display at least the date, type, and amount.
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]
Battery	Rechargeable battery, with minimum 4 hours battery life.
Power Adaptor	AC/DC Adaptor with surge protection.
Environment	Operating temp: 0°C to 50°C. Storage not including battery: 0°C to 55°C.
Magstripe reader and PIN pad	As per specifications in Section 4.3 (2) (3).
Speaker	A facility should be provided for voice confirmation of the transaction.
Location	The terminal should have the capability to communicate its location (Industry standard 16 channel NMEA Compliant GPS support or Cell Tower Location or any other dynamic method for approximate Lat-Long location)
QR code reader (Optional)	Ability to read QR code from the Aadhaar letter, of size 21mm x 21mm, 600 DPI, and Error Correction Code Level M (Medium).
EMV capability (Optional)	EMV Level 1 and Level 2 certification as per Section 4.4.
NFC reader (Optional)	Contactless smart card readers compliant to ISO 14443 A and B cards (for all four types of NFC tags) and ISO/IEC 18092.

Note - At a future date, as the device ecosystem matures, the MicroATM specifications may have to be refreshed and some of the optional items may be made mandatory. In case MicroATM specifications are refreshed, devices conforming to the earlier specifications do not need to be upgraded; the new specifications will apply only for new procurements thereafter

4.2 Biometric scanner specifications

All MicroATM devices should use the STQC certified Scanner+Extractor to meet the technical specifications as defined by UIDAI. Certified devices should carry the Aadhaar logo on the device. The use of the Aadhaar logo should be in accordance with the guidelines issued by UIDAI.

Detailed guidelines on the STQC certification process, and list of certified devices are available on the STQC website:
http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification

Parameters	**Specification**
Minimum Platen Area	**Optical/multispectral/capacitance technology** **1. If platen area is 15.24 mm x 20.32 mm or more:** 1.1 Provisional certificate would be issued without any fied testing; 1.2 Final certification would be subject to sensor-extractor meeting <2% FRR in Aadhaar athentication system (at FAR of 0.01%) for which detailed guidelines will be published by STQC. 2. If platen area is 12.8 mm x 16.5 mm or more but less than 15.24 mm x 20.32 mm, certification would be suject to sensor-extractor meeting <2% FRR in Aadhaar authentication system (at FAR of 0.01%) for which detailed guidelines will be published by STQC. **Any other Technologies** **3. <**2% FRR in Aadhaar authentication set up (at FAR of 0.01%) would need to be demonstrated. Detailed guidelines and other requirements specific to the technology will published separately by STQC.

Parameters	**Specification**
Image quality	Must be listed on "IAFIS Certified Product List" posted on https//www.fbibiospecs.org/IAFIS/Default.aspx under "PIV Single Finger Capture Devices" **OR** Lab Test conformance report showing compliance to ISO 19794-4 Annexure A **OR** any other equivalent conformance report (to be approved for equivalence by expert committee appointed by Competent Authority
Extractor Quality	• MINEX compliance • Number of Minutiae generated by extractor to be in conformance to ISO Specification. Tested for at least 12 Minutiae points generated under test conditions.
NFIQ Quality Software	Inbuilt NFIQ quality software either at device level or extractor level.
Resolution	Minimum 500 DPI with 5% margin on the lower side
Grey scale/ Image type	8 bit, 256 levels
Extractor & Image Template Standard	ISO 19794-2 for fingerprint minutiae template and ISO 19794-4 for Fingerprint Image Template
Latent detection	Preferable
Platen	Rugged, minimum IP 54 rating preferable Prefer scratch resistant features
Preferred Operating Temperature	0 to 45 degree Centigrade
Preferred Storage Temperature	0 to 50 degree Centigrade
Preferred Humidity	10 to 90%
ESD	>= 8Kv
Environment, health and safety	ROHS certification
Safety	UL or IEC60950 compliance

Parameters	Specification
EMC compliance	FCC class A or equivalent
Operating system environment	Vendor needs to declare the compatible operating system
Connectivity	• Standard USB connectivity for PC based application. • Connectivity for POS devices.

4.3 Magstripe reader and PIN pad specifications

Component	Specifications
Magstripe reader	ISO triple-track 1/2/3, bi-directional, high-coercivity
Security	1. 3DES encryption 2. TMK/TPK support with all keys remote download capability 3. UKPT / DUKPT capability
PCI-PED for POS	PCI (Payment Card Industry) PED (Pin Entry Device) for POS

The payment application on microATMs for processing card and PIN transactions should be certified with PA-DSS certification (2) (3). Until the application is PA-DSS certified, the microATMs may not be able to process card and PIN transactions, but may process BC transactions as defined in these standards, so long as all other security requirements are met.
Please refer to:

https://www.pcisecuritystandards.org/security_standards/documents.php?association=PA-DSS

4.4 EMV compliance

EMV capability is currently optional, but may become mandatory based on guidelines from RBI on securing card present transactions (2).

Please refer to:
http://www.emvco.com/approvals.aspx

5 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.

5.1 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.

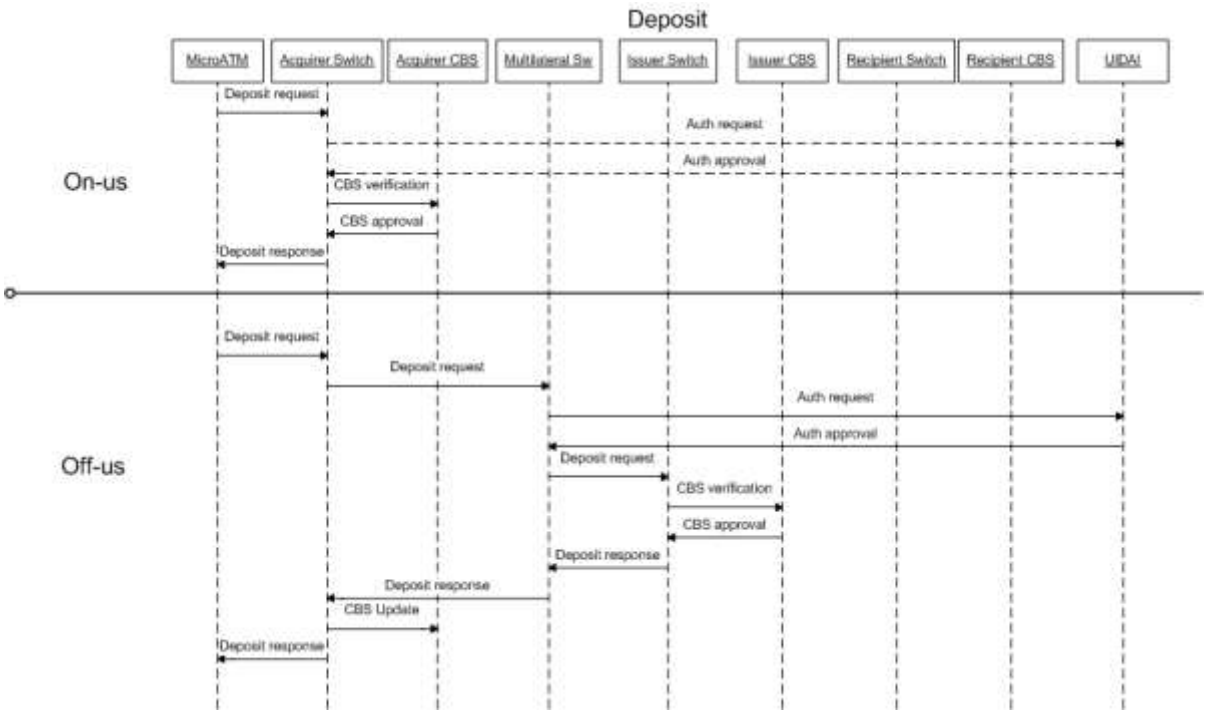


Figure 3: Sequence diagrams for deposits

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.

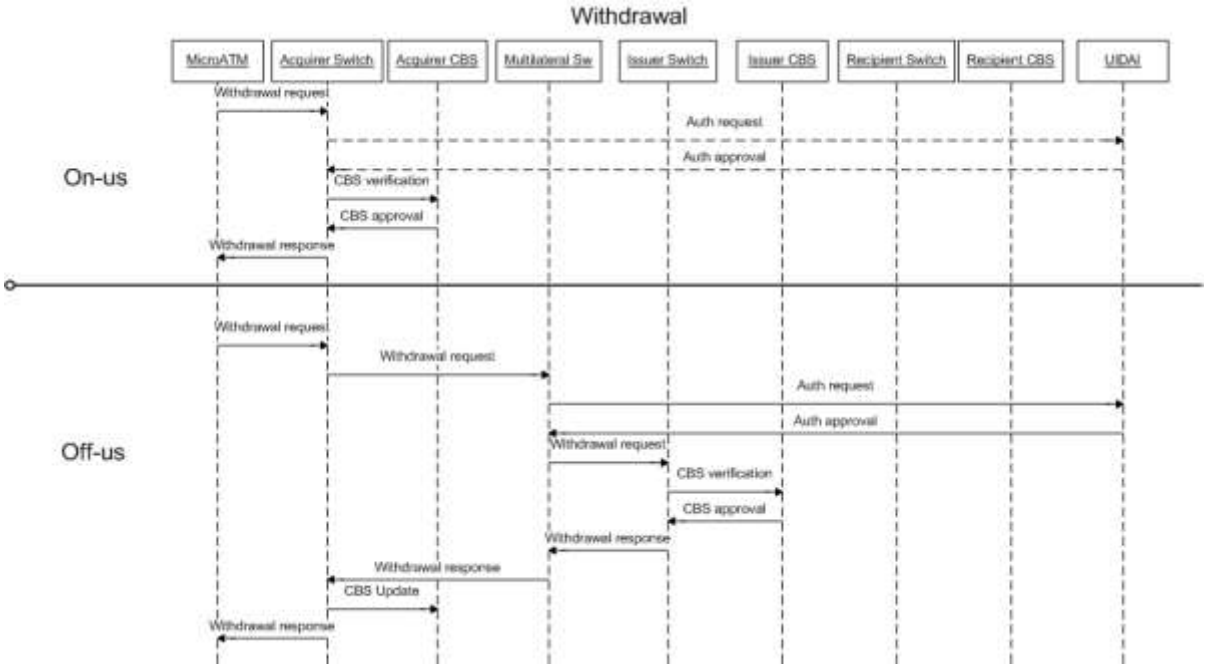


Figure 4: Sequence diagram for withdrawals

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.

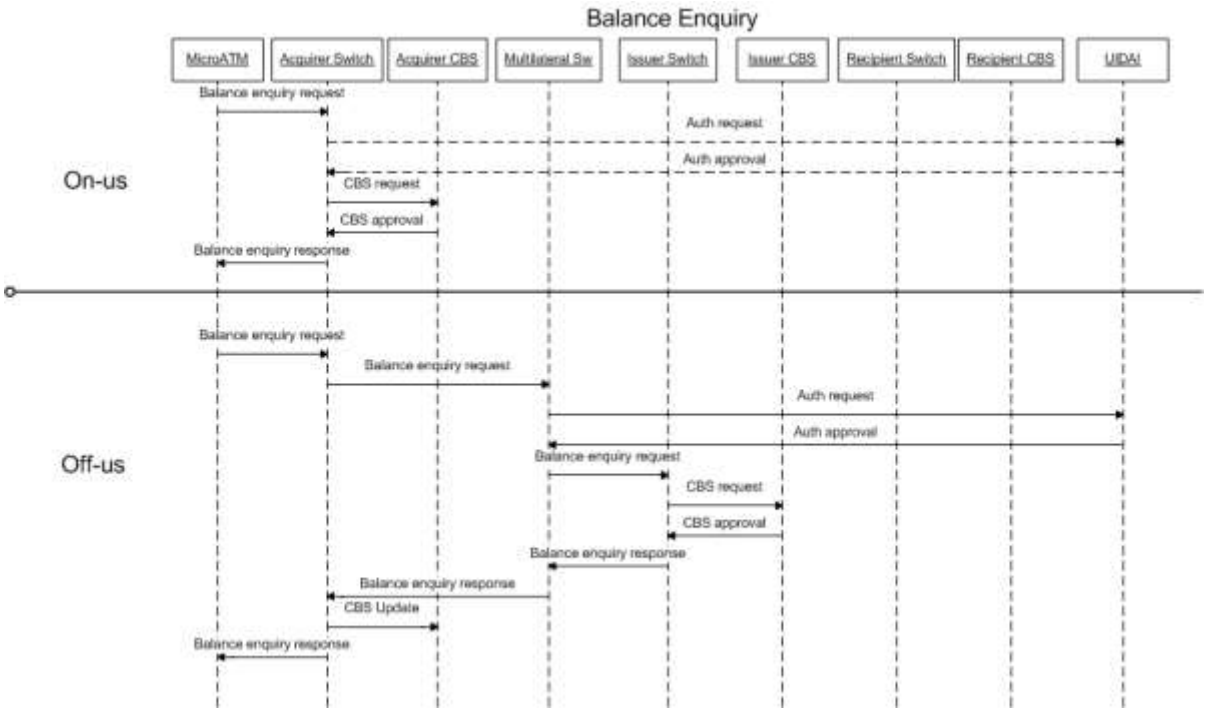


Figure 5: Sequence diagram for balance query

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.

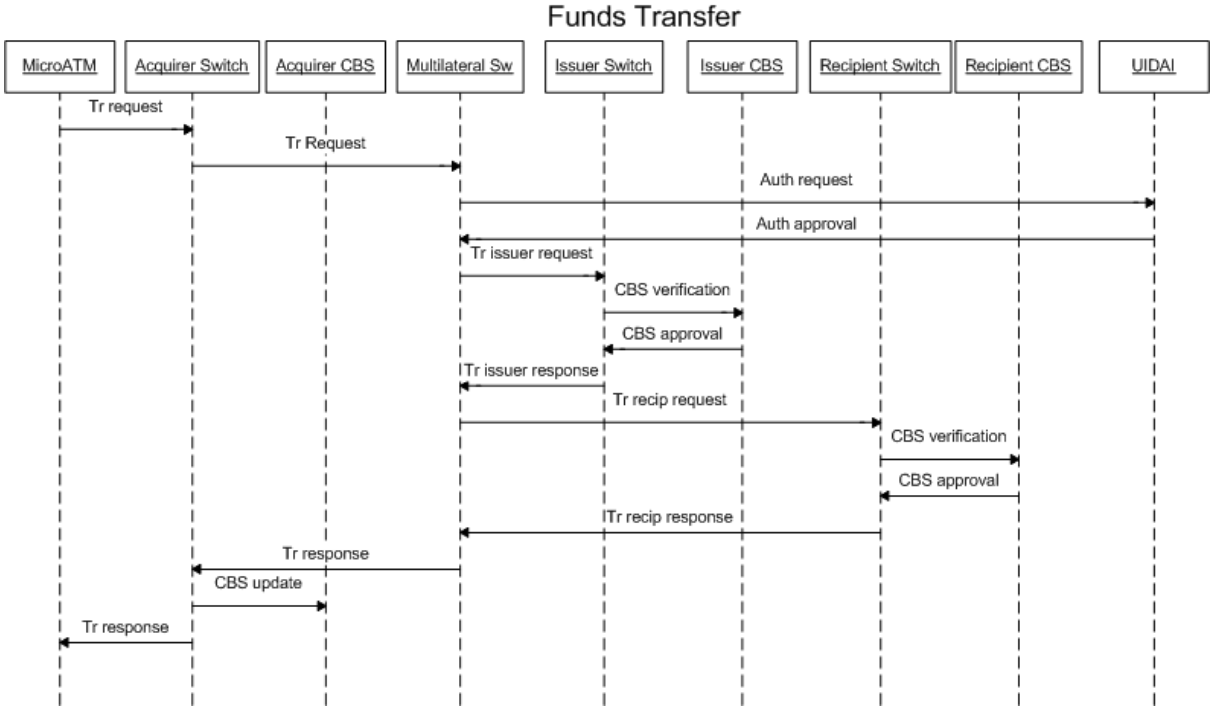


Figure 6: Sequence diagram for funds transfer

6 Biometric authentication best practices

In order to improve the reliability of authentication (16) for all residents, a two pronged approach is suggested:

1. Detect the resident's best fingers, which provide the best chances of successful authentication; and
2. Authenticate the resident using (up to) two of the best fingers.

6.1 Aadhaar number capture

The Aadhaar number is a 12 digit number, where the last digit is a check digit. Upon entry of the number, this check digit should be verified as described in the UID numbering scheme (11). The Aadhaar letter prints a 1d bar code for the Aadhaar number and/or a 2d QR code for the Aadhaar number and all the data on the letter. This data may be read electronically using a barcode scanner, in order to reduce the time for processing a transaction, and to reduce data entry errors.

6.2 Best finger detection (BFD)

The Best Finger(s) for a resident is the one that provides the best chance of successful authentication, when used for Aadhaar authentication. The best finger to be used for authentication depends on the intrinsic qualities of the finger (eg. ridge formation, wear and tear, cracks, etc.), as well as the quality of images captured during enrolment process and the authentication transaction.

Since many residents in India are engaged in manual labour, the quality of fingerprints vary considerably, even between fingers of the same resident. So it is important to identify the best finger(s) to improve authentication accuracy and hence be more inclusive in supporting Aadhaar authentication across all sections of society.

6.2.1 BFD API

A separate API (13) has been developed and should be deployed on the authentication device for the detection of the best finger. When BFD feature is implemented on an authentication device, residents can determine their best fingers, prior to authentication.

6.2.2 BFD implementation

All AUAs using fingerprint based Aadhaar authentication within their applications must implement BFD. A sample Java application is made available by UIDAI on the developer portal (https://developer.uidai.gov.in).

There are two scenarios under which BFD application needs to be used:

1. Authentication API (9) returns error code asking resident BFD to be carried out (error code “812”). Whenever this error occurs, the BFD process should be carried out.
2. If the resident specifically wants to get his/her best finger identified and get a BFD receipt, the BFD application should be proactively used. This may happen due to authentication errors even after initial BFD typically resulting from wear and tear of fingers, climatic conditions, etc. or due to the fact that resident may have re-enrolled and updated his/her biometrics in the Aadhaar system.

Recent studies have indicated that for most of residents, some fingers have higher chances of being best fingers as compared others. In view of the above findings, and in order to simplify the best finger detection process, a staged approach is suggested. This simplification saves time and effort for residents as well as operators.

The following section outlines the process of finger captures in order to determine the best finger(s).

1. Stage 1: Capture one finger at a time in the order specified in the BFD figure below. Ensure that the fingers are labelled correctly. As a best practice, the following order is suggested: Left middle, Left index, Left thumb, Right Thumb, Right index, Right middle fingers (refer figure below);
2. Stage 2: If best finger(s) is not detected in Stage 1, collect all 10 fingerprints. As a best practice following order is suggested: Left little, Left Ring, Left middle, Left index, Left thumb, Right Thumb, Right index, Right middle, Right ring and Right little fingers (refer figure below);
3. Once the best attempt is captured for all fingers, the application constructs the packet as per the BFD API specifications and invokes the BFD API through the AUA server (similar to authentication);
4. Based on the response, provide a printed receipt to the resident indicating the best fingers of the resident.

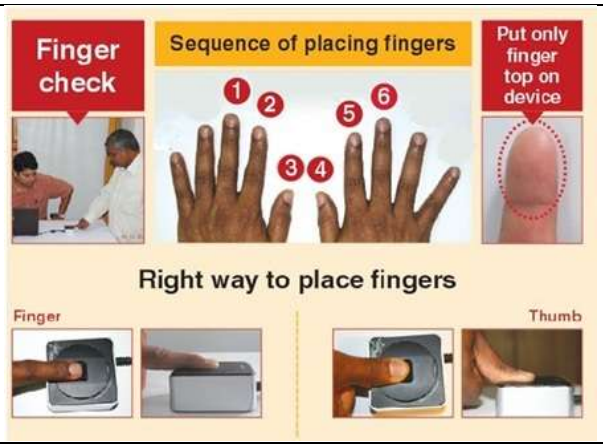


Figure: BFD Stage1 (1-6 fingers)

Figure: BFD Stage2 finger picture sequence

In case, best fingers are not detected even after providing all ten fingers, the resident can be directed to attempt the process again, or directed to take appropriate action as per the AUA's guidance.

The BFD server at UIDAI processes incoming requests to look for best fingers among incoming fingers. The best finger process is expected to indicate all good fingers apart from best finger(s) as well as indicate suggested actions in case no good fingers are found. The resident is expected to use his/her fingers in the order of rank for authentication.

The BFD Application must be able to distinguish between a finger that was not sent for BFD, and the finger which was found to be of poor quality.

1. Return code-"00"- Resident's two best fingers indicated with indicated with ranks 1 and 2. Other fingers that can also be used for authentication are ranked in ascending order. Fingers not ranked **cannot** be used for authentication.
2. Return code - "01"- Quality of enrolled fingers not good to achieve authentication. Resident can improve his chances by updating the biometrics through re-enrollment.
3. Return code - "03"- BFD capture quality was poor. The resident should retry BFD with an emphasis on capture quality.
4. Return code - "99"- Resident fingerprint quality is not good for authentication. Resident should be authenticated using other modalities.

BFD applications should display a message to enable both, the operator and the resident to take appropriate actions.

Authentication devices using biometric authentication implementing the BFD API should enable the following operator processes and software features:

1. Operator is expected to examine all ten fingers of the resident:
    a) In case the fingers are excessively dry, wipe with wet cloth;
    b) In case the fingers are excessively wet, wipe and dry; or
    c) In case the fingers are not clean (dust/oil/grease), the operator can request the resident to clean the fingers;
2. Resident/operator needs to clearly know which finger to capture and should be visible on screen;
3. There must be options to rescan after the capture is complete;
4. Capture high quality fingers in up to 3 attempts and pick the highest NFIQ image (if possible NFIQ 1 or 2);
5. Application should remember the finger position because it has to be sent along side NFIQ for every finger as part of BFD API input;
6. Application must have the capability for local matching to avoid the same finger from being sent in different positions and to also ensure same finger is indeed used during multiple attempts;
7. Application should send only templates and not images;
8. Provide for exception handling where the resident may not have all ten fingers. This can be achieved by providing a skip flag for every missing finger;
9. Application must not store any unencrypted data that involves resident information including biometrics;

10. The BFD application must provide a printed receipt UI indicating BFD output details preferably with a picture of the hand; and
11. Receipt needs to indicate rank as per response for each response and any action code/messages, if any.

6.3 Aadhaar authentication

After discovering the best finger(s), residents can use the best fingers for authentication using the Aadhaar authentication application. The proof of concept studies (16) showed that more residents can authenticate when two fingers are used, as compared to using a single finger.

6.3.1 Aadhaar authentication API

Authentication transactions should be conducted in accordance to the Aadhaar authentication policy and Aadhaar Authentication API Specification (9) published on UIDAI website, for biometric and non-biometric (eg. OTP (14), demographic, etc.) authentication methods.

6.3.2 Aadhaar authentication implementation

In accordance with the API, the authentication application on the MicroATM should have the capability to package the minutiae for a single finger or two fingers in the same transaction.

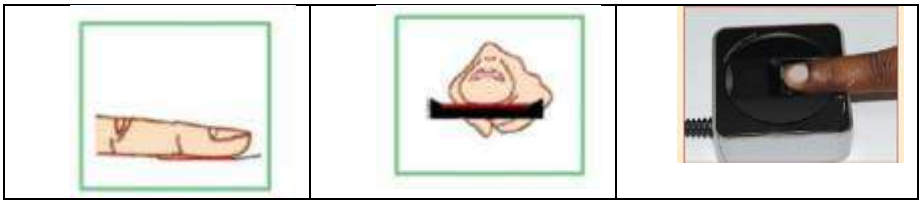
MicroATMs using biometric authentication implementing authentication API can benefit from the best known methods:

1. Operator is expected to examine fingers of the resident.
    a) In case the fingers are excessively dry, wipe with wet cloth;
    b) In case the fingers are excessively wet, wipe and dry; or
    c) In case the fingers are not clean (dust/oil/grease), the operator can request the resident to clean the fingers;
2. Quality checking software (NFIQ) can be implemented on the device helps measure quality of capture. Capture high quality fingers in up to 3 attempts and the application can use highest NFIQ image to enable more reliable authentication. (If possible, prefer NFIQ 1 or 2). NFIQ computation is expected to take more than 5 seconds on existing MicroATM implementations. Hence computing NFIQ is not mandatory and other means to provide quality feedback such as number of minutiae in the captured sample can be explored;
3. Improve authentication reliability by providing feedback regarding capture quality – submitting minutiae records with a very small number of minutiae points risks unsuccessful authentication. Headers of the ISO minutiae record provide information related to number of minutiae points. When less than 20 minutiae points are captured, the operator should capture once again in order to capture more minutiae points. Up to three capture attempts can be conducted in order to increase the minutiae points in the captured image;
4. During multiple attempts, a simplified two finger scheme can be implemented, which is detailed below. By retaining the last captured fingerprint minutiae in memory, the application can only request one best finger at a time from the resi-

dent, and form two finger authentication requests. A sample capture flow process is indicated below.

a) Capture 1: 1st best finger – single finger auth transaction;
b) If fail, Capture 2: 2nd best finger – two finger auth transaction (using capture 1 and 2)
c) If fail, Capture 3: 1st best finger – two finger auth transaction (using capture 2 and 3);
d) If fail, Capture 4: 2nd best finger – two finger auth transaction (using capture 3 and 4);
e) If fail: invoke exception handling process.

5. The application must not store any unencrypted data that includes resident information. Biometrics should never be stored in non-volatile storage;
6. The resident is expected to place the finger on the sensor platen as in the figure below. The resident should place the finger as straight as possible and should be able to apply mild pressure in order to enable good capture quality. The sensor must be mounted on the device in a manner that ensures good quality of capture in both, table top mode as well as handheld mode;



7. Devices can integrate the prompts on the screen (where picture display is possible) indicating the best ways to place fingers on the sensor to prompt the resident;
8. Training capsule should be provided on the device for operator training, as well as a sequence of images or videos to enable good fingerprint image capture;
9. Prompting the resident during fingerprint capture. The resident and operator benefit from prompting signals implemented on the device:
    a) Prompting can be achieved with a sound to signal starting time of capture;
    b) In case, option to light up sensors exists or providing lights around the sensor is possible, same can be considered; and
    c) Signaling end of capture to operator is important and helps during multiple captures; and
10. Authentication application must never attempt to alter either the minutiae or image record in any way to improve quality of capture.

7 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 authentication for payments, 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.

8 Bibliography

1. **RBI.** Financial Inclusion by Extension of Banking Services - Use of Business Correspondents (BC Interoperability). [Online] March 2012. http://rbidocs.rbi.org.in/rdocs/notification/PDFs/CCDBO020312.pdf.
2. —. Report of the Working Group on Securing Card Present Transaction. [Online] June 2011. http://www.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=634.
3. —. Revised Kisan Credit Card (KCC) Scheme. [Online] May 2012. http://rbidocs.rbi.org.in/rdocs/notification/PDFs/CRB5100512KC.pdf.
4. —. Mobile Banking transactions in India - Operative Guidelines for Banks - Technology and Security Standards. [Online] 2008. http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1660#ann1.
5. **MPFI.** *Interoperability Standards for Mobile Payments.* 2008.
6. **IBA, IDRBT.** Open Standards on Smart Card based solution for financial inclusion. [Online] 2010. http://www.idrbt.ac.in/news/openstandard.html.
7. **NPCI.** Procedural Guidelines for Aadhaar Enabled Payment System (Version 1.4). [Online] January 2011. http://www.npci.org.in/documents/Procedural_Guidelines.pdf.
8. —. Aadhaar Enabled Payment System Interface Specification (Version 3.0). [Online] June 2012. http://www.npci.org.in/documents/AEPS%20Interface%20Specification%20v3.0.pdf.
9. **UIDAI.** Aadhaar Authentication API Specifications (Version 1.6). [Online] April 2012. http://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_1_6.pdf.
10. —. From Exclusion to Inclusion with Micropayments. [Online] January 2010. http://uidai.gov.in/UID_PDF/Front_Page_Articles/Strategy/Exclusion_to_Inclusion_with_Micropayments.pdf.
11. —. UID Numbering Scheme. [Online] May 2010. http://uidai.gov.in/UID_PDF/Working_Papers/A_UID_Numbering_Scheme.pdf.
12. **STQC.** Biometric Devices Testing and Certification. [Online] 2012. http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification.
13. **UIDAI.** Aadhaar Best Finger Detection API (Version 1.6). [Online] February 2012. http://uidai.gov.in/images/FrontPageUpdates/aadhaar_bfd_api_1_6.pdf.
14. —. Aadhaar OTP Request API (Version 1.5). [Online] February 2012. http://uidai.gov.in/images/FrontPageUpdates/aadhaar_otp_request_api_1_5.pdf.
15. —. Aadhaar Mobile Number Update API (Version 1.0). [Online] June 2012.
16. —. Role of Biometric Technology in Aadhaar Authentication - Detailed Report. [Online] http://uidai.gov.in/images/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf.
17. —. Biometric Design Standards for UID Applications (version 1.0). [Online] December 2009. http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf.
18. **RBI.** *Report of the RBI working group on regulatory issues.* 2010.
19. —. *Report of the RBI appointed working group on issues/implications related to cash.* 2010.

9 Annexure I: Terms of Reference

भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

www.rbi.org.in

DBOD.BL.No. 12497 /22.01.001/2009-10 January 15, 2010

The Director General
Unique Identification Authority of India
Planning Commission
Government of India
3rd floor, Tower II
Jeevan Bharti Building, Connaught Circus
New Delhi 110 001

Dear Sir,

Unique Identification Number (UID) and Unique Identification Number Enabled Bank Accounts (UEBA) – Presentation by Unique Identification Authority of India at Reserve Bank of India on December 11, 2009

We forward herewith a copy of the gist of presentation and the discussions held on December 11, 2009 at Reserve Bank of India, Central Office, Mumbai, based on the presentation made by the Chairman, UIDAI, for your information and record.

Yours faithfully,

(Sonali Sen Gupta)
Deputy General Manager
Encl: As above

Department of Banking Operations and Development, Central Office, Centre 1, Cuffe Parade, Colaba, Mumbai - 400005
टेलिफोन /Tel No: 91-22-22189131 - 39 फैक्स/Fax No: 91-22-22150663 Email ID: cgmicdbodco@rbi.org.in
हिन्दी आसान है, इसका प्रयोग बढ़ाइये।

Annex

Details of the UIDAI Presentation

About the UIDAI and the UID

- The UIDAI was set up in February, 2009 and is attached to the Planning Commission.
- The UIDAI's purview would be limited to issue of unique identification number (UID) linked to a person's demographics through Know Your Resident (KYR) standards and bio-metric information. UID would only be proof of identity and does not confer/affirm citizenship.
- The KYR standard of UIDAI would primarily comprise name, date of birth, gender, residential address, parent/guardian's name with UID (in case of minors) and contact details such as mobile or email particulars.
- The UIDAI will be the regulatory authority for managing a Central ID Data Repository (CIDR), which will issue UID numbers, update resident information and authenticate the identity of residents, whenever required.

The need for UID-Enabled Bank Accounts (UEBA) and micro-transaction system

- The poor face problems of proving their identity through documentations as required under the current KYC regime for access to banking facilities. This impedes access to online and mobile banking for delivery of banking services to this section of society, which faces a lot of difficulties in availing of the benefits of Government sponsored social welfare schemes such as NREGA, SSA, JSY, IAY, Pension, PDS etc.
- Besides, the poor prefer to withdraw small amounts for their day-to-day expenses and these micro-payments are not attractive to bankers due to high transaction costs. (Banks bear an estimated cost of Rs.100/- for acquiring a 'No-Frill' account customer; Rs.40/- for each teller transaction and Rs.10/- for each ATM transaction).
- The UID aims to address the three pronged problems in providing banking services to the poor i.e. access, identity and non-attractive nature of micro-payments by linking the UID number to a designated bank account (changeable, if desired) and facilitating electronic small/micro- transactions, remotely and at low cost through a combination of network of business correspondents and mobile telephones.

- The UID number facilitates interoperability with a global network address (like an email-ID or mobile number) for the number holder and hence, the person could access banking facilities across banks, business correspondents and mobile service providers (accessing anywhere/any time banking on the analogy of inter-bank ATM facility as available now). This would not limit operation of the account locally and significantly help the poor on the move in search of livelihood like the migrant labourers.
- The biometric authentication system combined with KYR standards of UIDAI is expected to replace the KYC requirements for opening of bank accounts. Banks could verify customer both in person and online through the biometric process.

UEBA and UID-enabled micro-transaction system – Operational Features

- The UID will be linked to a bank account as designated by the UID holder and such bank accounts would be known as UID Enabled Bank Accounts (UEBA).
- There would be a National Electronic Settlement Network Platform enabled NPCI, which who would host a Real Time Micro Transaction (REMIT) switch for processing of all UIDAI related micro transactions from banks.
- Banks will set up a BC network of their own with a micro-ATM network (a simple device with a mobile phone, biometric reader and a printer) for processing transactions at BC level.
- The UID holder may approach any BC in his locality for deposit, withdrawal, payment, remittance, electronic transfer of funds and balance enquiry by submitting his fingerprints to the micro-ATM. The transaction information is transmitted to the BC's banker through the micro-ATM.
- The transactions would flow through a messaging system from BC to its banker, who would, ensure the genuineness of the flow of message. The bank would then seek confirmation of UID authentication from REMIT and the REMIT would, in turn, obtain the authentication from UIDAI as well as the bank account number and mobile particulars of the UID holder from the ID-Mapper of UIDAI. REMIT then would allow the requested transaction by crediting the account of the BC by debit to the account of the customer (in case of a withdrawal/payment transaction by the customer). SMS notification in confirmation of the transaction is sent to BC and resident by REMIT

DG clarified that there were no restrictions on banks in providing extending banking services in rural areas.

7. Complementing the UIDAI on its presentation, DG(UT) observed that urgent steps need to be taken to resolve the issues raised by bankers to facilitate speedy implementation of the UIDAI's proposal. DG further observed that the issues relate to four broad areas viz. Regulation, Technology, Connectivity and Cash. DG suggested that four working groups may be constituted to address the issues in the concerned areas. She also suggested that the composition of the groups and the illustrative list of issues that they could look into may be as under:

(a) Working Group on Regulatory issues

i) This group may be chaired and convened by Shri P.Vijaya Bhaskar, CGM-in-Charge, DBOD, RBI and have representatives from IBA and a few banks.

ii) The group may look into all regulatory issues in the context of the UID/UEBA model, including

- passbooks issuance
- handling government businesses
- KYC
- whether aggregators/distributors currently used by telecom companies can also be engaged by banks as aggregators under BC model
- Interest rate ceilings, if considered as priority sector.

(b) Working Group on Technology issues

i) This group may be chaired and convened by Shri M.V.Nair, CMD, Union Bank of India and Chairman, IBA and have representatives from IDRBT, NPCI. a few banks and RBI (DIT and DPSS) and UIDAI.

ii) The group may look into all technology issues including specifying parameters for micro-ATMs and coordinate with the UIDAI.

(c) Working Group on connectivity issues

i) This group to be chaired and convened by NPCI and may comprise representatives from NPCI, IDBRT, IBA and RBI (DIT and DPSS)

ii) The group may look into all issues relating to connectivity including central infrastructure, settlement network platform etc.

(d) Working Group on issues/implications relating to cash

i) This group may be chaired and convened by CGM, DCM and comprise representatives from a few banks.

ii) The group may look into all issues connected with cash requirement/ movement/storing etc. under the proposed system.

iii) The group could invite organisations like Little World and FINO for sharing their experiences.

8. The meeting ended with Chairman, UIDAI seeking support from all stakeholders in implementing the proposed solution. The bankers, IBA, NPCI and IDRBT assured their cooperation and support in implementation.

***

List of participants

UIDAI

1. Shri Nandan Nilekani, Chairman
2. Shri R.S. Sharma, Director General
3. Shri Shankar Maruwada
4. Shri Veeral Shah

RBI

5. Smt. Usha Thorat, Deputy Governor
6. Dr. K.C.Chakrabarty, Deputy Governor
7. Dr. S.V.Gokarn, Deputy Governor
8. Shri Anand Sinha, Executive Director,
9. Shri. G.Góplalakrishna, Executive Director
10. Dr. Pedgaonkar, Advisor, DSIM
11. Shri. S.Karupaswamy, CGM-in-C, DBS
12. Shri P. Vijay Bhaskar, CGM-in-C, DBOD
13. Shri B.Mahapatra, CGM, DBOD
14. Dr. Deepali Pant Joshi, CGM, RPCD
15. Shri Sivaraman, GM, DPSS
16. Shri K. Raghavendra, DGM, DNBS
17. Shri P.K. Das, DGM, DBOD
18. Shri S.Shankar, EA to DG(UT)

IBA and banks

19. Shri M.V.Nair, Chairman, IBA and CMD, Union Bank of India
20. Shri K.Ramakrishnan, CEO, IBA
21. Shri O.P. Bhatt, Chairman, SBI
22. Shri K.R.Kamath, CMD, PNB
23. Shri K.V.Kamath, Chairman, ICICI Bank Ltd
24. Ms. Chanda Kochhar, MD, ICICI Bank Ltd
25. Shri Aditya Puri, MD, HDFC Bank Ltd.
26. Shri J.M.Garg, CMD, Corporation Bank
27. Shri M.D.Mallaya, CMD, Bank of Baroda
28. Shri Aloke Misra, CMD, Bank of India
29. Shri S.Sridhar, CMD, Central Bank of India
30. Shri D.L.Rawal, CMD, Dena Bank
31. Shri R.S.Reddy, CMD, Andhra Bank
32. Shri M.S.Sunderarjan, CMD, Indian Bank
33. Shri O.V. Bundellu, DMD, IDBI
34. Shri Jagdish K L Pai, ED, Canara Bank

NABARD

35. Shri U.C.Sarangi, Chairman

NPCI

36. Shri A.P.Hota, CEO

IDRBT

37. Shri. Sambamurthy, Chairman

Department of Post

38. Shri Ashok Pal Singh, Dy. Director General

10 Annexure II: Key milestones

	Date	Milestone
1	Mar 19, 2010	Presentation on MicroATM and BC interoperability to Governor, RBI
2	Sep 15, 2010	Demonstration to Chairman, UIDAI and NASSCOM
3	Sep 25, 2010	Demonstration to IBA Working Group
4	Sep 29, 2010	Aadhaar formally launched at Nandurbar, Maharashtra
5	Oct 1, 2010	Demonstration to Governor RBI, along with Bank CMDs, UIDAI, NPCI, IDRBT
6	Oct 6, 2010	Demonstration to Department of Financial Services, Ministry of Finance
7	Oct 8, 2010	Demonstration to State Government officials from five States
8	Jan 11, 2011	RBI approval on AEPS Procedural Guidelines for pilot
9	Jan 21, 2011	Launch of field PoC in Jharkhand based on MicroATM Standards (version 1.3)
10	Nov 8, 2011	NPCI-UIDAI Authentication Service Agency agreement signed
11	Nov 22, 2011	UIDAI-AEPS integrated on NPCINet based on MicroATM Standards (version 1.4)
12	Dec 24, 2011	Bank of India launches production operations on pilot basis in Jharkhand
13	Dec 28, 2011	ICICI Bank launches production operations on pilot basis in Jharkhand
14	Dec 30, 2011	Union Bank of India launches production operations on pilot basis in Jharkhand
15	Jun 22, 2012	Demonstration to Parliamentary Standing Committee on Finance
16	Mar 2, 2012	RBI released guidelines for BC interoperability
17	Mar 16, 2012	Hon'ble Finance Minister announced the roll-out of Aadhaar based payments in 50 districts
18	Mar 23, 2012	Demonstration at RBI DPSS Annual Payments Conclave in Shillong, Meghalaya as a part of the Financial Inclusion outreach program "Look North East"
19	Apr 16, 2012	NABARD workshop for on-boarding of Regional Rural Banks (RRBs) on AEPS platform in Jharkhand
20	Jul 12, 2012	Dr. D. Subbarao, Governor, Reserve Bank of India, launched Aadhaar enabled Kisan Credit Card (KCC)
21	Aug 1, 2012	An additional twelve banks are in the process of AEPS integration

11 Annexure III: Proforma for MicroATM vendors

MicroATMs may be all-in-one integrated devices, or mobiles / PCs / tablets with accessories. Banks procuring microATMs may choose to award higher technical scores for particular form factors, or optional features, which meet their own business requirements. Banks may request vendors to supply the following proforma for MicroATMs being deployed.

11.1 Proforma format

The proforma format is provided on the next page.

Dated:

Dear Sir/Madam,

The device being submitted is fully compliant with MicroATM Standards version 1.5.1. The proofs of necessary certifications are attached with this letter.

Device

Make	List Device name
Model	List Device model number

Hardware

Component	Description
Biometric scanner	List make of scanner
Connectivity	List all channels available (Single/Dual SIM GPRS, CDMA, PSTN, Ethernet, Wifi, etc)
Non-volatile storage	List storage capacity
Display	List size of display
Printer	List whether thermal / impact
Battery	List whether battery is rechargeable, battery life in hours
Power Adaptor	Meets standards: Yes / No
Environment	Meets standards: Yes / No
Magstripe reader and PIN pad	Meets standards: Yes / No
Speaker	Meets standards: Yes / No
Location	Meets standards: Yes / No

Proofs of certification (Attached)

1. STQC certification of Scanner+Extractor meeting UIDAI standards
2. PCI-PED compliant PIN pad

Yours sincerely,

(Authorized signatory)