|  |
| --- |
|  |
| |  | | --- | |  | |  | |



**API SERVICE SPECIFATION**

**For**

**Aadhaar Pay**

**Version 3.7**

Contents

[1. Service: Login 4](#_Toc493166016)

[1.1. Prerequisites 4](#_Toc493166017)

[1.2. Description 4](#_Toc493166018)

[1.3. Request Parameter 4](#_Toc493166019)

[1.4. Request URL 4](#_Toc493166020)

[1.5. Request JSON 5](#_Toc493166021)

[1.6. Response JSON 5](#_Toc493166022)

[1.6.1. Success Response 5](#_Toc493166023)

[1.6.2. Failure Response 5](#_Toc493166024)

[1.7. Response Code & Error Message 5](#_Toc493166025)

[1.8. Response Parameters 5](#_Toc493166026)

[2. Service: AEPS TRANSACTION 6](#_Toc493166027)

[2.1. Prerequisites 6](#_Toc493166028)

[2.2. Description 6](#_Toc493166029)

[2.3. Request Parameter 6](#_Toc493166030)

[2.4. Request JSON 6](#_Toc493166031)

[2.4.1. Normal Request 6](#_Toc493166032)

[2.5. Response JSON 7](#_Toc493166033)

[2.5.1. Response received from Switch 7](#_Toc493166034)

[2.5.2. Response not received from Switch 7](#_Toc493166035)

[2.5.3. General Failure Response 7](#_Toc493166036)

[3. Service: Change Password 7](#_Toc493166038)

[3.1. Request JSON 7](#_Toc493166039)

[3.2. Response JSON 7](#_Toc493166040)

[4. Service: GET LAST TRANSACTION STATUS FROM SERVER ( REQUERY ) 7](#_Toc493166041)

[4.1. Prerequisites 8](#_Toc493166042)

[4.2. Description 8](#_Toc493166043)

[4.3. Request Parameter 8](#_Toc493166044)

[4.4. Request JSON 8](#_Toc493166045)

[4.5. Response JSON (SUCCESS) 8](#_Toc493166046)

[4.6. Response JSON (FAILURE) 9](#_Toc493166047)

[4.7. Response Parameters 9](#_Toc493166048)

# **Service: Login**

## Prerequisites

1. CSR should be created in mATM FI server Application.

2. Device to be used for transaction should be mapped with CSR.

## Description

This service is used by the CSR/PSM to login in mATM FI Tablet application. Response against the request gives the login SUCCESS/FAILURE result along with a freshness factor and the deviceId(provided by Bank to device while device creation). This freshness factor needs to be sent in next request and the same will be validated on the server.

## Request Parameter

1. terminalId:-

a. Device IMEI no Which is allocated to the CSR

2. freshnessFactor:-

a. Any Dummy value, as it is a login request

3. transType:-

a. Should be 106 for CSR/PSM login.

4. csrId:-

a. CSR/PSM ID

5. requestId: - Unique Id for request

6. resentCount:-1 (not in use)

7. deviceId:- Should be any value, can be empty value also.

8. txnTime:-

a. Request Time Stamp

9. Object:-

a. This object will contain the actual object of CSR login request.

i. csrId

ii. csrPassword (should be SHA1 hash of the entered password)

10. version:-

a. Current version of Tablet Application which is mapped in the mATM FI server

application.

## Request URL

<https://apideveloper.rblbank.com/test/sb/rbl/api/v1/Aadharpay>

## Request JSON

{"terminalId":"358296058007586","freshnessFactor":"-677290134806767521","transType":"106","csrId":"10001","requestId":"1","resentCount":1,"deviceId":"UP000102","txnTime":"Jul 23, 2015 4:20:54 PM","object":{"csrPassword":"hug","csrId":"10001"},"version":"1.2.8.1"}

## Response JSON

### Success Response

{"object":{"userType":"CSR","branchCode":"0169","deviceId":"Rblbank1","csrId":"10001","csrName":"Ratnakar Bank","invalidAttemptsCount":5,"loggingCsrGanasevaId":"002640","bcBranchCode":"NOC001","minimumCustomerLimit":4,"maximumCustomerLimit":6,"acquirerInstitutionId":"123457"},"responseCode":"00","responseMessage":"SUCCESS","requestId":"1","nextFreshnessFactor":"-2554965009285302613"}

### Failure Response

{"responseCode":"01","responseMessage":"FAILURE","requestId":"1","nextFreshnessFactor":"6084282440085020522"}

## Response Code & Error Message

SUCCESS: 00

FAILURE: 01

## Response Parameters

csrName – Full Name of logging CSR/PSM

userType – CSR/PSM

deviceId – Device code mapped to the device on mATM FI server

invalidAttemptsCount – No. of times CSR/PSM can login into mATM FI tablet application in case the tablet is out of network

loggingCsrGanasevaId – Ganaseva Id of the logging CSR/PSM

bcBranchCode – BC branch code, only in case logginguser type is CSR

minimumCustomerLimit – Minumum number of customer the CSR can create in a group, only in case logginguser type is CSR

maximumCustomerLimit - Maximum number of customer the CSR can create in a group, only in case logginguser type is CSR

acquirerInstitutionId – To be used in the ISO message and set at the mATM FI server.

# **Service: AadhaarPay TRANSACTION**

## Prerequisites

Requester should have a valid freshness factor (Received in the Login response).

## Description

This service is used to send Transaction request from tablet to mATM FI Server. FI server converts ISO8583 messages from tablet to desired format of ISO8583 for switch. Gets result from switch and converts the same in tablet application understandable format.

## Request Parameter

1. terminalId :-

a. Device IMEI no Which is allocated to the CSR

2. freshnessFactor :-

a. Freshness Factor received in the last request

3. transType :-

a. Should be 133 for AEPS Normal/Reversal Transaction.

4. csrId:-

a. CSR ID

5. requestId: - Unique Id for request

6. resentCount:-1 (not in use)

7. deviceId :- Device Code received as a part of login response.

8. txnTime:-

a. Request Time Stamp

9. Object :-

a. This object will contain the actual AEPS/ Reversal request.

i. isVoidTxn :- for normal Request false and for reversal request true

ii. iso8583Message :- Desired ISO8583 Message bytes for AEPS Normal/Reversal Transaction.

10. version :- Current version of Tablet Application which is mapped in the mATM FI server application

## Request JSON

### Normal Request

{"terminalId":"358296058007586","freshnessFactor":"393312380776036007","transType":"133","csrId":"10001","requestId":"1","resentCount":1,"deviceId":"UP000102","txnTime":"Jul 23, 2015 4:20:54 PM", "object":{" isVoidTxn ":false, "iso8583Message": "ISO\_MESSAGE\_BYTES\_FROM\_DEVICE"},"version":"1.2.8.1"}

## Response JSON

### Response received from Switch

{"responseCode":"00","responseMessage":"SUCCESS","requestId":"1","nextFreshnessFactor":"7888354794172966130","object":{"isVoidTxn":false, "isoMessage":"ISO\_MESAGE\_BYTES\_FROM\_SWITCH"}}

### Response not received from Switch

{"responseCode":"00","responseMessage":"SUCCESS","requestId":"1","nextFreshnessFactor":"7888354794172966130","object":{"isVoidTxn":false, "isoMessage":"SERVER\_GENERATED\_ISO\_MESAGE\_BYTES\_FOR\_DECLINE\_OR\_DISPUTE"}}

### General Failure Response

{"responseCode":"REPONSE\_CODE","responseMessage":"FAILURE\_MESSAGE","requestId":"1","nextFreshnessFactor":"7888354794172966130"}, where REPONSE\_CODE represents error occurred on server while processing the transaction.

# **Service: Change Password**

## Request JSON

{"terminalId":"358296058007164","freshnessFactor":"-2883698369162028451","transType":"133","csrId":"10001","requestId":"1","resentCount":1,"deviceId":"scl09822","txnTime":"Jul 23, 2015 4:20:54 PM","object":{"csrId":"23456","currentPassword":"abnsd56787asdhnxnkss766","newPassword":"asdbjkabsd347nnbsa233"}}

## Response JSON

{"responseCode":"00","responseMessage":"SUCCESS","requestId":"1","nextFreshnessFactor":"2693193920048386241"}

# **Service: GET LAST TRANSACTION STATUS FROM SERVER ( REQUERY )**

## Prerequisites

Requester should have a valid freshness factor (Received in the Login response).

## Description

This service is used to get the transaction status from the mATM server based on the STAN, Device Code and Transaction Time for the transaction.

## Request Parameter

1. terminalId :-

a. Device IMEI no Which is allocated to the CSR

2. freshnessFactor :-

a. Freshness Factor received in the last request

3. transType :-

a. Should be 135

4. csrId:-

a. CSR ID

5. requestId: - Unique Id for request

6. resentCount:-1 (not in use)

7. deviceId :- Device Code received as a part of login response.

8. txnTime:-

a. Request Time Stamp

9. Object:- This object will contain required parameters for OTP generation

a. originalTransactionStan – STAN of the original transaction

b. originalTransactionDeviceCode – Device Code used for the transaction (Field 41 of original ISO message)

c. originalTrnsactionTime – Date on which transaction initiated from device (Field 13 of original ISO message)

10. version:- Current version of Tablet Application which is mapped in the mATM FI server application.

## Request JSON

{"terminalId":"358296058007164","freshnessFactor":"-742114578919231493","transType":"135","csrId":"10001","requestId":"1","resentCount":1,"deviceId":"scl09822", "channel":"123","txnTime":"Jul 23, 2015 4:20:54 PM","object":{"originalTransactionStan":"000017","originalTransactionDeviceCode":"hradesh1","originalTrnsactionTime":"0806"},"version":"1.2.8.1"}

## Response JSON (SUCCESS)

{"object":{"transactionStatus":"00","rrn":"12345"},"responseCode":"00","responseMessage":"SUCCESS","requestId":"1","nextFreshnessFactor":"5017858902482996073"}

## Response JSON (FAILURE)

{"responseCode":"1258","responseMessage":"Original Device Id not provided", "requestId":"1","nextFreshnessFactor":"-9172936972347280850"}

## Response Parameters

1. Object for the response.

a. transactionStatus – Status of transaction available on the server

b. rrn – RRN of the transaction

2. responseCode – Response for the transaction processing on server

3. nextFreshnessFactor – Freshness factor generated by server to be sent by the client application in next request

4. requested:- Request Id received in the request

5. responseMessage:- Message for the response code