API SERVICE SPECIFATION
For
Aadhaar Enabled Payment System

Registered Device

Version: 3.8 –Updated

Document Version History:

Version	Change of Description	Created Date	Created By
3.8	Channel ID mandatory	20th Dec 2018	Deepak Yadav

Table of Contents

1. Service: Login

1.1 Prerequisites

1. CSR should be created in mATM FI server Application.
2. Device to be used for transaction should be mapped with CSR.

1.2 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.

1.3 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 - BCAgentID
5. **requestId**: - Unique Id for request
6. **resentCount**:-1 (not in use)
7. **deviceId** :- Should be any value, can be empty value also. – DEVICECODE
8. **Channel**: Channel code to be used for request validation (Mandatory)
9. **txnTime**:-
a. Request Time Stamp
10. **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)

11. **version** :- 1.2.8.1 – current version
a. Current version of Tablet Application which is mapped in the mATM FI server application.

1.4 Request URL

https://apideveloper.rblbank.com/test/sb/v1/rbl/api/aeps/transact

1.5 Request JSON

{"terminalId":"358296058119183","freshnessFactor":"-677290134806767521","transType":"106","csrId":"85000","requestId":"1","resentCount":1,"deviceId":"UP000102",”channel”:”123”,"txnTime":"Jul 23, 2015 4:20:54 PM","object":{"csrPassword":"40bd001563085fc35165329ea1ff5c5ecbdbbeef","csrId":"85000"},"version":"1.2.8.1"}

1.6 Response JSON

1.6.1 Success Response

{"object":{"userType":"CSR","branchCode":"0170","deviceId":"UP000102","csrId":"85000","csrName":"Mr. Asutosh Padhi","invalidAttemptsCount":5,"loggingCsrGanasevaId":"AO00609-D.Karnan","bcBranchCode":"4004","minimumCustomerLimit":1,"maximumCustomerLimit":9,"acquirerInstitutionId":"123456"},"responseCode":"00","responseMessage":"SUCCESS","requestId":"1","nextFreshnessFactor":"2730956799049947638"}

1.6.2 Failure Response

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

1.7 Response Code & Error Message

SUCCESS: 00
FAILURE: 01

1.8 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 logging user 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.

2. Service: AEPS TRANSACTION

2.1 Prerequisites

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

2.2 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.

2.3 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. channel : Channel code to be used for request validation.(Mandatory)
9. txnTime:-
a. Request Time Stamp
10. 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.
11. version :- Current version of Tablet Application which is mapped in the mATM FI server application.

2.4 Request JSON:

2.4.1 Normal Request

{"terminalId":"358296058007586","freshnessFactor":"393312380776036007","transType":"133","csrId":"85000","requestId":"1","resentCount":1,"deviceId":"UP000102",”channel”:”123”,"txnTime":"Jul 23, 2015 4:20:54 PM", "object":{" isVoidTxn ":false, "iso8583Message": "ISO_MESSAGE_BYTES_FROM_TABLET"},"version":"1.2.8.1"}

2.4.2 Reversal Request

{"terminalId":"358296058007586","freshnessFactor":"393312380776036007","transType":"133","csrId":"85000","requestId":"1","resentCount":1,"deviceId":"UP000102",”channel”:”123”,"txnTime":"Jul 23, 2015 4:20:54 PM","object":{"isVoidTxn":true, "iso8583Message": "ISO_MESSAGE_BYTES_FROM_TABLET"},"version":"1.2.8.1"}

2.5 Response JSON:

2.5.1 Response received from Switch

{"responseCode":"00","responseMessage":"SUCCESS","requestId":"1","nextFreshnessFactor":"7888354794172966130","object":{"isVoidTxn":false, "isoMessage":"ISO_MESAGE_BYTES_FROM_SWITCH"}}

2.5.2 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"}}

2.5.3 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.

2.5.4 Failure Response code

DD : Reasons of **DD**(Declined txn)
1. Network issue
2. Device not mapped @ RBL switch
3. RBL switch down

DS : Reason of **DS**(Disputed Txn)
1. No response from switch

NOTE: Also, DD will come in case of Successful Reversal and DS will come in case of Failure Reversal.

3. Service: Change Password

3.1 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"}}

3.2 Response JSON:

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

4 Service: GET LAST TRANSACTION STATUS FROM SERVER (REQUERY)

4.1 Prerequisites

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

4.2 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.

4.3 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. Channel :- Channel Code to be used for request validation(Mandatory)
9. txnTime:-
a. Request Time Stamp
10. 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)

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

4.4 Request JSON

{"terminalId":"358296058119183","freshnessFactor":"3249082878767928747","transType":"135","csrId":"85000","requestId":"1","resentCount":1,"deviceId":"UP000102",”channel”:”123”,"txnTime":"Jul 23, 2015 4:20:54
PM","object":{"originalTransactionStan":"000017","originalTransactionDeviceCode":"UP000102","originalTrnsactionTime":"0806"},"version":"1.2.7.2"}

4.5 Response JSON (SUCCESS)

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

4.6 Response JSON (FAILURE)

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

4.7 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

**** Note-**

1. For PID block creation Protobuf encryption is required. As data size is large in case of AEPS, XML encryption will not work.
2. License key will expire in production in every 1 year and in every 3 months in UAT, so please keep this configurable.
3. Apart from License key, UIDAI public certificate and Application version also needs to be configurable as this is also valid till some specific time period.
4. For Reversal Request "ISOVOIDTXN" should be true.
5. In Login You can pass any value in the Freshness Factor, Post success login you will get correct Freshness Factor value.
6. For ISO message please refer the ISO message Specs doc.
7. Password of the agent should be passing in Sha1 Hash encryption in the login API.
8. There is one to one mapping between CSR Agent, Device code and IMEI no (terminal id) to Device code.
9. In case register device the following values such as mc ,rdsid, rdsver, hmac,udc,dc,mi,bav, session key, ID …etc will be generated from device directly. please check the UIDAI website for sample codes for encryption for PID block, session key and HMAC.
10. Please decode the encoded HMAC, Session Key, PID directly generated from registered device and pass in hexadecimal format in the ISO message