OTPEKyc API GATEWAY DOC

Ujjivan Small Finance Bank Limited
Grape Garden, No.27, 3rd A Cross, 18th Main, 6th Block, Koramangala, Bengaluru – 560 095

Table of Contents

1. INTRODUCTION

1.1 Design Document Purpose

The purpose of this document is to provide a detailed specification of the **OTPEKyc** in sufficient depth to:

- Enable the component to be built and tested.
- Ensure that it can be enhanced, supported and maintained by other areas of the organization after initial implementation.

1.2 Design Reviews

The service design will be reviewed within Middleware team and security testing team as needed. Once finalized, design resource will provide an overview to other teams such as front end application development team and various project resources.

2. API CONNECT COMPONENTS

- API Connect is used to expose the service to front end applications.
- Within API Connect, there are multiple Products. The **OTPEKyc** API is exposed within **OTPEKyc Product .**
- Service Consumers must subscribe to the API. A unique application Identification (client-id) and a secret will be generated.
- The assigned Client-id must be supplied in the header for each API.
- URLs for invoking the services can be found in API Connect Developer portal and also mentioned in the below section.

3. STEPS TO ACCESS & SUBSCRIBE IN PORTAL

Refer Subscription User manual shared during initial on board.

4. API AUTHENTICATION

JWT Access token to be passed in JSON wrapper as string value in “JWTokenValue” field. The Token can be generated by subscribing to **TOKEN API**.

4.1 TOKEN API

- **Overview:** To retrieve access token.
- **Request Type**: GET
- **Mandatory HTTP Headers**:
  - X-IBM-Client-Id: xxxxxxxxxxxxxx
  - X-IBM-Client-Secret: xxxxxxxxxxxxxxxx
- **SIT URL**: https://apiuat.ujjivansfb.in/ujjivan/development/v1/tokens

5. API INTERNAL DESIGN

- **Overview:**

  Service is designed to send OTP to users mobile or Email. The API Gateway makes a backend **FinaKyc KUA Server.**

- **Request Type**: POST

- **API URL**:
  UAT : https://apiuat.ujjivansfb.in/ujjivan/development/v2/KUAServer/otp
  PROD : https://api.ujjivansfb.in/ujjivan/development/v1/KUAServer/otp

- **Mandatory HTTP Headers**:
  - X-IBM-Client-Id: xxxxxxxxxxxxxxx

- **Accept**: application/json

- **Content-type**: application/json

- **REQUEST PAYLOAD:**

At API Gateway the request has to be passed as JSON wrapper. The sample payload is as below,

```
{
"RequestEncryptedValue": "",
"TransactionId": "",
"JWTokenValue": ""
}
```

The individual fields of the Standard JSON Request Payload are described below-

- **RequestEncryptedValue** : This will contain the encrypted value of original REST-JSON request sample.
- **TransactionId** : External partners need to set a transaction ID to uniquely identify every request, in order to retrieve it from an audit trail at a later date.
- **JWTokenValue** : This value can be obtained by invoking Bank's token generator service.

(For more details on request encryption Refer UjjivanSFB_API_Integration_TechnicalProcess_document)

- **Actual REST-JSON Input Parameter:**

Element Name	M/ O/C	Data Type	Description
Uid	M	String	Aadhaar number of the customer (size 12) or Virtual Id (size 16) of the customer or AUA specific uidtoken (size 72)
securityToken	M	String	A unique security token to be used.
clientId	M	String	Registered client id from our database client table
Channel	M	String	Specify which channel (mobile or email) you want OTP to be sent. 01 - Mobile, 02- Email, 00- Both mobile and Email. If you don't pass anything, default is 01.

- **Output Parameters:**
- **For OTPEKYC,** the response will be actual JSON.

Element Name	M/O/C	Data Type	Description
TransactionId	M	String	Transaction Id
Status	M	String	Y or N
Xml	O/M	String	
Details	M	String	Success or Failed
OtpInfo	M	String	Info contains the mobile num to which otp is sent with last four digit and rest masked.
UIDAITxn	M	String	
ErrorCode	O/M	String	Incase of an error, error code will be populated else it is empty string.

- **Error Handling**

HTTP Status Code	HTTP Message	More Information
401	Unauthorized	Access token missing or validation
400	Bad Request	The parameters are invalid or missing.
503	Service Unavailable	The parameters were valid but the request failed.
200	Success	

6. ERROR CODES IN Finahub(Backend):

ErrorCode – Failure error code This attribute provides any of the following codes

o “110” – Aadhaar number does not have verified mobile/email
o “111” – Aadhaar number does not have verified mobile
o “112” – Aadhaar number does not have both email and mobile.
o “510” – Invalid “Otp” XML format o “520” – Invalid device
o “530” – Invalid AUA code
o “540” – Invalid OTP XML version
o “542” – AUA not authorized for ASA. This error will be returned if AUA and ASA do not have linking in the portal
o “543” – Sub-AUA not associated with “AUA”. This error will be returned if Sub-AUA specified in “sa” attribute is not added as “Sub-AUA” in portal
o “565” – AUA License key has expired or is invalid
o “566” – ASA license key has expired or is invalid
o “569” – Digital signature verification failed

- o “570” – Invalid key info in digital signature (this means that certificate used for signing the OTP request is not valid – it is either expired, or does not belong to the AUA or is not created by a CA)
- o “940” – Unauthorized ASA channel
- o “941” – Unspecified ASA channel
- o “950” – Could not generate and/or send OTP
- o “999” – Unknown error

----------**END OF DOCUMENT**----------