ujjivan SMALL FINANCE BANK

EKyc API GATEWAY DOC

Table of Contents

1. INTRODUCTION

1.1 Design Document Purpose

The purpose of this document is to provide a detailed specification of the **EKyc** 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 **EKyc** API is exposed within **EKyc Products .**
- Service Consumers must subscribe to the API. A unique application Identification (client-id) and a secret will be generated.
- The assigned Client-id and Client-Secret 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. API AUTHENTICATION

JWT Access token to be passed in header section of Authorization field. The Token can be generated by subscribing to **TOKEN API**.

3.1 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

4. API INTERNAL DESIGN

- **Overview:**

Service is designed to electronically know your customer through Aadhar authentication. The API Gateway makes a backend **FinaKyc KUA Server.**

- **Request Type**: POST
- **API URL**:
  UAT : https://apiuat.ujjivansfb.in/ujjivan/development/v1/KUAServer/kyc
  PROD : https://api.ujjivansfb.in/ujjivan/development/v1/KUAServer/kyc
- **Mandatory HTTP Headers**:

- X-IBM-Client-Id: xxxxxxxxxxxxxxx
- X-IBM-Client-Secret: xxxxxxxxxxxxxxxxx
- Authorization: <Access token to be passed, generated from TOKEN API.>

➢ **Minimum Required Input Parameter:**

Element Name	M/ O/C	Data Type	Description
bio	M/ O	String	Valid values are "Y" or "N". If the value is "Y" then at least one biometric element “Bio” (part of “Bios” element) should be used in authentication. If value is “n", “Bio” element is not mandated
bt	M/ O	String	(mandatory only if “bio” attribute has value "Y") provide a comma separated list of biometrics used. Valid values that can be used in this comma separated list are “FMR”, “FIR”, and “IIR”. If “FMR” is part of the list, then at least one “Bio” element with type FMR should be used. Similarly, if “FIR” or “IIR” are part of the list, then at least one “Bio” element with those types must be used. For biometric fingerprint reader only pass “FMR”. For Iris based authentication pass “IIR”
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.
Ci	O/ M	String	Certificate Identifier. (Pass UIDAI certificate's expiry date in YYYYMMDD format using GMT time zone)
dc	O/ M	String	(mandatory for bio auth) Unique Registered Device Code. Returned by RD Service when using biometric authentication.Else pass “NA”.
dpId	O/ M	String	(mandatory for bio auth) Unique code assigned to registered device provider. Returned by RD Service when using biometric authentication. Else pass “NA”.
EncryptedHmac	M	String	HMAC means Hash-based message authentication code.Compute SHA-256 Hash of Pid xml block. Then encrypt using session key (skey) and then do Base64 encoding.
EncryptedPid	M	String	Encypted PID (Person Identifiable Data) XML data.(Encrypted using the one-time session key and later done Base64 encoding)
EncryptedSessionKey	M	String	Value of this element is base-64 encoded value of encrypted 256-bit AES session key. Encrypted using UIDAI public key. Session key must be dynamically generated for every transaction (session key must not be reused) and must not be stored anywhere except in memory.
Fdc		String	Fingerprint device code. This is a unique code provided for the fingerprint sensor-extractor combination. AUAs should obtain this code from sensor providers for certified sensors. This is an alpha-numeric string of maximum length 10. For now pass “NC”
Idc		String	Pass “NC” for IRIS based authentications, otherwise pass “NA”

IsKyc		String	Set value as “true” for ekyc request and “false” for authentication.
Lov		String	Location Value. Pass attribute must have a valid 6-digit postal pin code.
mc	O/M	String	(mandatory for bio auth) This attribute holds registered device public key certificate. This is signed with device provider key. Returned by RD Service when using biometric authentication. Else pass “NA”.
mi	O/M	String	(mandatory for bio auth) Registered device model ID. Returned by RD Service when using biometric authentication.Else pass “NA”.
otp	M	String	(mandatory) Valid values are "Y" or "N". If the value is "Y" then OTP should be used in authentication. Otherwise, “otp” is not mandated.
pa	M	String	(mandatory) Valid values are "Y" or "N". If the value is "Y" then at least one attribute of element “Pa” (part of “Demo” element) should be used in authentication. If value is “n", “Pa” element is not mandated.
pfa	M	String	(mandatory) Valid values are "Y" or "N". If the value is "Y" then element “Pfa” (part of “Demo” element) should be used in authentication. If value is “n", “Pfa” element is not mandated.
pi	M	String	(mandatory) Valid values are “Y” or “N”. If the value is “Y” then at least one attribute of element “Pi” (part of “Demo” element) should be used in authentication. If value is “N", “Pi” element is not mandated.
pin	M	String	(mandatory) Valid values are "Y" or "N". If the value is "Y" then PIN should be used in authentication. Otherwise, “pin” is not mandated.
PublicIp		String	Public IP address of the device. If the device is connected to Internet and has a public IP, then this must be populated with that IP address. If the device has a private IP and is behind a router/proxy/etc, then public IP address of the router/proxy/etc should be set. If no public IP is available, leave it as “NA”.
rdsId		String	(mandatory for bio auth) Unique ID of the certified registered device service. Returned by RD Service when using biometric authentication. Else pass “NA”.
rdsVer		String	(mandatory for bio auth) Registered devices service version. Returned by RD Service when using biometric authentication. Else pass “NA”.
requestPrintFormatPdfFromUIDAI		String	Pass false by default. Use true , if we want print format pdf ekyc data from uidai
TerminalId		String	Client device id. Default value “public” For Registered devices, send its unique Terminal ID using “getTID()” function of the registered device
Ts		String	Timestamp at the time of capture of authentication input. This is in format “YYYY-MM-DDThh:mm:ss” (derived from ISO 8601). Time zone should not be specified and is automatically defaulted to IST (UTC +5.30).
Udc		String	Unique Host/Terminal Device Code. This is a unique code for the host device assigned within the AUA domain. This is an alpha-numeric string of maximum length 20. Suggested format is “[vendorcode][date of deployment][serial number]”. For now pass "UKC:SampleClient"

UIDAITxn	O/M	String	(mandatory for otp based ekyc) . Pass the UIDAI transaction id got as the response of successful OTP generation. All other case pass “NA”
Uid		String	Aadhaar number of the customer (size 12) or Virtual Id (size 16) of the customer or AUA specific uidtoken (size 72)
reasonForAuth		String	Pass Reason for EKYC / Auth as a String. Max Length 250.

- **Output Parameters:**

Element Name	M/O/C	Data Type	Description
TransactionId	M	String	Transaction id for this particular transaction in KUA server
Status	M	String	Possible values are “Y” for success and “N” for failure
Xml	O/M	String	Original xml returned from UIDAI. Will contain additional information related to this transaction
KycDetails	M	String	This JSON object contains the entire KYC data including photo,name, address,email,phone number etc
auaSpecificUidToken	M	String	AUA Specific 72 char UID Token from UIDAI.
UidaiTransactionId	M	String	Uidai Transaction id.
ErrorCode	O/M	String	Incase of an error, error code will be populated else it is empty string.
AuthResponseCode	M	String	Response code
maskedAadhaarNumberFromUIDAI	M	String	Masked aadhaar number from UIDAI. It contains aadhaar number in masked form with last 4 positions data visible. Eg: xxxxxxxx9248
ErrorCode	M	String	Display Error code
authErrorCode	M	String	Display auth Error code

- **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	

5. ERROR CODES IN Finahub(Backend):

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

- o “100” – “Pi” (basic) attributes of demographic data did not match.
- o “200” – “Pa” (address) attributes of demographic data did not match
- o “300” – Biometric data did not match
- o “310” – Duplicate fingers used
- o “311” – Duplicate Irises used.
- o “312” – FMR and FIR cannot be used in same transaction
- o “313” – Single FIR record contains more than one finger
- o “314” – Number of FMR/FIR should not exceed 10
- o “315” – Number of IIR should not exceed 2
- o “400” – Invalid OTP value
- o “401” – Invalid TKN value
- o “500” – Invalid encryption of Skey
- o “501” – Invalid certificate identifier in “ci” attribute of “Skey”
- o “502” – Invalid encryption of Pid o “503” – Invalid encryption of Hmac
- o “504” – Session key re-initiation required due to expiry or key out of sync
- o “505” – Synchronized Key usage not allowed for the AUA
- o “510” – Invalid Auth XML format
- o “511” – Invalid PID XML format
- o “520” – Invalid device
- o “521” – Invalid FDC code under Meta tag
- o “522” – Invalid IDC code under Meta tag
- o “530” – Invalid authenticator code
- o “540” – Invalid Auth XML version
- o “541” – Invalid PID 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 “550” – Invalid “Uses” element attributes
- o “551” – Invalid “tid” value for registered device
- o “552” – Invalid registered device key, please reset
- o “553” – Invalid registered device HOTP, please reset
- o “554” – Invalid registered device encryption
- o “555” – Mandatory reset required for registered device
- o “561” – Request expired (“Pid->ts” value is older than N hours where N is a configured threshold in authentication server)
- o “562” – Timestamp value is future time (value specified “Pid->ts” is ahead of authentication server time beyond acceptable threshold)
- o “563” – Duplicate request (this error occurs when exactly same authentication request was re-sent by AUA)
- o “564” – HMAC Validation failed o “565” – AUA license has expired o “566” – Invalid non-decryptable license key
- o “567” – Invalid input (this error occurs when some unsupported characters were found in Indian language values, “lname” or “lav”)
- o “568” – Unsupported Language
- o “569” – Digital signature verification failed (means that authentication request XML was modified after it was signed)
- o “570” – Invalid key info in digital signature (this means that certificate used for signing the authentication request is not valid – it is either expired, or does not belong to the AUA or is not created by a well-known Certification Authority)
- o “571” – PIN Requires reset (this error will be returned if resident is using the default PIN which needs to be reset before usage) o “572” – Invalid biometric position
- o “573” – Pi usage not allowed as per license o “574”– Pa usage not allowed as per license
- o “575”– Pfa usage not allowed as per license

- o “576” - FMR usage not allowed as per license
- o “577” – FIR usage not allowed as per license
- o “578” – IIR usage not allowed as per license
- o “579” – OTP usage not allowed as per license
- o “580” – PIN usage not allowed as per license
- o “581” – Fuzzy matching usage not allowed as per license
- o “582” – Local language usage not allowed as per license
- o “584” – Invalid pincode in LOV attribute under Meta tag
- o “585” – Invalid geo-code in LOV attribute under Meta tag
- o “710” – Missing “Pi” data as specified in “Uses”
- o “720” – Missing “Pa” data as specified in “Uses”
- o “721” – Missing “Pfa” data as specified in “Uses”
- o “730” – Missing PIN data as specified in “Uses”
- o “740” – Missing OTP data as specified in “Uses”
- o “800” – Invalid biometric data
- o “810” – Missing biometric data as specified in “Uses”
- o “811” – Missing biometric data in CIDR for the given Aadhaar number
- o “812” – Resident has not done “Best Finger Detection”. Application should initiate BFD application to help resident identify their best fingers. See Aadhaar Best Finger Detection API specification.
- o “820” – Missing or empty value for “bt” attribute in “Uses” element
- o “821” – Invalid value in the “bt” attribute of “Uses” element
- o “901” – No authentication data found in the request (this corresponds to a scenario wherein none of the auth data – Demo, Pv, or Bios – is present)
- o “902” – Invalid “dob” value in the “Pi” element (this corresponds to a scenarios wherein “dob” attribute is not of the format “YYYY” or “YYYY-MM-DD”, or the age of resident is not in valid range)
- o “910” – Invalid “mv” value in the “Pi” element o “911” – Invalid “mv” value in the “Pfa” element
- o “912” – Invalid “ms” value
- o “913” – Both “Pa” and “Pfa” are present in the authentication request (Pa and Pfa are mutually exclusive)
- o “930 to 939” – Technical error that are internal to authentication server
- o “940” – Unauthorized ASA channel
- o “941” – Unspecified ASA channel
- o “980” – Unsupported option
- o “997” – Invalid Aadhaar status (Aadhaar is not in authenticatable status)
- o “998” – Invalid Aadhaar Number
- o “999” – Unknown error

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