Identity Auth Internal REST Service

# Background

Identity Auth Internal REST service can be used to authenticate an Individual by MOSIP Products internally. It supports below types of authentications –

* Pin based – OTP, Static Pin
* Biometric based – Fingerprint, IRIS and Face

## Target Users -

MOSIP Products can use Identity Auth Internal REST service to authenticate an Individual by using one or more of the above types of authentication supported.

## Key Requirements -

* MOSIP Products to authenticate an Individual using Identity Auth Internal REST service
* MOSIP Products will send Individual’s UIN/VID to enable authentication of Individual
* Identity Auth Internal REST service to check Individual’s UIN/VID for authenticity and validity

## Key Non-Functional Requirements –

* Logging :
  + Log each stage of authentication process
  + Log all the exceptions along with error code and short error message
  + As a security measure, Individual’s UIN or PI/PA should not be logged
* Audit :
  + Audit all transaction details during authentication process in database
  + Individual’s UIN or PI/PA details should not be audited
  + Audit any invalid UIN or VID incidents
* Exception :
  + Any failure in authentication/authorization of TSP and validation of UIN and VID needs to be handled with appropriate error code and message in Auth Response
  + Any error in Individual authentication also should be handled with appropriate error code and message in Auth Response
* Security

<<TBD>>

# Solution

Identity Auth Internal REST service addresses the above requirements as explained below.

1. MOSIP Products to construct a **POST** request with below details and send to Request URL **identity/auth/internal**

Sample Request Body –

{

"id" : "mosip.identity.auth",

"ver" : "1.0",

"indId" : "1234567890",

"indIdType" : "V",

"authType" :

{

"face" : false,

"iris" : true,

"fingerprint" : false,

"otp" : false,

"pin" : false

},

"reqTime" : "2018-10-17T07:22:57.086+0000",

"pinInfo" :

{

"value" : "123456",

"type" : "SPIN"

},

"request" :

{

//JSON request as per the id object schema defined by the country

"identity": {

"name": [

{

"language": "ar",

"value": "ابراهيم"

},

{

"language": "fr",

"value": "Ibrahim"

}

],

"addressLine1": [

{

"language": "ar",

"value": "عنوان العينة سطر 1"

},

{

"language": "fr",

"value": "exemple d'adresse ligne 1"

}

],

"fullAddress": [

{

"language": "ar",

"value": "فاس-الدار البيضاء"

},

{

"language": "fr",

"value": "Casablanca"

}

],

"leftEye": [

{

"value": "encoded\_left\_eye\_image"

}

],

"rightIndex": [

{

"value": "encoded\_right\_index\_image"

}

]

}

}

}

1. Authenticate and Authorize MOSIP Product **<TBD>**
2. Integrate with kernel UIN Validator and VID Validator to check UIN/VID for validity. Validate UIN/VID for authenticity in AuthDB
3. Once the above validations are successful, Identity Auth Internal REST request is then validated based on specific authentication types as described below.
   1. OTP Auth – OTP value sent to the Individuals are validated
   2. Pin Auth – Static Pin generated by the Individuals is validated against the input pin
   3. Bio Auth – Fingerprint/IRIS/Face minutiae stored is validated against input bio minutiae
4. Respond to MOSIP Product with below success Identity Auth response -

{

"status" : true,

"err": [],

"resTime": "2018-10-17T13:40:19.590Z"

}

## Class Diagram:

## Sequence Diagram: