Auth Request & Response

Table of Contents

1. Overview

UIDAI has recently introduced *Registered Device* concept which will eliminate use of stored biometrics. They have also released new authentication api version-2.0 which only supports registered device. Currently your devices are considered as Public device As a result there are changes in some of the parameters. This document contains the new auth request and response format as per the new auth guidelines provided by UIDAI.

2. Demographic based Authentication request

a. Auth Json Request:

```
{
        "aadhaar-id": <12 digit aadhaar id>,
        "consent":"< Y / N>",
        "modality": "demo",
        "certificate-type":"<preprod / prod>",
        "demographics": {
        "name": {
            "matching-strategy": "<exact / partial>",
            "matching-value": "",
            "name-value": ""
        },
        "dob": {
            "format": "<YYYYMMDD / YYYY>",
            "dob-type": "<verified/declared/approximate>",
            "dob-value": ""
        },
        "age": "",
        "phone": "",
        "email": "",
        "gender": "<male / female / transgender>",
         "address-format": "<structured / freetext>",
         "address-freetext": {
            "matching-strategy": "",
            "matching-value": "",
            "address-value": ""
        },
        "address-structured": {
            "care-of": "",
            "house": "",
            "street": "",
            "landmark": "",
            "locality": "",
            "vtc": "",
```

```
                "subdistrict": "",
                "district": "",
                "state": "",
                "pincode": "",
                "post-office": "",
                 "country":  "",
            }
        }
```

Attribute	**Mandatory**	**Attribute Specifications**
Aadhaar id	Y	12-digit aadhaar no. without spaces
Consent	Y	“Y” if you want to proceed or else “N”.
Modality	Y	demo
Name (matching strategy)	N	“exact” - Exact Matching “partial” - Partial Matching (depends on the percentage specified in the matching value attribute)
Name (matching value)	N	The matching value defines what percentage of total words (rounded up) of the name (as recorded in the aadhar database) must be specified for a successful match.
Name (name-value)	N	Name which is to be authenticated
DOB(dob-format)	N	Date of Birth format. Valid values are “YYYY” or “YYYYMMDD”
DOB(dob-type)	N	Valid values are “verified”,“declared” or “approximate”. Default is “verified”
DOB(value)	N	Your date of birth in the chosen format.
email	N	The email id of the resident
Age	N	Should be less than or equal to the actual age.
Phone	N	Your phone number which is linked with Aadhaar

Gender	N	“male” / “female” / “transgender”
Address-Format	Mandatory when providing address	“structured” / “freetext”
Address-structured	Mandatory when address format specified is ‘structured’	
Address-structured(care-of)	N	‘Care of’ person’s name
Address-structured(house)	N	House identifier
Address-structured(street)	N	Street Name
Address-structured(landmark)	N	Landmark if any
Address-structured(locality)	N	Locality if any
Address-structured(vtc)	N	village/town/city name
Address-structured(subdistrict)	N	Subdistrict name
Address-structured(district)	N	District name
Address-structured(state)	N	State name
Address-structured(pincode)	N	Postal pin code
Address-structured(post-office)	N	Post office name
Address-structured(country)	N	Country name
Address-freetext	Mandatory if address format specified as ‘freetext’	
Address-freetext (matching-strategy)	N	“exact” - Exact Matching “partial” - Partial Matching

Address-freetext (matching-value)	N	The matching value defines what percentage of total words (rounded up) of the address (as recorded in the aadhar database) must be specified for a successful match.
Address-freetext(address-value)	N	full address which is to be authenticated eg: “407 B-wing, Sarjapur,Karanataka”

3. Otp based Authentication request

a. Generate otp json request

i. Generate otp, json request:

```
{
        "aadhaar-id": "<12 digit aadhaar number>",
        "channel":"<SMS / EMAIL / EMAIL_AND_SMS>"
        “type”: “A”
}
```

b. Json response for otp request

i. otp json response :

```
{
        "success":true,
        "aadhaar-reference-code":"unique ref number from UIDAI",
        "txn-id":"unique transaction id",
        "info":"information about otp transaction by UIDAI"
}
```

c. Otp based authentication json request

i. Auth Json Request:

```
{
        "aadhaar-id": “<12 digit aadhaar number>”,
        “consent”:”<Y / N>”,
        “modality”: “otp”,
        "txn-id": “<when using otp, this will be returned in otp response>”,
        “otp”: <6 digit otp value>
}
```

Attribute	Mandatory	Attribute Specifications
Aadhaar id	Y	12 digit aadhaar number eg: 999999999999
Consent	Y	“Y” if you want to proceed otherwise“N”.
Modality	Y	otp
Txn-id	Y	Transaction id would be returned in OTP response.
OTP	Y	6 digit OTP to be entered here.

4. Biometric based Authentication request

Steps for Authentication using Biometric:-

1. Install the RD Service on the device(mobile phone/desktop machine).
2. Capture the biometric and get the encrypted pid,hmac,session-key along with the device info from rd service.
3. Set all these parameters to biometric based authentication json request(below).

a. Auth Json request :

```
{
        "aadhaar-id": <12 digit aadhaar id>,
        “consent”:”<Y / N>”,
        “unique-device-code”:”<to identify uniquely application/machine/device from where request originated>”,
        "dpId" : “<returned from rd service>”,
        "rdsId" : “<returned from rd service>”,
        "rdsVer" :“<returned from rd service>”,
        "dc" : “<returned from rd service>”,
        "mc":  “<returned from rd service>”,
        "mi":<returned from rd service>,
        "hmac": “<you will get from rd service>”,
        “session-key”:{
                “cert-id”:<Skey.id from rd service>,
                “value”:<Skey.value from rd service>
        },
        “pid”:{
                “type”:”<xml / proto>”,
                “value”:<Data.value from rd service>
```

```
            }
        }
```

Table explaining parameters of Auth request using biometric data.

Attribute	**Mandatory**	**Attribute Specifications**
Aadhaar id	Y	12-digit aadhaar no without spaces
Consent	Y	Enter “Y” if you want to proceed or else enter “N”.
unique-device-code	Y	to identify uniquely the application/machine/device from where request originated
dpId	Y	Device Provider ID as assigned during certification.
rdsId	Y	RD Service ID as assigned during certification.
rdsVer	Y	RD Service Version.
mi	Y	Device Provider Model ID.
dc	Y	Unique Registered device code.
mc	Y	This attribute holds registered device public key certificate.
hmac	Y	SHA-256 Hash of Pid block, encrypted and then encoded
Session-key(cert-id)	Y	UIDAI public key identifier as per auth spec. Set this to value of “Skey.ci”.
Session-key(value)	Y	Encrypted session key as per auth spec Set this to value of “Skey.value”.
Pid(type)	Y	Set to “xml” when pid.type is “X” Set to “proto” when pid.type is “P”
Pid(value)	Y	Encrypted pid block as per auth spec Set this to value of “Data” element.

5. Authentication response

a. Auth Json Response:

```
{
        "success":<true/false>,
        "aadhaar-reference-code":"unique ref code from UIDAI",
        "info":"<detailed information about auth request >",
        "pid-timestamp":"YYYYMMDDhhmmss"
}
```

Table explaining parameters of Auth response using biometric data.

Attribute	**Attribute Specifications**
success	Status of auth request
aadhaar-reference-code	Unique ref id for each transaction
info	Detailed information about auth request
pid-timestamp	Timestamp when the pid was captured

6. Changes in Auth from 1.6 to 2.0

1. Auth Request

a. Parameter to get Aadhaar holder's Consent to perform authentication transaction added. This should not be hardcoded by any SubAUA. Upon obtaining consent you need to set *"consent":"Y"* in Auth Json requests as specified in documentation.
b. *Location* and *public-ip* attributes removed from Json requests.
c. *Country* attribute added to auth demographic request.
d. No public devices are allowed in biometric authentication.
e. Additional attributes added to support registered device in auth Json request (refer documentation).

2. Auth Response

a. new attribute ***action-code*** added (refer documentation).
b. New attribute **info** is added (refer documentation).
c. new attribute ***pid-timestamp*** added(refer documentation).