



India's Biometrics-e-Authentication



Dr.Y.L.P.Rao
Deputy Director General
Unique Identification Authority of India

Aadhaar Vision

To empower residents of India with a *unique identity and a digital platform* to authenticate anytime, anywhere

Current Status

- Started issuing Aadhaar in Sept 2010
- More than 75 crores enrolment
- Over 676.3 Million crore Aadhaar numbers issued so far
- Capacity to generate 1.5 million Aadhaar per day
- Target is Set to generate 1 Billion Aadhaar by end of 2015.
- Online Authentication services (Biometric, Demographic, OTP) are live.
- More than 18.36 crore Authentication Transaction completed till date
- Aadhaar Payment Bridge (APB) and Aadhaar Enabled Payment System(AEPS) are live with NPCI.



About UIDAI

Core Task

- Generate & deliver Aadhaar Number
- Develop & Maintain Infrastructure
- Provision for updating & authentication Identity

UIDAI

- Established in January 28, 2009

Vision

To empower residents of India with a unique identity and a digital platform to authenticate anytime, anywhere.

Deliver various services

- eKYC
- Collaborate with partners for Aadhaar linked application



Aadhaar Authentication Digital Platform

A digital online verification platform, to enable residents to prove their identity and for service providers to confirm that the residents are 'who they say they are'





'Un-tethering' identification to claim benefits

Any Place

Any Network

Any Provider

Any Device



Introduction: Aadhaar Authentication

Supports answering the question “is a person s/he claims to be”

Verifies resident information (demographics and/or biometrics) for a given Aadhaar number

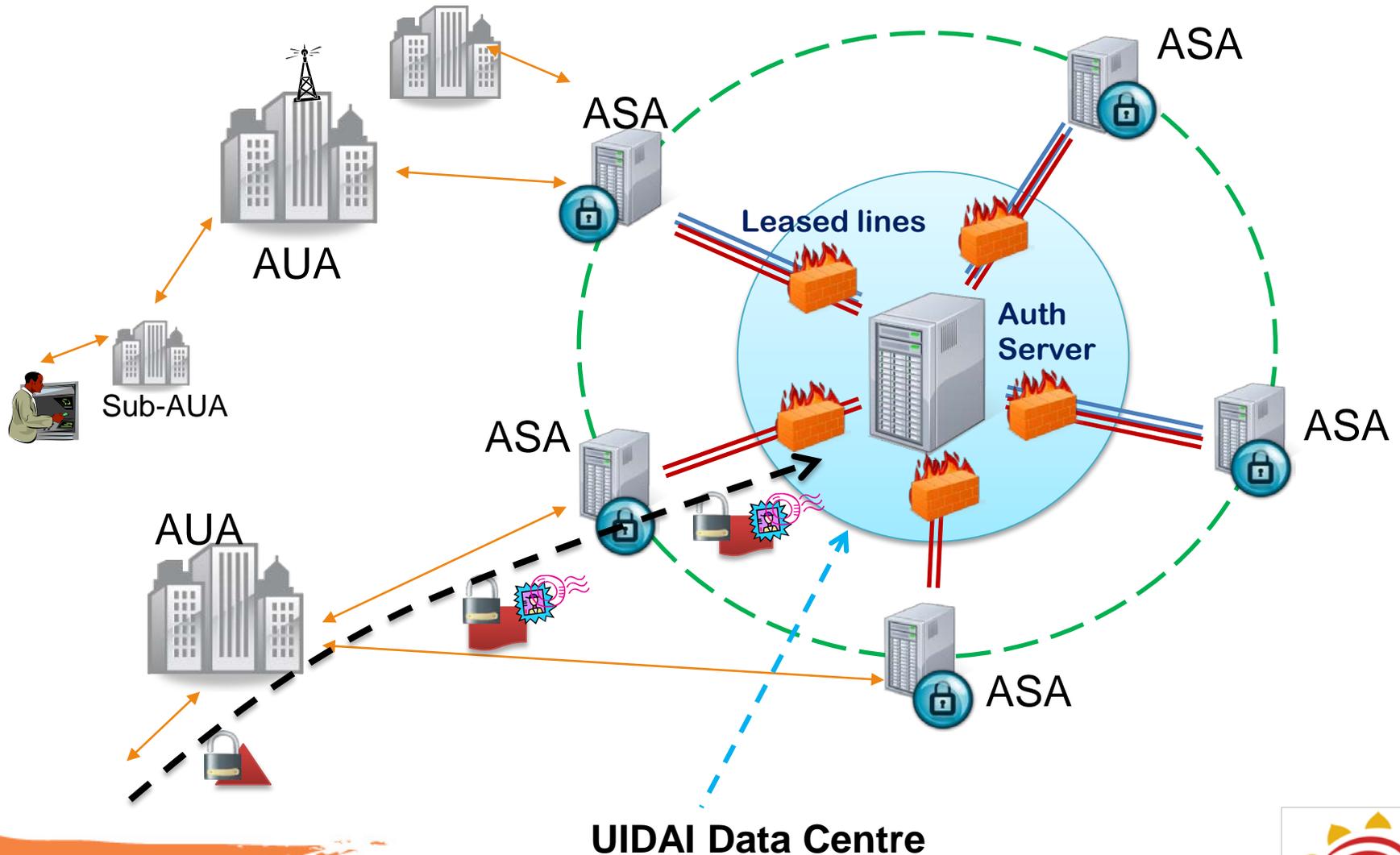
Online identification verification service that is lightweight, ubiquitous, and secure

Only a “yes or no” is returned as part of the response



Aadhaar Authentication Ecosystem Overview

21ASAs, 101 AUAs Live/on boarded



Aadhaar Authentication – Definition (1/3)

Stakeholders

Description



UIDAI

- Overall regulator and overseer of the Aadhaar authentication system
- Owns and manages, either by itself or through an agency, the Central Identities Data Repository (CIDR)
 - CIDR contains the personal identity information / data of all Aadhaar-holders.
- Presently UIDAI will manage the CIDR through a Managed Service Provider (MSP)



[Authentication Service Agency \(ASA\)](#)

- Agencies that have established secure leased line connectivity with the CIDR compliant with UIDAI's standards and specifications
- Offers their UIDAI-compliant network connectivity as a service to AUA
- Transmits AUAs' authentication requests to CIDR
- Agencies contracted with UIDAI as ASAs shall send authentication requests to the CIDR



[Authentication User Agency \(AUA\)](#)

- Agencies that uses Aadhaar authentication to enable its services
- Connects to the CIDR by itself (as an ASA) or through an existing ASA
- Could also transmits authentication requests from other entities that are "Sub AUAs" under it



Aadhaar Authentication – Definition (2/3)

Stakeholders	Description
 <p data-bbox="57 385 415 485">Authentication User Agency (AUA)</p>	<ul data-bbox="511 278 1864 478" style="list-style-type: none">• Could act as an aggregator offering authentication services to Sub-AUAs below them• Enters into a formal contract with UIDAI in order to access Aadhaar authentication
 <p data-bbox="57 678 241 721">Sub AUA</p>	<ul data-bbox="511 506 1864 778" style="list-style-type: none">• An agency / entity who access Aadhaar authentication services through an existing AUA• UIDAI has no direct contractual relationship with the Sub AUA• AUA shall be responsible for all authentication requests flowing through it, including those originating from its Sub AUA
 <p data-bbox="57 978 357 1078">Authentication Devices</p>	<ul data-bbox="511 799 1864 1192" style="list-style-type: none">• Electronic actors that form a critical link in the Aadhaar authentication service<ul data-bbox="608 913 1864 1192" style="list-style-type: none">—Devices that collect personal identity data (PID) from Aadhaar holders—Prepares the information for transmission,—Transmits the authentication packets for authentication and—Receives the authentication results

Aadhaar Authentication – Definition (3/3)

Stakeholders

Description



Authentication Devices

- They could be operator-assisted devices or self-operated devices
 - They could be operated by the AUA (or the Sub AUA) or agents of AUA / Sub AUA
- (Eg: desktop PCs, laptops, kiosks, handheld mobile devices, etc).



Aadhaar Holders

- Are valid Aadhaar numbers holders
- Seek to authenticate their identity towards gaining access to the services offered by the AUA or their Sub-AUAs.

Aadhaar Authentication

Supports multi-factor authentication using

- biometrics (fingerprint, Iris)
- One time pin (OTP)
- and combinations thereof

Supports all types of networks, protocols and devices

- GPRS, Edge, 3G, Wi-Fi, LAN, WAN, Broadband etc
- Personal computer, mobile, PoS terminals, etc.
- Works with assisted and self-service applications

Security

Data encrypted at source

Data tamper proof

Network security and encryption

Secure connectivity from device to UIDAI data centre

Data audited



Scalability for large volumes

Authentication data is about 500bytes -2.5Kb

Devices cost comparable to hand held devices

Under 1 sec in CIDR and 1-4 secs round trip

Can handle 100+ million authentication a day

Low cost, universal, easily deployable



Technology

Built on open standards - XML, https, ISO, AES-256/PKI-2048, SHA-256, etc

Biometrics basis FMR – ISO 19794-2:2005, FIR – ISO 19794-4 , IIR - ISO 19794-6:2011

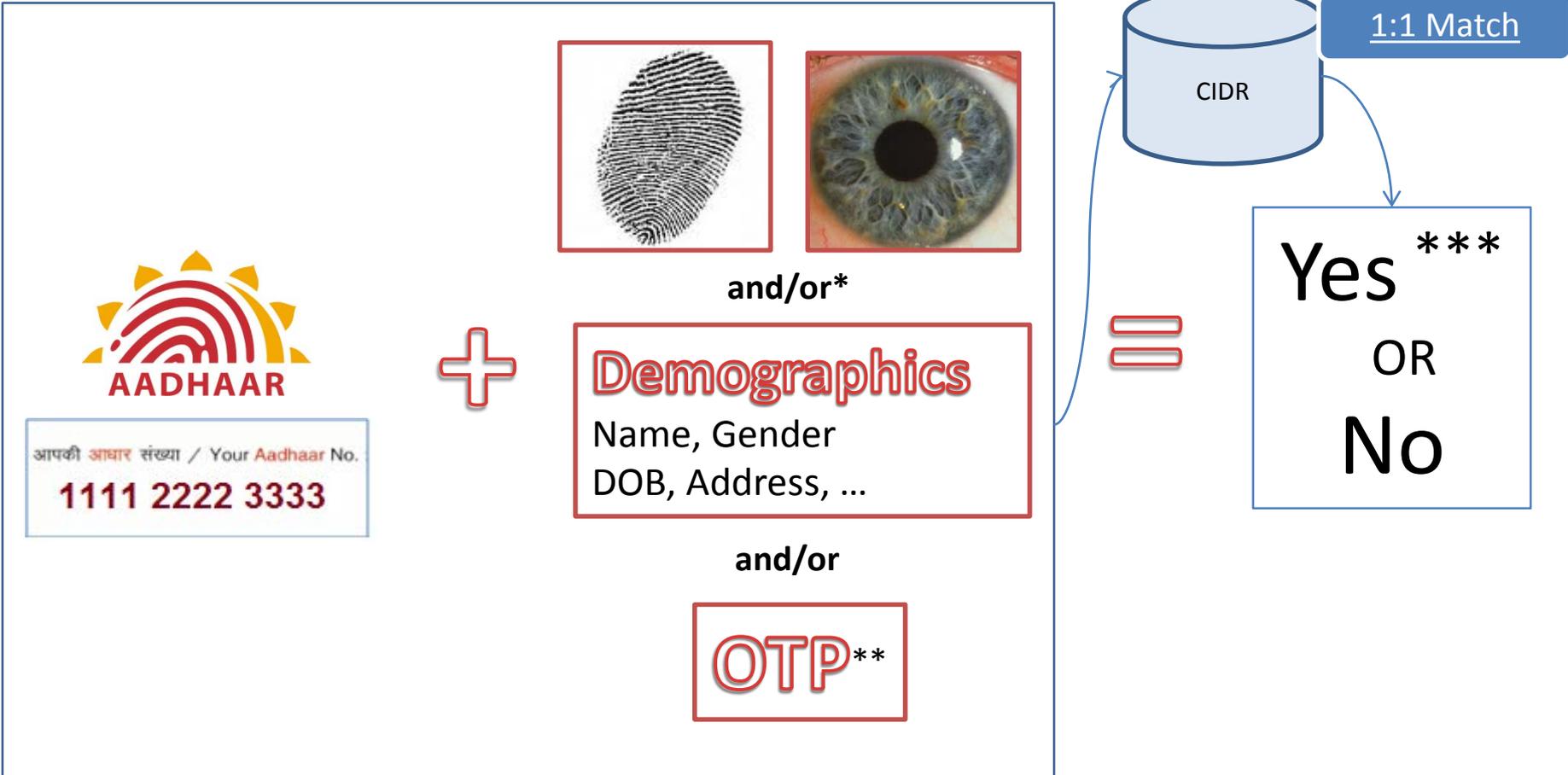
Built to scale - light weight and stateless

Flexibility provided in Authentication API to meet AUA's needs

Accommodates various business models and ecosystem based adoption



Authentication Processes At a Glance



*and/or – Single or multi-factor authentication

**OTP – One Time Pin

***Yes/No – Would enable service provider to take business decision

Aadhaar Authentication Usage Types

Aadhaar Number – Single Factor

- 12th digit (last digit) is a Verhoeff checksum for error detection

Demographic Only – Single Factor

- Demographic attributes like Name, Date of Birth, Gender, Address etc. can be used

*OTP Only – Single Factor

- Authentication using One Time Pin (OTP) alone

*Biometrics only – Single Factor

- Authentication using Biometrics (single factor authentication) – Fingerprint/ Iris

*Biometric & OTP – Two Factors

- Authentication using Biometrics (Fingerprint/ Iris) and OTP (two factor authentication)

*Three Factors

- Authentication using Fingerprint biometrics, Iris and OTP (three factor authentication)

*Any of the demographic attributes may also be used in Type 2 to Type 5



Authentication Service Usage Illustrations

Type 1 – Demographic Only – Single Factor

- AUA beneficiary database cleanup
- Periodic KYC/beneficiary verification
- Address, Date of Birth verification

Type 2 – OTP Only – Single Factor

- Authentication for internet- and mobile-based transactions
- Cases where deployment of biometric technology is difficult or not practical

Type 3 – Biometrics Only – Single Factor

- Authenticating residents at point of delivery
- Periodic verification of pensioners' database
- Attendance management
- Adding new beneficiary / customer
- Financial transactions

Type 4 – Biometric (Fingerprint/Iris) & OTP – Two Factors

- Where higher assurance levels may be required such as:
 - High Value Financial transactions
 - Accountability tracking (example – authenticating officials in charge for inspection in service delivery programs such as PDS & NREGA)
- Access to restricted/high security areas

Type 5 – Fingerprint + Iris + OTP – Three Factors

- Access to very high security areas such as army base, nuclear plants etc

Demographic Authentication



Demographics

Name, Gender
DOB, Address, ...



YES
OR
NO

आपकी आधार संख्या / Your Aadhaar No.

1111 2222 3333

Personal Address (Pa)

Care Of	<input type="text"/>	Building	<input type="text"/>
Landmark	<input type="text"/>	Street	<input type="text"/>
Locality	<input type="text"/>	PO Name	<input type="text"/>
Village/Town/City	<input type="text"/>	Subdist	<input type="text"/>
District	<input type="text"/>	State	<input type="text"/>
		Pincode	<input type="text"/>

Personal Identity (Pi)

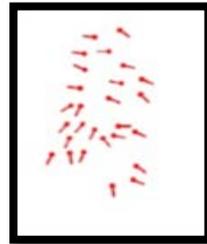
Name	<input type="text"/>	Match Value	<input type="text" value="100"/>
Match Strategy	<input checked="" type="radio"/> Exact match	<input type="radio"/> Partial match	<input type="radio"/> Fuzzy match
Local Name	<input type="text"/>	Local Match Value	<input type="text" value="90"/>
Gender	<input type="text" value="Select gender"/>	Age	<input type="text"/>
		DOB type	<input type="text" value="Select"/>
	<input type="text"/>	Date of birth	<input type="text"/> - <input type="text"/> - <input type="text"/>

Personal Full Address (Pfa)

Match Strategy (ms)	<input checked="" type="radio"/> Exact Match	<input type="radio"/> Partial Match	<input type="radio"/> Fuzzy match
Address value (av)	<input type="text"/>	Match Value (mv)	<input type="text" value="100"/>
	<input type="text"/>		
Local Match Value (lmv)	<input type="text" value="90"/>		
Local Address value (lav)	<input type="text"/>		



Biometric Finger Print Authentication



**Fingerprint
Minutiae record**
(ISO 19794-2:2005)

One or more

Size of less than
300 bytes



Yes

or

No

or



**Fingerprint
Image record**
(ISO 19794-4)

One or more

Size of about
150KB

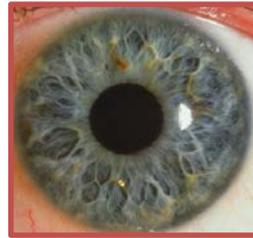


आपकी आधार संख्या / Your Aadhaar No.

1111 2222 3333



Biometric Iris Authentication



Iris Image Record
(ISO 19794-6:2011)



One or both iris Image

Image size (compressed)
Kind 7: 2 KB
Type: PNG or Jpeg2000

Yes

or

No

आपकी आधार संख्या / Your Aadhaar No.

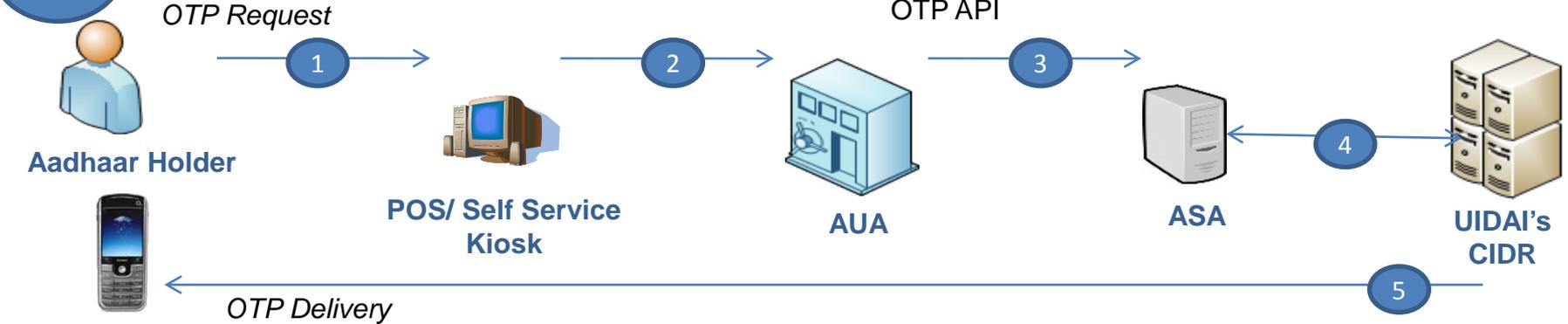
1111 2222 3333

- Inclusive Modality demonstrated by high population coverage (over 99.5%)
- Higher Accuracy, operating at a false accept rate of one in million (true accept rate of over 99%)

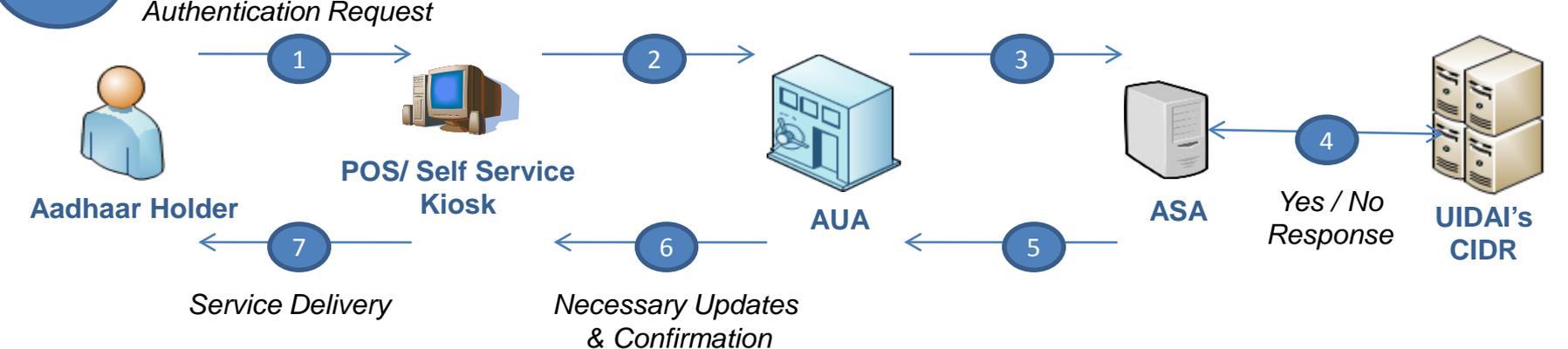


Aadhaar OTP Authentication Process

Step 1



Step 2



Aadhaar e-KYC Introduction

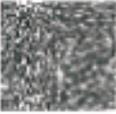
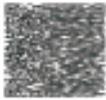
For availing any service, we have to prove our identity by providing a document called Proof of Identity (PoI) like Pan Card, Voter Id card etc. and a Proof of Address (PoA) like Ration Card, Voter Id card etc. This process is normally called KYC(Know your Customer).



Advantages of Aadhaar KYC

S.No.	Type of Document	Mode of Authentication	Remarks
1.	Passport	Physical Verification of the document	Time consuming
2.	PAN	Physical Verification of the document	Time consuming
3.	Driving License	Physical Verification of the document	Time consuming
4.	Voter's ID	Physical Verification of the document	Time consuming
5.	Aadhaar Letter	Demographic/Biometric / OTP	Low cost, accurate and instantaneous
6.	NREGA Job Card	Physical Verification of the document	Not fool-proof

Aadhaar Letter

 	 
<p>भारतीय विशिष्ट पहचान प्राधिकरण भारत सरकार Unique Identification Authority of India Government of India</p>	<p>निर्देश</p> <ul style="list-style-type: none">■ आधार पहचान का प्रमाण है, नागरिकता का नहीं।■ पहचान का प्रमाण ऑनलाइन ऑथेंटिकेशन द्वारा प्राप्त करें।■ किसी प्रकार की सहायता के लिए :- फोन नं. 1800 180 1947 पर सम्पर्क करें, अथवा पी.ओ. बॉक्स नं. 1947, बेंगलूरु-560001 पर पत्र भेजें, अथवा help@uidai.gov.in पर ईमेल करें।
<p>नगराजन क्रम/Enrolment No.: 1234/5678901234</p> <p>श्री, श्री. नदीम Mohd. Nadeem S/O Mohd. Saleem B-107, VKAS Vihar, Near Dwarka Metro Station Delhi 110078</p> <p>2102101010</p>  <p>AA123456789ZZ</p>  <p>आपका आधार क्रमांक / Your Aadhaar No. : 4567 8901 2345</p> <p>आधार — आम आदमी का अधिकार</p>	<p>INSTRUCTIONS</p> <ul style="list-style-type: none">■ Aadhaar is proof of identity, not of citizenship.■ To establish identity, authenticate online.■ In case any help is required:- Call 1800 180 1947 or; Write to P.O, Box No, 1947, Bengaluru - 560 001 or; Email at help@uidai.gov.in
<p>भारत सरकार GOVERNMENT OF INDIA</p> <p>श्री. नदीम Mohd. Nadeem जन्म वर्ष / Year of Birth : 1987 पुरुष / Male</p>   <p>4567 8901 2345</p> <p>आधार — आम आदमी का अधिकार</p>	<p>भारतीय विशिष्ट पहचान प्राधिकरण UNIQUE IDENTIFICATION AUTHORITY OF INDIA</p> <p>पता: श्री-107, विकास विहार, नियर ड्वारका मेट्रो स्टेशन दिल्ली 110078</p> <p>Address: B-107, VKAS VIHAR, Near Dwarka Metro Station Delhi 110078</p>
<p>आधार — आम आदमी का अधिकार</p>	<p>Aadhaar - Aam Aadmi Ka Adhikaar</p>



e-KYC & the Fields Shared

Aadhaar e-KYC Service

Identification

 **999900129017**

Identification

Resident Name	Vinod Kumar
Date of Birth	01-01-1972
Gender	M
Phone No	78389110070
Email Id	vinod.uldal@gmail.com

Identification

Care of		House No	
Landmark		Street	
Locality	Flat no 270 Sec C Pocket C	Post Office	
VTC Name	Vasant Kurj	Sub District	
District	South West Delhi	State	Delhi
		Pincode	110070

PDF Save New e-KYC

Data shared in e-KYC:

1. Name,
2. Gender,
3. DOB,
4. Photo,
5. Address,
6. Mobile No. (if available);
7. e-mail id (if available)

Features of e-KYC

Aadhaar based e-KYC Services provide a platform for verification of Proof of Identity (PoI) and Proof of Address (PoA) in the electronic format using the authentication services provided by UIDAI, with the following features:

- | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">• Compliant with IT Act• Scalable• Eliminates Document Forgery• Paperless• Consent Based | <ul style="list-style-type: none">• Digitally signed by UIDAI and thus non-repudiable• Instantaneous• Machine Readable• Inclusive• Low cost |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



Aadhaar Authentication Enabled Applications

1. Aadhaar Enabled Public distribution system (Andhra Pradesh State/Telangana).
2. MGNREGA & Social Security Pensions.
State wide Implemented (DOP – 12000 + terminals).
– Govt. of Andhra Pradesh and Telangana
Pilot Implementation: in Jharkhand, Haryana, Punjab, Chandigarh
3. Biometric Office Attendance
4. Social Welfare Schemes (Scholarships, Slum Rehabilitation etc)
5. Instant Money Transfer



Q&A

<http://uidai.gov.in/auth.html>



Thank You

