India UID project: An overview

Dhiren Patel
NIT Surat, India
dhiren@coed.svnit.ac.in

India UID Project

Have you got your Aadhaar yet?
Aadhaar is free!

Ease and Mobility

Any Place

Any Network
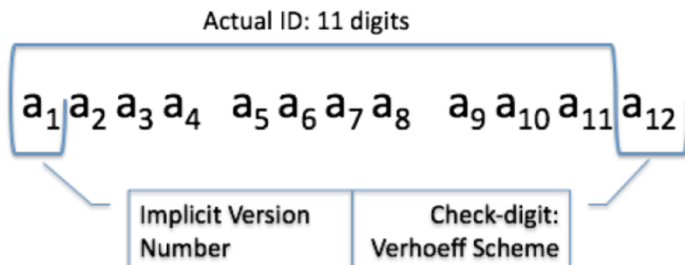
Any Provider

Any Device

Aadhaar UID - LBIMS

- Aadhaar (UID) is a national ID system to improve the efficiency and transparency of various e-Governance initiatives.

- Large scale Biometric Identity Management System

- Large scale (~1.2B subjects, ~4 Trillion transactions/day)

India UID initiative

- Unique ID (UID)
- UID Project Name – Aadhaar <i.e. support>
- Unique Identification Authority of India (UIDAI)
- As India moves towards large scale e-Governance adoption, a soft infrastructure for Government service delivery is needed to ensure efficiency and accountability across multiple systems.

Number Design: 12 Digits

Actual ID: 11 digits

$a_1\ a_2\ a_3\ a_4\quad a_5\ a_6\ a_7\ a_8\quad a_9\ a_{10}\ a_{11}\ a_{12}$

Implicit Version Number

Check-digit: Verhoeff Scheme

Aadhaar Vision (Authentication)

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

> 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'

Why Aadhaar?

- Every time individuals try to access a benefit or service, they must undergo a full cycle of identity verification

- Different service providers have different requirements in the documents they demand, the forms that require filling out, and the information they collect on the individual.

- Such duplication of efforts due to '*identity silos*' increase overall cost of identity verification and cause inconvenience

UID – Core Objectives

- The ID should be available to all residents of the country.

- The system should ensure that each resident gets only one ID, hence making it unique.

- The system should ensure that only the owner of the ID can use the ID to make a transaction.

- The system should be capable of electronically authenticating residents so that the government/private service delivery systems can ascertain identity of their customers.

- Authentication should be available online anytime, anywhere, so that the ID is recognized across the country over networks, thereby improving service delivery.
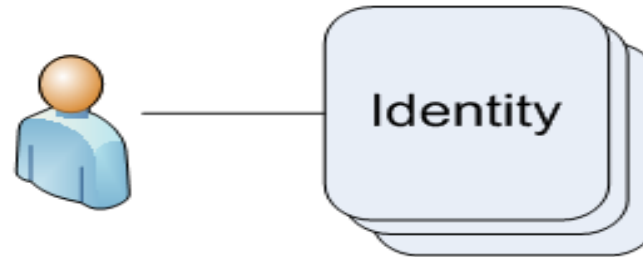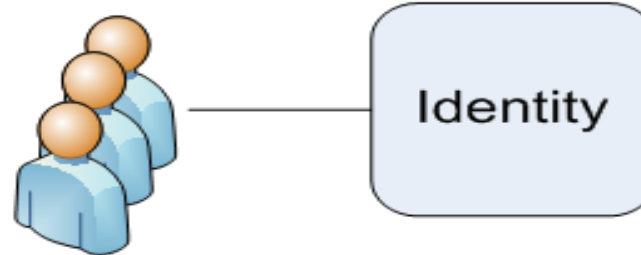
Avoid Fake Identities

One Person – One Identity
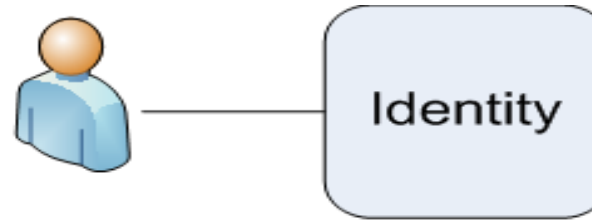
Identity ✔

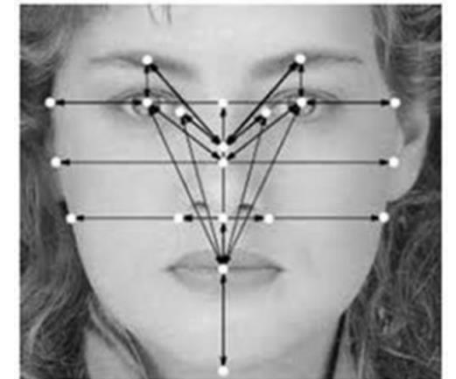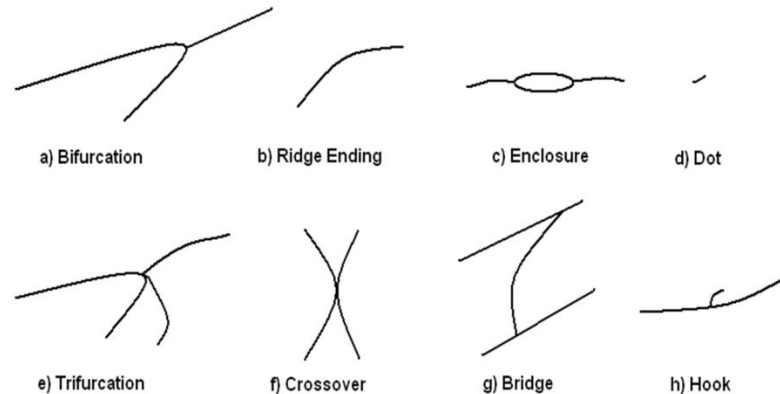One Person – Multiple Identities

Identity ✘

Multiple Persons – One Identity

Identity ✘

- : Identities created using fake documents of subjects that actually do not exist or identities of subjects who no longer exist.

Why Biometric?

- Identity systems that rely only on demographic fields and personal reference checks are vulnerable to forgery, falsification, theft, loss, and other corruption.

- Since biometric markers such as fingerprints, iris patterns etc. are unique to people, they can be used to ensure uniqueness.

a) Bifurcation   b) Ridge Ending   c) Enclosure   d) Dot

e) Trifurcation   f) Crossover   g) Bridge   h) Hook

Purpose

- Aadhaar system is built purely as an *"Identity Platform"*
- an identity infrastructure for delivery of various social welfare programs and for effective targeting of these services
- Aadhaar system has grown in capability, and more than 800 million Aadhaar numbers have been issued so far using the system.

Aadhaar enrolment

seeks the following demographic and biometric information:

1. Name

2. Date of birth (or Age)

3. Gender

4. Address

5. Mobile Number and Email (optional)

6. Ten fingerprints, two iris scans, and photograph

7. For children under five years old, Aadhaar number and name of the guardian (Father/Mother/Guardian)

Process to ensure no duplicates

- Registrars send the applicant's encrypted data packet to the UIDAI data centres for de-duplication.

- Aadhaar enrolment system performs a search on key demographic fields and on the biometrics for each new enrolment, to ensure uniqueness.

- 1:N search

Aadhaar Value Proposition

- **For residents** – Aadhaar system provides a single source of identity verification across the country for its entire population

- **For Governments** - Eliminating duplication under various schemes is expected to save substantial money for the government exchequer.

- It also provides governments with accurate data on beneficiaries, enable direct benefit programs, and allow government departments to coordinate and optimize various schemes.

- **For Service Agencies** – Uniqueness characteristic of Aadhaar number helps agencies such as banks, telecom companies, insurance companies, etc clean out duplicates from their databases, enabling significant efficiencies and cost savings.

Privacy by Design

- The approach of storing intelligence in identification numbers was developed to make filing, manual search and book-keeping easier prior to the advent of computers.

- This is no longer necessary, since centralized database management systems can index the records for rapid search and access without having to section data by location or date of birth.

- Aadhaar number is a random number with no built-in intelligence or profiling information.

- A 12-digit number was chosen based on the identification needs of the population in the next couple of centuries

- Aadhaar authentication only responds with a 'Yes' or 'No' response and no resident data is sent back

Privacy by Design

- **No Pooling of Data**

- It has no linkage information (such as PAN number, Driver's License Number, PDS card number, EPIC number, etc) to any other system.

- This design allows transaction data to reside in specific systems in a federated model.

- This approach allows resident information to stay in distributed fashion across many systems owned by different agencies.

Privacy by Design

- **Yes/No Answer for Authentication**
- it does not provide any scheme to ask questions such as *"what is the address of resident whose Aadhaar number is …?"*
- Aadhaar authentication allows applications to "verify" the identity claim by the resident while servicing them while still protecting their data privacy.
- **Explicit Resident Consented e-KYC**
- For every Aadhaar e-KYC request, only after successful resident authentication, demographic and photo data is shared in electronic format (via biometric/OTP authentication resident explicitly authorizes UIDAI to share electronic version of Aadhaar letter instead of sharing physical photocopies).

Privacy by Design

- **No Transaction History**

- does not have any knowledge of the transaction

- not designed to keep track of specific transaction details such as depositing money or obtaining pension or anything else

Aadhaar Authentication

Any combination of attributes

Demographics
Name, gender, DoB, Age, Address, Mobile, Email, ...

PIN / OTP

1111 2222 3333

Your Aadhaar No.

CIDR
Authentication Servers

Service Provider (Authentication User Agency)

YES
NO

Applications deployed on any device form-factor,
any OS, any programming language, any network

21
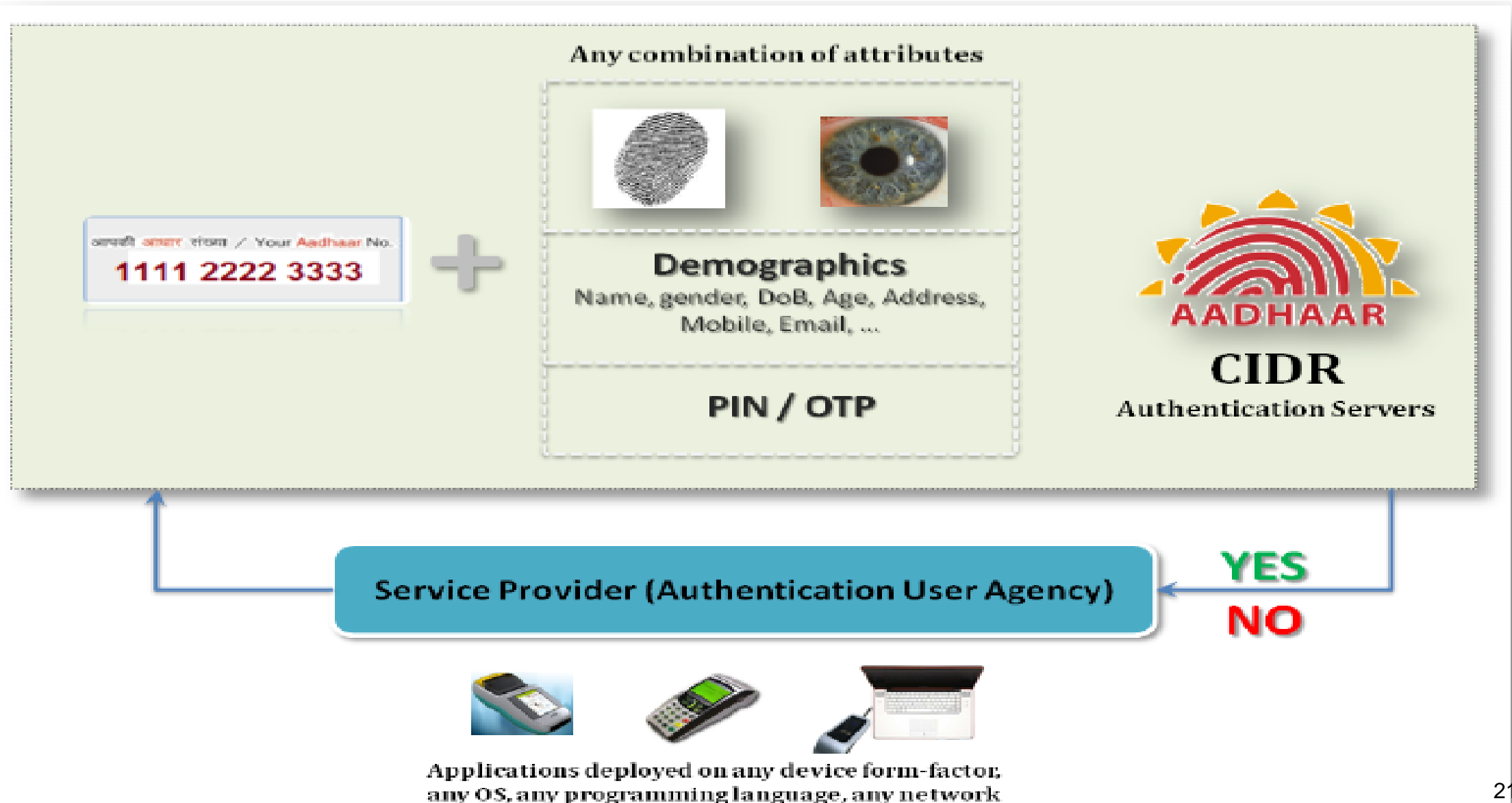
Authentication

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

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

Security connectivity from device to UIDAI data centre

Data audited

Scalable

Authentication data is about 500bytes -2.5Kb

Devices cost comparable to hand held devices

Under 1 sec in CIDR and 4-5 secs round trip

Can handle 100+ million authentication a day

Low cost, universal, easily deployable

Device Challenges, Acquisition Challenges
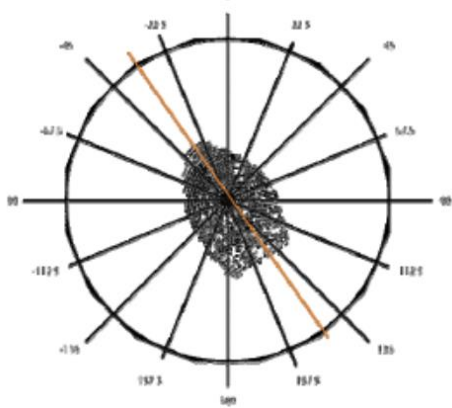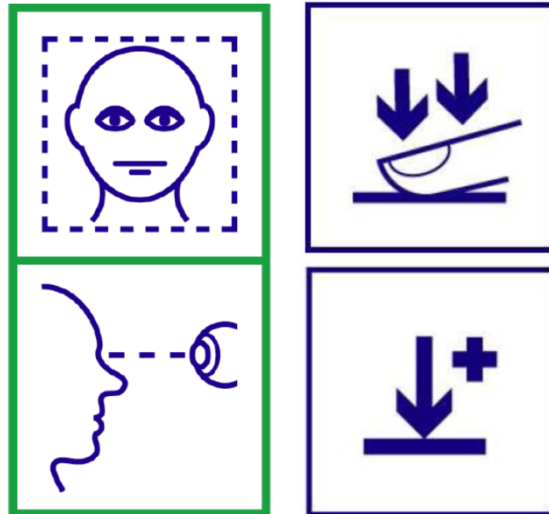
Service Usage Illustrations

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

Service Usage Illustrations

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

Service Usage Illustrations

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

Aadhaar Holders

Residents who have obtained their Aadhaar number

Authentication Devices

Point of initiation of Aadhaar authentication transaction e.g., PCs, kiosks, handheld devices etc

Authentication User Agency (AUA)

Agency that uses Aadhaar authentication to enable its services

Authentication Request

Aadhaar Holder → 1 → Authentication Devices → 2 → AUA → 3 → ASA → 4 → UIDAI's CIDR

Aadhaar Holder ← 7 ← Authentication Devices ← 6 ← AUA ← 5 ← ASA

Yes / No Response

Service Delivery

Necessary Updates & Confirmation
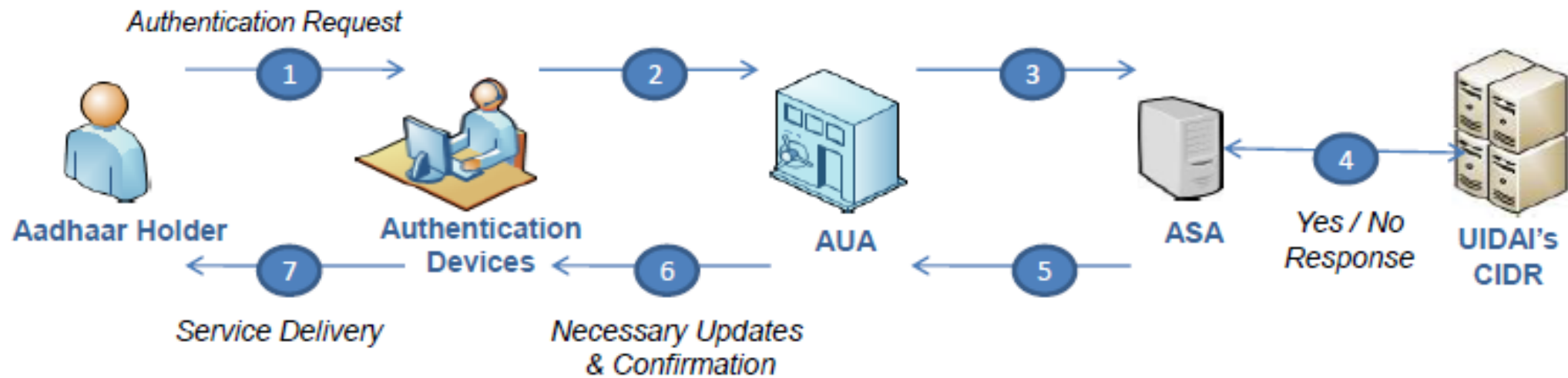
Authentication Service Agency (ASA)

Agency that has secured leased line connectivity with CIDR

Unique Identification Authority of India

Offers online authentication

Sub Auth. User Agency (Sub AUA)

Agencies that access Aadhaar authentication through an existing AUA

Authentication Ecosystem (Overview)
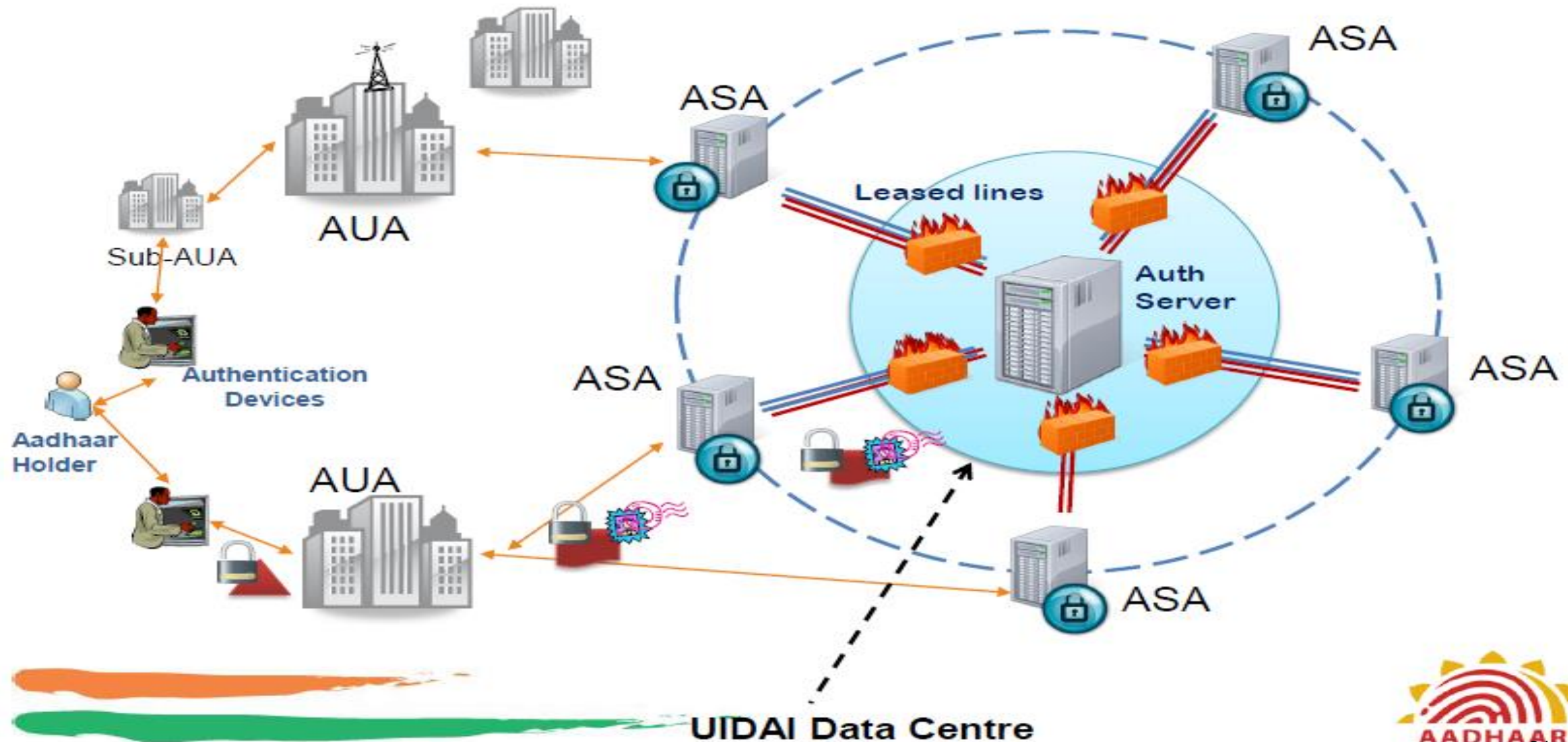
Summary of Authentication User Agencies

Sector	Live/on-boarded	In process	Total
Banking and Financial Services	56	33	89
Central Govt. Departments	6	2	8
State Govt. Departments	12	7	19
Credit Bureaus	1	2	3
Insurance Sector	5	7	12
Telecom Industry	5	3	8
Information Technology	4	13	17
Private sector (new applications)		23	23
Total	89	90	179

Passenger Check in Using Authentication

Systems proposed in each compartment

Passenger Inputs:
1. Seat No
2. Finger Print

N → **Verification by TTE**

- Authentication by UIDAI in first stage.
- TTE checks only passengers not authenticated

Y

Check in Output
1. Last 4 digit of UID
2. Tick /OK

Best Finger Detection
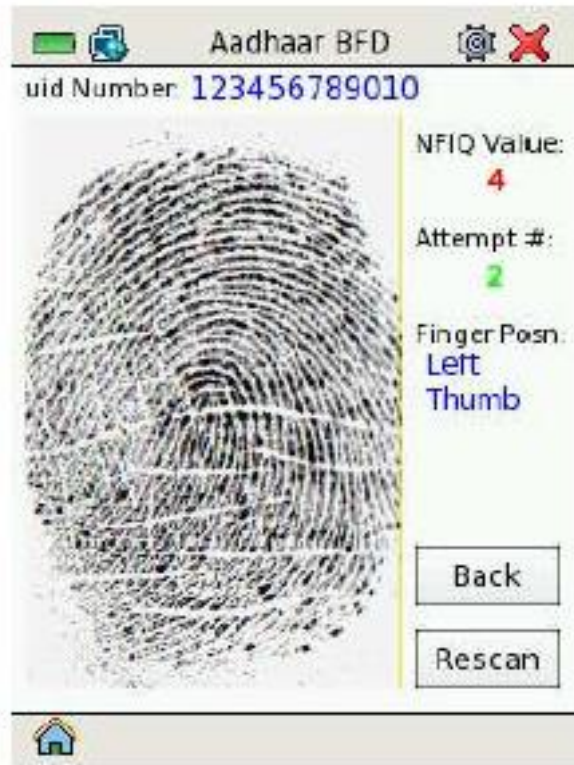
BFD

- Provides consistently higher authentication accuracy
- Improves reliability of authentication
- Reduces attempts to authenticate
- Helps to identify residents who are likely to need two fingers for authentication
- Identify residents who may need to update their biometrics
- Identify residents who may need to use alternate authentication mechanisms due to inherently poor finger quality

Effectiveness of using best fingers

Legend:
- Best Finger Labeled (1:1)
- 2nd Best Finger Labeled (1:1)
- Right Thumb Finger Labeled (1:1)
- Right Index Finger Labeled (1:1)
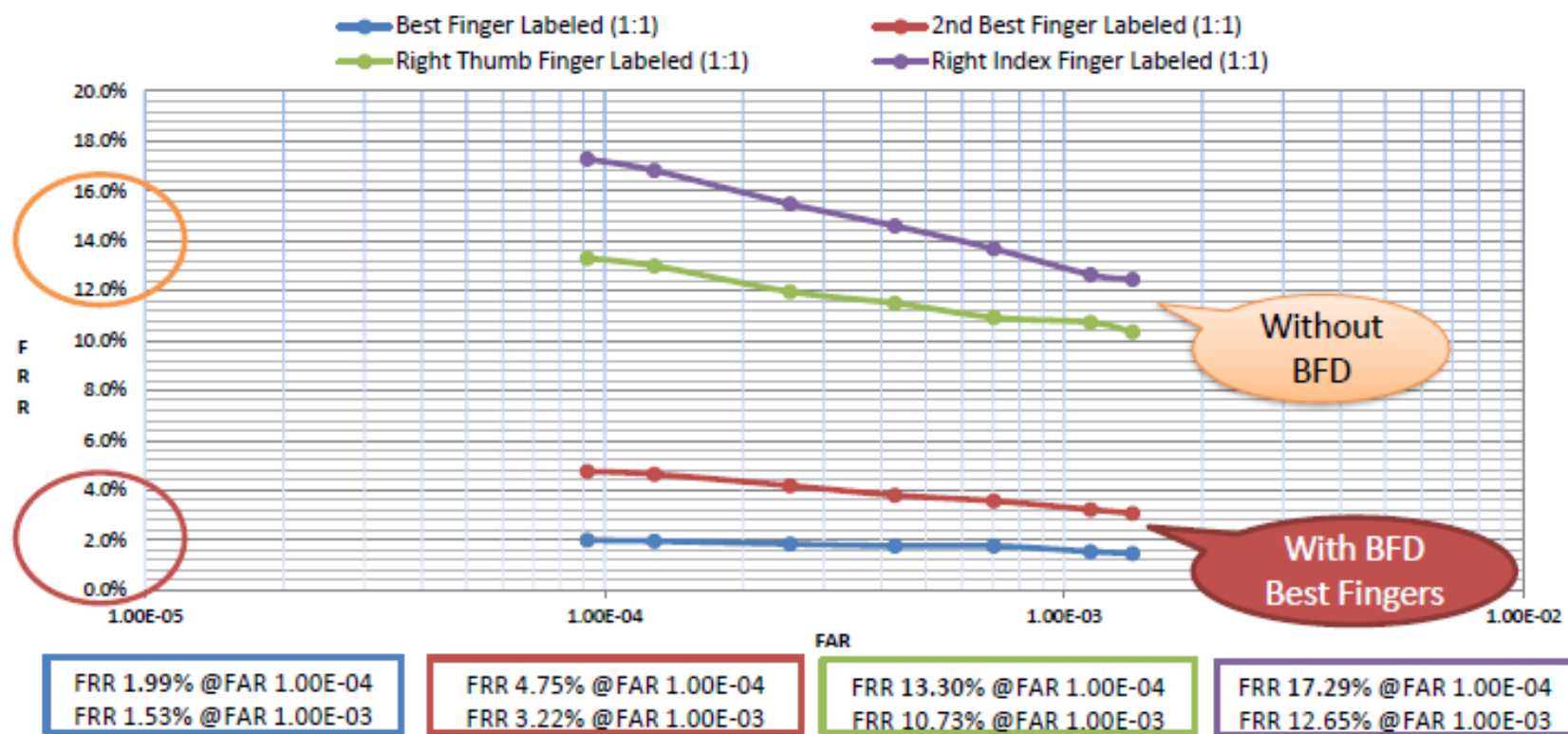
Without BFD

With BFD Best Fingers

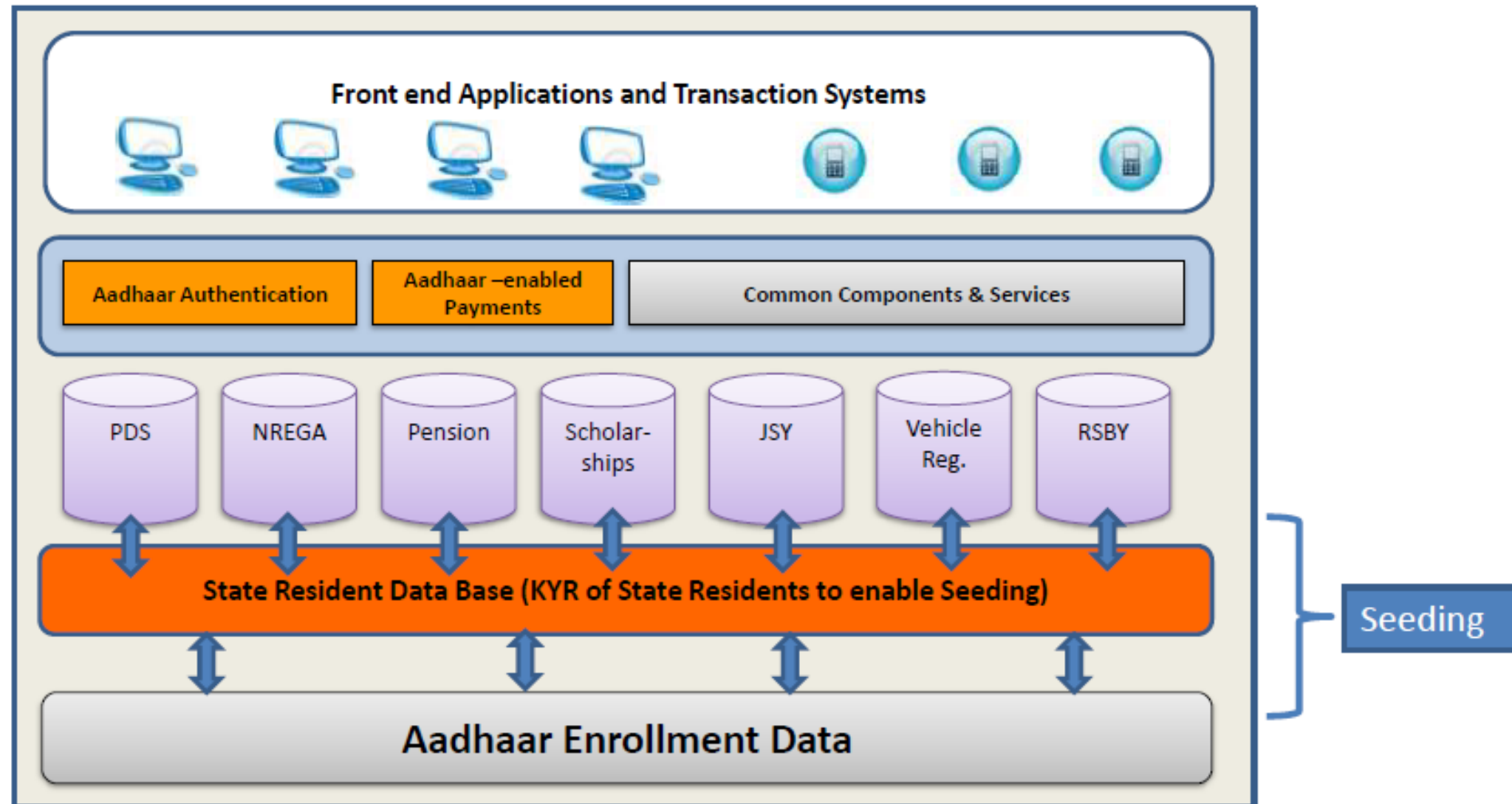| FRR 1.99% @FAR 1.00E-04 | FRR 4.75% @FAR 1.00E-04 | FRR 13.30% @FAR 1.00E-04 | FRR 17.29% @FAR 1.00E-04 |
| FRR 1.53% @FAR 1.00E-03 | FRR 3.22% @FAR 1.00E-03 | FRR 10.73% @FAR 1.00E-03 | FRR 12.65% @FAR 1.00E-03 |

- Slide demonstrates effectiveness of authentication using best finger as compared to using fixed finger(thumb/index for example) during authentication

- Best finger improves accuracy

Aadhaar Enabled Service Delivery

Front end Applications and Transaction Systems

Aadhaar Authentication	Aadhaar –enabled Payments	Common Components & Services

PDS | NREGA | Pension | Scholar-ships | JSY | Vehicle Reg. | RSBY

State Resident Data Base (KYR of State Residents to enable Seeding)

Seeding

Aadhaar Enrollment Data

Overview of Seeding

Seeding Activities

Capture	Validate	Link
Capture UID & Department ID	**Validate** Department KYR against Aadhaar KYR	**Link** Aadhaar in Department data

Accept/Reject Seeding Request

UID No. : 863226320794

Name : **Lalita Devi**

Care Of : W/O Suresh Paswan

Gender : Female

DOB : 1968-01-01

Address : Hazaribagh, Jharkhand

Pincode : 825313

Job Card Number : JH-16-001-020-003/81

Name : **LALITA DEVI**

Care Of : Suresh Paswan

Gender : None

DOB : None

Address : JHUMRA

Pincode : None

PHOTO NOT AVAILABLE

Accept Reject Keep Pending

*KYR = "Know Your Resident" = Name, DoB, Full Address, Gender, Photo

Services

- **Aadhaar Payments Bridge (APB)** – A common infrastructure through which money can be transferred to beneficiaries of various govt. Schemes using just the Aadhaar number and amount

- **Micro-ATM** – A standard handheld device for BC (Business Correspondent) based transactions capable of using UIDAI's authentication system

- **Aadhaar Enabled Payments System (AEPS)** – An inter-operable network using which people can conduct basic banking transactions through BCs by using online biometric authentication of UIDAI

- **E-KYC** – Method through which a resident's electronic Aadhaar document can be instantaneously shared with an agency (by customer consent)

- e-KYC - Only the DEMOGRAPHIC information collected during Aadhaar Enrolment is shared

Roles and Responsibilities

Central/State Government

1. Digitization of Data
2. Aadhaar Seeding with Schemes
3. Educating District/Block/Panchayat Level Officials
4. Preparation of e-Payment Advice
5. Agreement with Banks

Banks

1. Open Aadhaar Enabled Bank Account
2. Link Aadhaar with Account Number
3. Integrate with NPCI
4. Update APB Mapper on periodic basis
4. Define Exception Handling Process
5. Define Escalation Matrix
6. Educate Branch Officials

APB

UIDAI

1. Coordinate with State and Central Registrars for Aadhaar Enrolment
2. Ensure timely generation of Aadhaar Numbers
3. Provide Authentication Infrastructure

Aadhaar Enabled Payment System (AEPS)
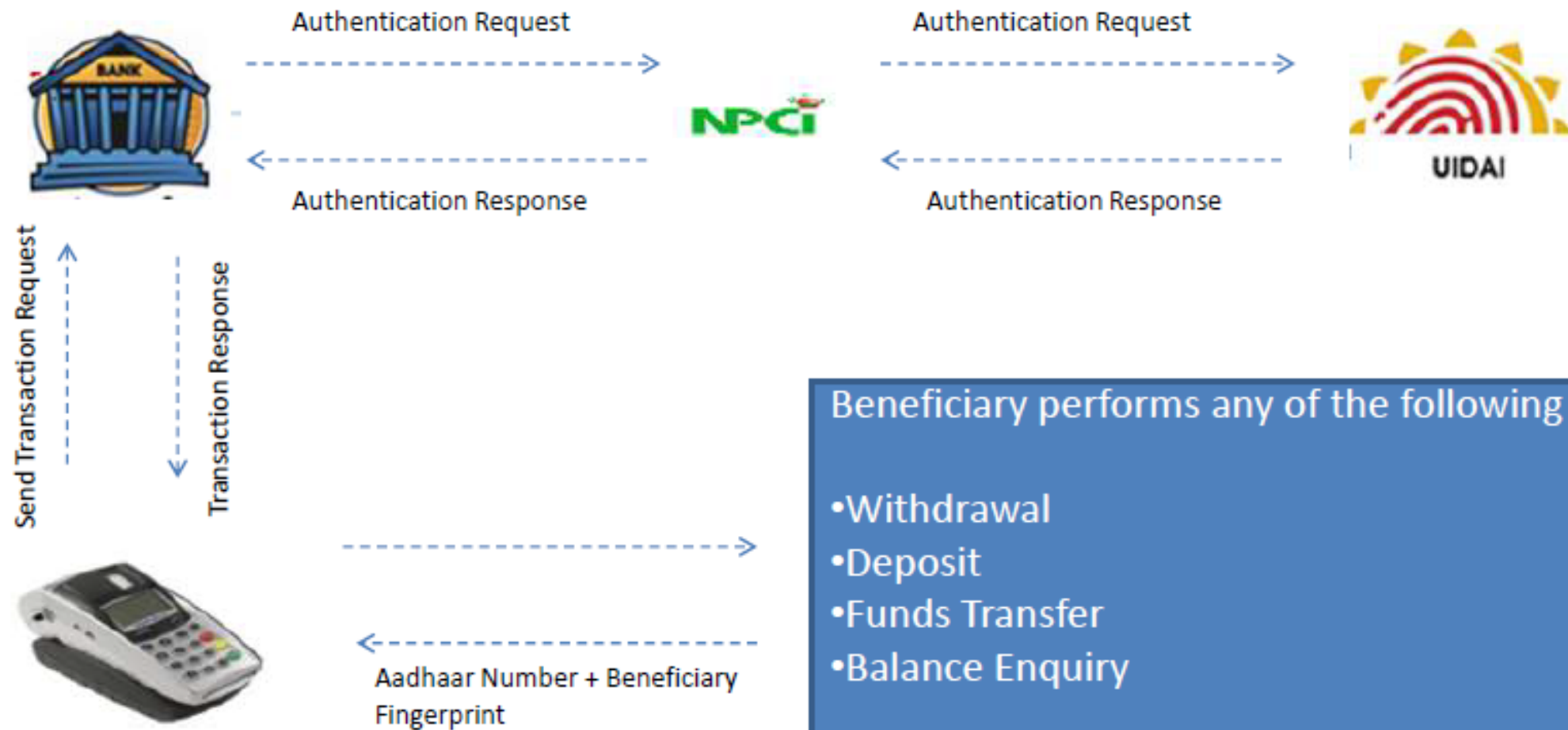
Advantages of AEPS
Aadhaar Enabled Payment System

- Beneficiary can receive money at doorstep

- Inter-operable system thereby ensuring customer is not tied to one bank's BC

- Network of BCs, bank branches and Post Office can leverage a single biometric authentication system accessible through microATMs

- Efficiency in public expenditure as no need for banks to separately capture biometrics and develop their own de-duplication and Authentication systems

Convenient Cash Withdrawal Through AEPS

Beneficiary approaches a BC of any Bank with her Aadhaar number

BC feeds the Aadhaar number, fingerprints and amount in the micro-ATM

Aadhaar server authenticates the ID of the resident.

After successful Aadhaar authentication, beneficiary can carry out the transaction

Aadhaar Payment Bridge

Govt. Department prepares an electronic file containing Aadhaar no and amount

Govt. Department sends the file to the bank where scheme account is maintained

Bank sends to Aadhaar Payments Bridge (APB) (owned and operated by NPCI)

APB routes money to the concerned banks. Banks credit the money in beneficiaries' accounts
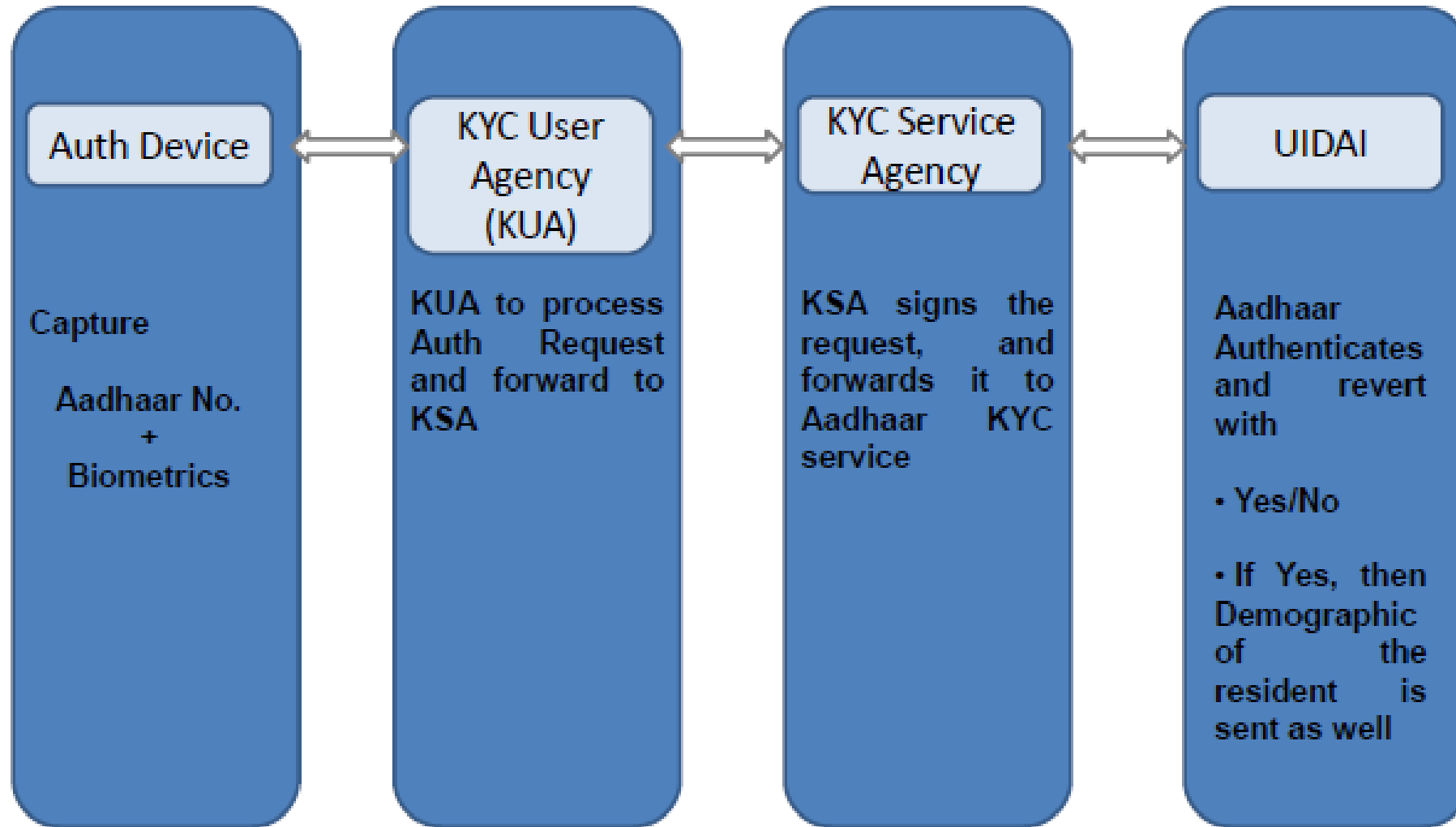
Department can send SMS informing the beneficiary about the money being sent. Banks can also send when the money arrives in the accounts

Advantage of APB to Beneficiaries

- No need to open multiple accounts. Just open one and link it to Aadhaar.

- Residents more comfortable in disclosing only the Aadhaar number to Govt. Agencies (e.g. LPG Dealers) rather than bank account details

- In case of change in bank account, resident does not need to convey account details or change in bank details to each department that he deals with

e-KYC Process

Auth Device	KYC User Agency (KUA)	KYC Service Agency	UIDAI
Capture Aadhaar No. + Biometrics	KUA to process Auth Request and forward to KSA	KSA signs the request, and forwards it to Aadhaar KYC service	Aadhaar Authenticates and revert with • Yes/No • If Yes, then Demographic of the resident is sent as well

e-KYC Use Case (Banks) – New Customer

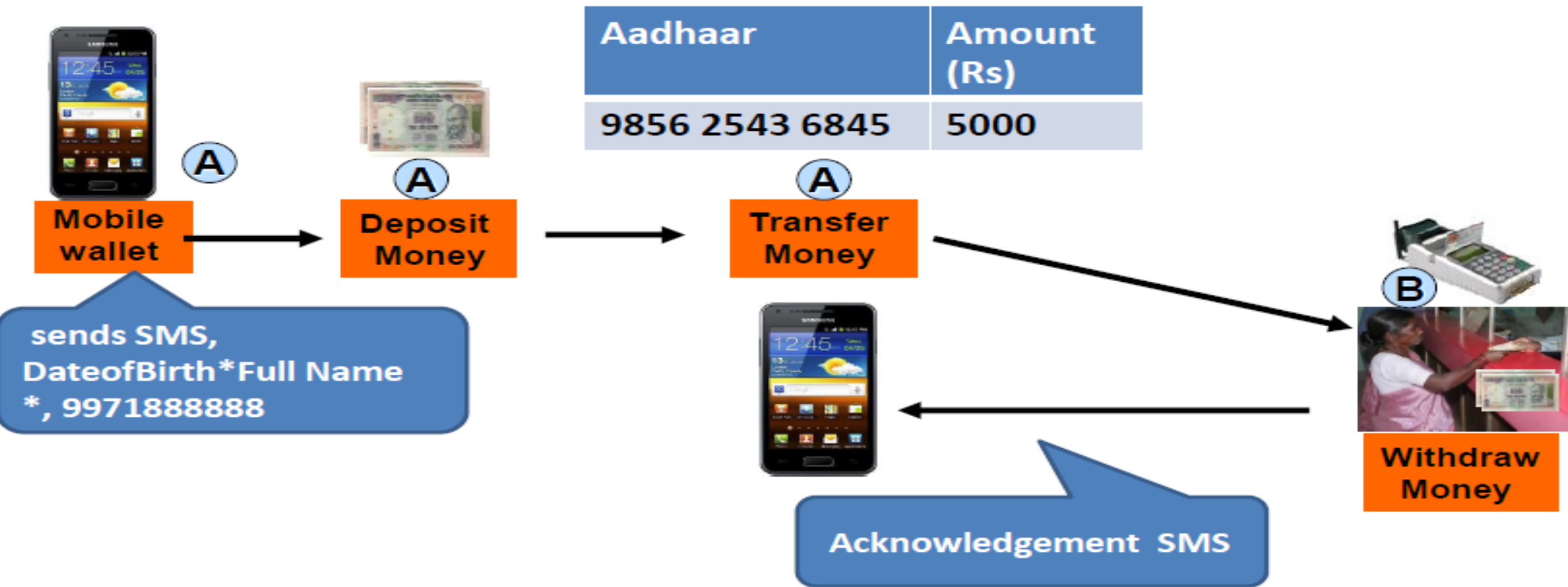Resident visits the Customer Service Point

KUA operator initiates KYC Service using a front-end application (microATM/desktop/etc)

KYC data is returned after successful authentication

KUA stores electronically UIDAI signed data in their database

New account is created at KUA system based on data retrieved from CIDR

Instant Money Transfer

Aadhaar	Amount (Rs)
9856 2543 6845	5000

(A) Mobile wallet → (A) Deposit Money → (A) Transfer Money → (B) Withdraw Money

sends SMS, DateofBirth*Full Name *, 9971888888

Acknowledgement SMS

Aadhaar for NewBorn

- Starting May 2, children born in Haryana state will be concurrently Aadhaar-enrolled and their birth certificate issued within seven days.

- This measure will help monitor delivery of all welfare and health-related benefits to an infant

- Also help in tracking the child from birth to immunization to school admission.

- Besides, it will seek to serve as a data-base of children for timely and assured delivery of services!!!

Jeevan Pramaan - Aadhaar-based Digital Life Certificate

- Aadhaar-based biometric verification system **'Jeevan Pramaan'** enables pensioners to submit a digital life certificate on-line

- a pensioner can now digitally provide proof of his existence to authorities for continuity of pension every year instead of requiring to present himself physically

- sparing the pensioners the trouble of visiting bank or any other pension disbursing agency for submission of life certificates

- It is possible to submit the life certificate from personal computers and laptops or by visiting a conveniently located common service centre

- There are about 5M central govt. pensioners

Aadhaar Authentication Enabled Applications

- **Public distribution system**
- **MGNREGA & Social Security Pensions**
- Mahatma Gandhi National Rural Employment Guarantee Act
- **Attendance Tracking**
- **Social Welfare Schemes (*Scholarships, Slum Rehabilitation etc*)**
- **Property Registration**
- **AEPS for financial transactions**
- Aadhaar Enabled Payment Systems – 40+ Banks
- **Credit Bureaus for De-duplicaton & KYC**
- **Insurance Sector for establishing identity & KYC**
- **Telecom Industry for establishing identity & KYC**
- **Certificate of Liveliness – 5 Million pensioners (retired old people) of India**
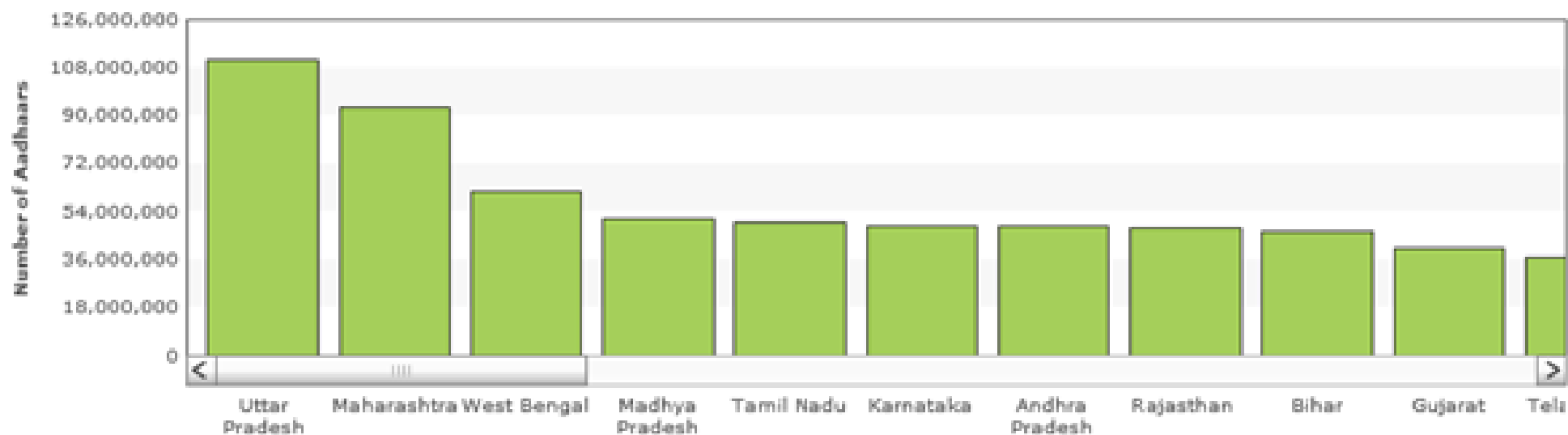
Thank You for your Time and Attention

Dhiren R Patel

Professor & Chair of Computer Engineering Department

NIT Surat, Gujarat, India – 395 007

dhiren29p@gmail.com