Unique Identification Authority of India

Planning Commission

Government of India

Aadhaar Enabled Service Delivery

February, 2012

AADHAAR

Table of Contents

Introduction

Applications that use Aadhaar authentication to identify and authenticate the resident as part of their service delivery are referred to as Aadhaar-enabled applications.

UIDAI offers a range of authentication services that enable a resident to authenticate themselves by providing relevant identity information such as demographics, biometrics, and One Time Pin (OTP). Aadhaar enabled applications primarily use electronic systems to deliver services. These applications are expected to be used in government as well as other sectors.

The draft electronic services delivery bill[1] envisions the migration of manual-based public services to efficient, automated electronic delivery of services over time. Aadhaar enables secure, scalable identity management platform for these electronic services as they get implemented.

Chapter 1 discusses current usage of identity in service delivery, challenges faced and how unique identity can solve them.

Chapter 2 describes how Aadhaar can be leveraged in service delivery, various types of Aadhaar usage and stakeholder benefits.

Chapter 3 provides overview of Aadhaar identity authentication, types of authentication available, factors to be considered for choosing authentication to be used and authentication operating model overview.

Chapter 4 provides details on applications of Aadhaar in specific domains.

Chapters 5 & 6 conclude this document with showing the way forward.

Annexure 1 at the end details out every feature of the authentication service with a brief usage scenario for each.

[1] Draft Electronic Services Delivery Bill: http://www.mit.gov.in/content/draft-esd-bill

List of Abbreviations

Social Programs

IAY	Indira Awaas Yojana
ICDS	Integrated Child Development Services
JSY	Janani Suraksha Yojana
MGNREGA	Mahatma Gandhi National Rural Employment Guarantee Act
NREGS	National Rural Employment Guarantee Scheme
NSAP	National Social Assistance Program
RSBY	Rashtriya Swasthya Bima Yojna
SGSY	Swarnjayanti Gram Swarozgar Yojana
SSA	Sarva Shiksha Abhiyan
TPDS	Targeted Public Distribution System

Financial Inclusion

AEA	Aadhaar-enabled accounts
AEPS	Aadhaar Enabled Payments System
APBS	Aadhaar Payments Bridge System
BC	Business Correspondent
KYC	Know Your Customer
NPCI	National Payments Corporation of India

Authentication

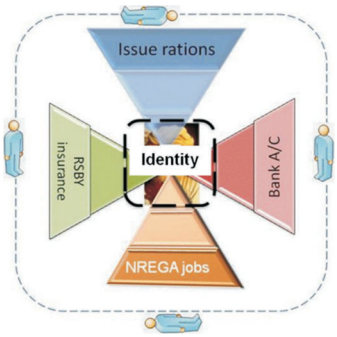
ASA	Authentication Service Agency
AUA	Authentication User Agency
CIDR	Central Identities Data Repository
OTP	One Time Pin

Others

APL	Above Poverty Line
BPL	Below Poverty Line
OMC	Oil Marketing Companies

1. Identity Usage in Service Delivery

From the advent of modern governance and structured commerce, both public and private service agencies across the country typically require proof of identity before providing services to individuals. Every resident in India from rich to poor has to go through identity and service entitlement establishment in day to day life, be it opening a bank account, withdrawing or depositing money, getting a ration card, receiving pension, or during travel.



1.1 What is Identity and How it is Used

For any service agency, establishing both identity and service entitlement of the beneficiary is necessary. Though individual identity should be unique and independent of services availed, entitlement is very specific for the service availed and has to be established by each service agency separately. For example creation of a ration card involves individual identity (name, address) verification and ration entitlement identification (BPL, APL).

Identity establishment typically involves two steps:

a) **Identity Creation –** It is a mechanism of defining an individual's identity by providing identity token(s) to the person in some form (physical and/or electronic). This is typically a onetime activity.

b) **Identity Authentication -** A process of verifying "who an individual claims to be" by checking identity tokens assigned to the individual. This can be manual, electronic or a mix of both.

Types of Identity tokens

An individual identity can be created and authenticated by providing three types of identity tokens:

What the user knows - e.g. user name, password, PIN, secret questions and answers. This can be used for electronic authentication only. It is never used for physical authentication as once it is known to another person; it loses its value for identity verification.

What the user has - e.g. paper ration card, PAN card, NREGS Job Card, access card, ATM card, mobile phone. For this type, authentication can be done electronic and/or manual based on the form of the token. for example – paper ration card, PAN card or NREGS Job card can only be used for manual authentication although ATM card, access card can be used for electronic authentication. This is currently the most common form of identity tokens in India

Who the user is e.g. fingerprint pattern, iris pattern, face pattern, body marks, and voice. For this type, authentication can be both electronic and manual. Though for manual authentication, mostly face image is printed on a card like PAN card.

1.2 Current challenges in Identity Creation and Authentication

In the absence of resident identity creation at national level, service agencies typically follow their own process for identity creation in addition to entitlement identification. The token(s) provided by the service agency to the individuals are used for both identity authentication and entitlement verification.

Challenges faced in Identity Creation

As part of identity creation process, most of the service agencies ask the individuals to furnish physical identity documents or service utilization bills provided by other service agencies like PAN card, passport, driving license, telephone bill etc. This approach results in a situation where certain population has multiple identity tokens though significant portion of population does not have any identity token as they do not avail any of those services. Also only certain identity tokens are accepted as identity proof at national level for example PAN card, passport, and ration card.

This approach for identity creation results in following challenges:

- Creation of multiple identities for the same person due to the lack of ability to uniquely identify an individual.
- Limited or no interoperability as most of the identity tokens are accepted for specific purpose and at specific location.
- Result in leakages of welfare benefits due to creation of large number of duplicate and fake identities within the same benefit program as it is impossible to uniquely identify the individuals.
- Higher risk of resident identity theft and misuse of photocopies of resident identity documents submitted as proofs. Easy to forge physical document based identity.
- Duplication of effort of identity creation in silos by each service agency increases overall cost of identification, and cause extreme inconvenience to the individual.
- Service agencies unable to correlate different benefits given to an individual through various programs resulting in inability to verify correct entitlement and a potentially lower impact of welfare programs.

Challenges faced in Identity authentication

Currently most of the service agencies create physical identity tokens of type **What the user has** like ration card, PAN card, NREGS Job card, pension card etc which can be authenticated manually only.

This authentication mechanism creates following challenges:

- Higher setup cost with limited scalability. It can only work in assisted mode.
- Difficult to identify fake documents and copies.
- Can not verify that the person carrying the identity token is indeed the same person defined in the identity token except where photo is printed on the identity token.

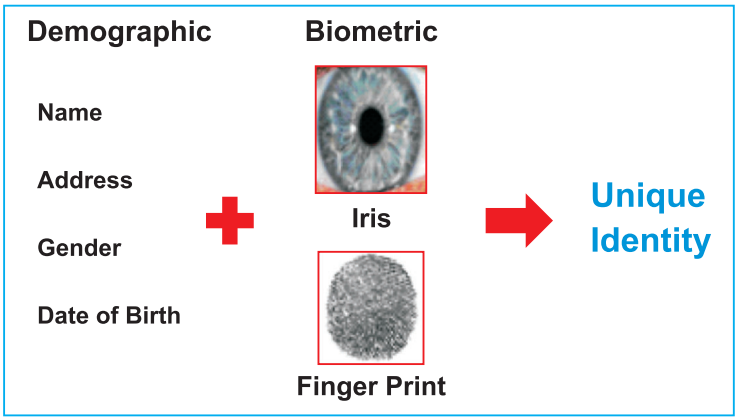
- Difficult to identify misuse. No authentic audit trail and requires exhaustive manual audit mechanism.

Finance industry has addressed manual authentication issues to an extent by adopting web based services and providing electronically authenticable identity tokens like ATM card with PIN, login/passwords, one-time passwords/PINs, credit cards.

1.3 National Unique Identity – Digital and Online Verifiable

Typically an individual identity is defined in terms of demographic attributes namely name, gender, age and address. But demographic data alone cannot guarantee uniqueness. Unique Identity is possible by linking demographic attributes with biometric attributes like fingerprint and iris patterns of the individual.

With recent advancement in technology, it is now possible to create a digital unique identity for an individual in a large population using biometric attributes (fingerprint and iris) which can be verified online. Each unique identity can be assigned multiple identity tokens of various kinds (**What the user knows -** PIN, **What the user has –** mobile/OTP, **Who the user is –** fingerprint, iris) which can be used appropriately for authentication as per the business need of service rendered.



Creation and usage of a national unique identity which is digital and verifiable online, can address the current challenges faced in identity establishment by service agencies. Following are the key benefits:

- Availability of portable (works anywhere in India) identity, verifiable online
- Removal of duplicate and fake identities plugging leakages of welfare benefits.
- Authenticate the individual always as the same and unique person, anywhere and anytime ensuring rightful claimant gets service or benefit.
- Higher scalability of services with online authentication, allowing the service agencies to use multiple channels for service delivery.
- Reduced beneficiary harassment and rent seeking due to reduced dependency on manual processes.
- More efficient service delivery process and reduced cost of identity establishment.
- No need to submit physical copies of identity documents. Reduced risk of identity theft associated with physical documents usage.

- Electronic audit trail can be created allowing service agencies to audit their service delivery process more effectively.

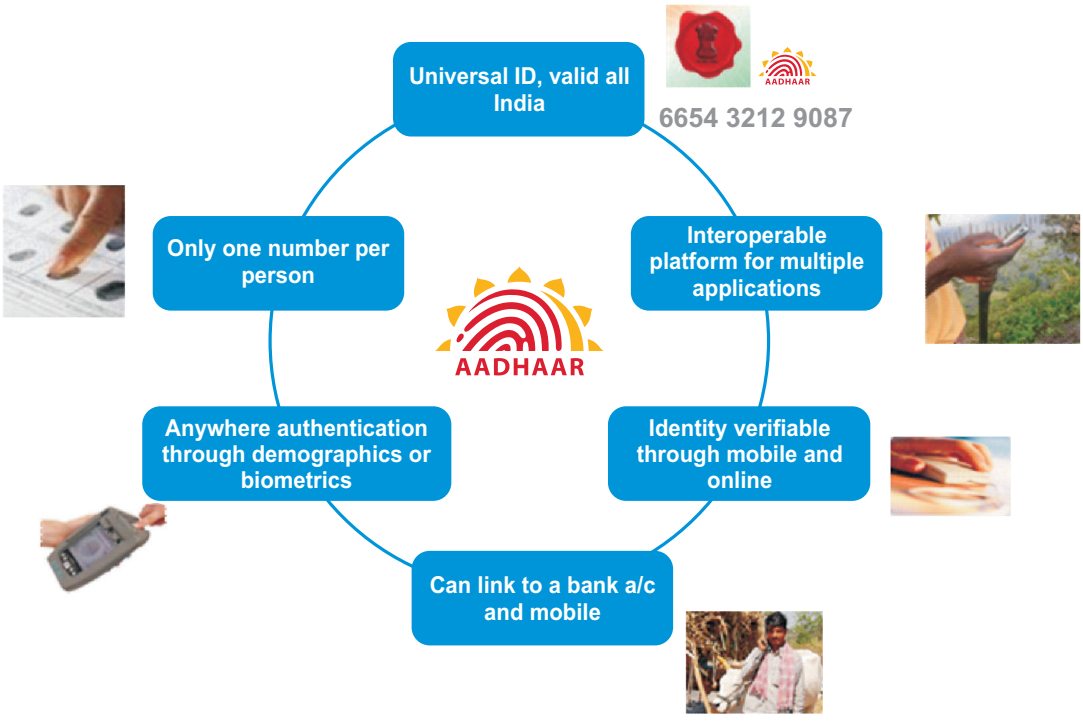
Highly relevant for Indian Context

Going digital and online in Indian context has always proven to increase access, convenience and transparency to the common man. Banking and railway reservation are the best two examples. Banking moved from specific branch only to anywhere banking through any branch, internet, ATM, phone. Similarly people can now reserve rail tickets through various channels (any railway reservation centre, internet, mobile). Though banking, railway reservation and other similar systems have benefited immensely by going digital and online; they still face challenges in proving the unique identity for an individual.

Availability of a unique identity for each resident of India is highly relevant for Indian context today. As discussed above, service agencies are currently facing challenges in terms of service delivery which can be addressed effectively by such an identity. Aadhaar program by providing a national unique identity to each resident which is digital and verifiable online is aiming to achieve that.

In addition, combining Aadhaar with the existing banking industry initiatives (microATM, business correspondent model, mobile banking) not only provides us the opportunity of making financial inclusion a reality but also allows us to potentially convert financial inclusion from social obligation to viable business opportunity.

Aadhaar combined with a bank account and a mobile phone can act as three foundation pillars which can be leveraged by service agencies (public and private alike) to open up new developmental and growth avenues for residents.



2. Leveraging Aadhaar in Service Delivery Applications

The key rationale for Aadhaar is to provide an identity infrastructure for delivery of various social welfare programs and for effective targeting of these services. While welfare is the prime focus of Aadhaar, it can also be utilized by other enterprises and service providers such as banks, telcos and others for improving their service delivery.

The potential of Aadhaar can be realized only upon use of the infrastructure as an ID proof and as a Unique key by various state departments, central ministries, PSU's and private sector entities to provide service delivery to residents in an integrated fashion. The Aadhaar number will also have value for the resident with applications in the ecosystem that leverage the identity authentication and applications therefore form a critical and vital role to Aadhaar's success.

Aadhaar applications are broadly e-Governance or IT initiatives (or sub-modules within those initiatives) within Government, Public Sector and Private Sector that utilize Aadhaar's properties of Unique key and linked ID verification in their service delivery processes. There are many benefits associated with such integration for the various stakeholders that range from better compliance management to significant savings in leakages and increased efficiency and accountability in service delivery.

2.1 Aadhaar Usage Types

Aadhaar and identity authentication can be used by the service delivery provider mainly for the following 3 broad usage types:

Establishing Presence and Proof of Delivery

- *Confirming Beneficiary* – Various social sector programs, where beneficiaries need to be confirmed before delivery of the service, are expected to be the most common users of the authentication service. Examples of some such usages include subsidized food and kerosene delivery to PDS beneficiaries, health service delivery to RSBY beneficiaries, registering job applications by NREGS beneficiaries etc. This usage would ensure that services are delivered to the right beneficiaries.

- *Attendance tracking* – Another key usage of authentication would be attendance tracking for programs such as SSA (for students & teachers), NREGS where wages / outlay is linked to actual number of days the beneficiary reports for the program etc.

- *Financial transactions* – Examples include banks that authenticate a customer using Aadhaar as well as bank-related identity information (account number/user id along with password/OTP, etc.) before enabling banking transactions such as funds transfer, funds withdrawal, etc.

Establishing Know-Your-Customer (KYC) Credentials

- *KYC for various services* – Identity and address verification is a key requirement for enrolling a new customer or opening a new account for an individual. Examples are the issuance of a new

PAN card, telephone connection, bank account or an internet service account for an online business. The service provider in all such cases can verify applicant identity and address using Aadhaar authentication. This is expected to substantially reduce the cost of KYC in providing these services.

- *General PoI* - for standard security related requirements such as entry to airports, hotels etc.; as identity proofs in various examinations (such as medical, engineering entrance etc.) where a large number of cases of impersonation are reported every year. Various internet, social networking and e-commerce related websites could also use Aadhaar Authentication to authenticate customers/ subscribers whenever it is required to establish the real identity of the person who subscribes or does a transaction.
- *Demographic Data and Address verification* – demographic data in service delivery databases may also be verified and this will help database cleansing and management.

As a Unifier for Resident-centric Information

Aadhaar may also be used a common identifier to link related databases. Applications of these can be:

- State view of residents across schemes e.g. number of schemes accessed by resident; potential linkage of JSY, ICDS and SSA to track health and education for every child.
- Healthcare and patient records database (local, regional and national level).
- Credit bureaus for customer rating information.
- National skills registry and enable tracking of individuals through the lifecycle.
- Large entities that need to implement single customer view across services provided such as banks, insurance companies.

2.2 Stakeholder Benefits Analysis

Government (State services)

- Better reach and targeting by ensuring inclusion of those without proper ID proofs.
- Remove duplicates and reduce leakages by linking beneficiary record with Aadhaar and using Aadhaar authentication at the point of delivery. Able to utilize scarce development funds more effectively.
- Reduce cost of service delivery by using direct payment to Aadhaar linked bank account of beneficiaries.
- Enhance accountability and traceability of service delivery to actual beneficiaries.
- Better engagement with residents through self service applications.
- Facilitate direct subsidy transfer to beneficiary accounts using Aadhaar linked bank accounts.
- Aadhaar number and its authentication can become an enabler for providing information to residents on status of service delivery

Industry/Enterprises (Telcos, Banks, Insurance, Oil & Gas companies)

- Lower customer acquisition cost and better compliance using Aadhaar for KYC.
- Reduced transaction fraud by enhancing customer verification using Aadhaar authentication.
- Prevent subsidy leakages and enable direct subsidy transfers using Aadhaar and Aadhaar linked bank accounts.
- Easier to implement single customer view across services using Aadhaar number as linkage.

Residents

- Portable and universal identity, able to authenticate anytime, anywhere.
- Receive full eligible welfare payments directly from the government without any delay.
- Able to conduct financial transactions from any micro ATM near their home using Aadhaar linked bank accounts, allowing residents to save travel time and money.
- Eliminate fraud related to rent seeking by middleman and benefits being siphoned off by an intermediate imposter.

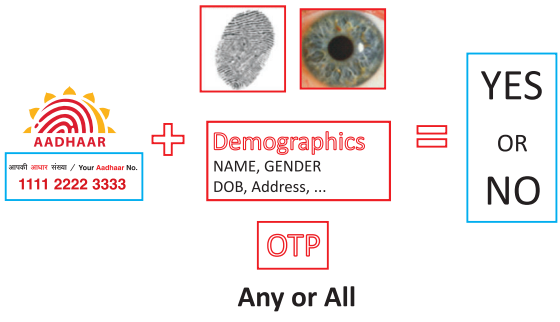
3. Aadhaar Authentication Overview

The purpose of Aadhaar Authentication is to enable Aadhaar-holders to prove their identity digitally and online, and for service providers to confirm the resident's identity claim in order to supply services and give access to benefits.

Aadhaar Authentication is the process wherein, Aadhaar number along with the Aadhaar holder's personal identity data is submitted to the Central Identities Data Repository (CIDR) at UIDAI for matching, following which the CIDR verifies the correctness thereof on the basis of the match with the Aadhaar holder's identity information available with it. The UIDAI confirms either proof of identity or verifies the information provided by the resident. To protect resident's privacy, Aadhaar authentication service responds only with a "yes/no" and no Personal Identity Information is returned as part of the response.

What Aadhaar Authentication Will Do	What Aadhaar Authentication Will Not Do
✓ Authenticate against resident's data in UIDAI's CIDR	✗ Authenticate against data stored on a smart card
✓ Return response to requesting agencies as Yes/No	✗ Return personal identity information of residents
✓ Initiate request over mobile network, landline network and broadband network	✗ Remain restricted to broadband network
✓ Require Aadhaar for every authentication request reducing transaction to 1:1 match	✗ Search for Aadhaar based on details provided requiring 1:N match

3.1 Aadhaar Authentication Offerings Suite



Aadhaar is meant to empower residents to prove their identity anywhere, anytime and in multiple modes. As a result, UIDAI shall provide multiple ways of authentication which may be used for delivery of any service oriented purposes. A service provider can choose either single-factor or multi-factor authentication. The Aadhaar number itself alone shall not be a factor for Authentication. Aadhaar number along with demographic attributes like the name/address, or OTP, or single/multiple biometrics (fingerprint, iris etc.) may be used to provide single factor authentication or these attributes may be used in combination (multi-factor) to achieve the required authentication needs.

Authentication Offering	Authentication Attributes	Indicative Usage
Type 1 – Demographic	Any single/combination of the following attributes can be used 1. Name 2. Address 3. Date of Birth / Age 4. Gender 5. Mobile, Email	Periodic basis to check validity of the credentials or for cleaning up the service provider database by removing duplicates. Agencies can also use demographic authentication for identifying beneficiaries/ customers/subscribers prior to any transactions.
Type 2 – OTP	One-time-pin. This is delivered to a mobile or email address on request initiated by a resident or an application.	May be used for authenticating residents for internet and mobile transactions as well as in cases where deployment of biometric technology is difficult or not practical
Type 3 – Biometric	Fingerprint/ Iris Biometrics. Requires residence to be present and provide fingerprint/iris capture on a device.	Where biometric authentication is considered essential such as KYC, financial transactions, attendance tracking etc.
Type 4 – Multi-factor	1. Either of Fingerprint or Iris and 2. OTP/ Mobile	Multi-factor authentication used for greater assurance
Type 5 – Multi-factor	1. Fingerprint and 2. IRIS and 3. OTP/ Mobile	Multi-factor authentication used for greater assurance

3.2 Choosing an Authentication Type

The decision to opt for a suitable authentication type such as single-factor or multi-factor authentication rests with the Service Provider. The multi-factor authentication may comprise both factors from UIDAI OR one factor from UIDAI and second factor from another entity including itself. For example, a bank may choose biometric + OTP as authentication factors from UIDAI. Another bank may choose biometric authentication from UIDAI & ATM card/OTP issued by the bank itself (example of federated model).

While Type 1 Authentication is based on demographic attributes, Types 2, 3, 4 and 5 provide additional factors such as biometric and/or OTP. In general, a biometric/ OTP based authentication offers a higher degree of authentication assurance than a demographic authentication system.

A demographic authentication indicates less certainty in an identity claim; while a biometric authentication indicates presence of that individual and OTP establishes presence of the mobile registered by the resident (notice that mobile can be shared among people in family, etc.). Authentication based on demographic attributes does not guarantee "proof of presence" and hence, is associated with a lower level of assurance when compared to authentication based on biometric attributes. The assurance potentially increases as different biometric modalities such as Fingerprints and Iris are introduced for authentication.

The concerned user entity shall assess the selection of appropriate authentication factors based on:

- Convenience and interests of the resident.
- Risks/impact of inaccurate authentication on the business transaction e.g. financial transactions may require stronger authentication factors.
- Relevant risks associated with an inaccurate authentication in terms of inconvenience and distress to resident, financial loss to resident, impact on business, information security and threat to national security.
- Cost and logistics of implementing a certain type of auth (e.g. biometric will require investment in devices and resident presence while OTP requires residents to have a mobile phone).
- Volume of authentications based on number of beneficiaries and frequency of authentication required e.g. stronger assurance level may be appropriate for KYC purpose of one time account opening / service issuance versus a lower assurance requirement for frequent transactions such as delivery of services.
- If the Provider has a large number of beneficiaries and needs to deliver services to a large population, the provider may not select a high or very high level of assurance, especially in cases where there limited liability or risk with a false acceptance. This shall reduce the turnaround time taken to deliver services to residents, which is critical in reducing the inconvenience and waiting time in queue for the resident.
- In cases where there is higher risk of identity misuse, multi-factor authentication may be considered to eliminate occurrence of such instances.

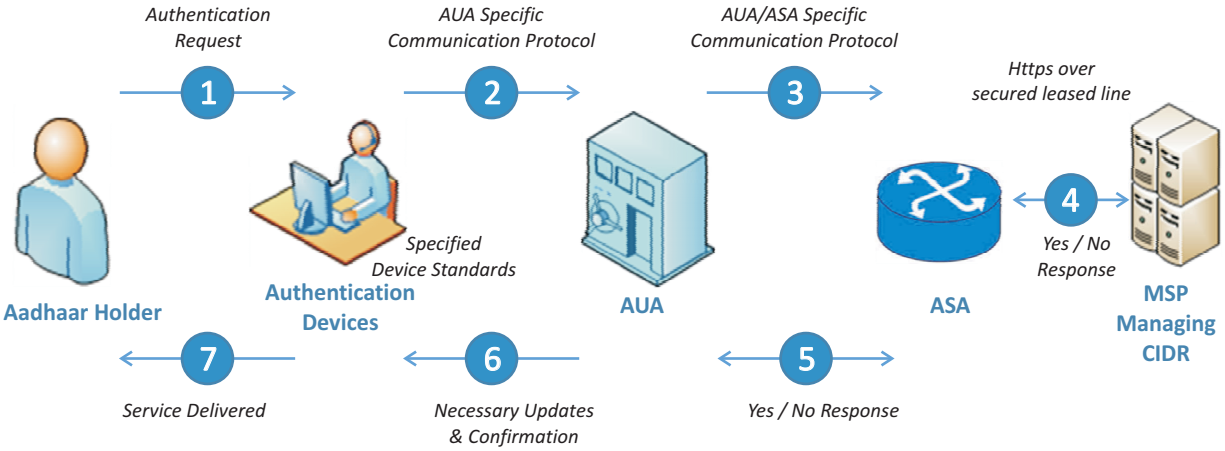
3.3 Authentication Features at a Glance

Aadhaar authentication allows user agencies to take advantage of many features exposed through the Application Programming Interface (API) specifications. Features such as name and address matching, use of biometrics and OTP, security across the system, features within the Aadhaar Authentication response to ensure non-repudiation and ability to audit/verify, etc. are provided through the API.

Annexure 1 of this document explains such features in detail along with use cases and scenarios.

3.4 Aadhaar Authentication Operating Model

Any agency that would like to utilize Aadhaar Authentication to enable its services will need to sign up as an 'Authentication User Agency' (AUA) and enter into an agreement with UIDAI. An AUA can use Aadhaar authentication to enable one or more of their services. The AUA in turn will need to engage with an 'Authentication Service Agency' (ASA). ASA is an agency that has established secure leased line connectivity to the Central Information Data Repository (CIDR) at UIDAI to transmit authentication request on behalf of AUAs and receive response back from CIDR. ASAs build and maintain their secure connectivity to CIDR in compliance with the standards and specifications set by UIDAI. An AUA has the option of connecting to the CIDR by itself or through an existing ASA. Further, an agency desiring to use Aadhaar authentication could choose to become an AUA or it could choose to access Aadhaar authentication services through an existing AUA. In the latter case, it becomes a sub AUA of the existing AUA which it engages. An overview of the operating model and the transaction process flow is illustrated below:



4. Application of Aadhaar across Domains

Aadhaar can be leveraged effectively across industry domains for improving service delivery to the residents irrespective of service being delivered by government, public sector or private sector. Aadhaar is an IT enabled identity solution which needs to be leveraged appropriately by service agencies along with required business re-engineering and computerization of their services through e-Governance and ICT initiatives.

Subsequent sections in this chapter cover high level usage scenarios of Aadhaar authentication within the following domains:

- Government Welfare Programs
- Fin ancial Inclusion and Electronic Payments
- LPG Distribution and Subsidy Management
- Telecom
- Internet and E-Commerce
- Aadhaar As Unifier

4.1 Aadhaar and Government Welfare Programs

Indian government has been investing large amount of funds in multiple welfare programs to cover under privileged and marginalized families; and helping them to be part of Indian growth and mainstream economy.

The welfare schemes are of three types:

a) ***Direct cash:*** This category includes schemes like NREGS, NSAP where cash is paid directly to the beneficiary. These can be classified as follows:

- In *Direct Cash Transfers,* money is either delivered directly to the beneficiary or transferred into the individual's bank account like social pensions. It carries no conditions after beneficiaries are identified.
- In *Conditional Cash Transfers,* transfers are made conditional on the achievement of certain social or development objectives like Janani Suraksha Yojana. In these programs, beneficiaries must fulfill certain conditions to receive the cash.

b) ***Subsidies:*** It includes schemes where the benefit is passed on to consumers in the form of subsidies. For example, Targeted Public Distribution System (TPDS).

c) ***Services to individuals:*** It includes schemes that involve payments to service providers providing supplies and services to consumers like Sarva Shiksha Abhiyan (SSA) program which promotes universal primary education for children; program covers funding for school infrastructure, teacher salaries, books, and uniforms.

The welfare programs of India are large, complex systems with millions of beneficiaries depending on these programs and they may not have full impact as a result of delays, leakages and other inefficiencies. Sections below will discuss the potential Aadhaar interventions in welfare programs and how they can enhance the effectiveness of the programs.

Use of Aadhaar in Beneficiary identification

Majority of welfare programs use physical identity documents and rely on manual processes for beneficiary identification. These practices results in following issues:

- Lack of identity documents prevent poor and marginalised residents from accessing the benefits program.
- Existence of duplicate and fake beneficiaries.
- Residents may avail of benefits from multiple programs simultaneously when they may not be entitled to. For example a resident can only avail one of the pensions like old age pension, widow pension, handicapped pension.

Use of Aadhaar to link beneficiaries with their Aadhaar numbers in Beneficiary identification and approval process can address these issues. Applicant provides his/her Aadhaar number as part of the application which is saved in welfare program database along with other application data. In addition, applicant authenticates his/her Aadhaar number through any chosen method (possibly fingerprint biometric) to confirm. The applicant name, address and date of birth provided in the application may also be verified against Aadhaar record with UIDAI through demographic authentication. As part of beneficiary approval step, the applicant's Aadhaar number is matched against existing beneficiaries to ensure that the applicant is not an existing beneficiary. Matching the applicant against national level beneficiary database will help to remove all the duplicates at national level.

By removing duplicate and fake beneficiaries, welfare programs can utilize scarce development funds more effectively. In addition the proposed intervention provides quick and reliable electronic verification for applicant name, address and date of birth; an easier and convenient way for applicants to prove their identity. It reduces dependency on document based proofs and facilitates faster application processing. If Aadhaar is adopted by all welfare programs, it will also allow the verification of beneficiary across different programs in case resident is not allowed to avail certain benefits simultaneously.

Verification of beneficiary presence

Many welfare programs require the verification of beneficiary presence in different context. Some of the scenarios are as follows:

a) For certain welfare programs like pension, once the payments have started for a beneficiary, it is very important to verify regularly the existence of the beneficiary as the benefit needs to be stopped in the event of beneficiary death.

b) For subsidy based welfare programs like TPDS, LPG, it is important to ascertain the person receiving the benefit is indeed the intended beneficiary

c) For conditional cash transfer based programs like NREGS or Janani Suraksha Yojana, it is important to verify the attendance of the beneficiary on the expected work site or benefit center.

d) Services to Individual based welfare programs like Sarva Shiksha Abhiyan needs the attendance and verification of actual recipients of service as basis for payments to the vendor providing the services.

Biometric based Aadhaar authentication can be leveraged to achieve this verification for all scenarios as it confirms the presence and existence of the person. Based on the program requirement, Aadhaar authentication can be implemented at the time of service delivery (e.g. TDPS), work site (e.g. NREGS) or beneficiary can be asked to come to a designated location for authentication at regular interval.

The proposed intervention eliminates fraudulent transactions and incorrect reporting of the work done. In addition for programs like pension, it ensures that benefits are not siphoned by others in the event of beneficiary's death. In programs like NREGS; implementation of beneficiary authentication at work site along with direct payments to Aadhaar linked accounts will allow the intended beneficiaries to receive full benefits as per the work done by them.

Cash based payments to Aadhaar linked accounts

Many of the direct cash transfer schemes such as pension, scholarships follow manual process of payment transfer to beneficiaries, which can be time consuming and sometimes error prone. For the last mile, different methods are used for transferring the cash including cash payment to the beneficiary and money order through India Post. This results in high processing costs and delays in disbursal of cash benefits. In addition, many times benefits never reach the actual beneficiary and are wrongfully availed by another individual or siphoned off by an intermediary. On the other hand, for subsidy based services like TPDS, movement of goods such as grains, kerosene etc at subsidized prices provides incentive for intermediaries for diversion of goods and services, and intended beneficiary is impacted.

Direct cash transfer schemes can leverage Aadhaar by transferring payments electronically into Aadhaar linked bank account of the beneficiary using Aadhaar Payments Bridge (APB). APB is an electronic benefit transfer system; being built by National Payments Corporation of India (NPCI) to enable direct transfer of entitlements provided by various government departments to Aadhaar linked bank accounts of beneficiaries in any bank.

The program can collect Aadhaar linked bank account information for all the beneficiaries. And for every payment release cycle, welfare department can send batch file containing Aadhaar number, bank

and payment information for each beneficiary to their sponsor bank. On receipt of data, sponsor bank transfer funds to beneficiary Aadhaar linked bank accounts through APB.

Use of Aadhaar linked bank account for direct payment coupled with linking of beneficiary with Aadhaar number ensures that payment is not transferred to a non beneficiary account or siphoned off by an intermediate imposter. Beneficiaries receive the full benefits without any delay to their account. In addition Aadhaar-enabled account can be used by resident to receive multiple welfare payments as opposed to one-scheme, one-bank approach followed by a number of welfare programs today. Direct payment to Aadhaar linked bank account will result in substantial saving of effort, time and cost for government. In addition it will give full traceability, audit, and non-repudiation for fund flow from the government to the beneficiaries.

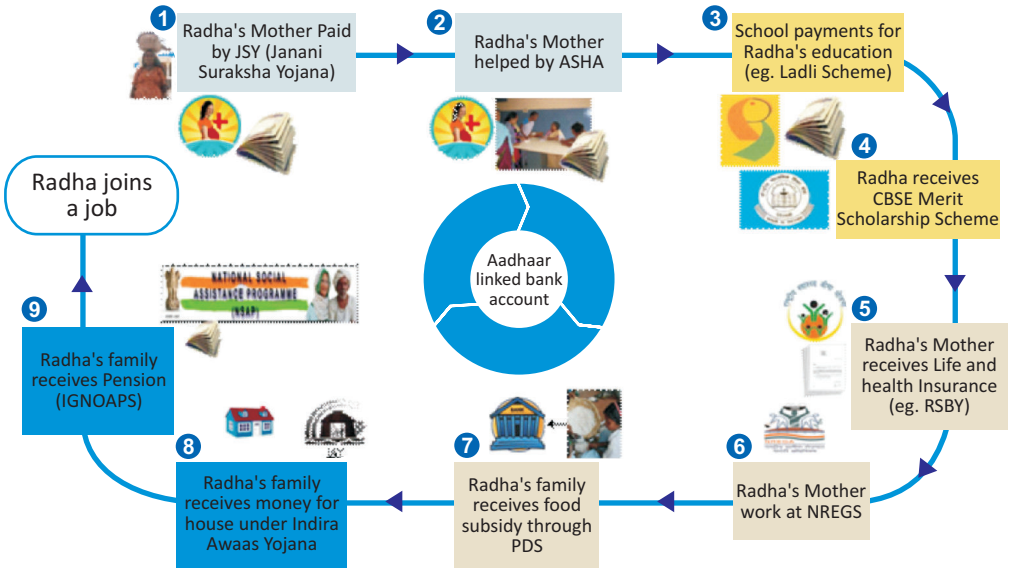
Subsidy based programs can also leverage Aadhaar linked bank accounts to transfer subsidy directly to the beneficiary while allowing beneficiary to buy goods at market price. This will remove the incentive for the intermediaries to divert goods.

Aadhaar authentication based micro ATMs for Funds withdrawal

With cash based payment directly transferred to beneficiary Aadhaar linked bank account, it is very important that beneficiaries are able to withdraw money from the account easily without requiring them to travel long distances. In addition, deposit of funds into the account should be regarded as welfare program payment disbursal and the beneficiaries should be allowed to keep the funds in their accounts. An interoperable payment solution has been discussed in the "Financial Inclusion and Electronic Payments" section below using Aadhaar, BC network and microATMs to enable access to banking for every resident near their location With the ability to withdraw funds near their home, beneficiaries do not have to travel to a distant bank branch saving transportation cost and work day loss. It also eliminates rent-seeking by middleman during disbursal

Summary

The Aadhaar interventions facilitate all three: *Access to Eligible Benefits, Access to Full Benefits, Access to Benefits when it is Due.* They increase the impact of existing welfare programs manifolds.



Imagine Radha and her mother, a BPL family, able to access all the cash and subsidy benefits available to them at the various stages and events of their life. The ability to avail all the eligible cash and subsidy benefits in full value at the time of need will provide Radha and her parents a great opportunity to come out of the poverty cycle. This is possible with Aadhaar enabled welfare programs.

4.2 Aadhaar in Financial Inclusion & Electronic Payments

Access to finance has remained scarce in India especially for the marginalized sections of society. This exclusion is debilitating. Economic opportunity is after all, intertwined with financial access. Such financial access is especially valuable for the poor—it offers a cushion to a group whose incomes are often volatile and small. However due to the lack of access to financial services, many of the India's poor face difficulties in accumulating savings.

To mitigate the lack of financial access in India, the regulator has focused on improving the reach of financial services in new and innovative ways — through no-frills accounts, the liberalization of banking and ATM policies, and branchless banking with business correspondents (BCs), which enables local intermediaries such as self-help groups and kirana stores to provide banking services. Related efforts have also included the promotion of core-banking solutions in Regional Rural Banks; and the incorporation of the National Payment Corporation of India (NPCI) to provide a national infrastructure for payments and settlements in the country.

UIDAI's goal of issuing a unique 12 digit number to the residents of India coupled with its online authentication services provides a unique opportunity to the financial sector and to the Government to reduce transaction costs and implement an electronic payments platform.

Aadhaar for Identification (Know Your Customer- KYC)

Aadhaar eases access to banking, insurance and securities market as it has been recognized as a valid document under KYC guidelines. Significant progress made in acceptance of Aadhaar as KYC:

- The Ministry of Finance has amended Prevention of Money Laundering Rules to recognize Aadhaar as an "officially valid" KYC document.
- The Reserve Bank of India has issued a notification (dated September 28, 2011) recognizing Aadhaar as a valid document for opening bank accounts.
- Insurance Regulatory and Development Authority (IRDA) and Securities and Exchanges Board of India (SEBI) have notified Aadhaar as a valid KYC document for insurance and securities markets respectively.

Aadhaar also provides a one of its kind opportunity for financial service providers to ride on the platform and reach the masses at minimal cost. In order to reduce the customer acquisition costs for the banking system and enable easy access to the hitherto financially excluded sections of the society, UIDAI has partnered with banks for opening of bank accounts during Aadhaar enrolment.

Aadhaar as a Financial Address

The ability of Aadhaar to uniquely identify an individual electronically makes it a valuable tool in administration of Government schemes and benefits, and a natural financial address on the basis of which funds can be transferred directly into a beneficiaries linked account.

Aadhaar as a financial address ensure that residents have mobility for access to financial services for the purpose of receiving Aadhaar-addressed payments as the beneficiaries could be authenticated from anywhere in the country. The beneficiary can link their Aadhaar number to their bank account to receive the payments seamlessly and would also have the option of changing this at any point in time.

Aadhaar Authentication for Financial Transactions

Aadhaar authentication can be used by the financial sector for verifying the customer identity for financial transactions. It can be done through any of the delivery channels e.g. branch, ATMs, Internet, mobile and microATMs. Appropriate authentication mode (biometric, OTP) can be used by the financial institute as per their business need.

Aadhaar - a platform approach to financial sector

Aadhaar offers a platform approach to financial sector by providing standardized:

- Electronic KYC platform (AEA)
- Payments Mechanism to Government Departments (APBS)
- Devices and Standardized consumer experience (AEPS & Remittances)

Aadhaar Enabled Accounts (AEA)

- Electronic opening of accounts at the time of Aadhaar enrolment in partnership with banks through an electronic process.
- Linking of Aadhaar to the existing bank accounts through any of the delivery channels e.g. branch, ATMs, Internet, mobile and microATMs.

Aadhaar Payments Bridge System (APBS)

- Easy to use mechanism for electronic credit of government welfare and subsidy payments on the basis of Aadhaar numbers as unique identifier.
- Provides end-to-end visibility of transactions to government ministries/departments.
- Ensures no duplicates/fakes exist in the system thereby reducing leakages in government spending.

Aadhaar Enabled Payments System (AEPS) and MicroATM

- Aadhaar Enabled Payments System (AEPS) is a payment mechanism that uses online Aadhaar authentication for customer identification.
- The online, inter-operable architecture of AEPS allows a resident to access his account from anywhere in the country and in the near future through any delivery channel e.g. ATMs, microATMs etc. unlike the current BC models.

- MicroATMs are standardized devices where residents can conduct basic financial transactions (Credit, Debit, Balance Enquiry, Remittances etc.) in assisted mode e.g. BCs.

Remittances

- The interoperable architecture of AEPS and microATMs enables online and real-time fund transfer across banks thus enabling an efficient and cost-effective remittance ecosystem.

Aadhaar Enabled Accounts (AEA) - Linking or Electronic Opening of Accounts

In order to facilitate disbursements, remittances or any financial transaction, a resident is required to link their Aadhaar number with his/her bank account number. A resident has the following options: (1) Link their existing bank account or (2) Open a new bank account.

Linking Bank Accounts

Aadhaar enrolment process provides an option to the resident to link his existing bank account. If the resident chooses to link his account at the time of enrolment, he must provide Account Number and Bank Branch Particulars. UIDAI has devised a mechanism wherein the captured data is electronically transferred to empanelled banks through a secure mechanism after obtaining residents' consent.

Opening Bank Accounts

UIDAI offers the choice of opening of bank accounts for residents at the time of Aadhaar enrollment. If the resident provides consent, their information is sent electronically to the bank of choice for opening the account. UIDAI has already partnered with 64 banks for the purpose of account opening.

Aadhaar Payments Bridge System (APBS)

The Aadhaar Payments Bridge System (APBS) offers a simplified payment mechanism to Government user departments to electronically transfer subsidies and benefit payments to individuals on the basis of their Aadhaar number. APBS enables payments to be credited to end beneficiaries' Aadhaar-enabled accounts (AEA) on the basis of Aadhaar number being unique identifier.

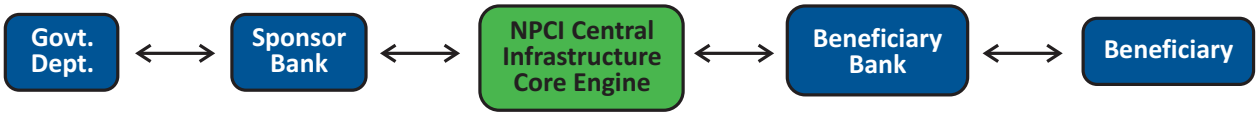


Fig 1- Aadhaar Payments Bridge (APB)

The Aadhaar Payments Bridge will facilitate the processing of payments file from the Government departments received via the sponsor banks (assigned bank), and subsequently routing of the payments file to the beneficiaries bank. The beneficiary's bank has the Aadhaar number mapping to the beneficiary's bank account number to credit the amount in the end beneficiary's account. Aadhaar Payments Bridge System (APBS) is a payments service offered by National Payments Corporation of India and the process for on-boarding of banks has also been defined by NPCI.

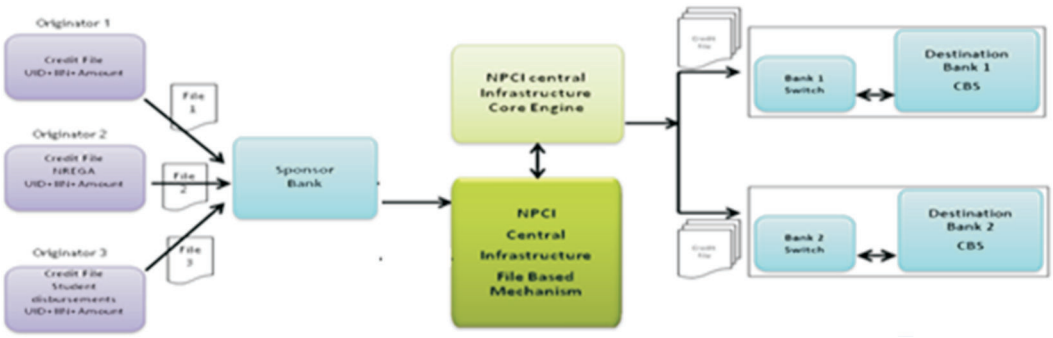


Fig 2- Funds Disbursement Architecture – Credit Transaction to Beneficiary Account

Aadhaar Enabled Payments System (AEPS) and microATMs

Aadhaar Enabled Payments System (AEPS) enables banks to route the financial transactions through a switching and clearing agency to empower the resident to use Aadhaar as his identity to authenticate and subsequently operate his respective Aadhaar enabled account and perform basic financial transactions.

A vital building block in this endeavor is developing a standard platform that will become cost effective with scale and provide real time authentication, even in remote areas. For this, standards for on-line, inter-operable devices termed microATMs were finalized by a committee consisting of members from RBI, Indian Banks Association (IBA), Banks, Institute for Development and Research in Banking Technology (IDRBT) and UIDAI. A Proof of Concept was done in Jharkhand in partnership with Bank of India, Union Bank of India and ICICI Bank for these microATM-based transactions in early 2011. The pilot project for payments has been started in December 2011 in Jharkhand (Refer to case study in later part of this document).

MicroATMs allow customers to perform basic financial transactions (Deposit, Withdrawal, Funds Transfer, Balance Enquiry and Mini Statement) using the Aadhaar number and their fingerprint as identity proof (along with a Bank Identification Number for inter-bank transactions). The cash-in / cash-out functions of the microATMs are performed by an agent of the bank. This would not only offer convenience to the resident but would also reduce credit and operational risks for the banking system apart from reducing transaction costs.

The interoperable Aadhaar-enabled payments architecture is an overlay on the existing payment architecture, where authentication information is routed to UIDAI.

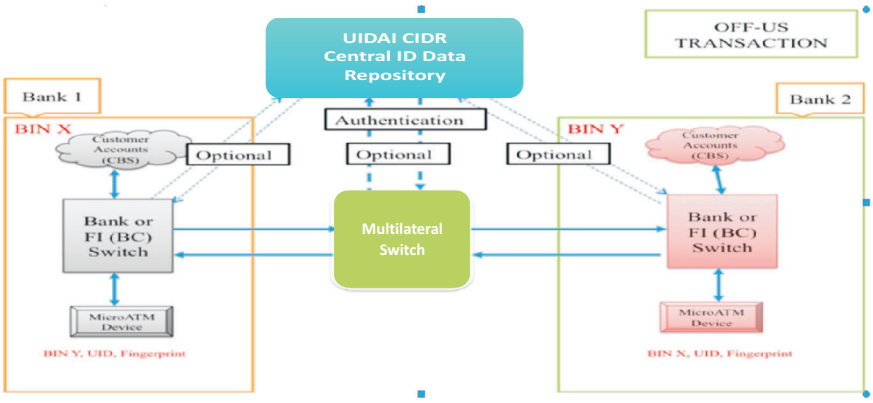


Fig 3- Interoperable architecture for MicroATM transaction between banks

Remittances

The current channels of remittances are generally expensive (like Money Orders) or risk-prone (informal channels like family, friends etc.)

The interoperable architecture of AEPS and microATMs enables online and real-time fund transfer across banks thus enabling an efficient, cost-effective remittance ecosystem within easy reach of the residents.

Key Benefits for Stakeholders

Benefits for Residents

- In the rural area, a recipient of welfare payment e.g. MGNREGA worker/ Old Age pensioner has to typically visit a bank branch to withdraw funds which has an associated opportunity cost which could be to the extent of the forgone daily wages because of the travel time to visit the bank branch. Availability of microATM in the village will save a trip to the bank, thus reducing opportunity costs and access costs significantly for the residents.
- Use of APBS and AEPS envisages electronic transfer of funds by the government thus reducing time delays from the resident standpoint.
- A microATM closer to the beneficiary's village will mean that the account will be active, and can be used for saving money and borrowing from the bank thus achieving the agenda of financial inclusion.
- Due to online nature of the microATM, the beneficiary may access their funds from any microATM, and not only from the one in their village. This can be a boon especially for the migrant population, which is estimated to be 100 million in India.

Benefits for Government

- Each Government department need not have separate resident accounts opened for the purpose of different schemes but can use a single Aadhaar-linked account for all welfare payments.
- Government does not have to maintain a list of bank account numbers for every beneficiary thus reducing administrative costs and operational difficulties.
- Aadhaar authentication ensures that funds reach only the intended beneficiary and in turn lead to better targeting.
- APBS can become the Single window platform with adequate security and access controls. It is a platform for government payments with a centralized, standard file based, and bulk upload based Government payments with easy reconciliation procedures.
- The APBS interface would also enable an electronic audit trail for the user departments and other audit agencies.
- Payments can be made centrally out of the State Government's treasury into the beneficiary's account, leading to higher liquidity and lower cost of funds for the State Government without disturbing the existing authorization procedures.

Benefits for Financial Institutions

- The customer acquisition costs for the banking system can reduce drastically as the banks can use the secure electronic KYC data provided to them for opening of accounts.
- Integrated authentication in the microATM devices enables Banks to rely on BCs to reach the unbanked population, eliminating the need for a physical bank branch or ATM's in remote areas.
- The introduction of the micropayments solution will provide an impetus to electronic payments and thus reduce cash management costs to the system.
- The online system reduces the credit and operational risks substantially in the branchless banking model.
- Every micropayment, remittance, micro-insurance and government welfare payments through the microATMs can be an additional source of revenue for banks thus reducing break even period for the BC model.
- Aadhaar online authentication can be used by the banks for their debit/ credit card transactions in order to reduce frauds thereby leading to increased usage of cards as a means of payment.

Use Case Illustrations

** Following use cases are fictional illustrations to showcase the solution benefits.*

1. Lack of identity documentation for KYC requirements to open bank accounts

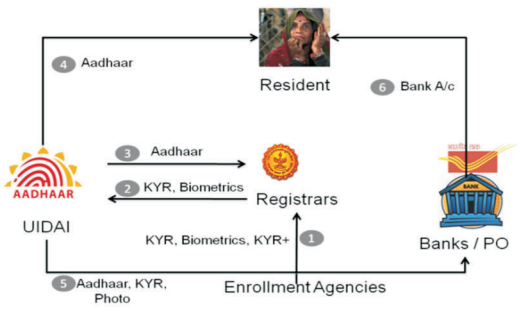
Lal Singh, a migrant labourer in New Delhi lives in slum in Vasant Kunj. He saves Rs.50 everyday, which he intends to send to his native village (Hariharpur village, Bihar). Lal Singh has no ID proof, which makes it difficult for him to get a bank account.

Every few months, Lal Singh saves enough money to send a remittance to his family. Initially, he used the Post Office with cost him 5% of the amount. However, his family experienced delays of a month or more in receiving the payment on certain occasions.

Lal Singh now uses a private agent, who charges 5–7%of the amount. This again is an expensive system with low accountability, and the money often takes a few days to reach his village.

Aadhaar provides identity to individuals enabling them to open bank account in compliance with the KYC requirements.

Lal Singh also has the option of requesting for a bank account at the time of Aadhaar enrolment. UIDAI facilitates the account opening process using the above architecture. With a bank account, Lal Singh could remit money to his family and store his savings safely.



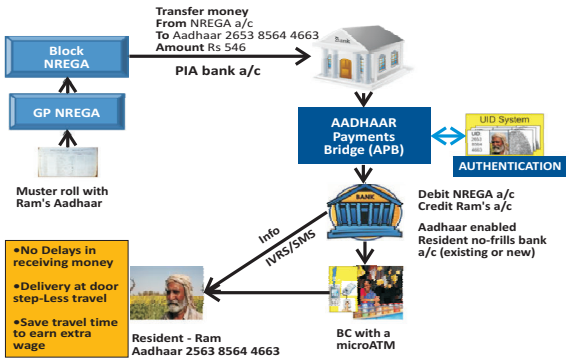
2. Higher costs of access to banking services

Needs to travel 20 Km to receive a cash payment - 15 days late and once a week

Ram lives in the village Atariya in Bundelkhand. To collect the MGNREGS wages deposited into his bank account, Ram must walk for an hour and a half to the village of Kakarwaha, six kilometres away. Travel from Kakarwaha to Badagaon, 14 kms away, where the nearest bank branch is based. Ram can collect his wages only on the Thursday of each week. He must reach the branch before closing time at 2:30 pm, else come again the following week.

The bus fare for Ram costs Rs.10, and the money lender gets a cut of his wages. The costs Ram pays in order to collect the Rs.500 in wages due to him are substantial. He incurs the loss of a day's wage, the cost of the bus fare, and additional interest charged by the money lender. In all, Ram incurs a cost of more than 20% of the benefit, in his efforts to collect the benefit payment.

With Aadhaar intervention rightful beneficiary can receive payment at their door step without undue delays. Electronic transfer of benefits can be done through Aadhaar Payments Bridge System (APBS) into any Aadhaar Enabled Bank Account (AEA). Delivery of basic financial services can be enabled through Aadhaar Enabled Payments System (AEPS) and Business Correspondents equipped with interoperable microATM. Aadhaar authentication at microATM will identify the right beneficiaries for electronic payment transactions.



CASE STUDY – Jharkhand Pilot

Residents in rural areas of Jharkhand have limited access to payment services due to higher cost of banking transactions in rural areas. Typically, the resident is required to travel long distances to visit the bank branch for payment transactions with concurrent travel and opportunity costs.

Aadhaar enabled solution implementation

To ensure ease of access to financial services for rural population, Government of Jharkhand decided to partner with UIDAI to undertake a Financial Inclusion and Welfare Payments pilot project in 12 blocks. The pilot project has been already initiated in 3 blocks.

District	Block
Ranchi	Ratu
Hazaribagh	Hazaribagh Sadar
Saraikela-Kharsawan	Chandil

Solution Overview

Part I: Aadhaar Payment Bridge (APB)

- Govt. of Jharkhand and the Block Administration were required to prepare an e-payment file containing Aadhaar Number, Bank Reference Number, Amount, Benefit Reference Number
- The e-payment file was then transferred to Sponsor Bank for onward transmission to NPCI. NPCI then uses the APB infrastructure to transfer the payment instructions to the respective beneficiary banks. The banks then credit the beneficiary Aadhaar Enabled bank account.

Part II: Aadhaar Enabled Payments System (AEPS)

- Once the payment was successfully credited to beneficiaries account, banks (Bank of India, ICICI Bank and Union Bank of India) deployed Aadhaar Enabled microATMs at Panchayat Level for the disbursement of money.

Key stakeholders & activities undertaken

- Government of Jharkhand
- Bank of India, ICICI Bank and Union Bank of India
- National Payment Corporation of India (NPCI)
- Unique Identification Authority of India (UIDAI)

Activities	Responsibility
MNREGA Job Card No mapping to Aadhaar No	Government of Jharkhand
Account Opening and Aadhaar Seeding in the Bank's Core Banking System	Banks
Defined Exception Handling (back-up) disbursement process to ensure "NO DENIAL OF SERVICE"	Banks
Gateway Service to Central Identification Data Repository (UIDAI)	NPCI
Provide authentication infrastructure and process authentication requests	UIDAI

In order to enable Aadhaar-enabled payments there were several business and IT infrastructure re-engineering activities undertaken. Based on our field experience and approach, UIDAI has devised a comprehensive checklist for all stakeholders.

Go Live

Post extensive lab and field testing, the pilot project was seamlessly rolled out in Jharkhand. BCs with microATMs were deployed in the field to process

As of 18th January, 2012

Description	Total
Successful Transactions	2223
Amount Disbursed through APBS	**Rs. 187482**

payments. The first transaction was done on December 24, 2011.

Key Learnings

- Better co-ordination and ownership between key stakeholders, especially between Government and Banks is vital for seamless execution of the program.
- Efficient information, education and communication programs are mandatory to better manage stakeholders and minimize resistance to change.
- GPRS Connectivity is critical for faster payments processing time and to reduce transaction exceptions.
- Robust monitoring mechanism required by Banks/NPCI/UIDAI.

Conclusion

Field experience shows that the residents are excited about the availability of BCs with microATMs at their doorstep. It was also observed that beneficiaries, especially women beneficiaries had a sense of empowerment. The coordination and support of various stakeholders including Central and State Governments, RBI and banks is significant and critical to the success of the program. Implementation of the Aadhaar-based unified payments infrastructure can ensure that every beneficiary receives their entitled amount at their doorstep through a business model that is commercially viable for the financial system.

Excerpts from interviews with the beneficiaries-
XXXXXXXX1420*- "Ab paisa ghar main chupa kar rakhna nahin padega. Hamara apna account hoga".*
"Now, we don't have to hide the money in our houses. We will have our own account".

XXXXXXXX0493*- "Hamne kabhi socha nahin tha ki bank wala khud aakar khaata kholega"*
"I never imagined that Bank officials shall come to me to open my bank account".

XXXXXXXX3942*- "Ab 10 km dur jaakar paisa nikalne ki zarrorat nahin. Gaon main bank wala aa gaya hai".*
"Now, I don't have to travel 10 kms to withdraw money. Bank services are delivered to my village"

References

1. Exclusion to Inclusion with Micropayments
http://www.uidai.gov.in/UID_PDF/Front_Page_Articles/Strategy/Exclusion_to_Inclusion_with_Micropayments.pdf
2. AEPS Procedural Guidelines-
http://www.npci.org.in/documents/AEPS%20operating%20procedures.pdf
3. APBS Procedural Guidelines-
http://www.npci.org.in/documents/APB%20operating%20procedures%20Final%2008-08.pdf
4. NPCI Notification: http://www.npci.org.in/notified.aspx

4.3 Aadhaar in LPG Distribution and Subsidy Management

LPG for household consumption is nearly 89% of total LPG off-take in India. Total LPG consumption in the country for the year 2011-12 is projected to be more than 16.5 MMT (Million Metric Tons) and is expected to grow at 8-9% as envisaged in Vision 2015 document of Ministry of Petroleum and Natural Gas.

LPG for Domestic Cooking is heavily subsidized. In order to restrict the use of subsidized LPG only for genuine domestic customers, every household is permitted for only one registered LPG connection in the name of one of the family members. However every registered customer is entitled to receive refills as per their domestic cooking need.

Challenges in LPG Distribution & Aadhaar Intervention

LPG is an exceptional fuel. It is considered as a green fuel and has wide range of applications. The environment friendliness and usability for multiple applications combined with the arbitrage available in its pricing entice the market players to divert the product meant for domestic cooking for other applications.

All LPG distribution operations are recorded using robust software provided by OMCs to distributors. The information thus generated is captured and made into meaningful reports providing business insights to OMCs. Hence, the market players use ways and means outside the software realm to manipulate and take advantage of arbitrage available in inherent vulnerability of Subsidized Domestic LPG Marketing.

Use of Fake Identities to draw subsidies

Over the years, such trends of diversion have been facilitated by obtaining more than one LPG connection per household violating LPG Control Order. This is achieved through duplicate and/or fake connections. Multiple connections in the name of existing customers and/or fake connections in the name and address of non-existent customers provide enough opportunity to draw subsidized cylinders and use them for purposes other than domestic cooking.

Aadhaar is providing a unique identity to every resident of the country. Integrating the Aadhaar number of the resident by one time validation to identify the beneficiaries of subsidized LPG across the OMCs will help to clean their digitized data base, by de-duplicating the Aadhaar numbers.

Lack of strong process to verify receipt by genuine beneficiary

LPG cylinders are home delivered. At the time of delivery, the household identity is manually verified and the receipt acknowledged by the resident / family member. Hence, the current process of LPG distribution to customers has a weak form of verification and consent from a residential consumer at the time of acceptance of delivery. Being a manual process, the system does not have a fool proof re-verification mechanism. This leaves an opportunity for diversion of the cylinder by stakeholders in the supply chain to non-genuine customers for non-domestic applications without the knowledge of registered customers.

The online authentication service provided by Aadhaar can be incorporated in the subsidized residential LPG process to verify the genuine beneficiary at the time of delivery. This strong verification of the resident is a deterrent to divert the cylinders by the business partners and supply the same to non-genuineness without the consent of customers.

Lack of Portability of Identity & Quality of Service

The access to subsidized LPG requires sufficient proof for local address and identity, with an increasing migratory population, this becomes a bottle neck. In addition, in the current system an LPG customer has his/her connection mapped to a specific OMC distributor in his/her locality, binding them to the distributor. In the event of below par service by the distributor, the customer does not have the freedom to move to distributor offering better service.

Aadhaar provides the resident an identity which can be verified across the nation. By incorporating Aadhaar in the customer KYC and using Aadhaar authentication for delivery with the centralized product movement monitoring software already in place with OMCs, there is an opportunity available for smooth portability of LPG connections across distributor's intra or inter OMC. (Recharging a mobile connection from any physical touch point across the country can be considered as an analogy). Such a facility would encourage competition between distributors and hence pave way for better customer service.

Availability of Infrastructure to facilitate direct transfer of Subsidy

Currently domestic LPG is supplied at the subsidized price and subsidy component is designed to be paid by the government directly to OMCs. It would be desirable for the government to distribute LPG in the entire supply chain at market price, removing the incentive for its diversion.

The integration of Aadhaar Number of the beneficiary and performing Aadhaar Authentication at the time of service delivery will enable the government to consider leveraging the Aadhaar Enabled Bank Account of the beneficiary where the subsidy amount may get directly credited for a verified residential delivery. In such a scenario LPG can be supplied at market price.

Integration of Aadhaar in LPG Distribution – Process Re-engineering

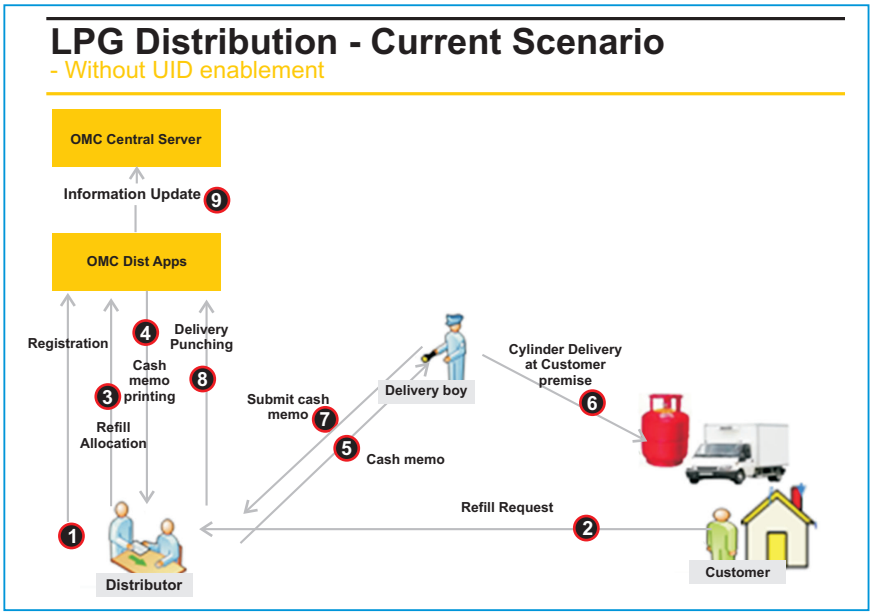
Current Process

1. OMC Distributor registers a prospective customer in a distributor application.

   (Prospective customer obtains a connection post fulfillment of official requirements for release of connection for domestic LPG applicable to the OMCs.)

2. Customer places a refill request to the distributor through various channels (Depending on the channel offered by the distributor i.e. manual, telephone, IVRS, SMS and web).

3. The refill request is updated automatically or the distributor enters the same in the application.



4. Distributor generates a cash memo against the bookings.

5. Delivery boy carries the printed copy of cash memo.

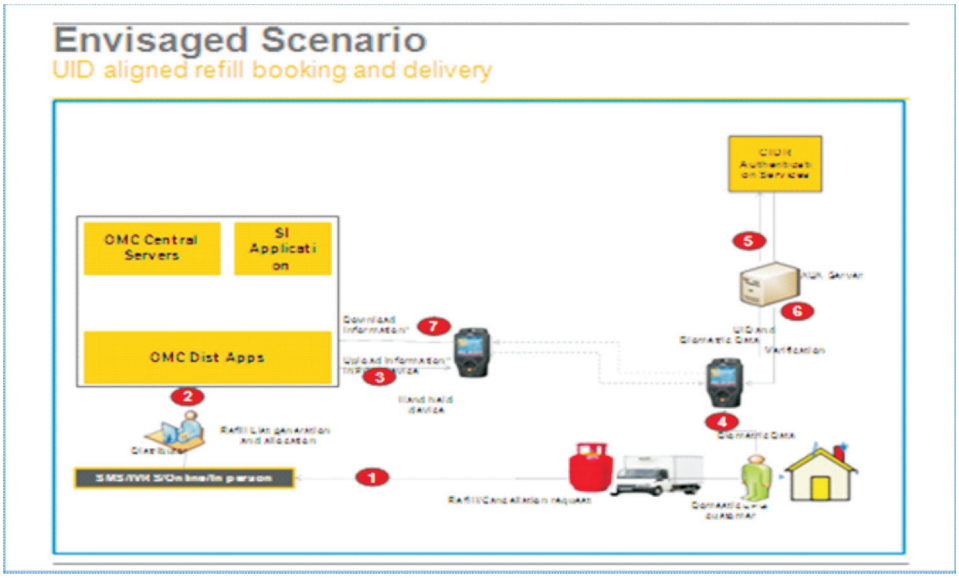
6. Delivery boy delivers filled cylinder to customer premises.

7. Delivery boy receives empty cylinder and payment at subsidized price against the delivery and submits acknowledged cash memo and empty cylinder back to the distributor.

8. Delivered cash memo details are entered into distributor application.

9. OMC central server is updated.

Aadhaar Integrated Process



1. At the time of enrolment Aadhaar number is validated through biometric and demographic authentication.

2. Customer places a refill request to the distributor through various channels.

3. The refill request is updated automatically or the distributor enters the same in the application.

4. Distributor loads the details of the day's delivery into a Point of Sale (PoS) device.

5. The delivery boy carries the PoS device and filled cylinders to customer premises.

6. Aadhaar Authentication request of customer sent to CIDR (UIDAI system).

7. Online verification response from CIDR to PoS device, receipt of empty cylinder, printing of cash memo and collects payment at market price against delivery.

8. Information from handheld device is uploaded into OMCs central system real time.

9. Central server sends a batch file at predefined frequency with Aadhaar Numbers of Customer (beneficiary) and subsidy amount to be paid to Sponsor Bank.

10. Sponsor Bank initiates cash transfer through NPCI Gateway to the bank account of the Customers.

Summary

The Aadhaar intervention in the LPG marketing has significant potential to improve its operational effectiveness. The integration of Aadhaar in the customer database will enable removing ghost & duplicate beneficiaries; and the integration of Aadhaar Authentication at the time of delivery can mitigate illegal diversion of cylinders. Aadhaar intervention is expected to bring about improvements such as portability, increased competition, enhanced customer satisfaction, and streamlining subsidy disbursement. To realize the envisaged benefits of Aadhaar, the OMCs have already started pilot implementation in few selected areas across the country to identify the challenges, process changes required before expanding to other areas.

Reference:

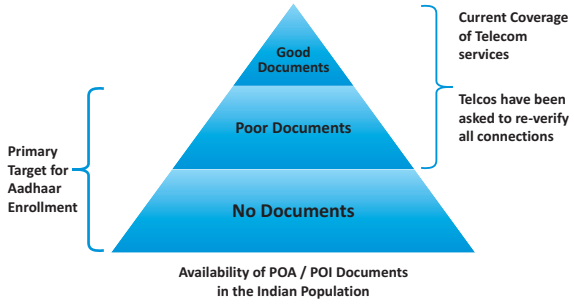
1. Task Force Report http://finmin.nic.in/reports/Interim_report_Task_Force_DTS.pdf

4.4 Telecom and Aadhaar

India's telecom sector, one of its flagship domestic industries has played a pivotal role in India's growth story. There has been a dramatic rise in mobile phone penetration over the last few years. Wide spread and easy access to communication has raised the potential of telecom connections being used for anti national activities or malicious intent. Current regulations demand a strong know your customer (KYC) process to make sure connections are issued only after proper verification of the subscriber.

Aadhaar as KYC for telecom and Internet connections

The objectives of inclusion and security can be mutually exclusive at times. Greater security demands stronger subscriber verification measures. Subscriber verification involves submitting know your customer (KYC) documentation, which includes proof of identify (POI) and proof of address (POA). Individuals lacking these documents get excluded from telecom services or resort to providing fake documents to get access to services. The use of improper identity documentation to obtain telecom connections is common and has been widely reported in the press.



Telecom operators have been under lot of scrutiny from the Department of Telecommunication (DOT) over the last few years to strengthen the KYC process used to issue a telecom connection. In 2008, DOT started imposing financial penalties on telecom operators for every instance of incorrect documentation. In 2009, Telecom operators carried out a massive re-verification of documentation for all existing subscribers.

Every month the Telecom Enforcement and Resource Monitoring (TERM) cell under DOT carries out an audit on the KYC documents for about 0.1% of the total operator base. Operators are levied a financial penalty based on the number of incorrect cases found.

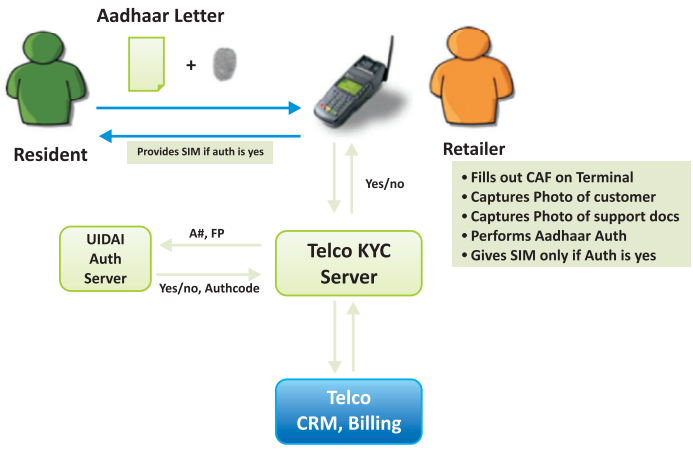
As per the Annual report of the Department of Telecom 2010 - 2011[2], the TERM cell imposed an amount of Rs 700 Crores on telecom operators for subscriber verification related penalties. Operators continue to face penalties of several crore rupees each month based on the findings in the TERM audits.

Aadhaar Authentication can change this eco-system making Telecom KYC stronger, cheaper and paperless. The process is incentive compatible enabling benefits for all parties involved including the resident, retailers, telecom operators and the government.

Retailers selling connections would use Aadhaar enabled terminals to scan the QR barcode printed on Aadhaar letters making the data capture of the resident details fast and error free. Using Aadhaar Authentication, The resident would then establish their identity in real time with a biometric authentication captured on the terminal. The telecom operator would store the digitally signed

[2] www.dot.gov.in/annualreport/2011/English%20AR%202010-11.pdf, Page 55

authentication response from UIDAI as proof of verification. The retailer can provide the connection to any resident for whom the auth is successful.



Discussions with industry experts indicate that paperless KYC using Aadhaar can save between Rs 25 – Rs 35 per subscriber by removing TERM fines and paper based backend processes.

Telecom operators are issuing over 30 million SIM connections every month that require KYC. Adopting Aadhaar Auth can result in a savings of over 1000 crore rupees annually for the industry.

DOT has started this process by issuing a circular[3] notifying Aadhaar as a valid POI and POA for residents to obtain a new telecom connection. A proof of concept for Aadhaar Auth in Telecom KYC is being developed by UIDAI and DOT along with the telecom operators.

Deploying Aadhaar enabled applications in retail outlets

There are over one million retailers selling telecom services in India. New revenue streams can be created for the small retailer by equipping them with Aadhaar enabled terminals. Telecom KYC is merely one possible application using this terminal. Another is the MicroATM, where the retailer acts as the Business Correspondent (BC) or a BC sub-agent for a bank.

The MicroATM[4] device has been standardized by an RBI appointed committee comprising of the Indian Banks Association, UIDAI, NPCI, IDRBT and Banks. The MicroATM solution has been accepted by the Finance Minister appointed Task Force on designing an Aadhaar Enabled Unified Payment Infrastructure, and the Inter Ministerial Group (IMG) report[5] on The Framework for Providing Basic Financial Services using Mobile Phones.

With multiple applications on the horizon, Aadhaar terminals at retailers must be multi-application capable. This will create a new eco-system that will deliver new revenue streams for the small retailer.

Accessing Government Services with mobile phones

With over 700 million mobile connections issued in India, the mobile phone is now ubiquitously available with all segments of the Indian population. This makes the mobile an excellent device to target for delivery of m-governance. Several initiatives are already underway and the Department of

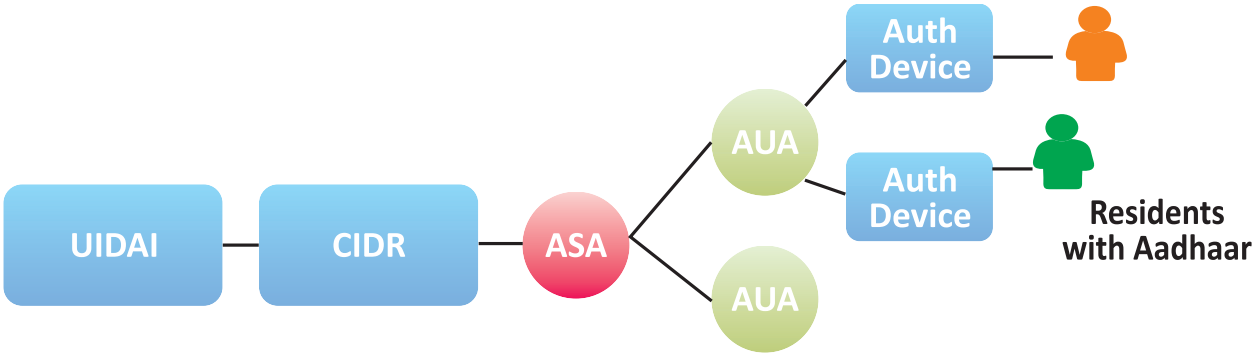
[3] DOT notification on usage of Aadhaar for Telecom KYC: http://www.dot.gov.in/as/2011/as_14.01.2011.pdf
[4] Micro-ATM Standards 1.3: http://www.iba.org.in/events/MicroATM1-3.pdf
[5] Inter Ministerial Group Report: http://www.mit.gov.in/content/government-approves-framework-provision-basic-financial-services-through-mobile-phones

Information Technology (DIT) is setting up a mobile services delivery gateway[6] (DIT) to make it easy for other government departments to get started.

Aadhaar authentication makes it possible for residents to securely identify themselves over self-service channels such as the Internet and mobile phones. Aadhaar provides a common authentication system making it easier for government and residents to interact over mobiles or the internet.

Telecom operators as service providers for Aadhaar authentication

Several Government Departments, public sector companies, banks and others are deploying services based on Aadhaar Authentication.



Aadhaar authentication is an online real-time service. Users of this authentication service are called Authentication User Agencies (AUA). Requests from AUAs are routed to UIDAI via Authentication Service Agencies (ASA), which have secure connectivity established with CIDR.

Given the expected scale of operations, telecom operators are natural candidates to act as ASAs. Telecom operators can bundle ASA services as part of their enterprise connectivity business. UIDAI will redirect any AUAs seeking to launch services to obtain connectivity from any of the empanelled ASAs.

[6] DIT paper on Mobile Governance
http://www.mit.gov.in/sites/upload_files/dit/files/Draft_Consultation_Paper_on_Mobile_Governance_28311.pdf

4.5 Internet and E-commerce

India is experiencing rapid growth in Internet usage and e-commerce. India currently has over 100 million internet users with increasing broadband penetration and mobile based internet usage.

Aadhaar, a national unique digital identity which can be verified online, can be leveraged by internet based services including ecommerce where there is a business necessity to establish customer identity. The availability of Aadhaar may spur the growth existing online businesses or create new online opportunities which critically depend upon the need to authenticate real identity of the individual. The subsequent sections below will showcase the potential Aadhaar usage in internet based services.

Building Trust in Cash on Delivery (CoD) model

There is a significant customer base in India who wants to buy online but still prefer cash payment instead of paying through online banking or credit card. These customers either do not have access to online banking and credit card or are not very comfortable with online payment methods. Such customers can be targeted by ecommerce players only through Cash on Delivery model. However, the CoD model has a risk of product going undelivered due to fake customer order or customer changing their mind on delivery and denying ordering the product.

This risk can be reduced by mandating Aadhaar authentication of the customer as part of online ordering for CoD orders. The customer can be required to authenticate his/her Aadhaar number through the OTP sent to the registered mobile with their Aadhaar record. In addition the shipping can be restricted to the address which can be verified against their Aadhaar record. This verifies the customer identity and authenticity of customer mobile number and address. It eliminates submission of fake CoD orders.

Furthermore, since Aadhaar allows linking of customer accounts to a “real person”, it can help build better cross-sell up-sell capabilities as well as smarter fraud detection platform within online e-commerce services.

Identity Verification based online services

Internet by design provides anonymity to the real identity of user; allowing the user to adopt any identity. While anonymity is extremely important in certain areas, in some other areas where stronger “trust” needs to be established, it is equally important to have some mechanism to authenticate the “real person”. As it is seen today, depending purely on virtual identities create a challenge for certain online businesses where ascertaining the real identity of the user is very important for building customer confidence and business growth.

Online recruitment/job service is one of the examples. Using Aadhaar authentication through OTP to verify user name, address, age and mobile as given in the candidate profile can be of great value. Such online service can use Aadhaar authentication to enable following features:

- Availability of "Aadhaar Verified" candidate profiles.
- Candidate job history, recommendations by "Aadhaar verified" people, etc. allowing companies to establish better trust.
- Higher security feature where a user can limit the access of their profile to only Aadhaar verified users.

Online auction sites allowing individuals to buy and sell products from each other. Given the seller is not an established company and transaction is being conducted online without a physical store, building creditability with buyers is a big challenge for sellers. "Aadhaar Verified" seller/buyer accounts can add trust in the market place helping sellers to attract more buyers.

Similarly certain social networking, and micro-blogging sites, and online portals are increasingly seen moving towards a mechanism to establish "real or verified identities" thus allowing users to establish stronger "trust" within the community. Currently there is no mechanism to verify the real identity other than manual verification which is not scalable. For these purposes, while creating the online account, Aadhaar authentication can be used to establish the real identity allowing an "Aadhaar Verified" trust model to be built in the online world.

Electronic Payments

Today the masses are excluded from the online commerce, be it selling products, content, tickets, insurance, or any other online service, due to their inability to verify their identity online and make electronic payments. Aadhaar as an online verifiable identity coupled with Aadhaar enabled payment platform's ability for millions of people to make electronic payment for services using their mobile or on assisted terminals allows e-commerce now be extended to a billion people!

4.6 Aadhaar as a Unifying Identifier

Aadhaar can also be used to provide resident centric information for analytics, single customer view, and decision making in a number of service industries. For services like healthcare, welfare programs, financial services; the service delivery efficiency can be increased provided data can be correlated across various sources and systems. However in the absence of universal unique individual identifier, it is very challenging task both from accuracy and data integration perspective. Adoption of Aadhaar by various services provides the opportunity to correlate data across disparate systems accurately with minimal integration.

The illustrations below showcase the potential Aadhaar usage as a unifier of data for improved public service in multiple domains.

Healthcare Services

Today there is no single accurate mechanism to track spread of diseases, timely identification of outbreak of epidemics and monitoring of the medical services being offered. Currently, most of the information on healthcare services is obtained by the Ministry of Health and Family Welfare through surveys. Information on patient healthcare records is maintained in silos across hospitals, insurers, and individuals. Use of Aadhaar in healthcare services can catalyze the formation of a national database.

This can be achieved by linking the Aadhaar number to existing and new information related to patient health records, diseases and medical treatments. It will also require creation of a master information system through the integration of legacy patient management systems used across hospitals and nursing homes. Ministry of Health and Family Welfare, and industry associations may be required to play a sponsor role for initiating this program of digitizing and linking patient healthcare records.

The key benefits are:

- Better medical care for patients because of availability of medical history across stakeholders.
- With an authentication done for each entry in the database, it would provide an effective means to track diseases, provide early indication of spread of epidemics and allow effective planning to meet the medical emergencies in different parts of the nation.
- Based on the address of the patient in the database, it would be possible to generate a pin-code linked map of diseases.
- It would provide an effective means to assess the medical services in the different parts of the country and help in the planning and development of medical services.
- Such services can also be offered as a means of authentication purposes to insurance providers to curb misuse and fraud.

Labour and Skills Management

Problems such as a large unorganized sector in Indian labour force, glaring skill demand and supply gaps and disguised unemployment and underemployment are some of the major challenges

characterizing the Indian labour market. In order to bridge the widening gaps in the required and the available skills levels, it is pertinent to assess and evaluate the existing skill levels of the vast labour force in the country. This will facilitate the identification of key skill requirements across sectors, geographies etc. This can be achieved by collecting labour market information at national level. The national labour market information can then be used to plan development of vocational education training institutes and other technical institutes like ITI and polytechnic colleges to close the skill set gaps.

UIDAI providing a unique Aadhaar number to all residents can catalyze the formation of a national skills database by linking the resident's Aadhaar number to their occupation, education and training. For example, trainings imparted to individuals can be captured at the training centers to track participation and skills development. The effectiveness of an individual's education and training can be correlated to employability. This database can also be used to monitor the working and livelihood conditions of the labour force.

Ministry of Labour, Ministry of Human Resources and organizations such as National Skills Development Corporation along with industry associations may be prime sponsors of such an initiative.

The key benefits are:

- Consolidated and clean database for monitoring the labour force•
- Provide an effective means to assess labour force productivity and allow mapping of skill sets with actual occupation
- Development of a lifecycle skill management program with possibility to contact people and offer them available options for upgrading their skills at suitable points in their life
- Data based decision making and planning for enhancing education and vocational training institutes
- Focused and targeted training programs resulting in potentially improved employability of individuals

Others

Besides the two illustrations mentioned above, banks and insurance carriers can use similar credit and risk bureaus to manage operations effectively. A unified identifier can also help them manage customer acquisitions and relationships better. Typical benefits can be in achieving efficiencies and risk reductions in microfinance and in monitoring of insurance claims.

Government programs can also look at beneficiary level views to identify those residents availing multiple schemes. A State resident data hub allows leveraging of Aadhaar to provide unified view. Such analytics can improve program beneficiary identification and targeting of welfare programs.

5. Conclusion

India is undergoing major change in how services are delivered to masses through use of technology driven solutions in both government and private sectors. Considering the fact that a large percentage of people in India still depend on Government benefits and services, it is imperative that a clear identification mechanism of beneficiaries is created. As we move towards a digitized service delivery scheme, there is a clear need for an online verifiable identity to ensure benefits are accurately targeted to those who deserve them. The ability to digitally establish individual unique identity and further authenticate the beneficiary during service delivery will be critical to achieve the expected result. Aadhaar, a National Unique Identity platform, provides the necessary identity solution.

Three key challenges in serving the large population directly are:

- "Reach" – ability to electronically reach the masses and ability for them to participate in the digital transactions from far corners of India.
- "Identification" – ability for service delivery applications to be able to identify their users and beneficiaries and ensure right person receives the right service.
- "Payment" – ability for the masses to be able to make electronic payments from their mobile or using an assisted terminal anytime anywhere in the country.

India's advances in mobile network and mobile adoption addresses "reach"; Aadhaar online identity platform addresses "identification"; and Aadhaar enabled payment platform addresses people's ability to pay and receive "payments" using their Aadhaar number and biometrics. The mass adoption of Aadhaar and Aadhaar enabled bank account along with mobile will empower the residents and will facilitate direct government to resident interaction in a transparent manner. Aadhaar enabled services on mobile platform and usage of mobile as a mechanism will serve as a platform to deliver resident centric self services.

Using a mobile, Aadhaar, and Aadhaar enabled payment platform, residents can now be given choice in accessing various services anytime anywhere. The time is now and the possibilities endless!

6. Way Forward

For interested stakeholders to leverage the Aadhaar Identity solution in their service delivery applications, UIDAI has created a support group and a set of artifacts.

The support structure includes an applications group at UIDAI, and empanelled consultants and software vendors to help service providers build necessary processes and applications.

Further there are detailed support documents for guidance on leveraging and integrating the Aadhaar solution such as:

- Applications On-boarding and Readiness for service delivery providers
- Authentication Framework, Operating Model and Guidelines
- Criteria, checklists and activity templates for becoming AUA, ASA
- Aadhaar Seeding solutions for Service Delivery databases to embed Aadhaar number

Full inventory and reference set of documents are available on UIDAI website http://www.uidai.gov.in/ and for technical and developer material, see Aadhaar developer website at https://developer.uidai.gov.in/

Any entity interested in engaging to participate in or adopt the Aadhaar solution should contact UIDAI.

Annexure 1: Authentication Features in Detail

Following table illustrates all the features offered through Aadhaar authentication service in detail. These features are explained below using examples to understand the uses cases and application needs. For technical details of authentication and feature usages, see UIDAI website for the "Aadhaar Authentication API Specifications 1.5" document.

Sl. No.	Feature	Usage
1	Demographic data matching	This feature allows verification of resident basic demographic attributes against what is stored within Aadhaar database. The feature provides response of "Yes" or "No" based on the verification. It allows matching of the following basic demographic attributes: • Name in English and Indian language • Address • Gender • Date of Birth (full date of birth or just year of birth) • Age (verifying if a resident is above/below a given age) • Phone (verified mobile of the resident) • Email (verified email address of the resident) Use of Aadhaar demographic authentication helps to clean up incorrect or out-of-date demographic data of a resident in the service agency database. This combined with online biometric/OTP authentication provides a strong value proposition to various applications. It is important to respect the privacy of the resident and only minimal, absolute necessary data should be captured by the application. Also, it is important that organizations that collect resident data and authenticate make the reasons for collecting such data clear to resident and ensure resident agrees for such collection, storage, and use.
2	Transaction ID	This field should be used by AUA to assign a logical business transaction identifier while integrating Aadhaar authentication. This feature allows request/response scheme to be made synchronous or asynchronous without worrying about how to correlate a request to its particular response. Whenever there is integration between two independent systems, it is critical that every handshake has a common "identifier" for correlating request / response and for later audits. For example, when conducting a payment transaction, a bank may have to keep track of a common transaction id across the flow. Authentication response contains the same transaction code that was in the request allowing applications to correlate a response with a particular request.

Sl. No.	Feature	Usage
3	Name Matching	It allows verification of resident name against their Aadhaar record. To support easier demographic matching and make it least painful for the resident, it is critical that name matching be flexible. Aadhaar name matching feature provide various matching strategies such as "exact" match, "partial" match, etc. with configurable match tolerance levels so that based on the application needs (for having a strict match against a slightly loose flexible match), different strategies can be used. For example, let us say, a resident with Aadhaar number "1234 4321 1234" has name in Aadhaar database as "Anil Kumar Singh" wants to open a bank account. As part of electronic Aadhaar based KYC, the banking application does a demographic authentication against Aadhaar system. While doing the demographic authentication, banking application may choose to not necessitate a full name exact matching and may allow partial name matching. So, if the application use "partial" matching strategy and a match value (or threshold) of "50" meaning that if more than 50% of full words match with Aadhaar database, it is OK to go ahead and create the customer account. So, by passing "ms" as "P" (partial) and "mv" as "50" along with "name" field as "Anil K Singh" (instead of resident's fully expanded name), application will get a "yes" response from Aadhaar authentication and can go ahead and create the bank account. It is important for various applications using this feature may choose a different matching strategy and match thresholds based on the level of "strictness" they need to maintain within their database. While a bank application (as in the above example) may choose a partial matching strategy, a passport / Visa application may choose an exact matching strategy since it requires resident's actual full name (as in Aadhaar database) within their databases.
4	DoB Matching	This field allows applications to verify resident's date of birth against what is stored within Aadhaar database. Either a full data of birth can be verified or just year of birth can be verified. This should be used when application absolutely requires the DoB field in their database to be correct. Since Aadhaar is an inclusive program and a very large percentage of Indians do not possess full date of birth, chances are only a year of birth is recorded within the Aadhaar system. This is critical to keep in mind while collecting date of birth and using Aadhaar authentication.

Sl. No.	Feature	Usage
5	Age Matching	Several applications require age verifications for asserting eligibility criteria for service delivery. For example, while booking tickets, senior citizen travel concession should assert that the resident is indeed above 60. Or for school admission may be a child age should be verified as at least 5. If application only needs to verify the age to be above or below a given age, then this option should be used instead of verifying full date of birth.
6	Mobile and Email Matching	Aadhaar system optionally captures this information for a resident and is available for matching while doing demographic authentication. During capture and updates, these are verified and can be used for reliable authentication. Although applications such as online banking may already have provisions to do the same, Aadhaar authentication with mobile/email matching extends the same advanced features and capabilities to several Government and non-Government applications that may not have such capability today.
7	Address Matching	Several services such as banking, communication, Government benefits schemes in India depends on address verification as part of their initial beneficiary creation and as part of regular 'Know Your Customer" activities. Currently most of these are done through hard copies of documents and management of paperwork in terms of preserving the trail as per regulatory requirements. Aadhaar authentication supports address verification against the central identity repository in a paperless online fashion. UIDAI has established, with the help of several ministries, departments, and other agencies a common address structure that can be used for storing and matching urban and rural address in electronic format. Address matching at a high level supports: • Structured address matching allowing fields such as district, state, pin code, etc. to be individually or in combination matched. • Unstructured address matching where address is matched as a single string so as to support matching of whole address without explicit understanding by the application at a field level To make data entry into applications easier, Aadhaar letter contains a 2-D barcode (QR Code) having the data in XML format that can be read using a standard web/mobile camera.

Sl. No.	Feature	Usage
8	Structured Address matching	When validating address, applications can choose to validate address using the Aadhaar standard address structure in full or in parts. For example, while issuing a SIM card, application can capture the address and just verify the "State" and "District" or "Pin code" to ensure that the resident belongs to a particular telecom circle. Structured address contains the following fields that can be verified individually or in combination: • Fields that are free flow (as provided by the resident) o Care of Person Name o House Identifier (single string containing house/ apartment/building number, name, etc.) o Street Identifier (single string containing street number, name) o Landmark details o Locality Name and details • Fields that are based on codified master data o Village/Town/City Name o Sub-district Name o District Name o State Name o Pin Code o Post Office Name Applications are encouraged to scan the 2-D barcode on the Aadhaar letter using a web/mobile camera so that the address data is populated in a structured fashion. If applications are not scanning barcode and manually entering complete address data as a single string by looking at the Aadhaar letter, "unstructured address" matching scheme should be used.
9	Unstructured Address Matching	For applications that are capturing address manually from the Aadhaar letter or from the information provided by the resident, it is recommended that "Unstructured Address" matching be used. This allows address to be captured as a single string and match it against the address in the Aadhaar system. Although this option is easy for verifying existing data or manually entered data, it requires matching without strict order and matching without all part of full address being there. For this

Sl. No.	Feature	Usage
		reason, Aadhaar authentication allows "Partial" matching strategy during address matching and applications can choose the match tolerance level based on their needs. In general, while structured matching provide much higher matching accuracy, unstructured matching allows flexibility.
10	Fingerprint Matching	Biometric authentication allows applications to verify if the resident is "who he/she claims to be". Several applications require physical, in-person verification to ensure only right people are being served and right beneficiaries are being authenticated for service delivery. Fingerprint matching allows one of multiple fingers to be used for matching based on the needs of the application. Use of multiple fingers allows better fusion strategy on the Aadhaar server for better accuracy. Fingerprint matching feature also allows either fingerprint minutiae (FMR) to be sent for matching or fingerprint image (FIR) to be sent. While use of FMR works well for applications that needs to work on low bandwidth network, FIR works well for applications that has higher bandwidth.
11	Iris Matching	Quite similar to fingerprint matching, Aadhaar authentication also supports Iris matching. In general, Iris matching is more accurate than fingerprint matching. Iris matching is supported only against Iris image (IIR). Currently this feature is in experimental stage and is available for development and testing purposes.
12	One Time Pin (OTP) usage	Resident authentication can be strengthened by verifying the possession of the mobile by resident. One Time Pin (OTP) is a mechanism to do achieve this. Aadhaar authentication supports biometrics and/or One Time Pin (OTP) based authentication. While biometrics provide one factor (who you are), OTP provide another factor (what you have). Applications that take advantage of Aadhaar Authentication can use OTP to provide single factor authentication or along with biometrics for achieving two factor authentication. In a nutshell, OTP request can be initiated by the resident by using SMS/USSD/Portal or it can be initiated by the application on behalf of the resident using OTP API. Notice that OTP is always delivered on the resident's mobile/email and application is expected to capture that during authentication so that OTP can also be validated along with authentication.

Sl. No.	Feature	Usage
13	"Yes/No" Response	Only responds with a "yes/no" and no personal identity information is returned as part of the response. This is one of the key strategic choices to ensure privacy of resident data. This actually means that there is no mechanism to "get" data of a resident through the authentication API. For example, authentication API answers questions such as: • Resident claims his/her name is "…", is this correct? While Aadhaar Authentication will respond to the above questions with a "yes/no", 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.
14	Digitally Signed Response	Aadhaar authentication allows applications to move towards fully online, electronic identity verification and avoid paper processing and reduce overall cost. Aadhaar authentication response is digitally signed by UIDAI. Digitally signing the response by UIDAI ensures that the integrity of the response is maintained and agencies can trust the fact that the response indeed came from UIDAI.
15	Response Code	Every authentication call responds with a unique code that can be used for audit and troubleshooting purposes. This code is what uniquely distinguishes every authentication transaction across the system. This is quite similar to the unique authorization code returned for every credit card transaction.
16	Response Timestamp	This timestamp allows applications to verify "when" this resident authentication was done. Applications can also use this for audit purposes. This has interesting usage such as verifying if authentication of a particular Aadhaar number was done within the last 3 months, etc. This combined with "info" attribute provides strong "proof" of a particular authentication.

Sl. No.	Feature	Usage
17	Self Verifiability of Response	Current practice of identity verification is by collecting "attested" copies of documents. Attesting allows the system to "trust" the fact that the copy is indeed verified against the original. At a high level Aadhaar authentication response allows agencies to self-verify the following: • Is this authentication indeed verified by UIDAI? Digital signature allows this check. This is quite akin to checking if a gazetted officer has signed. • Is this authentication for a given Aadhaar number? • Was this authentication done within last "n" months? Timestamp in response allows this. This is useful for knowing if the authentication proof is recent. • What was authenticated? "Usage Flags" within "info" allows this check. o Was name, DoB, etc. verified? o Was biometrics used? o Was full or partial address verified? • Is the address verified during authentication same as what is now provided by resident? Hash value of demographics data allows this check. For example, in the case of pension systems, residents need to establish the fact that they are alive every year. Currently this is done by residents having to go to an approved officer and signing a record. With Aadhaar authentication, an agency could authenticate resident separately and provide the response to pension system. By simply verifying the response XML pension application can answer the question "is the person with Aadhaar number so and so been biometrically authenticated in the last 6 months?" and trust the fact that the person is alive. Aadhaar authentication response is akin to today's physical document which says *"To Whomsoever It May Concern"* and signed by a Gazetted Officer on a particular date with the document clearly stating *"the person with Aadhaar number so and so has the name and address as given below ...".* Aadhaar response can be viewed simply as an electronic version of this physical paper and can be trusted and self-verified by 3rd party application. This is a powerful feature allowing de-coupling of authentication from actual usage and create a true electronic version of identity verification and proof for verification.

Sl. No.	Feature	Usage
18	Encryption and Tamper-proofing	Person Identity Data (PID) of the resident is encrypted at the time of capture using 2048-bit PKI providing strong security of resident data. PID block is never decrypted during transit and no servers in the path can decrypt due to the use of PKI. In addition HMAC (Hash-based Message Authentication Code) of the data ensures PID block is not tampered in transit.
19	Digitally Signed Request	In addition to encryption of data, API Request is digitally signed by the AUA establishing further trust and no-repudiation mechanism between user agencies and UIDAI. Source of the API call is strongly authenticated to ensure no malicious API calls are processed.
20	License Key Usage	Multiple levels of security and trust are established between AUA and UIDAI for accessing authentication service. Use of license keys is one of them. It is similar to a software licensing concept. It achieves following purpose: • Ensures that only specific approved AUAs can access the authentication API • Mechanism to enforce specific feature usage, expiry, etc. • Allow AUAs to extend API features to their Sub-AUAs and trust their requests

Unique Identification Authority of India

Planning Commission, Government of India

3rd Floor, Tower II, Jeevan Bharti Building, Connaught Circus, New Delhi-110 001