UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

LEVERAGING AADHAAR IN THE TELECOM SECTOR

VERSION 1.0

Table of Contents

Executive Summary

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. Data connectivity solutions to enterprises and mobile devices are pervasive in the market and expanding rapidly to cover most rural areas.

Telecom operators as ASAs for Aadhaar authentication

The UIDAI is issuing a unique identification number (Aadhaar) to every resident of India, which they can use for the purpose of identification. Residents can identify themselves using the Aadhaar *authentication* process wherein the Aadhaar number, along with other attributes, including biometrics, are submitted to the Central Identities Data Repository (CIDR) operated by UIDAI for verification. Aadhaar authentication is an online real-time service and only responds with a *yes* or *no*.

Users of this authentication service are called Authentication User Agencies (AUA). Requests from AUAs can be routed to UIDAI only via an Authentication Service Agency (ASA). ASAs are empanelled entities who have secure connectivity established with the CIDR and can provide last mile connectivity to anyone who wants to become an AUA.

Any telecom operator with an enterprise connectivity business is a natural candidate to become an ASA. They have the opportunity to bundle the Aadhaar authentication service along with their connectivity solutions to benefit the resident. Several Government Departments, public sector companies, banks and others will be deploying services based on Aadhaar Authentication and traffic from these entities will need to be routed through an ASA.

Aadhaar as KYC for telecom and internet connections

Wide and easy access to communication has raised the potential use of the telecom connections for anti national activities. This necessitates that connections be traceable and issued only after proper verification of the subscriber.

The objectives of inclusion and security can be mutually exclusive at times. Greater security demands stronger subscriber verification measures. Subscribers are verified using know your customer (KYC) documentation, which requires submission of a 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 for telecom connections is common and has been widely reported in the press. The Department of Telecommunications (DOT) has issued certain regulations, conducts monthly subscriber verification audits and levies financial penalties on telecom operators in order to encourage higher compliance in subscriber verification.

As per the Annual report of the Department of Telecom 2010–2011[1], the TERM cell imposed a penalty of Rs.700 crore on telecom operators related to subscriber

[1] www.**dot**.gov.in/**annualreport/2011**/English%20AR%20**2010-**11.pdf, Page 55

verification. 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. DOT has started the process by issuing a circular[2] notifying Aadhaar as a valid POI and POA for residents to obtain a new telecom connection.

Retailers selling connections can 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 can then establish their identity in real time with a biometric authentication captured on the terminal. The telecom operator then stores the digitally signed authentication response from UIDAI as proof of verification. The retailer can provide a connection to any resident for whom the authentication is successful.

Discussions with industry experts indicate that paperless KYC using Aadhaar can save substantially per subscriber by avoiding TERM fines and paper based backend processes. Telecom operators are issuing over 30 million SIM connections every month that require KYC. Adopting Aadhaar authentication can result in substantial savings of over Rs.1000 crore annually for the industry.

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

With a number of e-Governance and other applications on the horizon, Aadhaar terminals at retailers must be capable to run multiple applications. This will create a new eco-system that will deliver new revenue streams for the small retailer.

[2] DOT notification on usage of Aadhaar for Telecom KYC: http://www.dot.gov.in/as/2011/as_14.01.2011.pdf

[3] Micro-ATM Standards 1.4: http://uidai.gov.in/images/FrontPageUpdates/microatm_standards_v1.4.pdf

[4] Task Force report on an Aadhaar Enabled Unified Payment Infrastructure : http://finmin.nic.in/reports/Report_Task_Force_Aadhaar_PaymentInfra.pdf

[5] Inter Ministerial Group Report: http://www.mit.gov.in/content/government-approves-framework-provision-basic-financial-services-through-mobile-phones

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 deliver of m-governance. Several initiatives are already underway and the Department of 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 will provide a common authentication system making it easier for Government and residents to interact using mobile phones or over the internet.

Conclusion

The telecom sector can leverage Aadhaar in its core areas of providing connectivity and subscriber KYC to lower costs and bring in new revenues. It can help in the deployment of a **million** agent-assisted terminals using its large retail network and enable a **billion** mobile and internet self-service terminals for Aadhaar enabled applications increasing the quality of service by the Government and greatly empowering people at the same time.

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

List of Abbreviations

BC	Business Correspondent
CAF	Customer Acquisition Form
CIDR	Central Identities Data Repository
CRM	Customer Relationship Management
DOT	Department of Telecommunications
GDP	Gross Domestic Product
KYC	Know your Customer
IMG	Inter Ministerial Group
PIN	Personal Identification Number
POA	Proof of Address
POI	Proof of Identity
POS	Point of Sale
SIM	Subscriber Identity Module
SMS	Short Service Message
TERM	Telecom Enforcement and Resource Monitoring
TRAI	Telecom Regulatory Authority of India
UIDAI	Unique Identification Authority of India
USSD	Unstructured Services Supplementary Data

1. Telecom Operator as an Authentication Service Agency

1.1 Aadhaar Enabled Applications

Applications that use Aadhaar authentication to identify and authenticate the resident as part of their service delivery are referred to as Aadhaar-enabled applications. Aadhaar will offer a range of authentication services[7] that enable a resident to authenticate themselves on the basis of their demographic or biometric information. Aadhaar enabled applications primarily use electronic systems to deliver services. These applications are expected in government and other sectors.

The draft Electronic Services Delivery Bill[8] envisions the migration of manual-based public services to efficient, automated electronic delivery of services over time. Aadhaar will enable secure, scalable identity management for these electronic services as they get implemented.

The UIDAI will issue a unique identification number (Aadhaar) to every resident of India, which they can use for the purpose of identification. Residents can identify themselves using the Aadhaar *authentication* process wherein the Aadhaar number, along with other attributes, including biometrics, are submitted to the Central Identities Data Repository (CIDR) operated by UIDAI for verification. Aadhaar authentication is an online real-time service and only responds with a *yes* or *no*.

Aadhaar authentication can be used to verify identification related information on the basis of multiple factors. The following are examples of various factors that can be used in an authentication scheme:

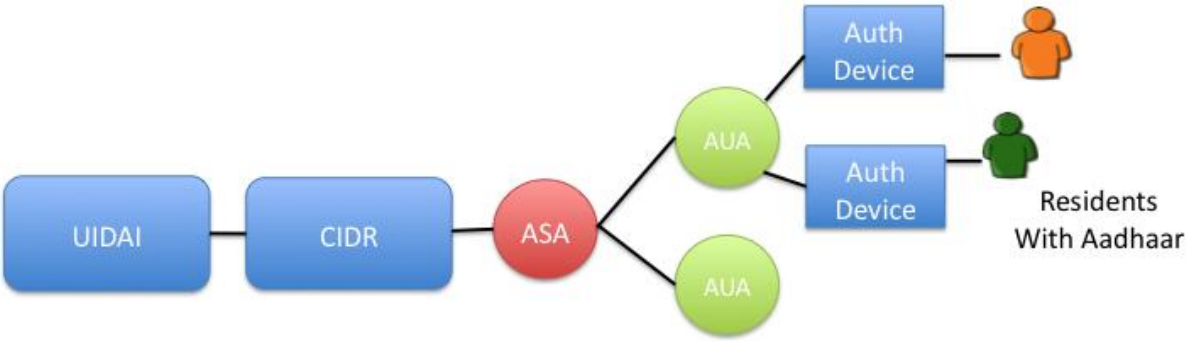
1. What you HAVE – possession of mobile number or a token
2. What you KNOW – a secret PIN, password
3. Who you ARE – biometrics such as a fingerprint scan or iris scan

Increased confidence levels can be achieved when authentication involves verification of two or more factors. Aadhaar authentication also allows for one or more attributes to be submitted along with the Aadhaar number and factors of authentication to the UIDAI's Central Identities Data Repository (CIDR) for verification. Such attributes may include demographic information such as name, gender, date of birth, address, mobile number etc. In all cases, the Aadhaar authentication service responds back only with a *yes* or a *no*.

[7] Aadhaar Authentication API ver 1.5.1

[8] Draft Electronic Services Delivery Bill: http://164.100.24.219/BillsTexts/LSBillTexts/asintroduced/3473LS,%20electronic%20delivery,%20eng..pdf

1.2 The Aadhaar authentication ecosystem



1. **Unique Identification Authority of India (UIDAI):** UIDAI is the overall regulator and overseer or the Aadhaar authentication system. It also owns and manages the CIDR that contains the identity information of all Aadhaar-holders, either by itself or through an agency. An Authentication service provider (AuSP) will offer Aadhaar based authentication services on behalf of UIDAI and is not shown in the diagram above.

2. **Authentication Service Agency (ASA):** ASAs are entities that have established secure network connectivity with the CIDR. AUAs can choose to connect to the CIDR by themselves, where the role of ASA and AUA is assumed by the same entity, or through an existing ASA. An ASA can serve several AUAs. ASAs can also offer any value added services to AUAs or simply act as aggregators.

3. **Authentication User Agency (AUA): An** AUA is an entity that uses Aadhaar authentication for service delivery and connects to the CIDR by itself or through an existing ASA.

4. **Authentication Devices:** These electronic devices form a critical link in the Aadhaar authentication service. These are the devices that collect identity information from Aadhaar holders, prepare the information for transmission, transmit the authentication packets for authentication and receive the authentication results. They could be operator-assisted devices or self-operated devices. Examples of authentication devices include desktop PCs, laptops, kiosks, handheld mobile devices, etc.

5. **Aadhaar holders:** These are holders of valid Aadhaar numbers who seek to authenticate their identity towards gaining access to services offered by AUAs.

1.3 Authentication Service Agency (ASA)

Several telecom operators are in the business of providing connectivity to enterprises. Central Government Ministries, State Governments, public sector organizations, and others are planning to launch Aadhaar enabled applications in the market. These organizations will become AUAs/sub-AUAs of UIDAI.

UIDAI will require AUAs to obtain access to authentication services only through empanelled ASAs. There are currently no charges being levied to become an ASA and authentication services will be offered free until December 2013 by UIDAI.

ASAs must connect to the CIDR over a private point to point leased circuit as part of UIDAI security policies. They must sign and manage the access to authentication services to any AUA as per the ASA services agreement to be signed between ASA and UIDAI.

Telecom operators can take advantage of this opportunity and apply to become an ASA with UIDAI.
Any telecom operator with an enterprise connectivity business can easily handle the tasks of being an ASA – providing connectivity, controlling access to AUAs, and measuring usage for any billing.

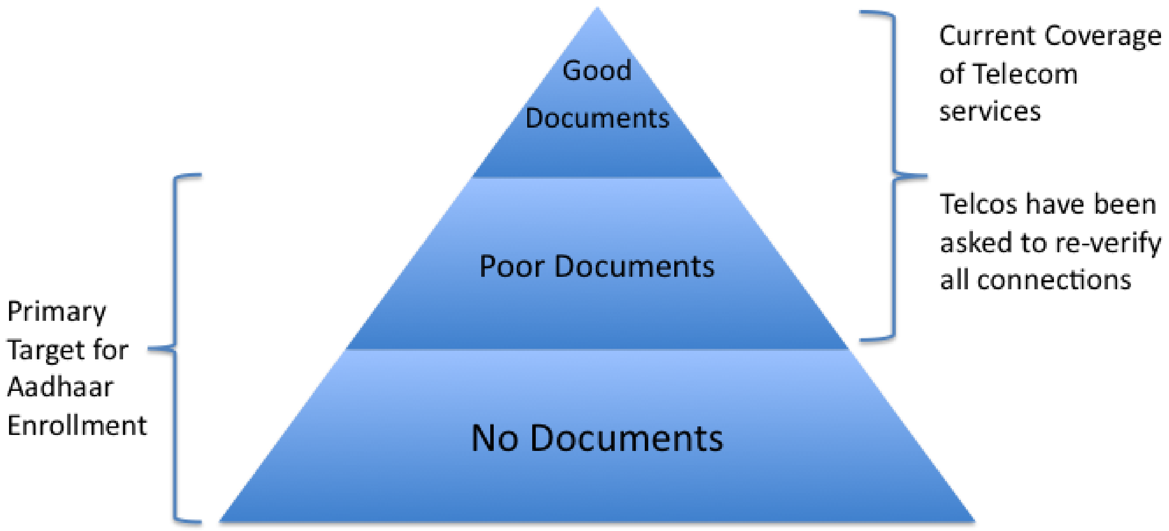
Connectivity between ASAs and AUAs should be secured. The ASA may choose any approach – VPN, MPLS, point to point leased circuit, HTTPS over internet, etc. to provide secure authentication services to AUAs.

2. Telecom KYC with Aadhaar

2.1 Telecom KYC – current state of affairs

Getting access to a telecom connection requires an individual to provide documentation that is acceptable as valid proof of identity (POI) and proof of address (POA) to satisfy the Know Your Customer (KYC) norms laid out by the Department of Telecommunications (DOT). It is well-established that a section of the Indian population is unable to get access to telecom services due to lack of proper documentation.

While no official estimates are currently available, it is estimated that about 20% of applicants in urban areas and 40% of applicants in rural areas are unable to provide appropriate documentation to obtain a telecom connection. The following diagram represents the current situation


Good Documents
Poor Documents
No Documents
Current Coverage of Telecom services
Telcos have been asked to re-verify all connections
Primary Target for Aadhaar Enrollment

Availability of POA / POI Documents
In the Indian Population

The high demand for telecom connections coupled with a population that has poor documentation has resulted in a number of connections being issued with improper documentation. This has led to DOT starting several measures to improve the compliance for subscriber verification. Aadhaar provides inclusive access without compromising security.

2.2 Subscriber verification is weak today

The current subscriber verification process relies on the telecom retailer to issue a connection to the customer in person and also verify the authenticity of documents being submitted for POI and POA.

In reality, not all retailers are sophisticated enough to verify the authenticity of documents. There have also been instances where some retailers have used fabricated documents or re-used documents of other customers to sell telecom connections[9].

2.3 Need for robust subscriber verification

Issues relating to KYC process used to issue a telecom connection by Telecom operators have been under scrutiny for the last few years now. In 2008, DOT started imposing financial penalties on telcos for incorrect documentation. In 2009, telcos were asked to re-verify the documentation of all their existing subscribers which required a mammoth effort.

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. A financial penalty is levied on operators based on the number of incorrect cases found.

As per the annual report of the Department of Telecom 2010–2011[10], the TERM cell has imposed an amount of Rs.700 crore on telecom operators for subscriber verification related penalties. Operators continue to face huge penalties each month based on the findings in the TERM audits.

The mobile subscriber verification audit being conducted by TERM Cells (VTMs) has helped improve the KYC process. Subscriber verification compliance as per TERM is now estimated to have improved from 60% to more than 85%[11] today.

2.4 Aadhaar delivers strong POI and POA

Aadhaar is the national identity program of Government of India and has the mandate for delivering a unique identity number to every resident in the country. The processes setup by UIDAI for issuing Aadhaar are designed to deliver a strong POI and POA. The following are the salient points from the process:

1. The identity and address of the resident are verified during enrollment with well defined standards[12]. The verification methods are:
    a) Document based verification, where the proof of identity / address documents are scrutinized and signed as verified by the registrar's representative;
    b) Introducer based verification, where Introducers authorized by the registrar, authenticate the identity and address of the resident; and

[9] No papers for SIM cards, Buy Forged ones – Times of India, Jun 3 2010: http://articles.timesofindia.indiatimes.com/2010-06-03/mumbai/28297149_1_sim-card-documents-bag

[10] www.**dot**.gov.in/**annualreport**/**2011**/English%20AR%20**2010**-11.pdf, Page 55

[11] TERM website -- http://www.dot.gov.in/vtm/vtm.htm retrieved on Mar 11 2011

[12] Demographic Data standards and verification procedure committee report

   c) Based on the NPR (National Population Register) process of public scrutiny.

2. Biometric data covering ten finger prints and iris scan of both eyes are captured and are used in de-duplication and authentication services;
3. Online authentication services using biometrics can be used to establish identity in real-time providing a strong POI;
4. In our present strategy of delivering the letters by speed post, the address is further verified by having the Aadhaar letter delivered using speed post; and
5. UIDAI, in strong collaboration with the postal department has established an integrated tracking system for the letter. POA verification for Aadhaar uses information from supplied documentation and proof of delivery.

The following table compares Aadhaar for POI and POA with a few other documents considered valid for the same today

Feature	Aadhaar	Voters ID	Passport	Driving License	Comments
Universal ID that can be issued to all residents.	✓	✗	✗	✗	Most documents are linked to entitlements or age limits
Physical document with photo identity	✓	✓	✓	✓	Easy to verify at local retailer
Ability to verify identity online and in real-time using biometrics or demographics.	✓	✗	✗	✗	Ensures fake or tampered Aadhaar documents to be of no value.
Address provided physically verified by a government employee	✓	✗	✓	✗	Apart from document or introducer based verification during enrollment, Aadhaar also uses registered post and tracks delivery to confirm address.

2.5 Aadhaar and telecom KYC

As per the communication[13] from the Department of Telecommunications on January 14, 2011, Aadhaar issued by UIDAI, along with suitable authentication can be treated as valid proof of Identity (POI) and valid proof of address (POA) documentation for the purpose of obtaining a new telecom connection.

Aadhaar authentication can be performed at the retailer's outlet where a mobile connection is issued. The retailer can capture the customer's Aadhaar number and demographic information as required by DOT for the purposes of Aadhaar authentication. The authentication will be performed in real-time and the UIDAI will return with a *yes* or *no,* which signals if the authentication was successful. A unique, digitally signed, authentication response code will also be provided that can be captured in the telecom customer acquisition form (CAF) to track this authentication. Operators can safely and immediately activate these connections as they have been authenticated.

Authentication proves that the person was present during the transaction and is who he claims to be in any document being provided. This process completely eliminates the chances of a false document being used and strengthens the subscriber verification process.

Aadhaar authentication is an online electronic process and demographic and biometric information will need to be captured electronically. This provides an opportunity to make the overall telecom KYC process fully electronic, thereby eliminating the need for paper based systems

2.6 KYC with Aadhaar – stakeholder analysis

Aadhaar provides an incentive compatible solution for Telco KYC enabling benefits for all parties including the resident, retailers, telecom operators and the government

Residents: Any resident can enroll and obtain an Aadhaar number. This allows residents currently with poor to no documentation to obtain an identity document after going thru the robust Aadhaar process. A telecom connection can be easily obtained post enrollment. Since residents must be present and go thru the authentication process when a telecom connection is issued, they can be confident that their identity documents cannot be misused. They now need to take the responsibility for safekeeping and right usage of their connections. Resident must report and block any lost / stolen SIMs to prevent their misuse.

Retailers and Distributors: Introduction of Aadhaar authentication in KYC will come as a relief to retailers and distributors. In the current process, retailers are responsible for physical verification of the resident and checking the original documents as part of the KYC. Investigations related to fake connections frequently involve the retailer and distributor. Retailers are not equipped to verify originality of documents and the

[13] Letter from DOT on usage of Aadhaar for Telco KYC - http://www.dot.gov.in/as/2011/as_14.01.2011.pdf

Aadhaar authentication provides a fool proof way to perform a subscriber authentication in real time. Aadhaar authentication also removes the ability for intermediaries like the retailer and distributor to create fake documentation just to sell connections.

Telecom operators: With Aadhaar authentication, telecom operators can meet 100% compliance on subscriber verification for all connections issued using this process. They will save significantly on financial and legal hassles that they currently face due to poor subscriber verification compliance

DOT, MHA: The Ministry of Home Affairs (MHA) and DoT can be certain that a Telecom connection is being issued to the resident who has authenticated his/her identity. This will strengthen their efforts in improving national security and prevent intentional misuse of connections.

Government: The use of Aadhaar authentication during issue of telecom connections will help strengthen the linkage of a mobile to an Aadhaar number. This will enable an eco-system for m-governance applications in the country. The Government will be able to identify, authenticate, and provide services to residents via the mobile phone.

2.7 Paperless telecom KYC with Aadhaar

The overall process for acquiring a telecom connection can be made fully electronic with no use of paper forms.. The Telecom industry is issuing over 30 million new connections each month in Dec 2011 that require KC. Making telecom KYC fully electronic will reduce reliance on paper to a great extent.

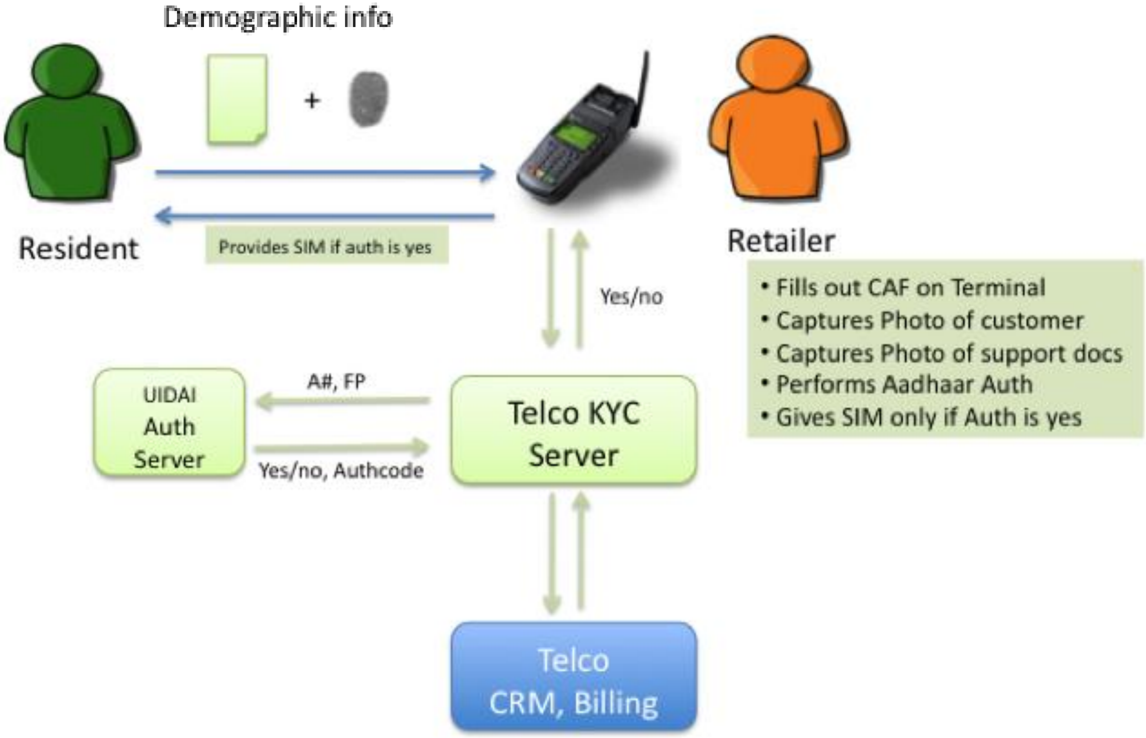
The Information Technology act, 2008, was designed to encourage the use of electronic documents when dealing with the government. Aadhaar authentication adds a *person-present* element to the filing of the electronic KYC form.

The paperless process can be adopted as outlined below:

1. Resident requiring a telecom connection goes to a retailer with an Aadhaar enabled terminal;
2. The retailer captures the details of the resident on an Aadhaar enabled terminal. Several details like Name, address, Aadhaar number can be filled out quickly by scanning the QR code printed on the Aadhaar letter;
3. The customer is photographed electronically using a digital camera that is part of the terminal;
4. The terminal is used to scan in the fingerprint of the resident;
5. The demographic data captured as part of the CAF and the biometric fingerprint data is sent to the KYC server of the telecom operator;
6. The telecom KYC server sends the Aadhaar number, demographic, and biometric information to the UIDAI Authentication service for verification;
7. Authentication is a real-time activity and UIDAI will respond with a Yes / No response back to telecom operator along with a digitally signed authentication

response code. The authentication response code must be saved in the telco KYC server for audit purposes;

8. If the authentication returns with an Yes, then the SIM can be issued by the retailer;
9. CAF data along with the authentication records can now be loaded into the telecom operator's CRM system and the operator can activate the SIM card.


Demographic info
+
Resident
Provides SIM if auth is yes
Retailer
• Fills out CAF on Terminal
• Captures Photo of customer
• Captures Photo of support docs
• Performs Aadhaar Auth
• Gives SIM only if Auth is yes
Yes/no
UIDAI Auth Server
A#, FP
Yes/no, Authcode
Telco KYC Server
Telco CRM, Billing

Industry experts estimate that paperless KYC using Aadhaar can have substantial savings per subscriber by avoiding TERM fines and the cost of paper based backend processes. Telecom operators are issuing over 30 million SIM connections every month that require KYC. Adopting Aadhaar authentication can thus result in huge savings annually for the industry.

3. Aadhaar enabled services at telecom retailers

3.1 India is serviced by the small retailer

India has an estimated 11 million retail outlets with an estimate of over 95% of them being in the unorganized sector. Small entrepreneurs who service local residents run the majority of the outlets that fall in the unorganized sector. Also referred to as kirana stores, these retail outlets are present extensively across India covering both urban and rural India.

Telecom services rely on these retailers to issue new connections or service the existing 770 million connections. With over 98% of the connections being pre-paid, subscribers need to recharge their pre-paid accounts regularly and easily. Over 1.5 million retailers in the country sell pre-paid recharge making it easy for subscribers to find an outlet that can service them.

3.2 Technology adoption by retailers

Telecom retailers use technology to deliver services today. Most pre-paid recharge transactions are fully electronic. The retailer uses an application on his mobile phone to transfer the recharge amount to the customer's phone. Mobile applications are also used in the issue of a new connection. The retailer submits customer details to the distributor and telecom operator usually via SMS. Telecom operators also rely on retailers to guide their customers with inserting SIM cards into phones, checking pre-paid balances, deciding on the right tariff plan and so on.

Telecom retailers are therefore well equipped in the market today to lead any adoption of technology in delivery of services to residents.

3.3 Telecom KYC requires Aadhaar enabled terminals

Aadhaar enabled terminals require to be rolled out at telecom retailers to enable authentication and verify subscribers before issuing a new telecom connection as discussed in Chapter 2.

These terminals are expected to work in the environment that is common for the small retailer. Space and power constraints, price and ruggedness are some factors that will be important in creating a successful product. India already has a vibrant terminal eco-system that can quickly respond to this need and create and deploy these terminals.

3.4 Multiple Aadhaar enabled applications expected

The Government and other sectors are actively looking at the applications of Aadhaar. The Inter Ministerial Group (IMG) report[14] on framework for providing financial services using mobile phones has visualized Business Correspondents (BCs) with mobile Micro-ATMs delivering financial services at every corner of the country.

Micro-ATM is an Aadhaar enabled application that can run on an agent-assisted terminal. The Indian Banks Association working with the UIDAI published the first Micro-ATM standards[15] in October 2010. Any retailer who becomes a BC or sub-agent of a BC, can perform financial transactions like deposits, withdrawals, account to account transfers, check balance, etc. using the Micro-ATM.

As part the financial inclusion drive, RBI announced[16] that for-profit companies could be appointed as Banking correspondents (BC). Since then, a series of partnerships between banks and telecom operators have been announced.

It is expected that telecom operators will use their current set of retailers to provide financial services. The provision of multi-application Aadhaar enabled terminals will enable retailers to leverage the same investment in the KYC terminal for multiple revenue streams.

3.5 Value of Multi-Application Terminals

All Aadhaar enabled applications require some common capabilities including:

1. Computing device for the application to drive menus, data entry etc.;
2. Fingerprint reader if biometric based authentication is required;
3. Connectivity for online authentication;
4. Printer for confirmation and receipts;
5. Effective size to operate in Indian retail environment; and
6. Power management with battery / UPS support.

Retailers are small entrepreneurs and their access to credit and ability to invest is usually low. Multi-application terminals will improve their return on investment by supporting multiple revenue streams from the same device.

Multi-application terminals will incorporate application management capabilities. These will allow new applications to be installed and existing applications to be upgraded over-the-air. The runaway success of App Stores[17] on mobile computing environments like iOS, Android and others are excellent examples of how this could be done.

[14] IMG Framework on Financial inclusion: http://www.mit.gov.in/content/government-approves-framework-provision-basic-financial-services-through-mobile-phones

[15] Micro-ATM Standards 1.4:
http://uidai.gov.in/images/FrontPageUpdates/microatm_standards_v1.4.pdf

[16] RBI Notification for-Profit BCs: http://www.rbi.org.in/scripts/NotificationUser.aspx?Id=6017&Mode=0

[17] http://en.wikipedia.org/wiki/List_of_digital_distribution_platforms_for_mobile_devices

The presence of a large number of retailers with multi-application terminals will create an ecosystem for the government and other sectors to rapidly deploy new applications that can benefit residents. An over-the-air upgradeable terminal creates an extendible model for newer Aadhaar enabled applications to be conceived and deployed over time.

Residents can access these new services locally at their convenience at any of the retailers with an Aadhaar enabled multi-application terminal.

3.6 Types of Aadhaar enabled Terminals

There a number of possible ways to implement multi-application Aadhaar enabled terminals. The following are examples of potential platforms for agent assisted terminals:

Personal computers and netbooks
The personal computer is the most widely used multi application device with billions of devices in production. Over the last few years these devices have been evolving rapidly to create newer class of lower priced devices in the form of Netbooks. These can be easily paired with the peripherals for fingerprint readers, printers and modems for connectivity. The current operating systems that power these devices are highly programmable and will easily allow deployment of multiple Aadhaar enabled applications.

Point of Sale and specialized terminals
Retailers have been using point of sale terminals for credit card and debit card transactions for several years. Several specialized terminals have also been deployed in the market for multiple tasks including bill payment, pre-paid recharge, ticketing etc. These terminals are designed to be rugged and run within the power and space constrains of a retail environment. Manufacturers of these terminals will be able to produce multi-application Aadhaar enabled terminals by integrating Aadhaar authentication capabilities into the same.

Mobile phones and tablets
Mobile phones are today are powerful computing platforms with rich programmable operating systems. Modern smart phones can provide 3G speed data connectivity, high resolution cameras, storage, large displays, full QWERTY keyboards, and ability to interface with peripherals over USB or Bluetooth. Tablets have emerged as a separate category in the last 2 years with larger screens, faster processors and more capabilities than mobile phones. Prices for smart phones and tablets have been consistently moving downwards for the last few years driven by significant volumes in a highly competitive environment. Coupled with a fingerprint reader and printer, the device can perform many Aadhaar enabled functions like Telco KYC, Bank account opening, deposits, etc. Several mobile phone and tablet operating systems support a powerful app store enabling updates and roll outs of new Aadhaar enabled applications to millions of retailers from a central cloud environment.

4. Accessing Government Services over Mobiles

4.1 Mobile Phone - widely available connected device

TRAI reported[18] an urban tele-density of 65.97% and rural tele-density at 34.03% with a total of 893.84 million wireless connections in India as of Dec 2011. With such a large number of connections, the mobile phone has become the first connected computing device that is accessible to most residents in this country.

The penetration of personal computers lag far behind.. Rural households are estimated to have a far lower PC penetration than urban households.

An emerging trend is the fast increase in number of smart phones that offer a wide variety of features at low prices. The connected nature of the mobile phone has converted the mobile phone into a powerful computing platform for delivery of services directly to the resident.

4.2 Mobiles can drive empowerment

In many cases, residents face difficulties in accessing services. India is large country with a geographically spread population. Service points for government or other services may be several kilometers away from their place of residence.

Using the mobile phone to deliver services electronically to residents therefore has many benefits including.

1. **Empowerment** – Residents can interact with the application and get services or benefits without having to deal with any intermediaries;
2. **Anytime Access –** Services can be made available 24 x 7. This removes any barriers they face due to availability of service provider staff;
3. **Convenience –** They can make use of the application from the comfort of their home or work area; and
4. **Extensibility –** This design allows newer applications to be launched over time as more services move to an electronic services delivery model.

The Government is actively looking to deliver services electronically to residents. The Electronic Services Delivery Bill[19] and the draft consultation paper on Mobile governance[20] from Department of Information Technology are steps in this direction.

The Interim report on the Task Force on Direct Transfer of Subsidies on Kerosene, LPG and Fertilizers[21] has visualized a Core Subsidy Management System (CSMS) which

[18] http://www.trai.gov.in/WriteReadData/trai/upload/PressReleases/869/PR-Dec-11.pdf

[19] Draft Electronic Services Delivery Bill: http://164.100.24.219/BillsTexts/LSBillTexts/asintroduced/3473LS,%20electronic%20delivery,%20eng..pdf

[20] Department of Information Technology paper on Mobile Governance

would transfer subsidies in real-time electronically much like in an electronic pre-paid recharge. Access to these subsides will be available from a variety of channels including the mobile phone.

4.3 Aadhaar authentication on the mobile

Any application that needs to identify and authenticate the resident on the mobile will be able to use Aadhaar mobile authentication services. Using Aadhaar authentication these applications can securely verify the identity of the resident and deliver access to the service.

The resident can declare his mobile number to UIDAI during enrollment, at an update station or in the process of kyc for a mobile connection. The mobile number is registered by UIDAI only after verifying possession of the mobile electronically. Only registered mobiles can be used for Aadhaar Authentication.

The resident can verify the possession of the mobile number via SMS, USSD, IVR or the Web with UIDAI. The resident can also setup an Aadhaar PIN with UIDAI. The Aadhaar personal identification number (PIN) is a resident chosen 6 digit number that acts like a password. When the user interacts with a self-service application over the mobile, the mobile number is securely retrieved from the network. The Aadhaar Number + Aadhaar PIN along with the mobile number forms an Aadhaar authentication scheme testing both the “what you have” and “what you know” from the resident.

Depending on the level of security required, Applications can use mobile authentication in the following ways:

1. Perform a demographic auth with Aadhaar number and Mobile Number;
2. Request for an OTP to be sent to the registered mobile and accept that for 2 factor authentication; or
3. Perform an authentication that involves the registered mobile number and other demographic details like name, date of birth, PIN code in address, etc. for additional factors in authentication.

4.4 Encouraging M-Governance

Telecom operators can encourage this move towards electronic service delivery from governments. In order to interact with residents on the mobile, departments will need short codes, low but uniform pricing, secure mobile number transfer and technology advisory and support.

The Mobile Services Delivery Gateway (MSDG) initiative by the DIT is an example of how delivery of services can be made easier.

M-governance services can drive large new revenue streams for the telecom operator and hence it makes immense sense in supporting Government Departments to bring services on to the mobile.

[21] http://finmin.nic.in/reports/Interim_report_Task_Force_DTS.pdf

4.5 Self-service channels on the mobile

For widespread usage of self service on mobile phones applications need to cater to all types of people from educated residents with a 3G enabled smart phones to the illiterate residents with just basic mobile phones.

Services can be developed on mobile phones for all types of residents using one or more channels on the mobile phone. Aadhaar authentication will be available for all channels enabling identification of residents on any channel.

The following section describes the various channels and outlines the advantages and restrictions of the same for development of self-service applications.

IVR or Voice Calls: IVR or Interactive Voice response is a way of building interactive applications on a voice call. Users dial a number and are connected to an automated system. Users can interact by pressing DTMF keys on their phone or in some cases by "saying what they want" with speech recognition.

IVR systems can be used by anyone and works on *all mobile phones.* The interface language can be chosen by the user and is very popular in India. This is the only medium with a local language interface that works on any phone. The voice user interface being a "serial" interface is not very good for long information delivery. IVR systems work well for simple short transactions.

Both notifications and inbound queries can be supported. For notifications the system calls out the resident (also called as outbound dialer or OBD) and once the resident has answered the call can "play out" the information to the user.

SMS: This is widely accepted and used channel especially for notifications. A text message of 160 (or longer) characters can be sent to the mobile with status or other information. This works on *all mobile phones.*

About 40% of the current mobile users in India are known to send SMS while a slightly larger number never send an SMS but only read incoming messages. Interactive applications can be developed on SMS where the user sends a keyword to a short code like 1947 and receives the response on SMS.

USSD: This is a session based text interaction and is *available only on GSM phones.* An example of a USSD transaction is to check prepaid balance. Users dial *123# on their mobile. This initiates a USSD session and the result is displayed as a popup on the mobile screen. With almost all users in India knowing how to dial a number, it is usually easy to educate users to adopt USSD based transactions.

The simplicity of USSD makes it an interesting channel for simple transactions like status information, simple menu choices and others. The language of this interface is similar to SMS and largely restricted to English in India. GSM is now the pre-dominant mobile system in India accounting for 85% of all mobile connections. On CDMA, it is possible to make the same sequence of code *123# be routed to an IVR.

Mobile Web: It is estimated that 80% of the phones now being sold in India support data connectivity via 2.5 G or 3G technologies. These mobile phones carry powerful browsers that can support almost the full HTML standard. Older phones support a subset of HTML and the oldest support the original mobile web standard called WAP / WML. India is currently estimated to have between 30 – 40 million "active data users". These are people who use the mobile web at least once a month.

Interactive self-service applications can be easily developed for mobile devices very similar to a website. The telecom operator is capable of passing a verified mobile number on the mobile web making it possible to securely authenticate users

Notifications via SMS can carry URLs. Most phones are now capable of allowing users to select these urls and launch the site on the mobile device.

The mobile web is available *only on data capable phones that have been activated for data plans by the resident.*

Mobile applications: The computing power and capabilities of the mobile phone has undergone a rapid change over the past 5 years starting with the launch of the first iPhone by Apple. Applications that can be downloaded to the mobile device and run on the handset (called Mobile Apps) have become very popular. This can be implemented on any platform for mobile applications.

5. Conclusion

The telecom industry can benefit greatly from Aadhaar:

1. By becoming ASAs, telecom operators can bundle authentication services along with connectivity to a large number of organizations who want to be AUAs.

2. Using Aadhaar authentication in their KYC process will help save significant sums of money paid as fines, and also avoid the expensive legal processes that result due to improper KYC checks. Aadhaar will also enable inclusive growth in the telecom sector as it covers residents without any existing identity documents, without compromising security.

3. Operators can leverage their existing network of retailers to create new markets and revenue streams with Aadhaar-enabled applications in retail. A million retailers with multi-application Aadhaar terminals will help delivering a range of electronic services to residents.

4. Government services can be easily accessed with various mobile applications wherein Aadhaar authentication can be used to verify the identity of the resident.