White Paper on
"Mobile as digital identity"
Version 0.1

Introduction

Mobile penetration in India currently is estimated to cover around 71 percent of the total population. Increasing internet usage on mobile, reduction in handset costs, introduction of low end smart phones has made mobile a convenient and cheaper channel. While all these reasons present tremendous opportunities for using mobile phones for public service delivery, at the same time, an innovative and practical use of mobile phones would be to use them as instruments of digital identity for delivery of public service. A large number of applications, like those used by banks, are already using mobile phones to authenticate their online users.

For mobiles to be instruments of authentication for digital identity, they should by unique, authenticable and fulfill requirements of non-repudiation. While institutions like banks can achieve the above requirements by physical verification and enrolment of the users for mobile banking and linking a user's mobile number to her already existing identity registered with banks, it is a challenge in case of public service delivery by government entities. For government, a possible way of achieving the same would be to link the mobile numbers of users to their Aadhaar, a unique and verifiable identity provided by a trusted authority, UIDAI.

Digital India Vision

Digital India is a programme to transform India into a digitally empowered society and knowledge economy.

Mobile is an integral part of Digital India Vision and has been embedded into the key vision areas

The vision of Digital India is centered on three key areas:

1. **Digital Infrastructure as a utility to every citizen**
2. **Governance & services on demand**
3. **Digital empowerment of citizens**

These vision areas talk about providing a) Cradle to grave digital identity that is unique, lifelong, online and, authenticable to every citizen b) Mobile phone & bank account enabling citizen participation in digital & financial space c) Services availability in real time from online & mobile platforms.

Solution Objectives

1. Enable remote and secure verification of an Aadhaar holder using mobile during mobile based services.
2. Enable use of mobiles as an identity instrument and trusted authentication factor that is attached to Aadhaar, thereby simplifying online access to public services.
3. Enhance reach of public services without any substantial cost implications by leveraging existing identity sources.
4. Provide a solution that is open, interoperable, transparent, robust and sustainable.

Aadhaar and Mobile

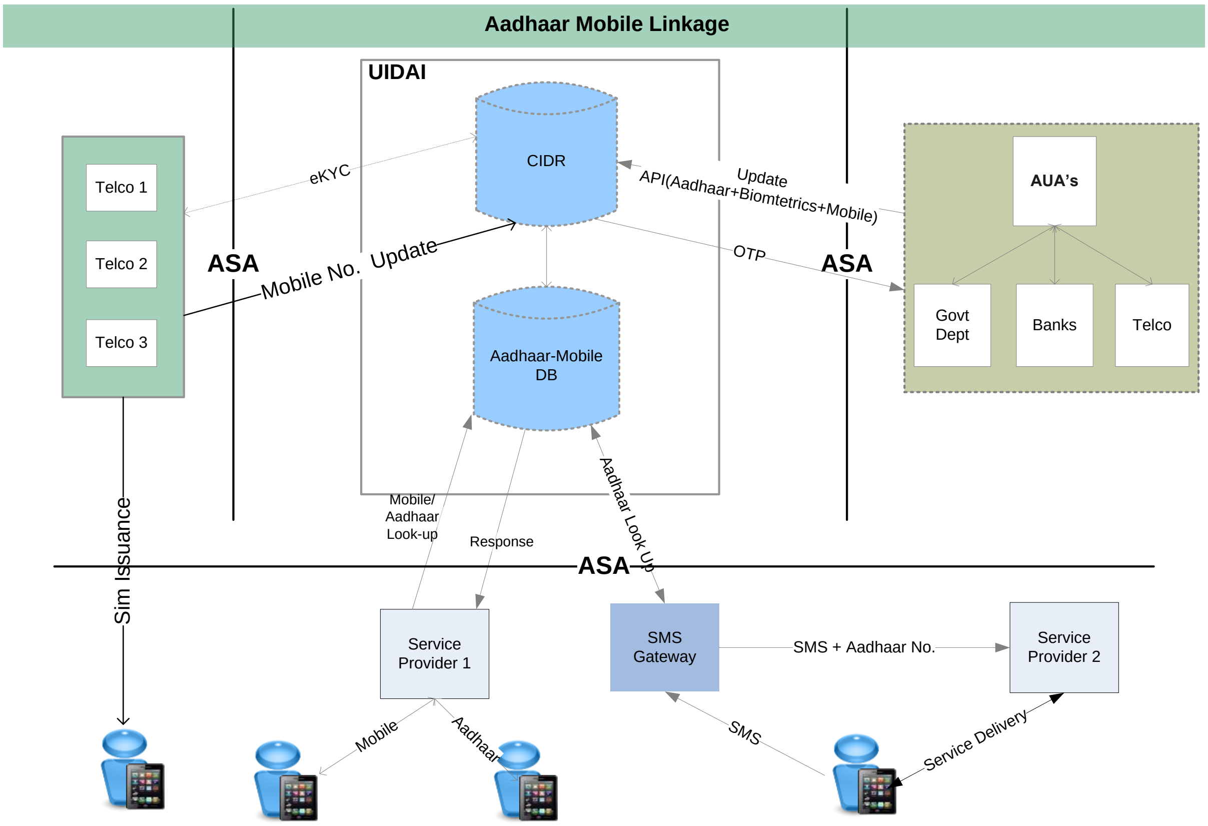
Aadhaar system already offers a mechanism to keep mobile number linked to Aadhaar identity. In addition to linking, Aadhaar authentication offers mobile OTP (One Time Pin) based authentication for Aadhaar holders. Government applications can easily take advantage of this strong linkage of Aadhaar to mobile within their applications in two ways:

1. Verifying mobile linkage via demographic authentication – Service delivery applications can easily check "Aadhaar to mobile number" link by doing a demographic authentication.
2. Using Aadhaar OTP service to authenticate Aadhaar holder – Service delivery applications can use Aadhaar OTP service to authenticate their beneficiaries without storing mobile number or creating their own authentication mechanisms.

Above two assumes that mobile number in Aadhaar database is up to date for every individual. If Aadhaar systems offers a mobile update API for "trusted" AUAs (Authentication Service Agencies), this issue can easily be addressed.

Proposed Steps

1. Build Aadhaar-Mobile DataBase



Multiple databases would feed "Aadhaar-Mobile DB" by providing the Aadhaar-Mobile link. These would be:

- Aadhaar database, which has collected the mobile numbers of the users while enrollment or while updating of profile.
- TSP(Telecom Service Providers) database, which would map mobile number of a subscriber with the Aadhaar number through Aadhaar e-KYC for old as well as new subscribers.
- Service Provider/Department (AUA's) like Bank, Telco's, Government. Department's which has seeded Aadhaar number.

To get the benefit of global mobile authentication for all Government service delivery applications and to establish a strong link between Aadhaar and mobile, it is imperative that the mobile number in Aadhaar database is kept up-to-date.

This can be achieved by taking the following steps:

A. **Adopt Aadhaar OTP authentication** – Government service applications adopting mobile authentication via Aadhaar OTP and hence generating "automatic incentive" for Aadhaar holders to update mobile number in Aadhaar system

a. Mobile/Internet applications can simply request Aadhaar holder to use his/her mobile OTP while authenticating into the application
b. Aadhaar system already provides all necessary APIs for this purpose.
c. This eliminates the need for every Government application across the country to capture, store, validate, send SMS, etc. to authenticate an Aadhaar holder.

B. **Offer AUA based Mobile Update API** – UIDAI should offer a mobile update API to "trusted" AUAs (TSPs, Banks, Government services, etc.) so that at any of the biometric authentication service of these AUAs, Aadhaar holder is able to update his/her mobile number in Aadhaar system with simple biometric authentication.
   a. Thousands of biometric terminals used for various applications can be used for updating mobile number via biometric authentication
   b. AUA applications can simply capture Aadhaar number, mobile number, and biometric data to allow Aadhaar holders to update their mobile number in Aadhaar database
   c. On successful Auth., UIDAI to send OTP for verification on the Updated Mobile no.
   d. On successful verification of OTP, Mobile No. updated in CIDR.
   e. This also allows Government application databases to be in sync (e-KYC based sync) with Aadhaar system without collecting and verifying mobile number and other core demographic attributes.

2. Use e-KYC and Aadhaar in Telecom Services

For creating a strong Aadhaar and mobile link, in addition to Aadhaar database having mobile number up to date (as described in above section), it is also critical that Telecom Service Providers (TSPs) adopt Aadhaar e-KYC and also offer capability to update mobile number in Aadhaar database. In a sense, Telecom Service Providers (TSPs) to form part of the trust chain.

1. **Use of e-KYC for SIM Issuance** – Whenever new numbers (SIM card) is issued, strong KYC is mandated. But, in reality paper based KYC is expensive and error prone. Aadhaar e-KYC offers a cost effective, secure, non-repudiable, paperless, KYC scheme for TSP's.

   - UIDAI offers the e-KYC service, which enables a resident having an Aadhaar number to share their demographic information and photograph with a UIDAI partner organization in an online, secure, auditable manner with the residents consent. The consent by the resident can be given via a Biometric authentication or a One Time

Password (OTP) authentication. Upon successful authentication and consent of the resident, the UIDAI will provide the resident's name, address, date of birth, gender, photograph, mobile number (if available), and email address (if available) to the service provider electronically.

- 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 based on OTP or Biometric based authentication issue the SIM card to the applicant. The authentication will be performed in real-time.

- Operators can safely and immediately activate these connections as the customers have been authenticated.

2. **Link Aadhaar to the mobile** – TSP databases should link Aadhaar number to mobile numbers. This ensures that all numbers are attached to a unique, verifiable national identity.

   - **Seeding of Aadhaar for new customers** - In all the cases discussed below, it is assumed that the customer will follow the UIDAI's process to register her existing Mobile Number (if available) in the Aadhaar database.

     i. **Customer already has a Mobile number and applying for an additional connection:** OTP/Biometric based e-KYC can happen at the retailer's outlet and the customer can be issued a new mobile number. Based on the customer's consent, same number can be updated by TSP in Aadhaar database and can be treated as a master Mobile number.

     ii. **Customer applying for a fresh connection:** Biometric based authentication can happen at the retailer's outlet and the customer can be issued a new mobile number and based on customer's consent same number can be updated by TSP in Aadhaar database.

   - **Seeding of Aadhaar for existing customers**

     i. Customer may visit their respective Telco's retail outlet wherein OTP/Biometric based e-KYC can be performed to link Customer's Aadhaar number in TSP's database.

     ii. Customers can also send an SMS mentioning their Aadhaar number to a pre designated Number (as desired by TSP) or use USSD channel to allow linkage option, Telco's can then extract the Mobile number along with Aadhaar number and can do Demographic based Aadhaar authentication and can subsequently seed the Aadhaar number against the corresponding Mobile number in their database.

3. Fund Integrated Biometric on Mobile

India is seeing a revolution in phone with availability of cheap smart phones in the market. Currently India already has about 120 million smart phones which is expected to grow to 500 million in the next 4-5 years. Considering touch based smart phones are easy for a common person to use, most of the next generation Government and private applications are sure to be on smart phones.

India is the only country where a strong national authentication utility, Aadhaar, is established with open APIs boosting many ecosystem applications to be developed using this open Government utility. Many applications require either single factor (1-FA) or two factor (2-FA) authentication. For a large population of diverse background it is best to use "implicit" factors that are "always available". Two such strong factors are mobile ("what you have" factor) and biometric ("what you are" factor). Hence it is necessary that Indian Government pushes biometric on the Smartphone (fingerprint or iris) which can work with national authentication framework.

Bootstrapping the market with Government funding for providing integrated biometric sensors within the Smartphone will allow applications that can offer single click 2-factor authentication features boosting secure electronic payments, digital signature (e-Sign), and a set of paperless services.

Mobile device manufactures can be encouraged to "Make in India"/"Make for India" via such bootstrapping fund. Even with orders of a few million quantity (compare it to 100 million smart phones already used in market) can bring BoM (bill of material) cost of sensors (especially Iris) to less than 2-3 USD. This means that mobile device manufactures can easily offer Iris sensors integrated to their phones for a fractionally low cost. Real issue is the initial bootstrapping support which is required to break the "wait and watch" mode of mobile device vendors.

Biometric enabled smart phones can completely change the way Government and private applications can work in Digital India. It is necessary that Government of India sets aside a small fund to bring out biometric enabled smart phones to Indian market. This can be for initial 2-4 years after which market demand will automatically sustain the innovation.

Digital India vision calls for such innovative approaches that can trigger a slew of self-service applications in various fields available to people on their smart phones.

Future Considerations

Following are some of the ideas that can be considered in future once the Aadhaar linked mobile authentication is in place across many applications.

1. Obtaining Mobile Number using TSP Service

Currently to verify "possession of a linked phone", applications have to depend up on OTP scheme. While Aadhaar based central OTP authentication can avoid individual applications to collect, store, and verify mobile numbers, use of OTP as a mechanism to validate possession of mobile and used as a "what I have" factor is less secure since it can be "shared" and used in other mobiles. For example, when an application validates using OTP, user can share the OTP with another individual who then can use OTP to authenticate as he/she had obtained it on his/her phone.

This issue of "ability to share" an OTP can be avoided if applications can "reliably obtain" the mobile number using a TSP service. Such mechanism needs to be "reliable", "trustable", and "privacy protected" (only with user's consent). **This can completely eliminate OTP as we know today and enable mobile applications can seamlessly authenticate users without user interaction and data entry**.

There are 3 broad ways this can be achieved:

- Use of secure SIM service – SIMs available in India can offer a service integrated to mobile operating systems to obtain the mobile number in a signed fashion via secure SIM API.
- Use of TSP provided OS services – TSPs in India can offer an integrated service within mobile operating systems with a secure API to provide mobile number in a signed fashion to mobile applications.
- A mechanism to obtain mobile number from the network – This can work like a cookie in browser world. Mobile applications should have a secure way to fetch this TSP signed token and authenticate.

Above suggestions are broad and only indicative. Detail specifications need to be worked out to establish most effective, easy to offer, secure, and privacy protected method before any implementation can take place.

2. Aadhaar based PKI via Mobile

Digital signatures are legally valid as per Indian IT Act 2000. Till date, one of the most prominent methods to use digital signatures was to store those on USB devices. Being legally accepted in India, a mechanism for widespread use of digital signatures for establishing identity and authentication in digital world could be mobile digital signatures. Mobile digital signatures can thus provide customers and service providers a legally recognized method of electronic transactions that fulfill confidentiality, integrity and non- repudiation aspects.

There are two ways to increase the use of PKI so that true paperless services can be offered and digitally signed documents can become mainstream.

1. **Aadhaar biometrics Based PKI** – In this scheme, the authentication of the signer is proposed to be carried out using e-KYC of Aadhaar. When smart phones start integrating biometric sensors, this become even easier to self-sign a document using a fully legal, IT Act compliant, digital signature scheme.

2. **Aadhaar Linked SIM based PKI** - The implementation of PKI credentials (private, public keys) using secure hardware crypto tokens(which can be used on Mobile phones) helps in achieving the requirements of legally accepted digital signatures as laid out by CCA. Such Mobile Digital Signature enabled devices store the user's private key on the mobile phone using various embedding technologies. A viable solution to securing the private key is to encrypting it and there are various technologies such as Cryptographic SIMs, Secure SD Cards, and Slim SIMs which are used in order to provide secure data transmission from a mobile device. As mentioned in previous section, these Cryptographic SIMs can be issued based on Aadhaar based e-KYC.

Use Cases

Aadhaar Notification Bridge

Most Government applications today send notifications (SMS / Email) to Aadhaar holders. This requires every application to capture, store, and validate mobile and email addresses. Applications normally store these in their own databases. Many applications may not have a convenient way to update this data once captured and also may not have appropriate data protection considering IT Act has stringent rules of protecting PII data.

Such usage creates two issues:

- Handling of change of mobile numbers or email IDs require change in every application and;
- Mobile numbers and emails are made available to many applications which may or may not have appropriate protection from misuse of such data.

"Aadhaar Payment Bridge" under National Payment Corporation, where "money can be sent to an Aadhaar number" by Government applications without having to capture, store, and validate bank account details, has dramatically simplified direct benefits transfer. Along the same line, if an "Aadhaar Notification Bridge" can be created for Government applications to "send notification to an Aadhaar number", it can simply a lot of notification process, mobile/email update, and consumer preferences of receiving such notifications on their preferred device or application.

Such schemes can make notifications "loosely coupled" allowing "receiving applications" to offer innovative features such as automatic translations, read-out-loud, etc. without sending applications to have these features. Aadhaar holders can sign up with "best notification application" of their choice to receive such notifications.

Such notification platforms must be "ecosystem driven", "API based", "secure and privacy protected", and most importantly allow Aadhaar holders full freedom of choice of "providers" and "opt-in and opt-out" capabilities. But, a scheme such as this can surely make notifications be delivered to Aadhaar holders in a reliable and most innovative ways!

Government Welfare Schemes (MGNREGA)

As per the operational guidelines 2013, the workers in need of employment under MGNREGA are promptly provided work, the process of submission of applications for work must be kept open and available on a continuous basis through multiple channels so designated by Gram Panchayats. The multiple channels to receive applications for work and issue dated receipts could be ward members, anganwadi workers, school teachers, SHGs, village-level revenue functionaries, Common Service Centres (CSCs) and Mahatma Gandhi NREGA Labour Groups. As most of the workers are illiterate, the system must be made convenient to them and should include Interactive Voice Response System (IVRS) and voice-enabled interactions. This option must automatically register the demand for work and keep date and time stamp of such demand.

Apart from the above mentioned channels to register workers "demand for work", SMS as an alternate channel to receive demand for work can be made operationalised. Workers can register for "Demand for work" by sending an SMS to a pre designated number. NREGASoft application would capture the Mobile number and will do a look-up in Aadhaar-Mobile DB and can register the Worker's demand for work against his corresponding Aadhaar No. (which is mapped to Job card No. in NREGA Database{currently 4.65 cr Aadhaar Number seeded in NREGA}). The application will provide acknowledgement of the receipt of "Demand for Work" over the SMS to the worker. The worker can show this SMS along with his JOB Card to appropriate authorities in-case he is not allocated the work within 15 days of his Demand for work application.

Conclusion

India will see an explosion of Smartphone and mobile Internet making most application delivery to move to mobile applications. It is expected that at least 400-500 million Smartphone with Internet connection will be in use within next 4-5 years. Aadhaar is also expected to cover all of India in next 12-18 months provide a universal digital identity to everyone.

Usage of Aadhaar and strong mobile authentication can boost identity verification via mobile services across the service delivery schemes. It allows next generation mobile applications to offer convenience and security, enable single click 2-FA mobile electronic payments, establish a mechanism to use digital signature via mobile (using e-Sign), and ensure all mobile numbers have strong KYC backing and attached to a national digital identity.