

Guidelines

On

Mobile as Digital Identity



Government of India
Ministry of Communications & Information Technology
Department of Electronics and Information Technology
New Delhi – 110 003

Metadata of Document

S. No.	Data elements	Values
1.	Title	Guidelines On Mobile as Digital Identity
2.	Title Alternative	Guidelines on Mobile and Aadhaar Linkage
3.	Document Identifier <i>(To be allocated at the time of release of final document)</i>	Mobile ID
4.	Document Version, month, year of release <i>(To be allocated at the time of release of final document)</i>	V1.0, July 2015
5.	Present Status	Approved
6.	Publisher	Ministry of Communication and Information Technology, Department of Electronics and Information Technology
7.	Date of Publishing	
8.	Type of Standard Document <i>(Policy / Technical Specification/ Best Practice /Guideline/ Process)</i>	Guideline
9.	Enforcement Category <i>(Mandatory/ Recommended)</i>	Recommended
10.	Creator <i>(An entity primarily responsible for making the resource)</i>	Ministry of Communication and Information Technology, Department of Electronics and Information Technology
11.	Contributor <i>(An entity responsible for making contributions to the resource)</i>	DeitY, National e-Governance Division(NeGD), UIDAI
12.	Brief Description	For mobiles to be instruments of authentication for digital identity, they should by unique, authenticable and fulfil requirements of non-repudiation and for government, a possible way of achieving the same would be to link the mobile numbers of residents to their Aadhaar Number, a unique and verifiable identity provided by a trusted authority, UIDAI.

		This document outlines the Concept, Architecture and Ecosystem for linking Aadhaar Numbers with Mobile Numbers.
13.	Target Audience <i>(Who would be referring / using the document)</i>	UIDAI, Public Service Delivery Government Departments, Telecom Operators, Mobile Handset manufacturers, CCA
14.	Owner of approved standard	Ministry of Communication and Information Technology, Department of Electronics and Information Technology
15.	Subject <i>(Major Area of Standardization)</i>	Mobile ID
16.	Subject. Category <i>(Sub Area within major area)</i>	Guidelines On Mobile as Digital Identity
17.	Coverage. Spatial	India
18.	Format	PDF
19.	Language <i>(To be translated in other Indian languages later)</i>	English (To be translated in other Indian languages later)
20.	Copyrights	Ministry of Communication and Information Technology, Department of Electronics and Information Technology
21.	Source <i>(Reference to the resource from which present resource is derived)</i>	Different resources, as indicated in the document.
22.	Relation <i>(Relation with other e-Governance standards notified by DeitY)</i>	-

Executive Summary

Digital India initiative of Government of India envisages providing a digital identity to all individuals to facilitate online delivery of public services through their electronic authentication. Also, such digital identity should be unique, lifelong, online and authenticable.

Mobile phones and digital identity could be linked so that mobile phones can be used as instruments for electronic authentication of individuals' identities. Online authentication using Aadhaar, which is already being offered as an authentication mechanism by UIDAI, can be made seamless if mobile numbers of individuals are linked to their Aadhaar numbers. This would do away with users providing Aadhaar number for every transaction as their mobile numbers would represent their Aadhaar number.

Table of Contents

Table of Contents.....	5
1 Introduction.....	7
1.1 Digital India Vision	7
1.2 Objectives	8
2 Target Audience	8
3 Type of Standard Document & enforcement Category.....	8
4 Aadhaar and Mobile.....	9
5 Proposed Steps	10
5.1 Build Aadhaar-Mobile Database	10
5.2 Adopt Aadhaar OTP authentication.....	11
5.3 Offer AUA based Mobile Update API	11
5.4 Use e-KYC and Aadhaar in Telecom Services	11
5.4.1 Use of e-KYC for SIM Issuance.....	12
5.4.2 Link Aadhaar to the mobile.....	12
5.5 Fund integrated enablement of biometric on mobile	13
6 Future Considerations	15
6.1 Obtaining mobile number using TSP Service	15
6.2 Aadhaar based digital signatures via mobile.....	16
6.2.1 Aadhaar biometrics based digital signatures.....	16
6.2.2 Aadhaar linked SIM based digital signatures.....	16
7 Steps for Mobile updation in Aadhaar.....	17
8 Use Cases.....	18
8.1 Financial Inclusion.....	18
8.2 Aadhaar Notification Bridge.....	18

8.3	IRCTC.....	20
8.3.1	IRCTC Current Process	20
8.3.2	IRCTC Proposed Process	20
8.4	Government Welfare Schemes.....	21
8.4.1	MGNREGA (Mahatma Gandhi National Rural Employment Guarantee Act).....	21
8.4.2	PDS (Public Distribution System).....	22
8.5	Commercial Applications	23
9	Conclusion.....	24
	Annexure I: International Mobile Identity Solutions.....	25

1 Introduction

Mobile penetration, in India currently, is estimated to cover around 71 percent of the total population. Factors such as increasing use of internet on mobile, reduction in handset costs, introduction of low end smart phones have made mobile a convenient and cheap channel to transact. 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 services. A large number of applications, such as 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.

1.1 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**

The vision areas talk about 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.

1.2 Objectives

The objective of the solutions proposed in the documents is to:

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

2 Target Audience

UIDAI, Public Service Delivery Government Departments, Telecom Operators, Mobile Handset manufacturers, CCA

3 Type of Standard Document & enforcement Category

This document, as the name suggests, provides norms and recommendations termed as guidelines for linking mobile number to Aadhaar identity.

4 Aadhaar and Mobile

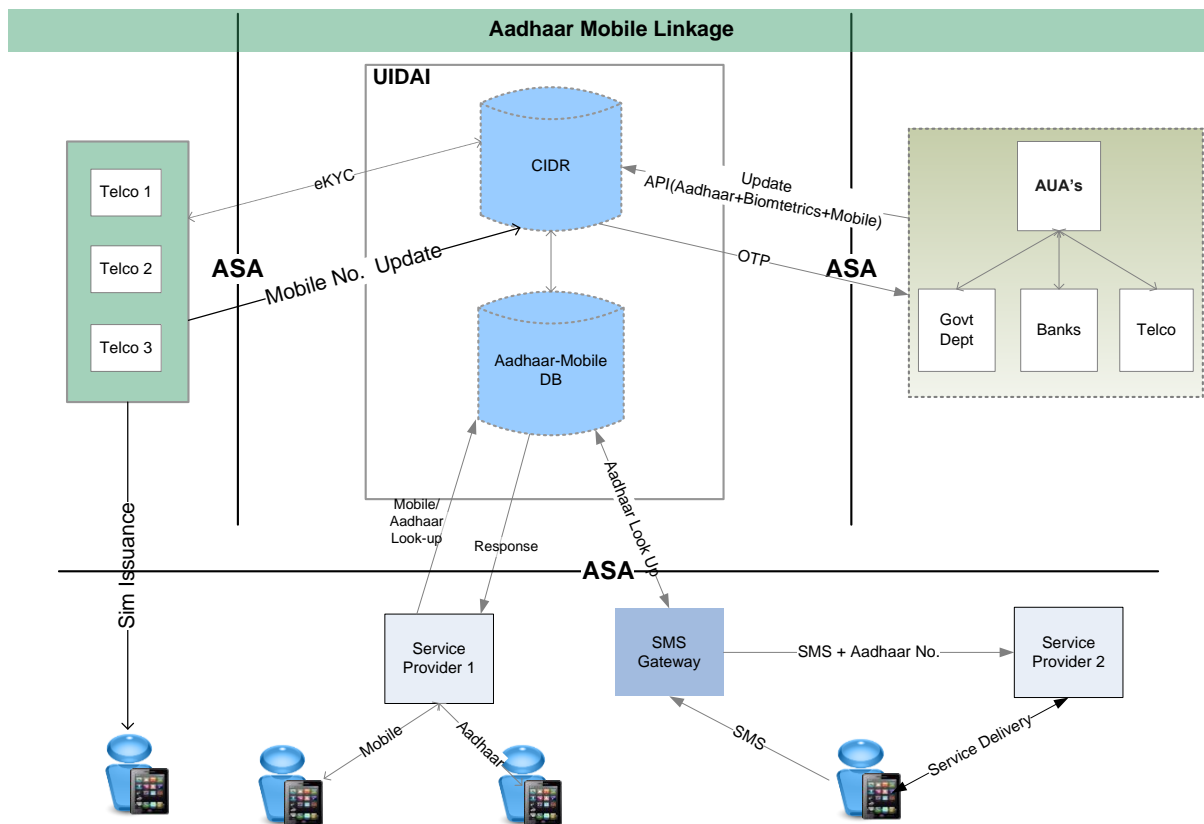
UIDAI's Aadhaar system already offers a mechanism to keep mobile number linked to Aadhaar identity. In addition to linking, Aadhaar authentication offers mobile OTP (One Time Pin) based authentication for Aadhaar holders. Government applications can easily take advantage of this strong linkage of Aadhaar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

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

For this, the mobile number in Aadhaar database is required to be up to date for every enrolled individual which in turn, requires a convenient and secure process to be in place to allow individuals to update their mobile numbers in Aadhaar database, as and when they change their mobile number. Aadhaar system can cater to the requirement by offering a mobile update API to the “trusted” AUAs (Authentication User Agencies) in the Aadhaar ecosystem.

5 Proposed Steps

5.1 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 enrolment or while updating individual’s record.
- 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).
- “Trusted” Service Providers/Departments (AUA’s) like Bank, Telco’s, Government Departments having Aadhaar number and mobile number seeded in their database.

For establishing a strong link between Aadhaar and mobile, it is imperative that the mobile numbers in Aadhaar database is kept up-to-date.

This can be achieved by taking the following steps:

5.2 Adopt Aadhaar OTP authentication

Government service applications adopting mobile authentication via Aadhaar OTP would generate an “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 to the service delivery applications 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.

5.3 Offer AUA based Mobile Update API

UIDAI should offer a mobile update API to “trusted” AUAs (TSPs, Banks, Government services, etc.) so that any individual enrolled to Aadhaar is able to update his/her mobile number with simple biometric authentication.

- a. Thousands of biometric terminals, used by various applications, can be used for updating mobile number through 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 authentication, UIDAI would send OTP for verification on the updated mobile number.
- d. On successful verification of OTP and other details of the requestor, mobile number would be updated in CIDR.
- e. This would also allow 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.

5.4 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.

5.4.1 Use of e-KYC for SIM Issuance

Whenever new numbers (SIM cards) are 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.

- a. UIDAI offers e-KYC service, which enables an individual having an Aadhaar number to share their demographic information and photograph with a UIDAI partner organization in an online, secure, auditable manner with the consent of the individual. Such consent by the individual can be given through biometric or a One Time Password (OTP) based authentication. Upon successful authentication and consent of the individual, the UIDAI provides the individual's name, address, date of birth, gender, photograph, mobile number (if available), and email address (if available) to the service provider electronically.
- b. Aadhaar authentication can be performed at retailer outlets which are the points of sale for new mobile connections. The retailers can capture the customer's Aadhaar number and based on OTP or Biometric based authentication issue the SIM card to the applicant. Such authentication would be performed in real-time.
- c. Operators can safely and immediately activate these connections as the customers have been authenticated.

5.4.2 Link Aadhaar to the mobile

TSP databases should link Aadhaar number to mobile numbers of its subscribers. This ensures that all numbers are attached to a unique and verifiable national identity.

5.4.2.1 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.

- a. **Customer already has a Mobile number and applying for an additional connection:**
OTP/Biometrics 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 primary mobile number.
- b. **Customer applying for a fresh connection:**

Biometrics based e-KYC 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.

5.4.2.2 Seeding of Aadhaar for existing customers

- a. Customer can visit their respective TSP's retail outlet wherein OTP/Biometric based e-KYC can be performed to link customer's Aadhaar number with his mobile number in the TSP's database.
- b. 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.

5.5 Fund integrated enablement of biometric on mobile

India is seeing a revolution in phone with availability of cheap smart phones in the market. Considering touch based smart phones are easy for a common person to use, most of the next generation Government and private applications are going 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 biometrics ("what you are" factor). Hence it is necessary that Indian Government pushes for biometric enabled smartphones (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.

6 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.

6.1 Obtaining mobile number using TSP Service

Currently to verify “possession of a linked phone”, applications have to depend upon OTP method. 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.

6.2 Aadhaar based digital signatures 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.

6.2.1 Aadhaar biometrics based digital signatures

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

6.2.2 Aadhaar linked SIM based digital signatures

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. 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.

7 Steps for Mobile updation in Aadhaar

For user authentication using Aadhaar and mobile number, it is essential to establish a strong link between the two and hence it is imperative that the mobile number is present in Aadhaar database and is kept up-to-date.

Currently residents can follow any of the below mentioned steps to provide/update their mobile number:

1. Residents can provide their Mobile Number during Aadhaar enrolment camps.
2. Online through Self Service Update Portal (SSUP) <https://ssup.uidai.gov.in/ssup-home>.
3. Residents can send Aadhaar data update/correction form through post.

8 Use Cases

8.1 Financial Inclusion

Economic Survey 2014-15 published by Ministry of Finance, GoI, has acknowledged that technology would play a major role in improving the economic lives of the poor. Especially, the JAM number Trinity – Jan Dhan Yojana (PMJDY), Aadhaar and Mobile Numbers has been cited as a potential game changer w.r.t. implementation of welfare schemes and policies of the government. As per the survey, today there are about 125.5 million Jan Dhan bank accounts, 757 million Aadhaar numbers, and approximately 904 million mobile phones. It is possible to envisage that when the JAM trinity becomes linked, the goal of periodic and seamless financial transfers to bank accounts after identification through the Aadhaar number can be implemented with immeasurable benefits to helping the lives of the poor¹.

Aadhaar-mobile identity when linked to bank accounts created under the Jan Dhan Yojana would impart a further thrust to the government's goal of transferring benefits directly to the targeted beneficiaries there by reducing leakages, faster transfers, better access to the benefits and bring overall transparency in the system.

8.2 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

¹ Economic Survey 2014-15

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 simplify 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!

8.3 IRCTC

8.3.1 IRCTC Current Process

Journey Details

Train No./Name :	12463 / RAJSTHN S KRANTI	Journey date :	27-Feb-2015	Class :	THIRD AC
From Station :	DELHI CANTT - DEC	To Station :	JAIPUR - JP	Quota :	GENERAL
Boarding Station :	<input type="text" value="DELHI CANTT - DEC"/> Schedule	Reservation Upto :	JAIPUR - JP		

[Save Journey list](#)

Passenger Details Select Your Travel List Select Passenger From Your Master List

S. No.	Name *	Age *	Gender *	Berth Preference	Senior Citizen	AADHAAR No.(Optional)
1	<input type="text"/>	<input type="text"/>	Select <input type="text"/>	No Preference <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	Select <input type="text"/>	No Preference <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	Select <input type="text"/>	No Preference <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	Select <input type="text"/>	No Preference <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	Select <input type="text"/>	No Preference <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	Select <input type="text"/>	No Preference <input type="text"/>	<input type="checkbox"/>	<input type="text"/>

[Reset Passengers Details](#)

Children Below 5 Years (Ticket Is Not To Be Issued)

S. No.	Name	Age	Gender
1	<input type="text"/>	Select <input type="text"/>	Select <input type="text"/>
2	<input type="text"/>	Select <input type="text"/>	Select <input type="text"/>

[Reset Child Details](#)

Consider for Auto Upgradation
 Book only if confirm berths are allotted
 None
 Book , only if all berths are allotted in same coach
 Book, only if at least 1 lower berth is allotted
 Book, only if 2 lower berths are allotted.
 Preferred Coach ID :

Berth preference does not guarantee allotment of preferred berth type.
If you need assured Lower Berths or assured compact accommodation (in same coach), please select one of the options
If 'None' is selected, the berths will be allotted based on the system logic, depending on availability at that point of time
This choice shall not be applicable in case confirmed accommodation is not available in the train
Booking shall be done in PRS in the coach given by the user if seats are available, otherwise the passenger is allotted in any other coach.

[Refresh Captcha](#)
 Case-sensitive

Mobile Number :
SMS will be sent to this number

- While booking ticket the user mentions the Master passenger name in traveling column and also his mobile number to receive the SMS.
- Master Passenger shows the SMS received from IRCTC on his mobile along with a valid ID proof in original to the ticket checker.

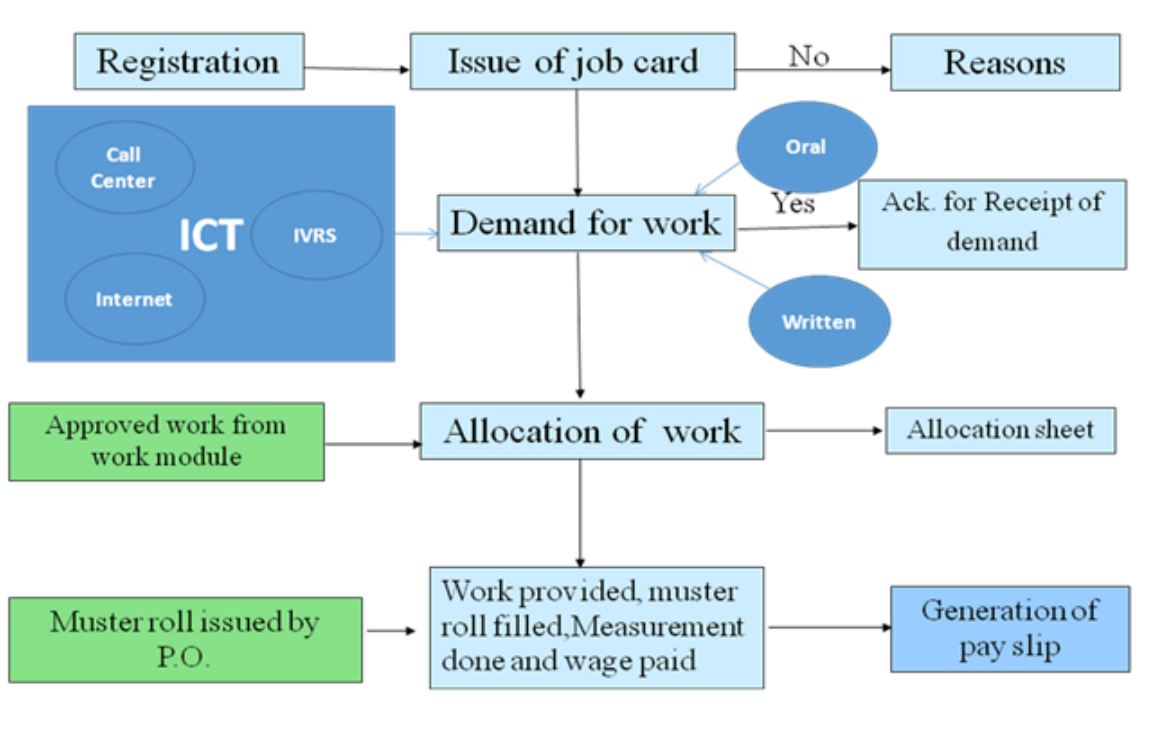
8.3.2 IRCTC Proposed Process

- IRCTC will do OTP based Aadhaar e-KYC of the master passenger and will save the details received from UIDAI (Name, Date of Birth, Gender, Phone & Photograph).
- Once the master passenger gets successfully authenticated, SMS having PNR will be sent to the mobile number (Mobile as mentioned in Aadhaar Database).
- The e-KYC details of all the master passenger of a particular train will be uploaded in the tablet of ticket checker.

- The ticket checker will check the SMS and will also verify the passenger physically by looking at the details of e-KYC stored in his tablet.
- **This will ensure that the passengers will no longer be required to carry the Original ID proof while travelling in trains.**

8.4 Government Welfare Schemes

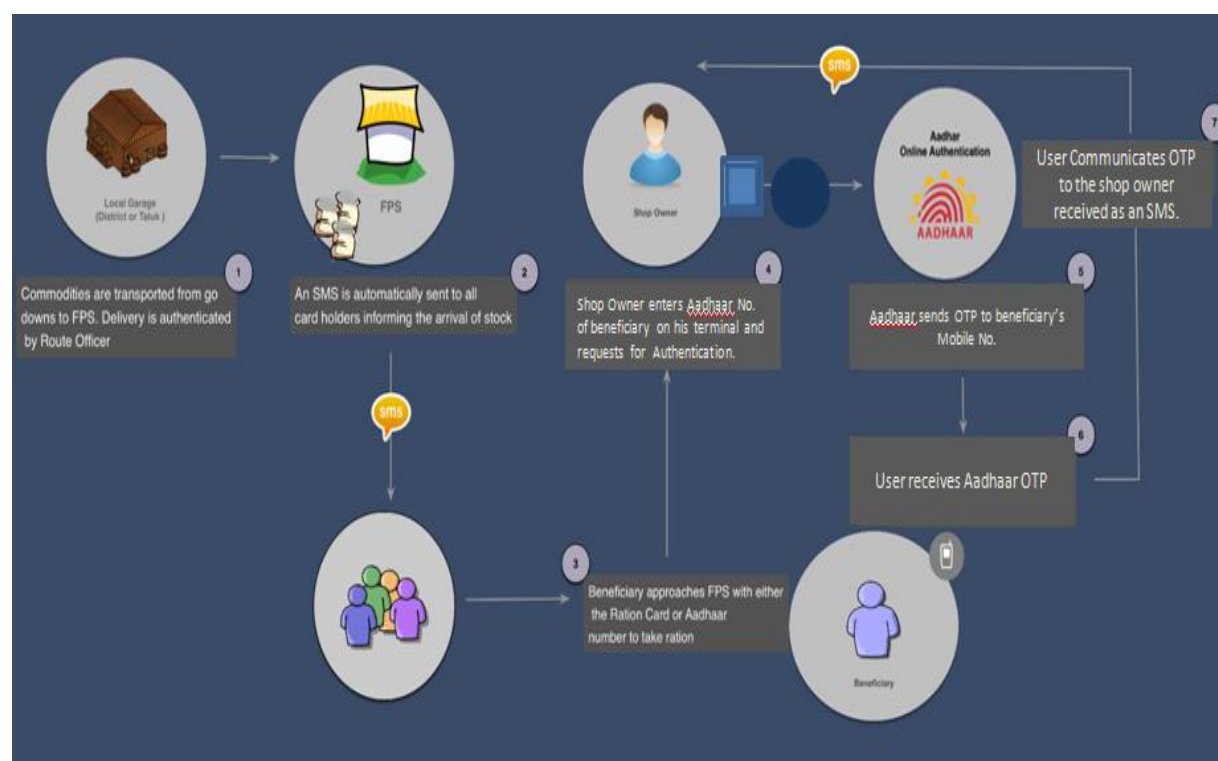
8.4.1 MGNREGA (Mahatma Gandhi National Rural Employment Guarantee Act)



As per the operational guidelines 2013, the workers in need of employment under MGNREGA are promptly provided work. Also, the process of submission of applications for work must be kept open and available on a continuous basis through multiple channels designated by Gram Panchayats. The multiple channels are required receive applications for work and issue receipts with date on them. The applications can be received through 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 operationalised. Workers can register for “Demand for work” by sending SMS to a pre-designated number. NREGASoft, the application for MNREGA, would capture the mobile number and will do a look-up in Aadhaar-Mobile DB and register the worker’s demand for work against his corresponding Aadhaar number (which is mapped to job card number in MNREGA database (currently 4.65 crores Aadhaar numbers are seeded). 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.

8.4.2 PDS (Public Distribution System)



1. Beneficiary approaches FPS with ration card or Aadhaar.
2. FPS owner enters the beneficiary’s Aadhaar number on his system and invokes Aadhaar based OTP verification.
3. Beneficiary receives OTP on his mobile and provides this OTP to shop owner who then inputs the OTP on the system and verifies the beneficiary.

8.5 Commercial Applications

- e-Commerce transactions
 - Reducing risks for Cash on Delivery transactions
 - Authenticate User through OTP based Aadhaar Authentication.
- Matrimonial Websites (Prospective Groom/Bride Aadhaar authenticated)
- Job Websites (Aadhaar verified profiles)
- Auctioning Websites(e-bay)(Sellers are Aadhaar verified)
- Extortion calls/Criminal Calls can be traced
- Banking Transactions
 - Along with UserID/Password use Aadhaar based OTP allowing users to conduct financial transactions.

9 Conclusion

Mobile as digital identity offers a range of opportunities for service delivery by both, government and private entities.

Many countries have already moved ahead in this direction. In Estonia, for example, citizens have been using their mobile as digital identity (called “Mobile-ID” in Estonia) to engage with over 400 public and private sector services since 2007. These range from electronic banking, to applying for a driver’s license, to entering or accessing academic grades at university or changing a pension plan. All services are completed using the electronic signature function of the mobile device - which holds legal equivalence to a physical signature.

While, Aadhaar is positioned to cover almost all of the Indian population in near future, India is also witnessing an exponential growth in the smartphone penetration and usage. Both these factors combined have a potency to bring a paradigm transformation in the way services are delivered currently.

Annexure I: International Mobile Identity Solutions²

Looking ahead to 2020, many studies show the predominant role that mobile devices and - more broadly - connected objects are going to have in our lives. The OECD reports that over 96% of the world population will be equipped with a cell phone by 2018 with over 7 billion cell phones in circulation. Mobility will be an essential factor for the agility and adaptability of the individual. Some visionary countries have made the leap to mobile as digital identity for accessing online services with a high level of security thanks to mobile devices

The pioneers included countries where market penetration of cell phones and new technology is strong such as Austria, Estonia, Finland, Norway and Turkey. It was sometimes (Austria 2003) spurred by the need for a universal form of identification, sometimes (Estonia 2007) supplementing the national card program and accelerating the development of identity and electronic signature with the success that we know. In 2014, Oman was the very first country in the Middle East to complement its national electronic ID card with a mobile identity scheme. Over the last few years, mobile as digital identity has seen a tremendous uptake by citizens thanks to its ergonomics and high level of security.

To help gain a better understanding of what is being done in the pioneering countries, an overview below of the approaches being adopted in electronic Identity and mobile identity is presented.

Estonia³

Estonia is arguably the world's most advanced country within the realm of digital and mobile identity. The country's "Mobile-ID" (as known in Estonia) service allows an individual to use their mobile phone as a form of secure electronic identity. Like an ID card, the "Mobile-ID" can be used for securely accessing government services and for digitally signing documents (a process which has already become an established norm in Estonia). The service uses a W-PKI SIM card, which individuals must request from their mobile phone operator (all of the country's mobile operators offer such SIMs). Private keys are stored on the SIM card along with an application for authentication and signing.

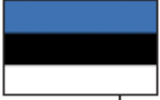
In brief overview, the service works as follows:


² White Paper – National Mobile ID schemes, Gemalto, Dec 2014


³ Mobile Identity Global Review 2013, Mobile networks and digital identity, the convergence of strategy and opportunity, GSMA


- The individual clicks the “Log in with mobile ID” option on a supported website;
- The phone displays a message indicating that a connection is being made;
- The user is prompted to enter a PIN code into the phone;
- The message on the phone disappears and the website is automatically reloaded with a logged in screen.


The list of applications of this mobile digital signature service is broad and growing. Individuals can vote (even when overseas), pay for goods and services online, pay for municipal services such as parking, access social security services and even register a new business.


 Estonia	Governance	Foundations of Trust framework	State of eID program	State of ID program	Leading mobile applications
<p>National program</p> <p>eID and mobile ID are part of daily life since 2005 and 2007.</p> <p>Level of maturity of use: Very high thanks in particular to education and communication</p> <p>Estonia is proving to be a source of inspiration to its neighbours and is cooperating with Lithuania, Latvia, Denmark and Finland</p>	<p>Involvement of the Public Authority at the highest level to coordinate deployment across public and private entities.</p> <p>Technical Management of the Program by the Ministry of Economic Affairs and Communications</p> <p>Choice of a single Certification Authority SK (AS Sertifitseerimiskeskus), Linked by a Public-Private Partnership.</p> <p>The Authority was created by four companies from the world of banking and telecoms: EMT, Hansapank, Eesti Ühispank and Eesti Telefon</p>	<p>European Directive 1999/93/EC and the subsequent Estonian law concerning electronic signature adopted on December 15, 2000</p> <p>agreement for recognition of qualified signature with Finland, Belgium, Portugal and Lithuania for the creation of companies</p> <p>Law prohibiting the government from requesting data that it already has in its possession</p> <p>Introduction of criminal sentences for cyberattacks</p>	<p>Electronic identification and authentication by contact-based national identity smart cards as of 2005.</p> <p>100% of the population has this card.</p> <p>eID and its three functions secured by a national PKI network: identification, authentication and qualified electronic signature (with same validity as written signature)</p> <p>Heavy promotion of the model at international level</p>	<p>Since 2007, mobile identity on SIM card can be activated online by means of a specific application which uses the electronic identity card as a means of identification.</p> <p>Then by acquiring a special SIM card from mobile operators. Certificates are valid for 3 years</p> <p>Electronic signature and mobile authentication by PKI SIM.</p>	<p>More than 300 private and public organizations use mobile ID</p> <p>e-Banking is the flagship application</p> <p>Numerous applications for students & universities</p> <p>The GoSwift application for reserving one's place to cross borders won the 2013 prize for innovation. It dematerializes the queue by creating a virtual queue. An application developed at the request of the Ministry of the Interior.</p>


 USA	Governance	Foundations of Trust framework	State of eID program	State of mobile ID program	Leading mobile applications
<p>No national identity card</p> <p>No national digital identity program</p> <p>But driver's license serves de facto as an identity card</p> <p>Digital identity cards issued by the State for its personnel</p> <p>No national population register</p>	<p>The White House</p> <p>Department of Homeland Security</p> <p>Department of Commerce</p> <p>-----</p> <p>Standardization body: The National Institute of Standards and Technology (NIST)</p> <p>Department of Commerce</p> <p>-----</p> <p>Various initiatives taken in particular by the DMV (Department of Motor Vehicles)</p> <p>With a view to studying a mobile-based driver's license (Georgia and Florida)</p>	<p>Homeland Security Presidential Directive 12 (HSPD-12) dated August 27, 2004 (HSPD-12) defines a policy for a common identification standard for Federal employees and contractors. Smart cards arrive on the scene as of 2007: Personal Identity Verification (PIV) cards</p> <p>Presidential initiative in 2011: NSTIC (National Strategy for Trusted Identities in Cyberspace) supervision of the Department of Commerce</p>	<p>DoD (Department of Defense) cards for military personnel in place since 2001 (cryptography, PKI)</p> <p>Electronic identification and authentication by contact-based PIV smart card for many government administrations</p> <p>Pilot projects financed by the NIST in September 2014 to implement a reliable system for digital identification as part of the NSTIC initiative</p>	<p>No centralized mobile ID project</p> <p>In March 2014, the NSTIC published a guide to derived mobile identity making it possible, within certain limitations, to use derived identity credentials on mobile from PIV cards.</p> <p>Very recent projects on derived identity credentials on Mobile within the framework of the DoD's CAC and driver's licens</p>	<p>Not yet in place</p> <p>But numerous solutions in the private sector use mobile telephones for two-factor authentication</p>


 Finland	Governance	Foundations of Trust framework	State of eID program	State of mobile ID program	Leading mobile applications
<p>National program</p> <p>eID card launched in 1999, electronic certificate on all cards. Card updated in 2003 to support electronic signature.</p> <p>Health insurance information added on the card upon request.</p> <p>The interoperable mobile ID service developed by the three national operators was launched in Nov 2010.</p>	<p>Initiative coordinated by the national population register center (VRK) in association with the Ministry of the Interior</p> <p>VRK is no longer responsible for the issuing of electronic certificates for Mobile ID but issues a unique identification number (SATU) to citizen or resident.</p> <p>The mobile ID working group members include the three MNOs and FiCom (Finnish Federation for Communications and Teleinformatics)</p>	<p>European Directive 1999/93/EC and the subsequent Finnish law concerning electronic signature adopted in 2003</p> <p>Modification of the law in 2009 to take account of mobile signature and make it legal for the signature of contracts, agreements, etc.</p>	<p>Unit cost of eID card: €53, Not mandatory. 10% of the population has one. The health insurance card Kela can also be incorporated into the ID card.</p> <p>Electronic identification and authentication by contact-based national identity smart cards.</p> <p>Very low level of use online. The private BankID, Tupas system is in fact the country's official authentication system.</p>	<p>The creation of national mobile ID standard supported by the three operators in 2010 allowed rapid progress to be made with services.</p> <p>Acquisition of a special PKI SIM card from mobile operators at a face-to-face meeting, or pre-registration online via Tupas</p>	<p>Over 300 public and private services accepting mobile ID.</p> <p>Most popular services are: Getting involved with citizens' initiatives Working with Insurance services Checking one's medical prescription Applying for benefits Opening a gaming account Reporting an offence to the police Accessing health services</p> <p>source www.mobiilivarmenne.fi/en/</p>


 Denmark	Governance	Foundations of Trust framework	State of eID program	State of mobile ID program	Leading mobile applications
<p>National digital identity program since 2007</p> <p>No physical identity card</p>	<p>Nem-ID program coordinated by the Ministry of Finance</p> <p>Cooperation between banks and government</p> <p>Managed by a private company Bank + public sector. Steering by (STS) ministries, regions and municipalities for the country's eGov strategy.</p>	<p>Law on communication by e-mail with government authorities (mandatory in 2015 – no more paper letters)</p>	<p>Nem-ID: requested online with unique citizen number + passport or driver's license number. Cross-checked by police and issuing of a login/password and a list of passwords on paper. Simple OTP Easy to use and popular: 90% of citizens 99% of businesses</p>	<p>No specific mobile ID in the same way as in Finland or Estonia.</p> <p>Nem-ID can be used on mobile as only a simple login and password is required</p>	<p>Single point of entry to services: Portal for citizens, businesses and healthcare</p> <p>eGov applications have to be extensively adapted to mobile mode</p>


 UAE	Governance	Foundations of Trust framework	State of eID program	State of mobile ID program	Leading mobile applications
<p>National program</p> <p>eID: Pilot phase in 2005 and national launch in 2007 the project combines registration of the population and issuing of the card</p> <p>mobile ID: pilot phase in 2014</p>	<p>The program to modernize the sovereign identity system has been entrusted to an independent public authority, the EIDA (Emirates Identity Authority) responsible for implementation of all phases of the program. The core of the system is the national population register</p> <p>Infrastructure that is interoperable for all ministries and government administrations, and is open to the private sector</p>	<p>Created in 2004 by decree No. 2 of the independent authority EIDA responsible for the national register and the distribution of eID cards</p> <p>Federal Law No. 1 of February 2006 concerning Electronic Transactions and Commerce (electronic signature)</p>	<p>Nearly 95% of the population is registered and 80% are holders of the eID card. The biometric card is issued to Emiratis and residents who account for the majority of the population (80%). The card is a contact AND contactless card</p> <p>Electronic identification and authentication by contact-based national identity smart cards.</p> <p>EIDA manages a PKI public key infrastructure</p>	<p>As part of a project announced in May 2013, mobile ID is being tested in 2014 with a pilot involving PKI SIM cards (with operators) with face-to-face identification.</p>	<p>No major deployment yet</p> <p>Generalization in progress</p>


 Qatar	Governance	Foundations of Trust framework	State of eID program	State of mobile ID program	Leading mobile applications
<p>National program</p> <p>eID was launched in 2005</p> <p>Next steps may include extending the program with the use of mobile PKI where citizens log on to the Hukoomi portal using either their eID or mobile phone.</p>	<p>The eID program is managed by the Ministry of the Interior.</p> <p>Information technology, and in particular aspects concerning identification, authentication and signature, is managed by the Ministry of Information and Communications Technology (ictQatar) for all ministries.</p>	<p>Decree Law No. 36 of 2004 establishing ictQatar Ministry of information and communication technologies</p> <p>Law of August 19, 2010 on Electronic Commerce and Transactions and electronic signature in particular.</p>	<p>90% of Qataris and residents have the biometric card</p> <p>Electronic identification and authentication by contact-based/ PKI national identity smart cards.</p> <p>500 services on the country's eGov network by ictQatar offering Single Sign On and Electronic Signature since February 2014</p>	<p>The PKI infrastructure and certificate authority put in place in 2007.</p> <p>It may be hosting the mobile ID pilot program in a few months time.</p>	<p>Not yet in place, still in project phase</p>


 Belgium	Governance	Foundations of Trust framework	State of eID program	State of mobile ID program	Leading mobile applications
<p>National eID program</p> <p>Launched in 2004</p> <p>mobile ID program: technical solutions studied and in validation phase</p>	<p>Coordinated by the Ministry of the Interior</p> <p>Main parties involved National population register (Ministry of the Interior) FEDICT (FEDERAL PUBLIC SERVICE, INTERIOR)</p> <p>Transverse body providing technical IT resources for the deployment of the interoperability infrastructure</p> <p>A Public Trusted Third parties Organization to protect data flows</p> <p>Five personal data protection organizations at the core of the technical system deployed</p>	<p>European Directive 1999/93/EC and the subsequent Belgian law adopted on October 20, 2000.</p> <p>Royal Decree on eID in 2004 and law on access to personal data 2012 : Fedict responsible, for security and respect of privacy in exchanges of personal data and electronic cooperation between services.</p> <p>Law on the non-duplication of administrative information requests in 2014</p>	<p>10 million contact-based cards in circulation (100% of the target population)</p> <p>30% of cards activated for use for online identification.</p> <p>More than 700 applications use eID</p> <p>Electronic identification, authentication and signature by contact-based national identity smart cards.</p> <p>Signature widely used in the professional sphere</p>	<p>Program ready but pending decision by new government formed in September. 2014</p>	<p>mobile ID not yet in place</p> <p>But ambitious NFC mobile payment program very well disseminated since 2012</p> <p>SMART CITY at the forefront</p> <p>A European first: European Bank investing 400 million euros to support «Smart Cities & Sustainable Development» in all Cities</p>

 Austria	Governance	Foundations of Trust framework	State of eID program	State of mobile ID program	Leading mobile applications
<p>eID available since March 2004 on all media including cell phones</p> <p>New mobile ID since 2009</p> <p>The citizen can choose the medium used to store their eID: either on card or mobile. Model is the Only One of It's kind in Europe</p>	<p>Chancellery</p> <p>eGovernment Innovation Center with the technical support of the University of Graz</p> <p>National population register (citizens and residents)</p> <p>Center for online security</p>	<p>European Directive 1999/93/EC and Austrian law of December 2001</p> <p>Law of March 2004 for eGov program</p>	<p>Digital identities derived from National Register per domain (Liberty Alliance model). The citizen's electronic card can be used for identification and authentication (signature and mandate). Physical medium can be a bank card, health card, student card, signature card, service card or mobile telephone</p>	<p>eID and Signature on mobile since 2009 developed within STORK project</p> <p>In 2014: 300,000 signatures a month and 20 to 25,000 new mlds/month</p> <p>Authentication uses the mobile phone number + password + OTP code. The eID is stored in the mobile ID system's database - not in the phone - and accessed after successful authentication with the system. SMS channel, no cryptography</p>	<p>More than 200 applications use the federated identity for businesses and citizens</p> <p>Job search with eJob room Online services for breeders SMART CITY</p> <p>Lots of innovative applications at city level VIENNA in Top 10 of SMART CITIES</p> <p>KLAGENFURTH</p> <p>NFC City - a genuine mobile library</p> <p>Generalization of Mobile payment in progress</p>

 France	Governance	Foundations of Trust framework	State of eID program	State of mobile ID program	Leading mobile applications
<p>No sovereign national digital identity program (either for eID or mobile ID)</p> <p>Numerous semi-public and private initiatives such microchip-based service smart cards for many public organizations</p> <p>France connect national scheme announced as a state driven facebook connect (digital ID federation)</p>	<p>The French National Agency for Secure Documents (Agence Nationale des Titres Sécurisés - ANTS) created in 2007 – body under the supervision of the Ministry of the Interior</p> <p>Ministry of Industry and the Digital Economy</p> <p>The CNIL (National Commission on Information Technology and Civil Liberties)</p> <p>Standardization body dependent on the prime minister French national agency for the security of information systems (ANSSI)</p>	<p>European Directive 1999/93/EC and the subsequent French law concerning electronic signature adopted in March 2000</p> <p>The French Data Protection Act of 1978 («Loi Informatique et Liberté de 1978»)</p> <p>Law on eID in 2012. The Constitutional Council has limited the scope of the card. Project not launched; not currently on the agenda (Sept. 2014)</p>	<p>The federated portal «mon service publique» («Mypublic service) provides a single login/ password for several government and healthcare/social security services. . The payment of VAT is secured by PKI token. Various initiatives in the banking sector based on OTP...</p> <p>France Connect announced in Sept 2014 will be a public service like facebook connect and will federate public identities for the second half of 2015</p>	<p>No national mobile ID program</p> <p>No private m-ID offer from operators at this time</p> <p>France Connect announced in Sept 2014 will be in pilot phase in 2015. It will act as a proxy and will not be an ID provider.</p>	<p>eGov2.0 blends with the numerous SMART CITY programs</p> <p>CITIZY consortium created by the Operators and Public Authorities to develop a deployment of Mobility-oriented local programs with use of NFC for identification and payment</p>

 Germany	Governance	Foundations of Trust frame	State of eID program	State of mobile ID program	Leading mobile applications
<p>National eID program launched in Nov 2010</p> <p>Credit card Format contactless smart card with identification but no signature capabilities yet</p> <p>No national mobile ID project proposed either by the government or operators</p> <p>Electronic signature available since 2000 by token or OTP</p>	<p>Coordinated by the Ministry of the Interior for the card component</p> <p>But no promotion of services</p> <p>Standardization body: BSI</p> <p>The Fraunhofer national institute for public research conducted the pilot scheme provided technical support for startup</p> <p>Cards are issued by the country's 3,200 municipalities</p>	<p>European Directive 1999/93/EC the German law concerning electronic signature</p> <p>Legal amendment in 2012 and 2013 for identification signature the new card and the electronic residency as an equivalent physical only came effect in 2013.</p>	<p>More than 30M eID and residents cards in circulation in 2014. 30% of cards activated for use for online identification. Electronic identification and authentication by contactless national identity smart cards Six-figure PIN code</p> <p>eID not promoted by municipal authorities</p> <p>Difficulty of training over 136,000 people</p>	<p>Possibility considered of deriving a digital identity from the contactless card by reading with an NFC telephone.</p> <p>Project abandoned mid-2013 due to lack of public and private financing for development</p> <p>No offer in Germany at this time (September 2014)</p>	<p>No national project in 2014</p> <p>and not yet on the agenda (September 2014)</p> <p>In Germany, MasterCard working with Deutsche Telekom, Telefónica Deutschland, Vodafone to create a new mobile platform and to accelerate development of mobile payment in the country.</p>

 Iceland	Governance	Foundations of Trust framework	State of eID program	State of mobile ID program	Leading mobile applications
<p>National digital identity program since 2008</p> <p>mobile ID program launched in 2014</p>	<p>Project coordinated by the Ministry of Finance and Economic Affairs and financed by the banks.</p> <p>1 national CA: Audenni responsible for technical aspects of project, itself under the responsibility of the Ministry of Finance</p>	<p>Law on electronic signatures adopted in Iceland in 2001</p>	<p>Certificate available on credit cards</p> <p>NO national identity card</p> <p>National PKI Infrastructure since 2008</p> <p>Little use by citizens between 2008 and 2013</p>	<p>National launch of mobile ID in 2014 financed by the banks</p> <p>On the same PKI network deployed in 2008 (PKI SIM)</p>	<p>Banking applications are now available and using Mobile ID to authenticate and validate transaction with digital signature. eGov applications are also in service, and government department are using mobile ID for its own purpose.</p> <p>Reykjavik at the forefront of the SMART CITY trend For a Sustainable Iceland</p>

 Turkey	Governance	Foundations of Trust framework	State of eID program	State of mobile ID program	Leading mobile applications
<p>National eID card project initiated since 2010 with full-scale pilot conducted.</p> <p>Mobile ID Turkcell 1st generation Then 2nd gen with Turkcell, with Cloud-ID Project for 2015-2016</p>	<p>Very strong willingness at political level Coordinated by the Ministry of the Interior Main parties involved</p> <p>General Directorate of Population and Citizenship Affairs</p> <p>Partnership with public research body Tübitak which define the technical environment (cryptography, key management, etc.) Coordination of industry and suppliers with national test laboratory placed at their disposal</p>	<p>Electronic Signature Law 5070 of January 2004</p> <p>Law on eID set to be adopted at the end of 2014</p> <p>Adapted banking practices and law on financial crimes</p>	<p>Pilot carried out successfully in the city of BURSA. Project ready for national launch. Project on standby since August 2014. Parliamentary decision expected at the end of 2014</p> <p>Signature widely used by professionals on the PKI network</p>	<p>Started to deploy an mobile ID solution in 2007 (electronic signature by mobile telephone), based on PKI with the operator Turkcell</p> <p>----- First generation with applet on SIM and SMS and second generation based adaptable Secure Element in the Cloud - Tests in 2015. Proof of concept planned for 3Q 2015</p>	<p>Main uses in the world of banking due to the initial support of main banks</p> <p>Identification on eGovernment portal with mobile ID</p>