

# The uidai and identity management essay



**ASSIGN  
BUSTER**

In India, a failure to provide evidence of identity is one of the major barricades preventing the poor to access benefits and subsidies. Private as well as public sector agencies throughout the nation typically require evidence of identity before facilitating individuals with service. But as of now, there is no nationally acknowledged, verified identity number which both agencies and residents can utilize with simplicity and confidence.

### **The UIDAI -developing an approach to identity**

The Indian Government undertook an effort to give a clear identity to people first in 1993, when the Election Commission issued photo identity cards. Next in 2003, the Government permitted the Multipurpose National Identity Card(MNIC).

The Unique Identification Authority of India (UIDAI) was recognized in January 2009, as an appended office to Planning Commission. The idea of the UIDAI is to provide a unique identification no. (UID) to all the residents of India. It should be

Strong enough to abolish duplicate and false identities, and

Can be verified and validated in a simple, cost-effective way.

The UIDAI's approach will take into account the learnings from the previous efforts of the government at issuing identity.

The UIDAI will be formed as a constitutional body under a separate legislation to accomplish its objectives. The law will also specify regulations, processes and set of rules to be followed by diverse agencies collaborating with the UIDAI in providing and validating unique identity numbers.

<https://assignbuster.com/the-uidai-and-identity-management-essay/>

The agency holds a cabinet rank and is headed by a chairman. The UIDAI is part of the Planning Commission of India. Nandan Nilekani, a former co-chairman of Infosys Technologies, was appointed as the first Chairman of the authority in June 2009.

R. S Sharma, an IAS Officer of Jharkhand Government cadre has been appointed as the Director General and Mission Director of the Authority. He is known for his best effort in e-Governance project for Jharkhand State and working as an IT secretary he received a number of awards for best Information Technology Trends State in India.

In the first phase, the people living in the coastal villages of Kerala, Andhra Pradesh, Karnataka, Goa, Maharashtra, Tamil Nadu, Gujarat , Orissa and West Bengal will be issued the UID's. The Union Territories of Puducherry, Lakshadweep, Andaman & Nicobar and Dadar and Nagar Haveli Islands will also be covered in this initial phase likely to distribute the identity cards by early 2010.

## **Features of the UIDAI model**

The Unique Identification number (UID) will only provide identity

The UID will prove identity, not citizenship

A pro-poor approach

Enrolment of residents with proper verification

A partnership model

The UIDAI will emphasize a flexible model for Registrars

<https://assignbuster.com/the-uidai-and-identity-management-essay/>

Enrolment will not be mandated

The UIDAI will issue a number, not a card

The number will not contain intelligence

The UIDAI will only collect basic information on the resident

Process to ensure no duplicates

Online authentication

The UIDAI will not share resident data

Technology will undergird the UIDAI system

Objectives of UID project

Obviate need for multiple documentary proof

Facilitate easy verification

Facilitate easy availing of government or private services

Help welfare programmes reach intended beneficiaries

Serve as basis for e-governance services

The ID shall also serve the following purposes:

To prepare a National Population Register (NPR).

To prepare National Register of Indian Citizens (NRIC).

To prepare National Register of Residency (NRR) – for non-citizens.

To provide National Identity Number (NIN) to each person.

To provide Multi-purpose National Identity Card (MNIC) to each citizen.

To provide Multi-purpose Residency Card to non-citizens.

## **Name and logo**

UID project is branded as AADHAAR meaning ‘ foundation’or ‘ support’, and its symbol is a yellow sun with a fingerprint embedded in its centre.

C: UsersRONDesktopAadharImg. jpg

The Logo

## **The Mission**

The role that the Authority envisions is to issue a unique identification number (UIDAI) that can be verified and authenticated in an online, cost-effective manner, which is robust enough to eliminate duplicate and fake identities.

## **The Timelines**

The first UIDAI numbers will be issued over the next 12-18 months counted from August 2009. The first number would be issued between August 2010 to February 2011. Over five years, the Authority plans to issue 600 million UIDs. The numbers will be issued through various ‘ registrar’ agencies across the country.

## **Organization Details**

UIDAI was set up as an attached office of the Planning Commission through Notification dated 28. 01. 09 with a core team of 115 officers and staff.

Under the Notification, 3 Posts (DG, DDG and ADG) were sanctioned for Headquarter with 35 UID commissioners in each of the States. It was thereafter decided to have Regional Offices in Bangalore, Chandigarh, Delhi, Hyderabad, Guwahati, Lucknow, Mumbai and Ranchi with their jurisdiction covering specific states across the country. A Technology Centre has been set up in Bangalore. 268 additional posts were created in September 2009. UIDAI at present has a total sanctioned strength of 383 officers and subordinate staff.

## **Head Office (HO)**

<http://uidai.gov.in/images/FrontPageUpdates/orgcharthoason29092010.jpg>

## **Regional Offices (RO)**

<http://uidai.gov.in/images/FrontPageUpdates/orgchartason29092010.jpg>

## **Projected costs and business opportunities**

One estimate of the cost to completely roll-out National IDs to all Indian residents above the age of 18 has been placed at Indian Rupee â,150, 000 crore (US\$32. 55 billion).[16] A different estimate puts it at US\$ 6 billion.[17] A sum of Indian Rupee â,100 crore (US\$21. 7 million) was approved in the 2009-2010 union budget to fund the agency for its first year of existence.[1] UID has received a huge boost with Dr Pranab Mukherjee, Minister of Finance, allocating Rs 1900 crore to the Unique Identification Authority of India (UIDAI) for 2010-11.

Initial estimates project that the initiative will create 1000 new jobs in the country, and business opportunities worth Indian Rupee â,16, 500 crore (US\$1. 41 billion) in the first phase [10] of implementation.

## **Project Risks and Risk Management**

While the potential of the UID project is enormous, its scope is massive and inherent challenges substantial. We believe that the major risks to the successful implementation of this programme are concerns about privacy, security and fraud; obtaining the necessary political support; and achieving the desired scale within a reasonable time period. Demand creation will determine whether the project can achieve the necessary scale, which in turn will be critical to ensure early adoption by various participants in the UID ecosystem, which should draw in new users.

## **Privacy and confidentiality**

Most of the information that UIDAI is amassing is collected by different agencies (both public and private). This includes some, but not all, of the biometric information. While already today a variety of agencies collect this information, they do not “ speak” to each other. Under this new scheme, information will reside in the Central ID Data Repository (CIDR). However, the idea that a person can at any time be identified from the data stored in a central database may be unnerving for some people.

UIDAI recognises that privacy must be guarded and is committed to protect the rights of anybody seeking a UID number. To ensure transparency in its operations, and to alleviate concerns and apprehensions from individuals using its services, UIDAI plans to do the following:

Ensure that the person seeking the UID number is aware that the information being provided will be part of a central database and will be used for identification and authentication purposes;

Will enter into contracts with the Registrars to ensure confidentiality of the information that they collect directly or through other agencies and subregistrars; and

Set protocols for information gathering and storage to be followed by the Registrars and enrolling agencies.

### **Adverse publicity has to be avoided**

Information leaks and the attendant publicity could adversely affect the UID project and so it must ensure proper security of data. Any such story that blows up in the media could slow down or even scuttle the project.

Additionally, the UIDAI database itself could be the target of an attack by hackers and others with malicious intentions. Therefore, under the UIDAI Act the organisation will have to be granted sufficient “teeth” to deal with any such problems.

### **The challenge of scale – Capacity building necessary as information gathering scales up rapidly**

UIDAI expects that its peak run-rate of enrolment could touch one million people per day in the very first year of operation. Every part of the organisation – physical infrastructure, systems, sub-systems and processes – will need to scale up to manage this load. Among other things, water-tight legal contracts and frameworks will have to be in place, aligned with the



wide variety of stakeholders likely to make up the UID ecosystem across the length

and breadth of the country, and even abroad. The biometric “ de-duplication” algorithm needs to scale up to be able to verify and check a finger print or iris scan against every record in the database to ensure it is unique, and it will need to handle multiple queries – possibly running into hundreds of thousands – simultaneously.

### **Early adoption – key to success – Sufficient demand will have to be generated early enough**

For the project to be a success, there must be no controversy in the early days and no significant leakages of data, nor poor quality of data collection. At the same time, it will be very important to generate sufficient demand early enough into the enrolment cycle to ensure that critical mass is reached as soon as possible. If UIDAI has to generate demand from within the ecosystem rather than being mandated from the top by the government, demand will have to come from all cross sections of society, particularly from the urban and rural poor, where the benefits are likely to be more tangible and quantifiable.

### **A robust grievance redress mechanism necessary**

Along with quality of data and scale, the project will need a robust grievanceredress mechanism. According to UIDAI, a procedure for the correction of data will be laid down ensuring incorrect information can be corrected at specified enrolling agencies. UIDAI will set up a grievance-

redress mechanism to address various issues caused by incorrect data, including issues of identity theft, fraud and lost numbers.

## **Responsibility for Data Accuracy**

Apart from the risk of impersonation, the other risk associated with the UID system which is also going to be integrated with many downstream data is the possibility of “ Errors” of the data. Today, many of the Voters find that the information about their name, sex and age on the Card are incorrect and make them ineligible to exercise their franchise. The reason for such inaccuracies is that the system for “ Correction” is too complicated and once a clerical error gets into the system, they tend to remain.

In view of the criticality of the UID system, it is essential that inaccuracies need to be eliminated at the time of generation and then there should be an expeditious but strong process of correction of inaccuracies.

It must be remembered that UID will be “ Information Residing Inside a Computer Resource” and is subject to the provisions of Information Technology Act 2000 (ITA 2000) and the proposed amendments through Information Technology Amendment Act 2008. (ITA 2008).

Any alteration of UID information which is unauthorised and causes wrongful harm is therefore an “ offence” under Section 66, 72, 72A of ITA 2000/8 and is also subject to payment of compensation under Section 43 and 43A ITA 2000/8.

The UID authority is also subject to the provisions of Sec 67C since the ultimate owner of the data is that of the data subject and the UIDAI is only an “ Intermediary” as per the provisions of ITA 2000/8

Maintenance of “ Inaccurate Data” leading to wrongful loss would constitute lack of “ Due Diligence” and could make the UIDAI liable.

One option for the Government is to pass a law making the UIDAI and its staff immune to any legal challenges. This would be perhaps the most likely happening since this is the trend in Government functioning. This would however result in “ Authority without Responsibility” and ideally should be avoided.

## **Responsibility for Data Security**

Data Security will remain to be the biggest challenge in the UID project and multiple strategies are required to be adopted for the purpose.

The law of the land provides some protection to the data subjects through the ITA 2000/8 and imposes certain responsibilities to the UIDAI for reasonable security practices to be maintained by UIDAI.

If there is no attempt by the Government to shield the UIDAI from the provisions of the existing law, then we may consider that there is a legal structure for data security. It may still be necessary to define the “ Reasonable Security Practice” for this service.

In view of the criticality of the UID operation, the “ Reasonable” security practices may have to be substantially stringent. It is necessary to

implement globally acceptable principles of data security and privacy protection to meet the requirements.

Some of the specific requirements under this framework for ITA 2008 compliance includes

Obtaining the consent of the UID holders for inclusion of the data which would be in the form of an application made by the data subject and validated in its electronic form.

If data is validated on paper and the UIDAI takes the responsibility for digitization then some member of UIDAI should be held accountable for any inaccurate data that may creep in . Such a person has to validate the electronic form of the data with his digital signature and take the legal liability for the inaccuracies.

A copy of the data as entered in the data base has to be provided to the data subject in print form with appropriate certification under Section 65B of Indian Evidence Act as per established principles of Cyber Evidence Archival.

As a part of this data validation process, it may be necessary to provide access to the data in the data base to the holder of the UID so that he can verify the data any time and any number of times during the lifetime of the data.

This may require validation of the person making the query. If we need to use “ Digital Signatures” for validation, the UID itself may have to also include an “ E-Mail Address” in the minimum as a “ Digital Identity parameter”.

<https://assignbuster.com/the-uidai-and-identity-management-essay/>

Data has to be encrypted in storage and every element of the data base has to be digitally signed by an officer of the UID.

Appropriate audit trail of who accessed the data and what was the hash value of the data accessed before and after the access session etc will have to be captured along with the mode of access, IP address etc and archived in such a manner that they are available for judicial scrutiny when required.

The hardware and software used by UIDAI should be source code audited and certified for integrity. Supplies from countries suspected to be preparing for Cyber Warfare against India must be avoided.

The UID project does face certain risks in its implementation, which have to be addressed through its architecture and the design of its incentives. Some of these risks include:

### **Adoption risks**

There will have to be sufficient, early demand from residents for the UID number. Without critical mass among key demographic groups (the rural and the poor) the number will not be successful in the long term. To ensure this, the UIDAI will have to model de-duplication and authentication to be both effective and viable for participating agencies and service providers.

### **Political risks**

The UID project will require support from state governments across India. The project will also require sufficient support from individual government departments, especially in linking public services to the UID, and from service providers joining as Registrars.

## **Enrolment risks**

The project will have to be carefully designed to address risks of low enrolment – such as creating sufficient touch points in rural areas, enabling and motivating Registrars, ensuring that documentary requirements don't derail enrolment in disadvantaged communities – as well as managing difficulties in address verification, name standards, lack of information on date of birth, and hard to record fingerprints.

## **Risks of scale**

The project will have to handle records that approach one billion in number. This creates significant risks in biometric de-duplication as well as in administration, storage, and continued expansion of infrastructure.

## **Technology risks:**

Technology is a key part of the UID program, and this is the first time in the world that storage, authentication and de-duplication of biometrics are being attempted on this scale. The authority will have to address the risks carefully – by choosing the right technology in the architecture, biometrics, and data management tools; managing obsolescence and data quality; designing the transaction services model and innovating towards the best possible result.

## **Privacy and security risks**

The UIDAI will have to ensure that resident data is not shared or compromised.

## **Sustainability risks**

The economic model for the UIDAI will have to be designed to be sustainable in the long-term, and ensure that the project can adhere to the standards mandated by the Authority.