

Aadhaar

Ideas and lessons from India

April, 2020





About MicroSave Consulting

MicroSave Consulting (MSC) is a boutique consulting firm that has, for 20 years, pushed the world towards meaningful financial, social, and economic inclusion. We are a globally trusted, yet locally based organization that offers high-quality, practical market-led solutions to accelerate financial, economic, and social inclusion in the digital age.

With about 190 staff of different nationalities and varied expertise, MSC is proud to be working in over 50 developing countries. We have offices in Bangladesh, India, Indonesia, Kenya, Philippines, Senegal, Singapore, Vietnam, Uganda, and the United Kingdom.

We work with participants in financial, economic, and social ecosystems to achieve sustainable performance improvements and unlock enduring value. Our clients include governments, donors, private sector corporations, and local businesses. We can help you seize the digital opportunity, address the mass market, and future-proof your operations.


Table of Contents

1. Objective of the module	04
2. An overview of Aadhaar	05
3. How does Aadhaar work?	06
4. The evolution of Aadhaar	08
5. Key use-cases of Aadhaar-based authentication	10
6. The role of Aadhaar in financial inclusion	13
7. Privacy concerns around Aadhaar	15
8. International examples of digital identity	17





1. Objectives of the module





01
 What is *Aadhaar*? What information does it encompass?

04
 How *Aadhaar* aids financial inclusion

02
 The milestones in the *Aadhaar* journey

05
 The privacy discourse

03
 Benefits of *Aadhaar* in direct benefit transfer (DBT) programs

06
 Digital identity endeavors in other parts of the world



2. An overview of Aadhaar

Aadhaar is a unique digital identity for more than **1.25 billion** residents of India

The unique identification number—*Aadhaar*—is issued by the [Unique Identification Authority of India \(UIDAI\)](#). Preceding the date of application, any Individual who has resided in India for **more than 182 days** in a year is eligible for an *Aadhaar* card, it allows **cross-functional proof of identity**. It is a database with **no duplicates** which serves as an identity and address proof. Since it is digital, it contains biometric information.

Key features



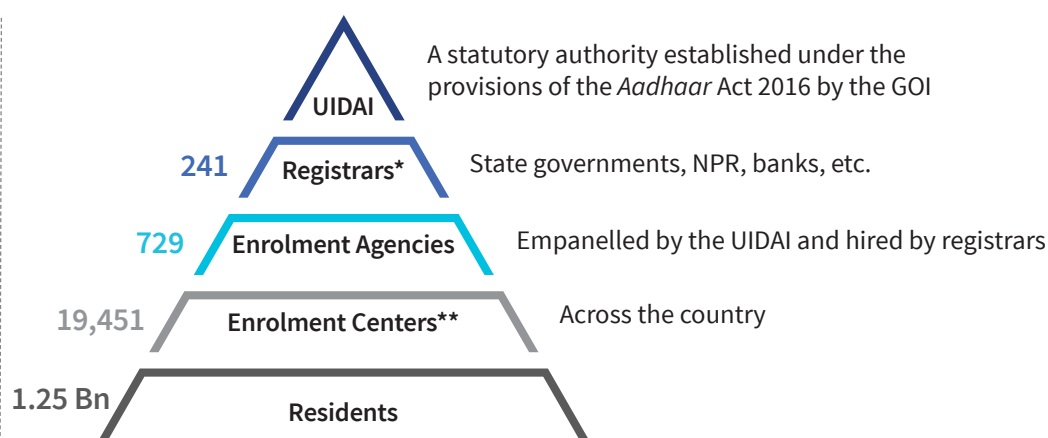
- It is a random and unique number;
- One person can own only one *Aadhaar*;
- It is for all residents, including infants;
- It is an online identity and authentication platform;
- It allows the update of information

Details captured

- Name
- Date of birth
- Address of a resident
- Gender
- Photograph
- Fingerprints
- Iris

(Data as on April, 2020)

Enrolment hierarchy



* Registrar: Entities authorized by the UIDAI to enrol individuals. They are partner to UIDAI vide an MOU.

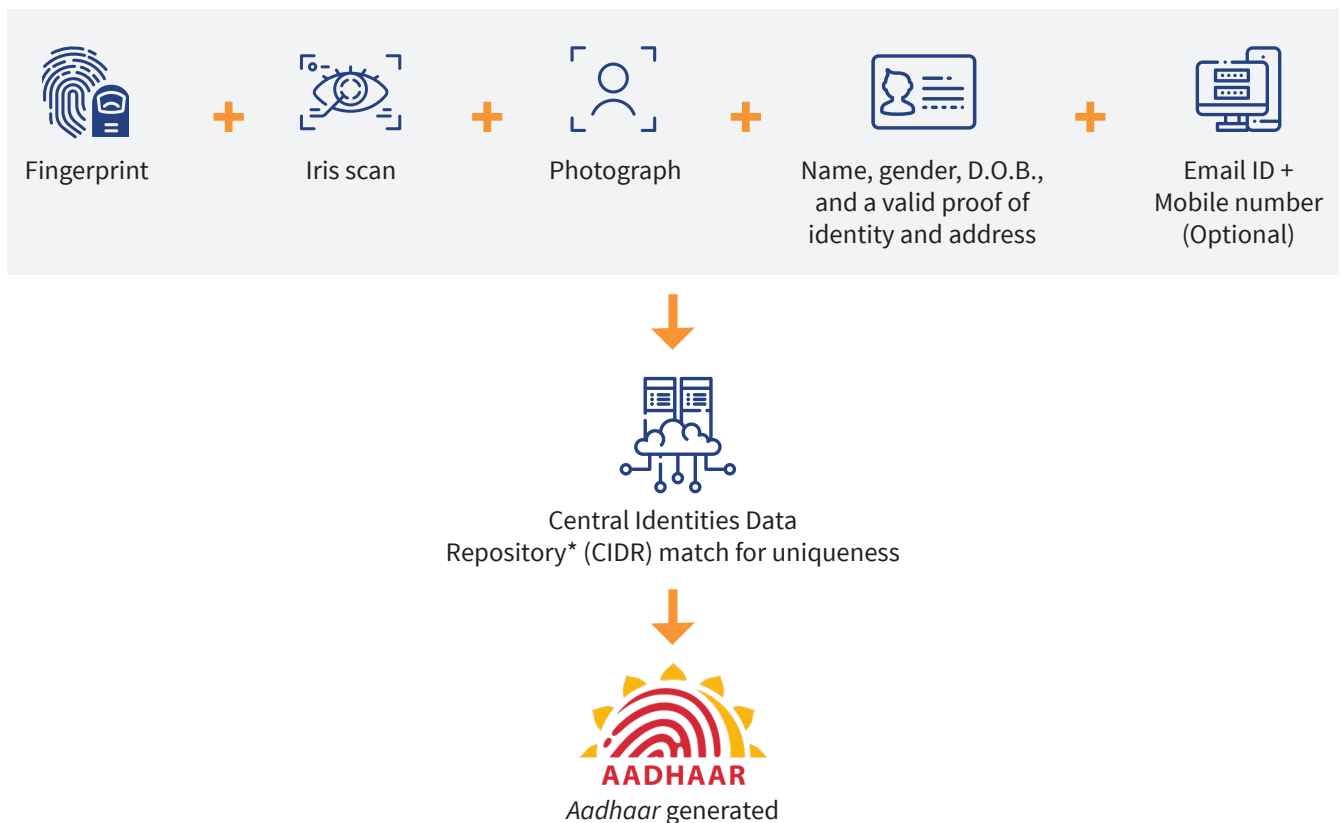
** Enrolment centers: Entities that have the responsibility of enrolling residents by collecting their demographic and biometric data in conformation with the UIDAI enrolment process, figure as on January 2019

3. How does Aadhaar work?



Cumulatively, over 27 billion Aadhaar identities have been authenticated

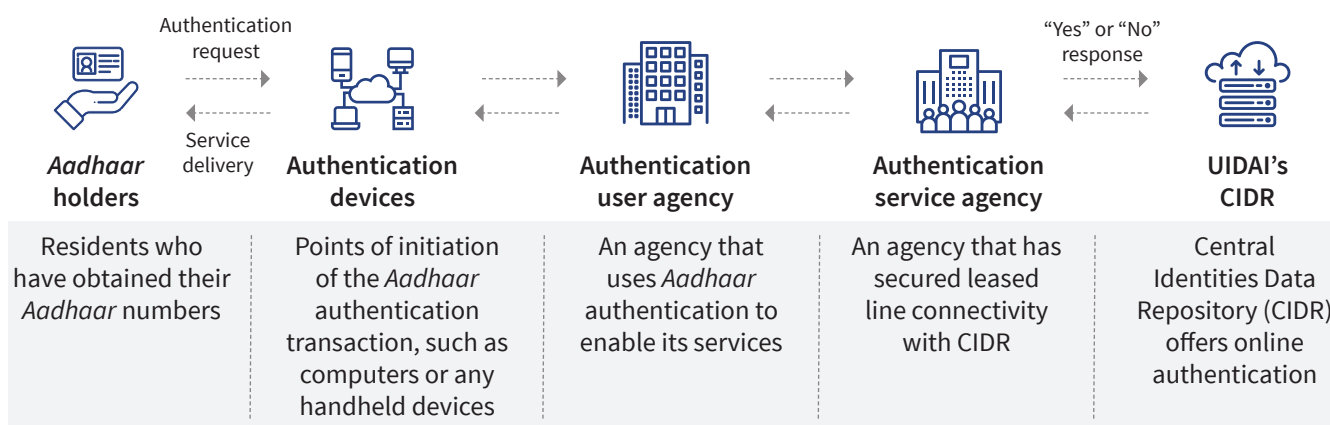
Aadhaar generation process



Source: [State of Aadhaar](#)

*CIDR is a government agency in India that stores and manages data for the country's Aadhaar project

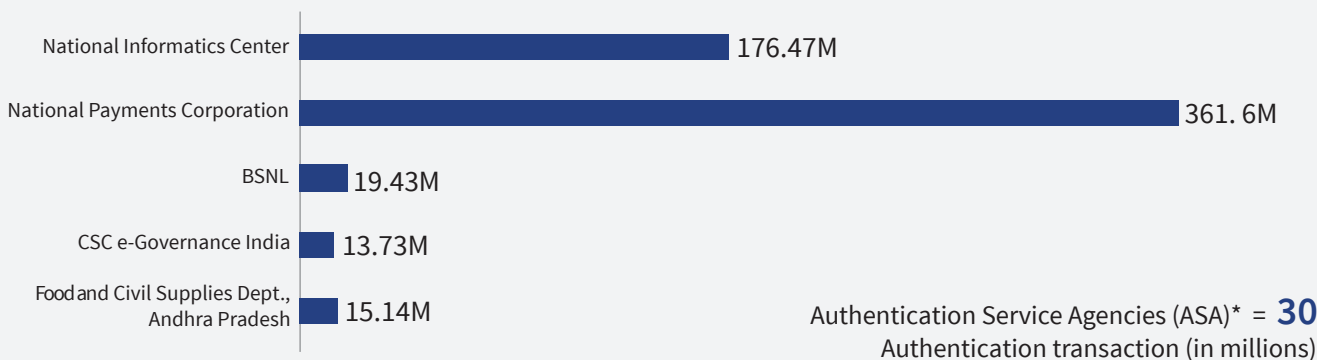
Aadhaar “Yes” or “No” authentication



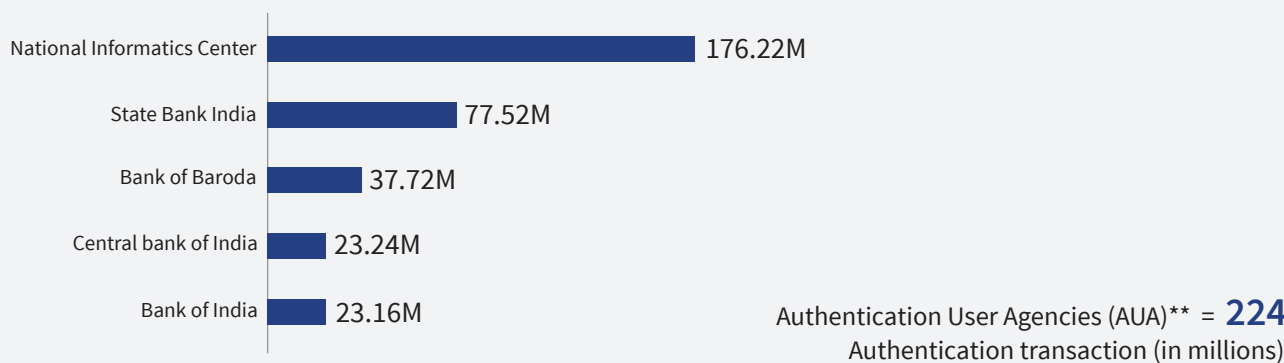
Aadhaar plays a vital role in authenticating over 40 billion identities and over 8 billion e-KYC transactions on a monthly basis (February, 2019 data)

Total number of citizens enrolled	Total cumulative instances of Aadhaar authentication	Total e-KYC transactions
>1.25 billion	>40 billion	>8 billion

Top five ASA-wise authentication transactions in 17th April, 2020



Top five AUA-wise authentication transactions in February, 2019



*ASA is any entity that acts as enabling intermediaries. They have an established secure connection with the CIDR and acts as the medium for AUAs authentication requests.

**AUA is any agency seeking to conduct Aadhaar authentication of its customers/associates etc. for service delivery. These may include any govt./public/private legal entity registered in India.

4. The evolution of Aadhaar



Milestones in the journey of Aadhaar

2000-03

In 2000, the government of India's identity projects started taking a shape. The GOI was contemplating to prepare a national register of Indian citizens and issuing multi-purpose national identity cards (MNICs) based on the registry.

2009

Recognizing the overlap, the UIDAI was constituted as the agency responsible for issuing *Aadhaar*. The UIDAI was established by an [executive order in 2009](#), and initially functioned as an office attached to the Planning Commission.

2016

The parliament passed the *Aadhaar Act*. This established the UIDAI as a statutory authority under the Ministry of Electronics and Information Technology (MeitY)

In addition, the government approved a separate unique identity project for below-poverty-line families in 2006.

2006-08

Between 2006-2008, the Registrar General of India, which conducts the national census, was engaged in creating the National Population Register and issuing MNICs. About 1.2 million citizens were issued MNIC in nearly 12 districts.

2010

In 2010, the *Aadhaar* enrolment was initiated. Since then, it has increased steadily, with 85% of India's population enrolled, which amounts to roughly 1.2 billion of individuals.

2018

Supreme Court [verdict](#): *Aadhaar* is mandatory for filing income tax returns and availing social welfare services. However, it is not mandatory for school admissions, travel tickets, opening bank accounts, etc.

Source: [State-of-Aadhaar](#)

Source: Aadhaar dashboard (Data as on 14 February, 2019)

* Electronic-Know Your Customer (e-KYC or eKYC) is a paperless Know Your Customer (KYC) authentication process, wherein the identity and address of the subscriber are verified electronically through Aadhaar authentication.

Total instances of Aadhaar authentication	Total number of citizens enrolled	Total e-KYC* transactions
40,015,516,144	1,257,491,270	8,042,985,889

* Electronic-Know Your Customer (e-KYC or eKYC) is a paperless Know Your Customer (KYC) authentication process, wherein the identity and address of the subscriber are verified electronically through Aadhaar authentication.

UIDAI has been ensuring the issuance of Aadhaar and managing the database and authentication process effectively

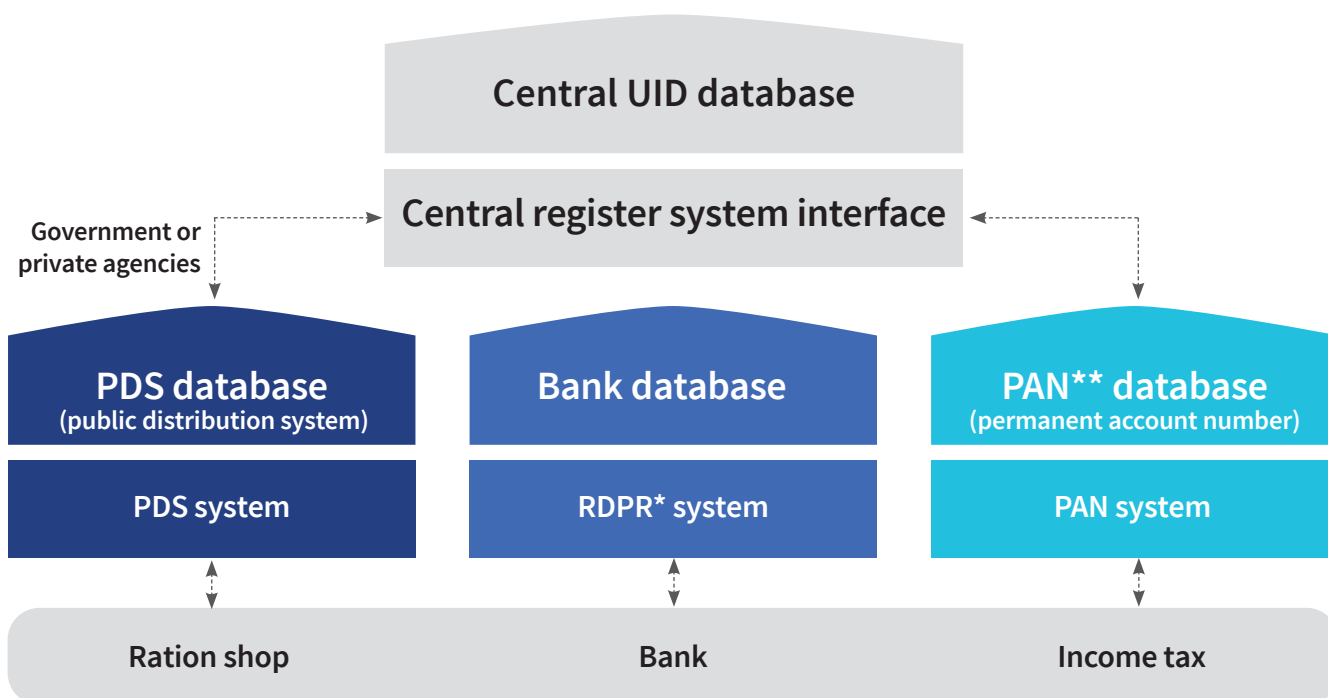
The Unique Identification Authority of India (UIDAI) is a statutory authority established by the Aadhaar Act, 2016, under the Ministry of Electronics and Information Technology (MeitY).

Roles of UIDAI:

- Acts as the supervisory body for Aadhaar enrolment and authentication;
- Oversees the operation and management of all stages of the Aadhaar life-cycle;
- Develops the policies, procedures, and systems to issue Aadhaar numbers to individuals;
- Ensures the security of the information related to the identities of individuals.

What is the Central Identities Data Repository (CIDR)?

The CIDR is a central data repository. It functions as a managed service provider. It implements the core services around the UID, such as keeping track of resident records, issuing unique identification numbers, and verifying, authenticating, and amending resident data. The CIDR holds the minimum information required to identify the resident and eliminate instances of data duplication.



Examples of CIDR connection with resident touch points

System architecture: The CIDR is the central database of all residents, containing the minimal set of fields sufficient to confirm someone's identity.

* RPDR: Rural Development and Panchayat Raj (system of local self-government in India) Department

** PAN: A Permanent Account Number (similar to Tax Identification Number in other countries) is an identification number assigned to all taxpayers in India and issued a card
Source: [Aadhaar dashboard](#) (Data as on 14 February, 2019)

5. Key use-cases of Aadhaar-based authentications



Aadhaar has made various schemes under Direct Benefit Transfer (DBT) more efficient and effective

The DBT is an ongoing endeavor by the Government of India to reform the delivery mechanisms of welfare schemes by ensuring last-mile delivery and by plugging leakages.

Database de-duplication

Aadhaar has helped eliminate fake, duplicate, and ghost records to improve the data quality and ensure last-mile delivery of welfare program benefits to eligible beneficiaries.
Example: [How Aadhaar is killing the ghosts that haunt welfare schemes](#)

Know your Customer* (KYC)

[Banks are required](#) to accept valid identity and address documents to open accounts to ensure that DBTs are transferred directly into beneficiaries' bank accounts. Now, *Aadhaar* is sufficient to open an account through e-KYC.
Example: [Paperless bank account opening](#)

Transactions

Government subsidy transfers and consumer transactions rely on an *Aadhaar*-based platform for secure and verified movement of money.
Example: [NREGA wages](#), consumer transactions using [Aadhaar Enabled Payment System \(AePS\)](#) **

Presence and access control

In government offices, employees now can mark their attendance using their *Aadhaar* numbers through a biometric authentication device. This helps to ensure better administration of human resources, which results in a more effective project execution.
Example: [Aadhaar enabled biometric attendance system](#)

* KYC is a process that financial institutions have to comply with, whereby these set of institutions obtain information about the identity and address of the customers.
** AEPS is a bank-led model that allows online interoperable financial transaction at PoS (Point-of-Sale / microATM) through the Business Correspondent of any bank using the *Aadhaar* authentication.

Aadhaar seeding and authentication in the distribution of subsidized food grains helped the government save USD 4.2 billion

The [Targeted Public Distribution System](#) (TPDS) is an in-kind food subsidy program that is financed and managed by the Government of India. It is the largest safety net program in India. Government expenditure for TPDS amounts to [approximately USD 23.6 billion](#), providing subsidized grain through a network of more than 500,000 fair price shops (FPS) across the country.

Pre-Aadhaar issues



Inefficiency in targeting beneficiaries



The lack of accountability in TPDS value-chain resulted in the leakage of subsidies, which is estimated at about [40-50%](#)



The presence of opportunities to manipulate the system with widespread collusion across the supply chain

Roles of Aadhaar



The government-seeded *Aadhaar* number in the beneficiaries database as a first step and then installed biometric PoS devices at ration shops to ensure the authentication at the time of the uptake of ration



The linking of *Aadhaar* with ration cards helped eliminate fake beneficiaries and reduce pilferage

Benefits



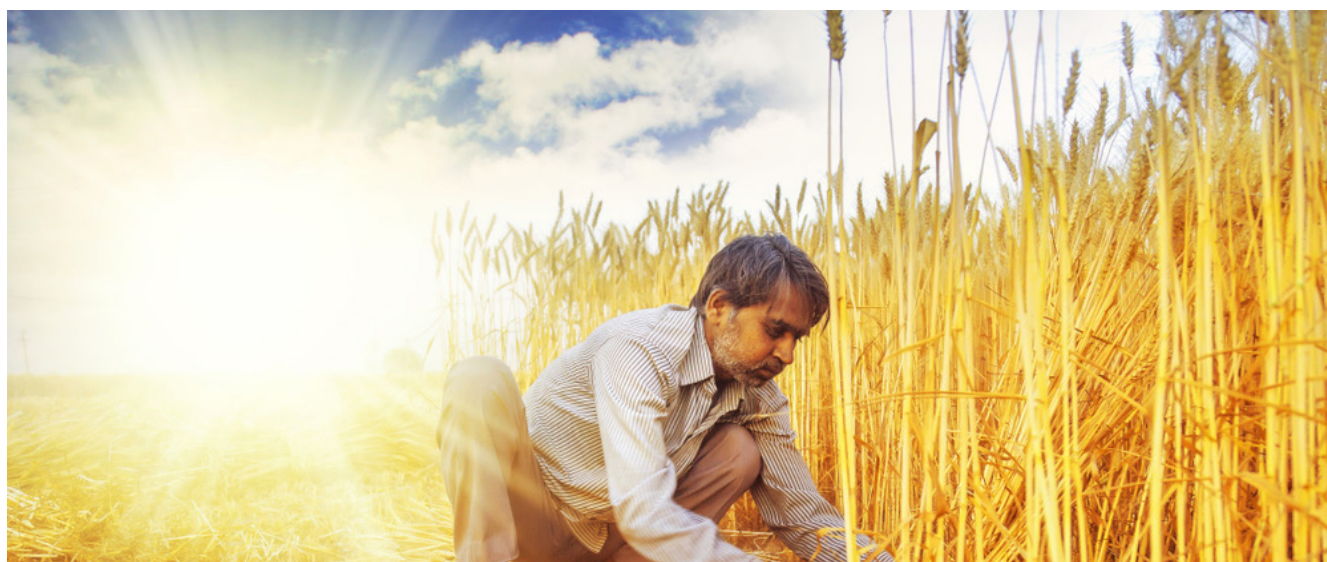
More than [65 million](#) households are covered under TPDS.



Over [28 million](#) bogus ration cards were deleted. This helped the government save USD 4.2 billion.



[Our study](#) on biometric authentication for PDS found it catalytic for better transparency and efficiency. At all-India level, [leakage declined](#) from 58.6% of official TPDS grain offtake in 2004–05 to 43.1% in 2011–12.



Aadhaar is instrumental in the authentication of sales of subsidized fertilizers to reduce its black marketing

India is primarily an agrarian economy and input subsidies comprise a powerful instrument for accelerating the agricultural growth. The fertilizer subsidy of approximately [USD 10 billion](#) annually aims about 95 million farmers with the objective to improve productivity and hence their livelihoods.

Pre-Aadhaar issues



After 1977, the government introduced a range of fertilizer subsidies. However, it was observed that only [35%](#) of the total subsidy reach farmers.



The subsidy was paid directly to fertilizer manufactures when they provided simple receipts upon delivering the units to the designated railway stations and warehouses. This gave enough leeway for manufacturers and retailers to divert urea to alternate sectors.

Roles of Aadhaar



Sales have to be authenticated at the point of sales using *Aadhaar* number and biometric details of customers.

Subsidies are transferred to manufacturers on the basis of actual sales instead of the produced quantity.

Manufacturers receive the difference between the actual value and the subsidized price of fertilizers in the company's bank account after providing the details of sales done through PoS machines installed at 200,000+ retail shops.

Benefits



Cross-border sales across states, which act as a proxy indicator for leakages, have decreased after the introduction of DBT-fertilizers



The new system has increased the overall accountability of stakeholders and enhanced the transparency in the system. Retailers fear that the government can track transactions and hence diversion of subsidized fertilizer for non-agricultural use has decreased. The introduction of *Aadhaar* based DBT has helped save approximately [USD 12 billion](#).



6. The role of Aadhaar in financial inclusion



The use of Aadhaar has removed challenges to catalyze [financial inclusion](#)

Aadhaar is a comprehensive solution to [challenges](#) that existing documents, such as Voter ID, permanent account number (PAN), etc. have failed to address. These include:

- Financial exclusion;
- A lack of interoperability with other identity databases;
- Inefficiencies and overlaps that arise from creating identity in multiple, siloed systems;
- Security and identity theft risks.

Opening a bank account through e-KYC Simplifies the documentation requirement

- As per [RBI regulations](#), Aadhaar is a sufficient form of documentation to open a bank account through e-KYC.
- e-KYC, Aadhaar number, and biometric details can be used as proof of identification and documentation for easy account opening.
- In 2015, [approximately 125 million](#) no-frill accounts were opened. By 23rd January, 2019, the number increased to [approximately 340 million](#) accounts.

Aadhaar-enabled microATMs* Addresses the issue of access

- A microATM uses an individual's Aadhaar number and biometrics to authenticate their identity to allow the individual to withdraw money or make bank transfers.
- This system is economical, secure, and portable, which makes it accessible to citizens in remote areas.

*A microATM is a portable, handheld point-of-sale device that facilitates banking transactions. The mobility of microATMs transported to remote villages by business correspondents (BCs) can offer services to individuals who do not live close to a brick-and-mortar bank.

Payments systems: Providing multiple options for safe and easy transactions

- [Aadhaar Enabled Payment System \(AEPS\)](#) This system employs the UIDAI's authentication services to allow an individual to conduct banking transactions using the details of their bank, *Aadhaar* number, and biometrics.
- [Aadhaar Payment Bridge System \(APBS\)](#) This system is used for the disbursement of government benefits using an individual's bank name and *Aadhaar* number.
- [Unified Payments Interface \(UPI\)](#) It is a mobile banking application, which is available for both smartphones and feature phones. It allows the use of an *Aadhaar* number as a payment address. [The BHIM](#) app uses UPI.



7. Privacy concerns around Aadhaar



The right to privacy has been recently recognized as a fundamental right [Justice K.S. Puttaswamy \(Retd.\) v. Union of India](#)

Aadhaar was envisioned as a tool to provide an identity for the poor and thus ensure their inclusion ability or inability to access government and private sector programs and services. However, there are several concerns surrounding India's digital identity project that have evolved over the years.

Common concerns

Digital identities, such as *Aadhaar*, carry a number of potential risks with regard to the privacy of an identity holder. The [World Bank](#) highlights four important general concerns:

- **Unauthorized access**, use or disclosure of information;
- **Profiling** through linking databases in illicit ways, including for surveillance objectives;
- **“Function creep”** refers to the act of using a holder's data for a purpose other than the one for which it was collected originally without seeking the holder's consent;
- **Inaccuracies in data** often lead to mistaken identities, unjust treatment, or exclusion from eligible government benefits.

“In a nutshell, the concern is with the creation of a centralized database, where we don't have control of our own data and an ecosystem, where a single identifier (that is, the *Aadhaar* number) links databases. It becomes an infrastructure for **profiling and surveillance**.” [Mint, October, 2018](#)

“While more subsidies, benefits, and services were brought under the project, **“function creep”** also began. Ministries and Departments were directed to insist on *Aadhaar*; *Aadhaar* was mandatorily linked to a number of aspects of daily life.” [Indian Express, September, 2018](#)

“The introduction of *Aadhaar*-Based Biometric Authentication (ABBA), was meant to enhance efficiency, but on occasions can lead to **exclusion**. But no *Aadhaar* card means no rations, [as has been the case in rural Jharkhand](#). Further, the point-of-sales (PoS) machine—a simple, hand-held device that relies upon internet connectivity—which is crucial for ABBA to function, is prone to malfunctions, despite the presence of fail safes. A non-functioning PoS machine means no rations.” [Economic and Political Weekly, October, 2018](#)

The verdict declared by the Supreme Court of India in 2018 is a step to simplify the use of *Aadhaar* and address privacy concerns associated with it

In September, 2018, the Supreme Court initiated several reforms to address escalating privacy concerns around the unique identity project. Highlights of some of the prominent and [milestone judgments](#) on *Aadhaar* that also address the concerns raised by the World Bank are as follows:

- Section 57 of the *Aadhaar* Act allowed an unrestricted extension of the *Aadhaar* platform to users, such as government agencies or private sector operators. This provision created a significant scope for “function creep” and threats to data privacy. For recognizing these risks, the Supreme Court struck down section 57. Now, *Aadhaar* authentication is not mandatory to open a bank account or avail financial services. Commercial banks, payments bank and e-wallet companies like Paytm can no longer deny services to customers if *Aadhaar* e-KYC is not done. *Aadhaar* is also no longer compulsory for school admissions.
- *Aadhaar* card is mandatory to avail government welfare schemes subsidies as it empowers the poor and marginalized. However, any child cannot be deprived of the benefits of government schemes irrespective of the unavailability of an *Aadhaar* card.
- *Aadhaar* is mandatory to file income tax returns (ITR) and the allotment of a permanent account number (PAN) to prevent income tax evasion.
- *Aadhaar* will **not lead to a surveillance state** because:
 - The biometric information obtained is minimal and is stored securely in CIDR for the purpose of authentication. During the authentication process, only biometrics are matched.
 - The CIDR is not controlled by the state or the police force.
 - No profiling data is collected with respect to religion, caste, tribe, language, records of entitlement, income or medical history of the applicant at the time of *Aadhaar* enrolment.
 - Within a few seconds of the biometrics having been collected by the ASA or AUA, the information is transmitted to the CIDR in an encrypted form. This information then becomes inaccessible to the enrolling agency.
- Authentication failures do not mean the exclusion or denial from subsidies, benefits or services since the requesting entities are obliged under the law to provide for exception handling mechanisms.

8. International examples of digital identity

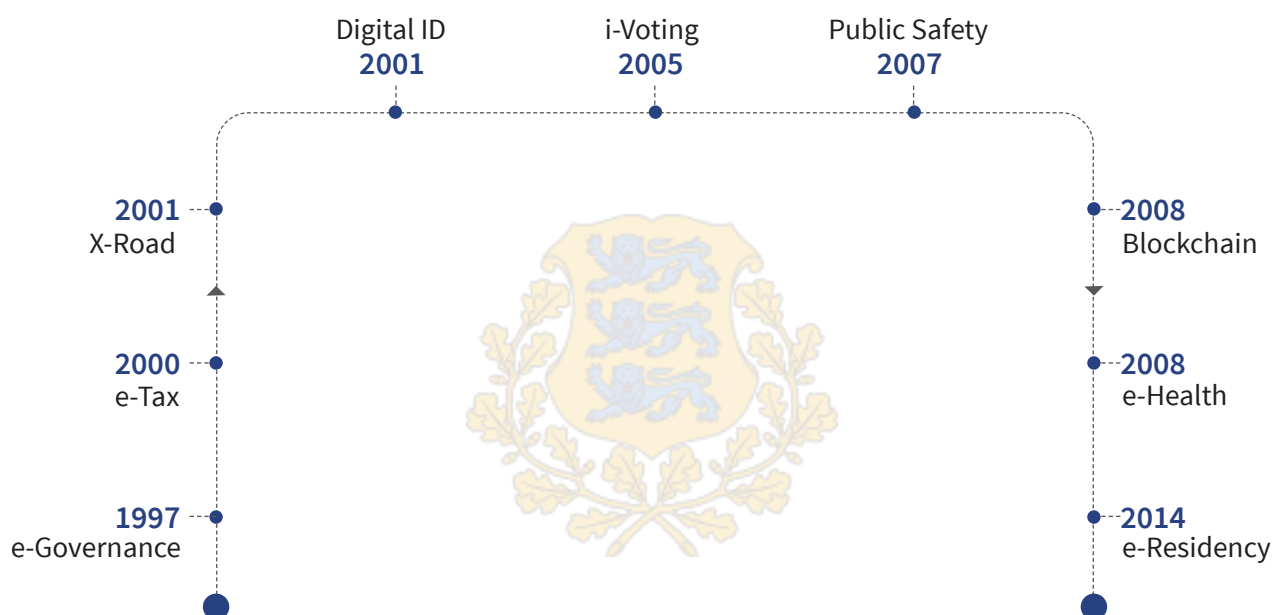


Estonians can update, monitor, and control access to their personal information



e-Estonia

An Estonia ID card is a cryptographically secure digital identity card that allows an Estonian to access various public, financial, medical, and emergency [services](#).



Estonia focused on a seamless interoperability and a citizen identity system using the concept of [X-Road](#). It is a layer between the various silos of government data which connects them together securely. To ensure secure transfers, all outgoing data from X-Road is digitally signed and encrypted, and all incoming data is authenticated and logged. The X-Road technology saves Estonians 1400 years of working time every year.

The ID card

Each issued [ID card](#) contains two certificates—one for the authentication and one for the digital signing. There are also two associated private keys. These keys are protected by two separate PIN codes mentioned on the card.

Data available on the card:

- Personal details: Name, sex, date of birth, citizen's birthplace, and citizenship
- Assigned identification details: National ID code, residence permit details, card number, card issuing date, and card expiry date
- Holders' data in a machine-readable format like in a passport

E-residency

Similar to the citizens and residents of Estonia, e-residents receive a government-issued digital ID and full access to Estonia's public e-services. This enables them to establish an EU business and use their secure digital identity to manage their company entirely online from anywhere around the world with minimal cost and hassle.

[31 million](#) citizens registered under National Identity Number in Nigeria

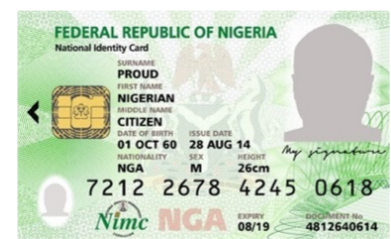


National Identity Management Commission, Nigeria

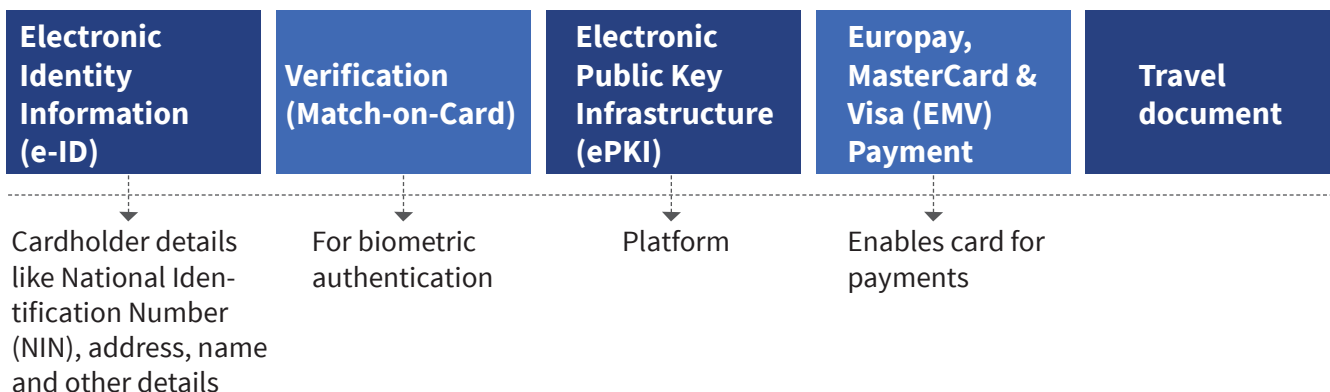
The Nigerian National Identity Card is a microprocessor chip-based general multi-purpose identity card (GMIC). The National Identity Management Commission Act of 2007 requires every Nigerian citizen and legal resident to enroll with NIMC, but does not confer a citizenship status to the resident. [The Commission](#) (NIMC) has been responsible for building [Nigeria's identity system](#).

Key features of the e-ID card are as follows:

- It is an 11-digit random unique identity number;
- Its uniqueness is determined by demographics and biometrics, which are ten-finger prints and a facial image;
- It is assigned to every citizen of Nigeria. The information can be updated on the database in case of any changes;
- It is an instrument for financial inclusion to identify and bring financial services to all classes of society. The MasterCard prepaid payment facility allows cardholders to deposit funds on the card, receive social benefits, pay for goods and services, and withdraw cash from ATMs that accept MasterCard.



The e-ID card has provisions for 13 applets, out of which five are activated at the point of collecting the card.

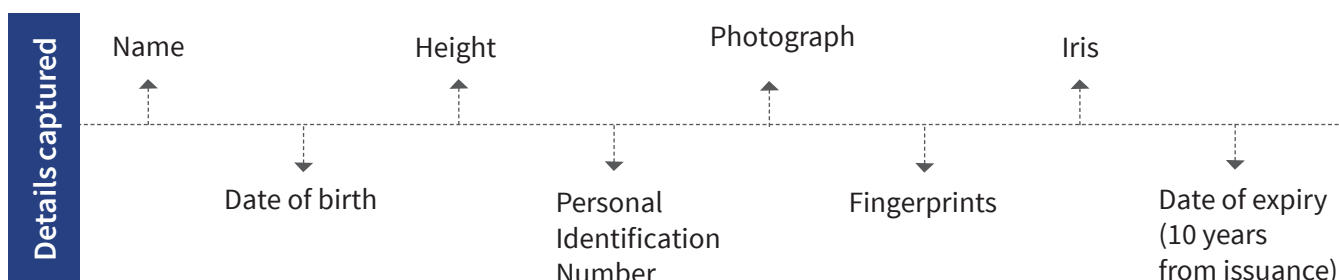


The Ghana Card has been formalizing the economy and enhancing e-governance

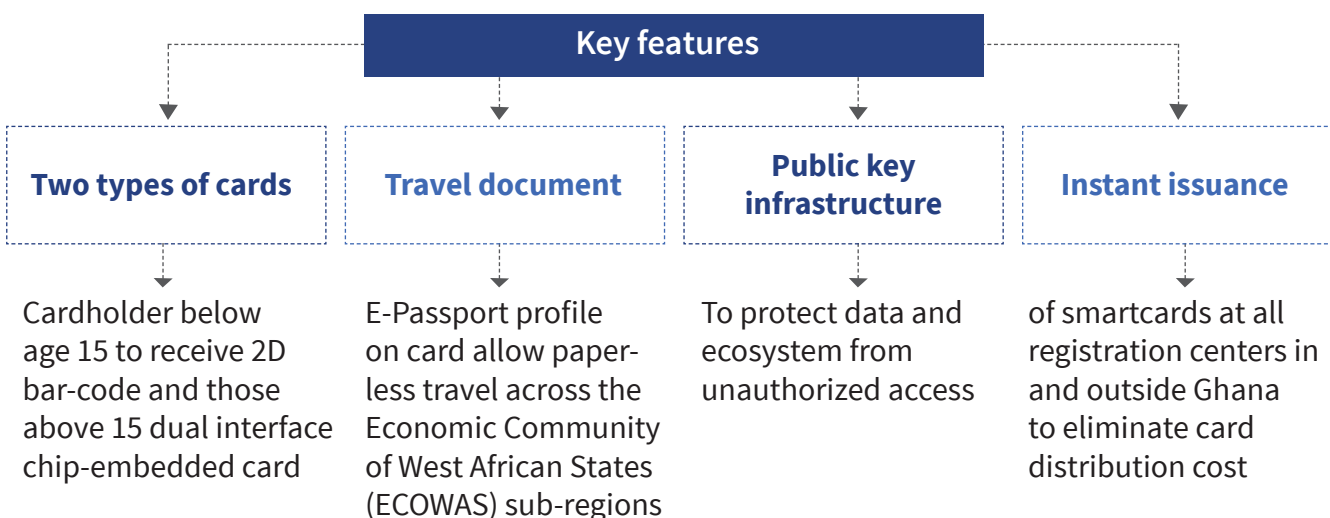


National Identification Authority, Ghana

The NIA was established by an Act of Parliament in 2003. It is mandated to register all Ghanaians alongside legally and permanently resident foreign nationals who have stayed for at least six years in Ghana. The NIA, under the National Identification System (NIS), creates a national database or register, issues them with National Identity Cards (Ghana Cards), and manages the use of the database.

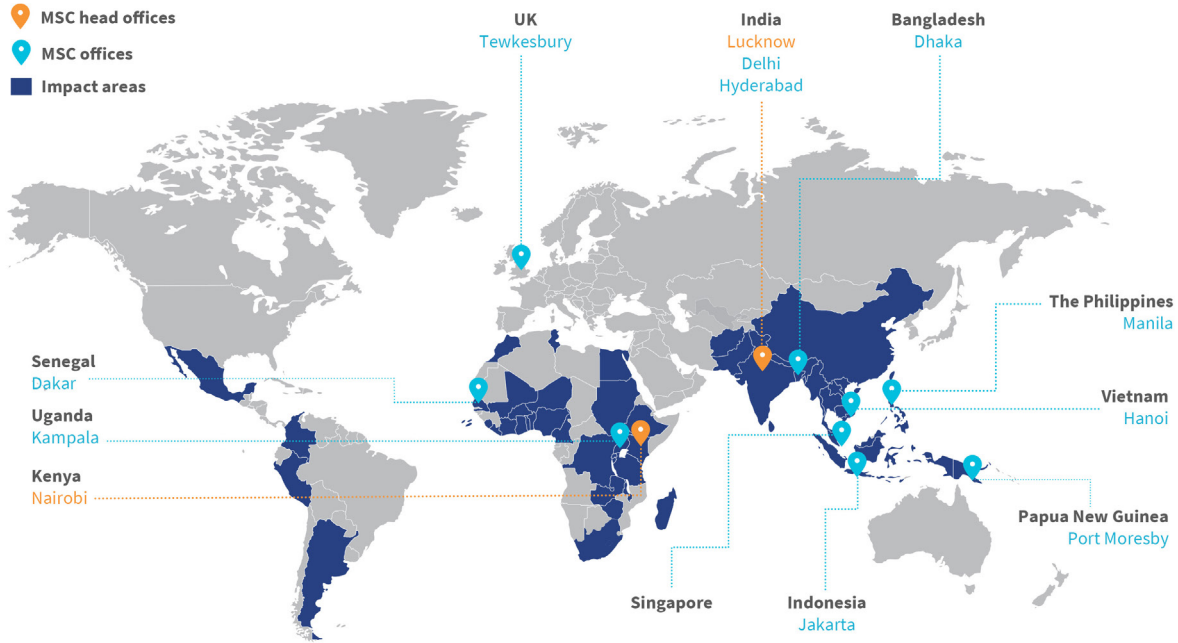


The NIS goes beyond just the issuance of identity cards; it includes citizenship recognition or determination or both, data integration, harmonization of identification systems, as well as data storage and exchange systems for all Ghanaians living in Ghana or and abroad, from the cradle to the grave.



List of abbreviations

ABIS	Automatic Biometric Information Systems
AEBAS	<i>Aadhaar</i> Enabled Biometric Attendance System
AEPS	<i>Aadhaar</i> Enabled Payment System
APBS	<i>Aadhaar</i> Payment Bridge System
ASA	Authentication service agency
AUA	Authentication user agency
CIDR	Central Identities Data Repository
DBT	Direct benefit transfer
e-KYC	Electronic-Know Your Customer
FPS	Fair price shop
GOI	Government of India
LPG	Liquefied Petroleum Gas
MeiTY	Ministry of Electronics and Information Technology
MNIC	Multi-purpose national identity cards
OTP	One-time password
PAN	Permanent Account Number
PDS	Public Distribution System
PIN	Personal Identification Number
PoS	Point-of-Sale device
RDPR	Rural Development and Panchayat Raj
TPDS	Targeted Public Distribution System
UIDAI	Unique Identification Authority of India



Asia head office

28/35, Ground Floor, Princeton Business Park, 16 Ashok Marg,
Lucknow, Uttar Pradesh, India 226001

Tel : +91-522-228-8783 | Fax : +91-522-406-3773

Email : manoj@microsave.net

Africa head office

Shelter Afrique House, Mamlaka Road, P.O. Box 76436,
Yaya 00508, Nairobi, Kenya

Tel : +25-420-272-4801 | Fax : +25-420-272-0133

Email : anup@microsave.net

www.microsave.net