मेरा आधार
मेरी पहचान

Unique Identification
Authority of India

# Building the Future of Aadhaar Authentication

## Simplifying Onboarding, Accelerating Innovation




September 2026

# Message - Chairperson
# Unique Identification Authority of India



Aadhaar lies at the heart of India's Digital Public Infrastructure, allowing residents to use their digital identity to seamlessly and securely establish trust across the country for a whole range of services. The value of Aadhaar lies in its use, and we at UIDAI are obsessed with making it easier for holders to use it, and for entities to blend it easily into their workflows.

We see the flywheel of greater-usage-driving-greater-adoption gaining momentum, with 370% cumulative growth in authentication over the last five years. Not only have more than 670 entities been onboarded, the revamped Aadhaar app now has more than 5 crore (and growing) downloads, with the immediacy and convenience of services made available on the app significantly improving data quality as well.

But we have a long way to go, and we are committed to engaging with ecosystem partners to accelerate adoption and usage. The bi-annual Aadhaar Samvaad, and the constant engagement with user entities helps the UIDAI understand emerging needs, enable innovation, and keeps us on the path of continuous improvement in the ease of adopting Aadhaar-based authentication services.

It is due to this engagement, combined with our ambition to keep the flywheel moving, that we launch this playbook on "**Ease of Onboarding**." It will help ecosystem partners, especially FinTechs, leverage Aadhaar-based identity verification to innovate and drive further adoption. These efforts will further strengthen India's leadership in digital public infrastructure and help shape new global standards for digital identity.

**Neelkanth Mishra**
Chairperson UIDAI

# Foreword - Chief Executive Officer
# Unique Identification Authority of India



I am pleased to present this playbook on "**Ease of Onboarding**," which will appeal to private sector entities seeking to join the Aadhaar authentication ecosystem. Over the years, UIDAI has worked relentlessly to reduce the complexity and time required for entities to join the Aadhaar ecosystem.

UIDAI has reduced onboarding timelines for regulated entities by over 70% through process improvements, standardized application formats, and simplified audit frameworks. These improvements reflect UIDAI's commitment to making the Aadhaar authentication ecosystem more accessible to every eligible entity. They also uphold the security and trust that underpin the ecosystem.

Newer onboarding routes and process changes have further expanded access for private-sector entities, including banking, financial services, and insurance (BFSI) companies, FinTech companies, and other startups. The Social Welfare, Innovation, Knowledge (SWIK) framework is operationalized under the Aadhaar Authentication for Good Governance (Social Welfare, Innovation, Knowledge) Rules, 2020. These rules enable entities that work in the public interest or support the ease of living to access Aadhaar authentication through a faster and simpler process. The framework also covers entities that are not regulated by financial sector regulators. It extends Aadhaar authentication to cooperative banks, which enables secure, efficient, and transparent delivery of financial services, especially to underserved populations. UIDAI has also introduced the LITE framework for entities that perform 500,000 or fewer transactions annually. This framework provides a simple, fast, and cost-effective onboarding route.

UIDAI has also introduced several technological enhancements, including the use of artificial intelligence and machine learning (AI/ML), to improve the security, reliability, and ease of Aadhaar authentication. UIDAI remains committed to working closely with all eligible entities seeking to join the Aadhaar authentication ecosystem and to further improve onboarding ease. I invite all eligible entities across banking, financial services, insurance (BFSI), FinTech, and other sectors to use this playbook as their starting point.

**Saurabh Vijay, IAS**
CEO UIDAI

# Table of contents


Glossary i

About this playbook ii

Chapter 1: What is Aadhaar authentication? 1

Chapter 2: How can I get onboarded for Aadhaar authentication? 8

Chapter 3: I am non-government. Am I still eligible? 12

Chapter 4: What options are available for ease of onboarding? 14

Chapter 5: What's new in Aadhaar authentication ecosystem? 17

Chapter 6: What are the key use cases? 22

Contact Us 26




# Glossary

**"Authentication"** is the process by which the Aadhaar number along with demographic information (such as name, date of birth, gender etc.) or biometric information (fingerprint, iris or face) of an individual is submitted to UIDAI database for its verification and UIDAI verifies the correctness of the details submitted, or the lack thereof, based on information available with it.

**"Authentication User Agency"** or **"AUA"** means a requesting entity that uses the Yes/No authentication facility provided by the Authority for ID verification of Aadhaar number holder.

**"e-KYC authentication facility"** means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity is matched against the data available in the UIDAI database, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction.

**"e-KYC User Agency"** or **"KUA"** shall mean a requesting entity which, in addition to being an AUA, uses e-KYC authentication facility provided by the Authority for ID verification of Aadhaar number holder.

**"Requesting Entity"** means an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the UIDAI database for authentication.

**"Sub-AUA"** means a requesting entity that uses the Yes/ No authentication facility provided by the UIDAI through an existing AUA.

**"Sub-KUA"** means a requesting entity that uses the e-KYC authentication facility provided by the UIDAI through an existing KUA.

# About this playbook

**What is this playbook about?**

This playbook serves as a comprehensive guide for entities seeking to perform authentication using the Aadhaar authentication facility. It explains how Aadhaar authentication works, the available onboarding routes for requesting entities, the legal and regulatory framework for permitting Aadhaar authentication and governing regulations its use, and the various initiatives undertaken by UIDAI to enhance the ease of onboarding for such entities.

**What it contains?**

This playbook provides the step-by-step process, along with all prerequisites, documentation, and compliance measures required for the onboarding routes such as Authentication User Agency (AUA), e-KYC User Agency (KUA), Sub-AUA and Sub-KUA, e-KYC Setu, Sub-AUA Less in Transaction Entity (LITE) framework, and approval of authentication use case under Social Welfare, Innovation, Knowledge (SWIK) rules.

**This playbook is for?**

Financial services organizations, fintech, startups, and other private sector companies seeking to leverage Aadhaar authentication for service delivery.

**Through this playbook, entities will be able to:**

- Understand Aadhaar's journey as a foundational DPI
- Gain practical guidance on technical, audit and compliance requirements
- Explore onboarding routes-AUA/KUA, Sub-AUA/Sub-KUA, e-KYC Setu, and Sub-AUA (LITE)
- Learn about latest initiatives and support provided by UIDAI

By combining operational guidance and practical use cases, this playbook empowers ecosystem entities to use Aadhaar authentication securely, responsibly, and efficiently, unlocking new opportunities for service delivery and innovation.



Our success with Aadhaar, UPI, and other digital public goods was not accidental. It stemmed from a few replicable principles. First, we built digital infrastructure as a public good, not a proprietary platform. This open and interoperable architecture allowed innovation to flourish on top of a common base layer

**- Narendra Modi**
Hon'ble Prime Minister of India
17 Feb 2026



# 1 What is Aadhaar authentication?

Aadhaar is a foundational layer of India's digital public infrastructure, which provides a 12-digit unique identification number to each resident based on their demographic and biometric data provided during enrolment process.

## 1.1 Aadhaar's journey as a foundational DPI

**1999**
Kargil Review Committee - recommended national ID

**2005-08**
EGoM constituted for creation of unique national ID

**2009**
Unique Identification Authority of India (UIDAI) established

**2010**
First Aadhaar generated

**2012**
Launch of fingerprint authentication

**2013**
Launch of Aadhaar-enabled Direct Benefit Transfer (DBT), OTP authentication and e-KYC services

**2016**
- Aadhaar Act passed
- UIDAI became a statutory authority

**2018**
Supreme Court judgment gave constitutional validity to Aadhaar Act

**2020**
SWIK Rules promulgated

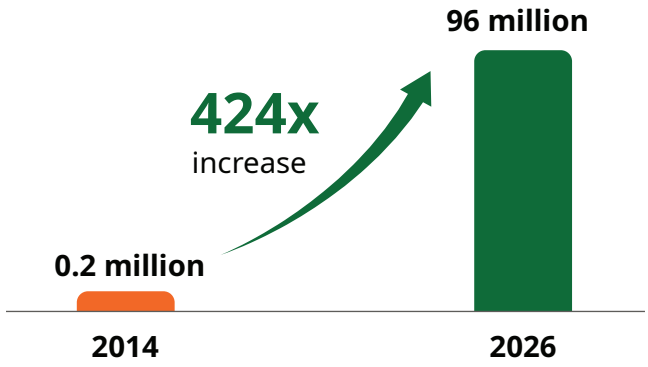
**2021**
Launch of face authentication

**2025**
SWIK Rules amended to include non-government entities

**2026**
- Launch of face auth SDK and Sub-AUA (LITE) framework
- Completed >180 billion authentication transactions

**1.45** billion Aadhaar numbers generated

**Average daily authentication transactions**




**Peak transactions per day**

**132 million**

on 10.01.2025

## 1.2 About Aadhaar authentication

Requesting entities perform Aadhaar authentication to validate resident information against the information available at UIDAI database by sending a request and obtaining authentication responses.

### Aadhaar authentication flow

**Aadhaar Number Holder**




Shares Aadhaar number, consent & authentication modalities such as:

- Demographic
- OTP
- Biometric (face/finger/iris)

**Requesting Entity**



Sends a real-time request to UIDAI database to confirm identity

Request

Response

**UIDAI Database**

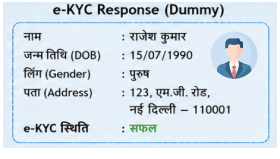


**Responds either**

Yes | No

(AUA & Sub-AUA)

**or**




(KUA & Sub-KUA)

## (a) Types of Aadhaar authentication

UIDAI provides the following two types of authentication facilities, which requesting entities can use to electronically authenticate the identity of an Aadhaar number holder.

### Yes/No authentication facility

**Requesting entities role**

Requesting entities obtain resident's Aadhaar details with consent and submit it to UIDAI to match the information available with UIDAI database for identity verification

**UIDAI's role**

UIDAI shares Yes/No response on whether the matching request is successful, without sharing the resident's identity information

**Key Benefit**

Enables secure identity verification without sharing resident information

### e-KYC authentication facility

**Requesting entities role**

Requesting entities obtain resident's Aadhaar details with consent and submit it to UIDAI to match the information available with UIDAI database for customer onboarding

**UIDAI's role**

UIDAI shares digitally signed e-KYC information such as demographic details (name, DoB, gender, address, and photograph)

**Key Benefit**

Enables faster, secure & paperless onboarding

## (b) Modes of Aadhaar authentication

Requesting entities can submit request to UIDAI for any of the four modes of authentication.

| | | | | | UIDAI response |
|---|---|---|---|---|---|
| **1. Demographic Authentication** | Aadhaar No | + | Demographic Infomation | = | Yes/No |
| **2. OTP Authentication** | Aadhaar No | + | OTP | = | Yes/No or eKYC |
| **3. Biometric Authentication** | Aadhaar No | + | Biometric (face/finger/iris) | = | Yes/No or eKYC |
| **4. Multi-factor Authentication** | Aadhaar No | + | Combination of two or more of the above | = | Yes/No or eKYC |

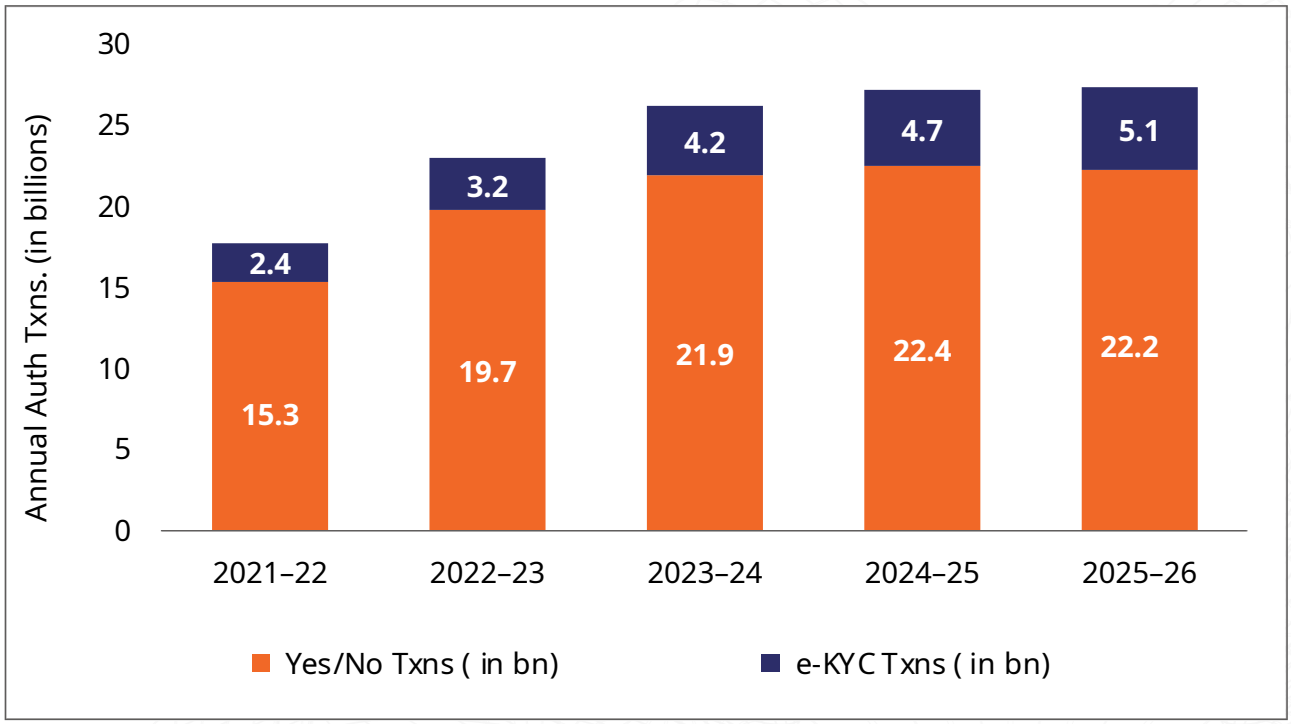
## 1.3 Legal framework for Aadhaar authentication

The Aadhaar authentication system operates under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, and the Aadhaar (Authentication and Offline Verification) Regulations, 2021. The framework provides the legal basis for entities to participate as requesting entities in the Aadhaar authentication ecosystem. Some of the relevant sections of the Aadhaar Act are:

| **The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016** |
|---|
| **Section 4(4)(b)(i):** Aadhaar authentication by an entity is permitted under the provisions of any other law made by Parliament |
| *Requesting Entity Type:* Entities regulated by RBI, SEBI, IRDAI, PFRDA, TRAI, etc.<br>*Sectors covered:* Banking, Insurance, Pension, Credit Rating Agencies, Pre-Payment Instruments, Capital Markets, Fintech and Telecom |
| **Section 4(4)(b)(ii):** Aadhaar authentication is sought for a purpose prescribed by the Central Government, in consultation with UIDAI, in the interest of the State |
| *Requesting Entity Type:* Entities as per the use case on good governance and ease of living<br>*Sectors covered:* E-commerce, healthcare, travel, tourism, hospitality, education, skill assessment and municipal services |
| **Section 4(7):** Mandatory Aadhaar authentication for the provision of any service, if it is so required by a law made by Parliament. |
| **Section 7:** Where Aadhaar is required for receiving a subsidy, benefit or service, the expenditure for which is incurred from, or the receipt therefrom for part of the Consolidated Fund of India or Consolidated Fund of State, for establishing identity |
| *Requesting Entity Type:* Central/State Ministry/Department<br>*Sectors covered:* Welfare schemes, subsidies and public services |
| **Section 8:** Authentication of Aadhaar number |
| It defines the role(s) and responsibilities of requesting entities:<br>• obtain resident consent before collecting identity information for authentication<br>• use identity information only for submitting authentication requests to UIDAI database<br>• inform residents about:<br>  ○ the nature of information shared during authentication<br>  ○ the purpose for which information may be used<br>  ○ available alternatives to submitting identity information<br>UIDAI responds to authentication requests with a positive, negative or other appropriate response, without sharing core biometric information. |

## 1.4 Scale of Aadhaar authentication

Aadhaar authentication transactions have grown substantially over the years, reflecting widespread adoption across sectors. Cumulative authentication transactions have witnessed steady growth over the last five years, growing at a compound annual growth rate (CAGR) of 20%. It has increased from 71.9 billion transactions in FY 2021-22 to 175.4 billion in FY 2025-26. The authentication transactions are further split into Yes/No authentication transactions and e-KYC authentication transactions. The share of e-KYC authentication transactions has steadily grown from 13.47% in FY 2021-22 to 18.72% in 2025-26.

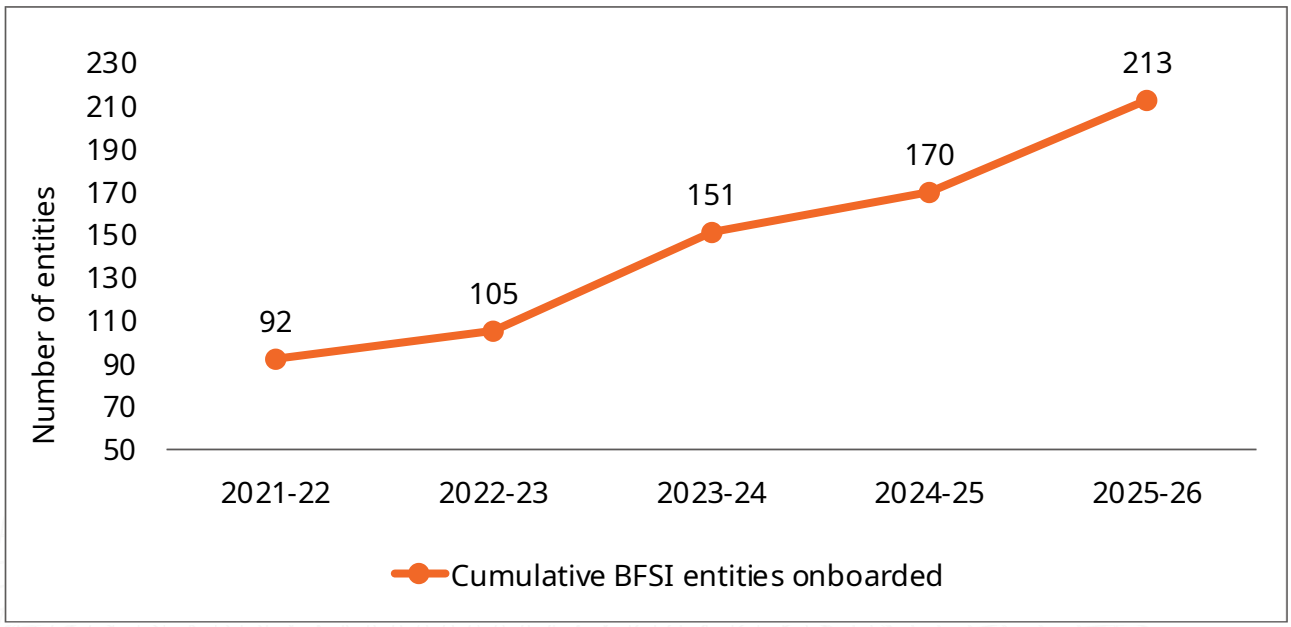



The sector-wise distribution of authentication transactions has government, banks, and telecom consistently accounting for the largest share during FY 2022-23 to FY 2025–26.

**Sector-wise cumulative Aadhaar authentication transactions (in millions)**

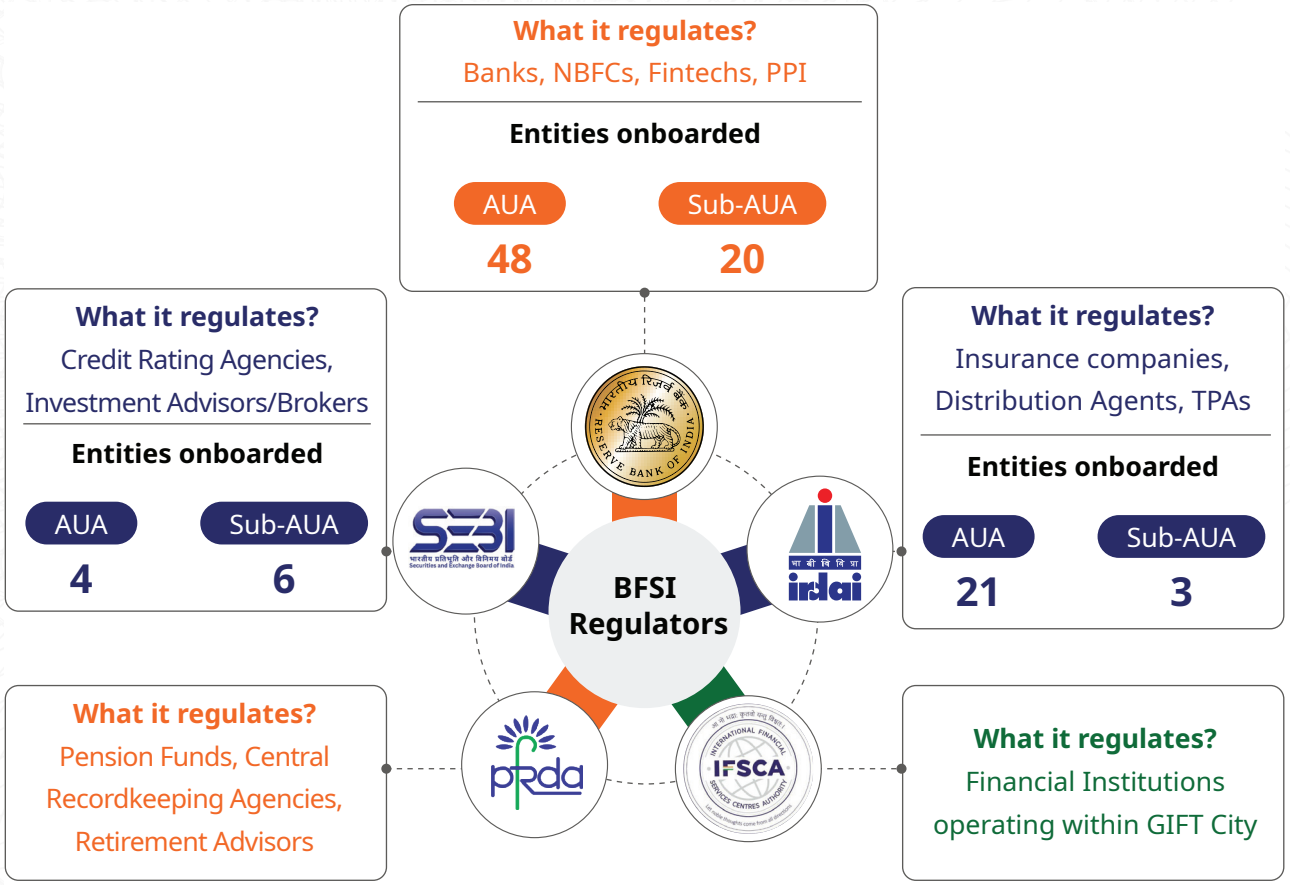
| Sector | 2022-23 | 2023-24 | 2024-25 | 2025-26 |
|---|---|---|---|---|
| **Central Government** | 9,140 | 18,804 | 30,119 | 41,572 |
| **Bank** | 7,572 | 16,786 | 26,262 | 35,502 |
| **State Government** | 3,121 | 6,830 | 9,989 | 13,001 |
| **Telecom** | 1,231 | 2,370 | 3,437 | 4,535 |
| **PSU** | 39 | 237 | 469 | 867 |
| **Certifying Agency** | 94 | 263 | 448 | 646 |
| **NBFC, Brokerage Firm, Insurance & Section 8 Co.** | 16 | 75 | 221 | 512 |

## Aadhaar authentication in BFSI sector




## Regulatory ecosystem for fintech seeking to perform Aadhaar authentication

India's fintech ecosystem operates under sector specific regulatory agencies including RBI, SEBI, IRDAI, PFRDA, and IFSCA which shape entities eligibility and compliance requirements. Aadhaar authentication provides regulated entities with a trusted identity layer for secure customer onboarding, compliance, and scalable digital service delivery.



India built something no other country has built - a digital identity for 1.4 billion people

**- Emmanuel Macron**

President of France

19 Feb 2026



# 2 How can I get onboarded for Aadhaar authentication?

### Who can apply?

All government and non-government entities.

### How to apply?

| | Application form | Audit checklist | Onboarding video |
|---|---|---|---|
| AUA/KUA | | | |
| Sub-AUA/ Sub-KUA | | | |

Reach out at onboarding@uidai.net.in and complete the onboarding process as prescribed by UIDAI.

The selection of the AUA/KUA/Sub-AUA/Sub-KUA onboarding route will depend on the entity's use cases, authentication transaction volume, technical capabilities, etc.



## Onboarding process for AUA & KUA

| Step | Description | |
|---|---|---|
| 1 Application Submission | • AUA/KUA submits<br>◦ Application form<br>◦ Copy of Gazette notification<br>◦ Supporting documents as prescribed by UIDAI<br>• UIDAI issues in-principle approval letter upon satisfactory evaluation | 45 to 90 Days |
| 2 Pre-Onboarding Audit | • AUA/KUA complete pre-onboarding audit by a UIDAI nominated CERT-In empaneled audit agency<br>• Submits fully compliant audit report along with relevant artefacts<br>• UIDAI provides approval upon satisfactory compliance | |
| 3 Agreement Execution and Pre-Production Access | • Execute AUA/KUA agreement and pays license fees<br>• UIDAI verifies the Bank Guarantee<br>• UIDAI issues pre-production access key | |
| 4 Complete Test Transactions | • Complete and validate the prescribed number of test transactions for each authentication modality | Upto 30 Days |
| 5 Onboarding Audit | • Undertake an audit through a CERT-In empaneled audit agency<br>• Submit fully compliant audit report along with artefacts | |
| 6 Migration to Live Production | • UIDAI provides access to the live production environment upon successful audit approval | |

## Onboarding process for Sub-AUA & Sub-KUA

| Step | Description |
|---|---|
| **1 Application Submission** | • Sub-AUA/Sub-KUA submits<br>◦ Application form<br>◦ Joint Undertaking through selected AUA/KUA<br>◦ Supporting documents as prescribed by UIDAI<br>• UIDAI issues in-principle approval letter upon satisfactory evaluation |
| **2 Pre-Production Access** | • Payment of license fees<br>• UIDAI issues pre-production access key |
| **3 Complete Test Transactions** | • Complete and validate the prescribed number of test transactions for each authentication modality |
| **4 Onboarding Audit** | • Undertake an audit through a CERT-In empaneled audit agency<br>• Submit fully compliant audit report along with artefacts |
| **5 Migration to Live Production** | • UIDAI provides access to the live production environment upon successful audit approval |

**45 to 90 Days**



India has done a wonderful job with Digital Public Infrastructure. Now, the focus is on how to make and use this to improve the lives of the people

**- Queen Maxima**

Queen of the Netherlands & United Nations Secretary-General's Special Advocate for Financial Health (UNSGSA)

24 Jun 2026



# 3 I am non-government. Am I still eligible?

## Short answer: Yes! Read on...

While regulated entities can be onboarded into Aadhaar authentication ecosystem as AUA/KUA/Sub-AUA/Sub-KUA, several large sectors remain outside its ambit. Social Welfare, Innovation, Knowledge (SWIK) Rules, 2020 were introduced to bridge this gap.

### Who can apply?

Govt. and non-govt. entities having use cases for good governance, ease of living of residents, or enabling innovation are allowed.

### How to apply?

Select a use case from the approved list available at the SWIK use-cases list and apply at Aadhaar Good Governance Portal




**Onboarding process for SWIK**

| Step | Description |
|---|---|
| 1 Registration and Proposal Submission | • Registration of applicant organization at SWIK portal (https://swik.meity.gov.in/)<br>• Concerned Ministry/Dept. submits the proposal to MeitY |
| 2 Review of Proposal | • MeitY reviews, and, if deemed appropriate, forwards the proposal to UIDAI for examination<br>• UIDAI examines the proposal and upon satisfactory evaluation, recommends to MeitY |
| 3 Authorization and Gazette Notification | • MeitY authorizes the use-case to concerned Ministry/Dept.<br>• Concerned Ministry/Dept. issues a Gazette notification and the entity can now apply to UIDAI for onboarding |

Non-government use case approved under SWIK - Bharat Matrimony, Shaadi.com, Indigo Airlines, IBPS, CIBIL, etc.

Implementation of DPIs such as Aadhaar, a foundational digital ID system, is considered to have played a critical role in moving ownership of transaction accounts from approximately one-fourth of adults in 2008 to over 80 percent now, a journey that it is estimated could have taken up to 47 years without DPIs

**- World Bank, Excerpts from Report on G20 Policy Recommendations on DPI**

03 Oct 2023



# 4 What options are available for ease of onboarding?

There are multiple frameworks introduced for ease of onboarding of entities to use Aadhaar authentication.

## 4.1 e-KYC Setu

Simplifying Aadhaar authentication for regulated entities to use Aadhaar e-KYC services through a secure and standardized framework leveraging e-KYC Setu of NPCI.

### Who can apply?

Regulated entities registered with RBI, SEBI, IRDAI, PFRDA, or IFSCA seeking faster onboarding.

### How to apply?

Entities can send an application to ekycservices@npci.org.in




**Onboarding process for e-KYC Setu**

| Step | Description |
|---|---|
| 1 Application Submission | • Regulated entity submit application form to NPCI<br>• NPCI reviews & forwards application to UIDAI for review |
| 2 Audit Report & License Fee | • Regulated entity submits onboarding audit report issued by CERT-In empaneled audit agency and pays license fee |
| 3 MoU execution and Onboarding | • MoU is executed between NPCI and the entity<br>• Entity is onboarded by UIDAI |

Within 21 Days

Under e-KYC Setu system, regulated entities are onboarded without requiring a Gazette Notification.

# 4.2 Sub-AUA (LITE) Framework

Quick & simplified access for entities conducting low-volume authentication transactions to accelerate digital service delivery.

### Who can apply?

Govt. and non govt. entities that perform ≤ 500,000 authentication transactions per financial year can be onboarded through simplified Sub-AUA Less in Transaction Entity (LITE) framework.

### How to apply?

The entity submits a formal request to sponsoring AUA/KUA.
The AUA/KUA submits the request to UIDAI.




**Onboarding process for Sub-AUA (LITE) framework**

| Step | Description |
|---|---|
| 1 Application Submission | • Entity submits application form for Sub-AUA (LITE) and pays a one-time registration fee of ₹25,000 |
| 2 Pre-Production Access | • UIDAI provides in-principle approval & issues pre-production access key |
| 3 Complete Test Transactions | • Complete and validate the prescribed number of test transactions for each authentication modality |
| 4 Migration to Live Production | • UIDAI provides access to live production<br>• Sub-AUA (LITE) uses existing AUA infrastructure only |

Within 14 Days

If the transaction volume exceeds 500,000 transactions in a financial year, Sub-AUA (LITE) is charged with the standard Sub-AUA/Sub-KUA license fee.

**One Framework. One Infrastructure. Multiple Entities.**

EU’s cooperation with India on digital is focused on the interoperability of our two digital public infrastructures, which actually are the world’s largest and most advanced. India’s Aadhaar and the EU digital wallet aim to offer public and private services to nearly 2 billion citizens

**- Ursula von der Leyen**

President of the European Commission

28 Feb 2025



# 5 What's new in Aadhaar authentication ecosystem?

## 5.1 Process improvements

### (a) Streamlined onboarding process

UIDAI has simplified AUA/KUA and Sub-AUA/Sub-KUA onboarding audit checklist.

| | AUA/KUA | Sub-AUA/Sub-KUA |
|---|---|---|
| Onboarding audit checkpoints (keeping security intact) | Before 127 → After 77 ~40% ↓ | Before 111 → After 58 ~50% ↓ |

Entities having requisite IT infra and security policies as per UIDAI guidelines are onboarded in much lesser time period

| | | |
|---|---|---|
| PFMS 45 days | Appnit Tech 35 days | PhonePe Wealth 20 days |

Pre-onboarding audit checklist comprising of 60 checkpoints, is conducted by UIDAI identified CERT-In empaneled audit agency.

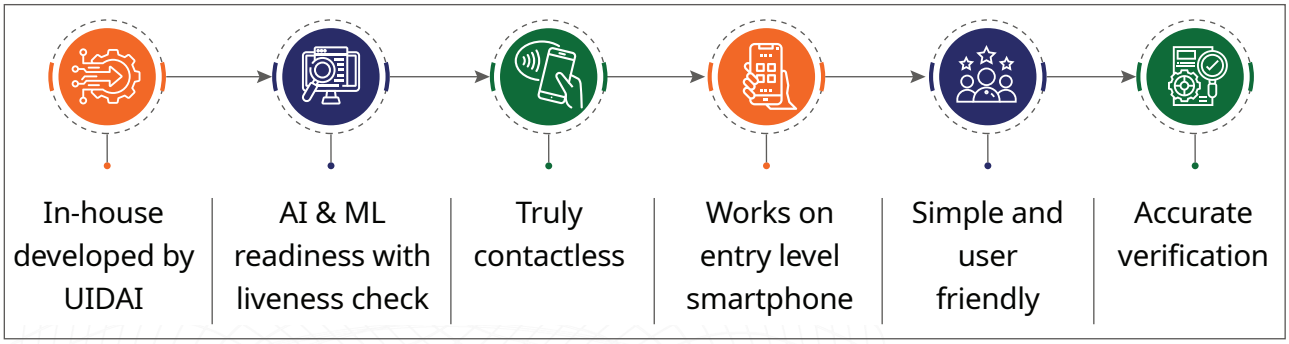
### (b) Enhanced guidance and expedited processes

UIDAI has introduced measures to simplify the onboarding journey and help entities achieve readiness for seamless integration. These include:

- Expert guidance and support from UIDAI dedicated teams to help entities understand application, compliance, and technical requirements.
- Dedicated audit team at UIDAI to enable faster review and clearance of applications.
- Digital onboarding platforms that enable online application submission, status tracking, integrated audit workflows and timely resolution of queries.

### (c) Simplified face authentication integration

Face authentication is a 1:1 matching process that compares the individual's live facial image with their image captured at the time of enrolment. It is gaining wider adoption for identity verification, due to its accuracy, convenience, adaptability and no device dependency.




UIDAI has significantly simplified face authentication audit checklist for increasing adoption in digital first entities, including fintechs, NBFCs, tourism and hospitality platforms, gig economy players, delivery services providers, and telecom service providers.

| Audit checkpoints (earlier) | Audit checkpoints (now) |
|---|---|
| 70 | 18 |

## 5.2 Technological enhancements

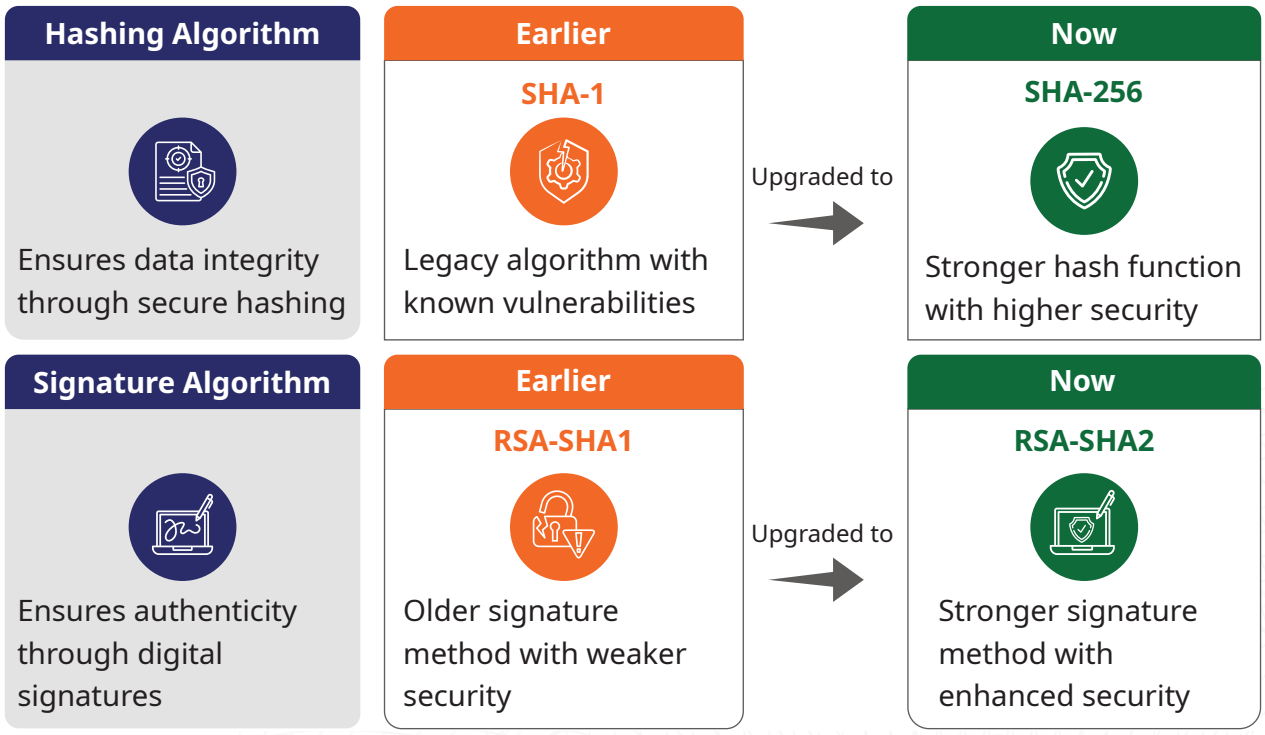
UIDAI has introduced several technological enhancements that strengthen the Aadhaar authentication ecosystem to deliver secure, reliable, and scalable digital services.

### (a) Stronger security standards (SHA-1 to SHA-2 migration)

UIDAI has completed the migration of digital signatures from SHA-1 algorithm with SHA-2 (aka SHA-256). This migration enhances the security of Aadhaar authentication ecosystem by providing stronger protection against cyberattacks and is aligned with global security standards such as ISO and NIST Hash Standards. UIDAI has migrated two components of the digital signature concurrently:

i. Hash algorithm (Digest Method) which generates a unique hash (fingerprint) of the authentication request, being migrated from SHA-1 algorithm (160-bit hash) to SHA-256 algorithm (256-bit hash)

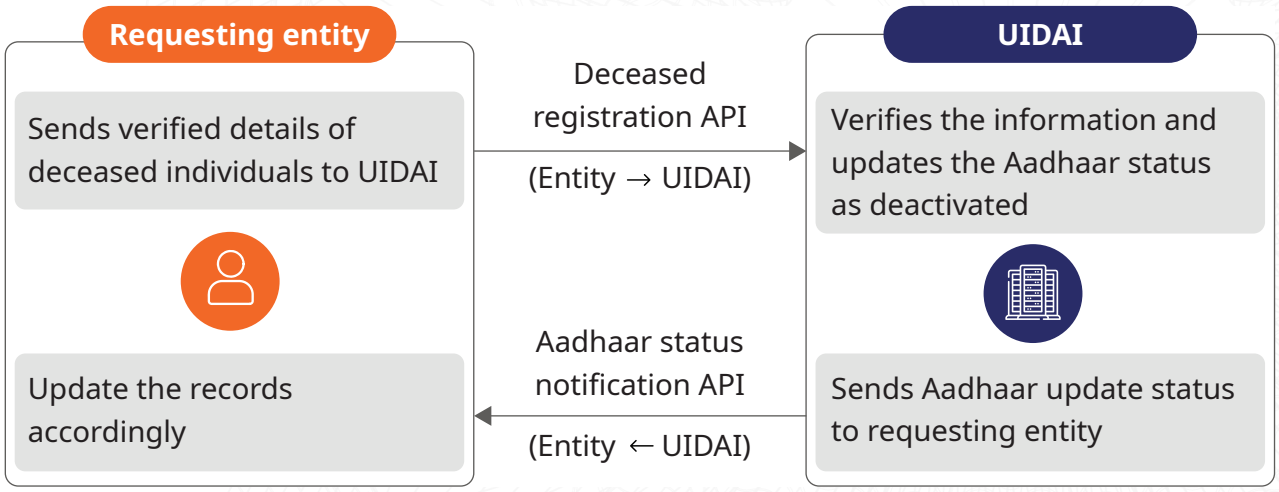
ii. Signature Method which digitally signs the generated hash using the entity's private key is being migrated from RSA-SHA1 algorithm to RSA-SHA2 algorithm




## (b) Aadhaar status notification API and Deceased registration API

UIDAI's Aadhaar status notification API provides timely sharing of Aadhaar status changes (deactivated, omitted or re-activated) to the requesting entities, helping to maintain accurate records and prevent identity misuse.

The deceased registration API enables requesting entities to electronically share verified information of deceased Aadhaar number holders with UIDAI. It facilitates timely updation of Aadhaar records and prevent misuse of Aadhaar belonging to deceased individuals.




## (c) Face authentication SDK for Point-of-Sale devices

UIDAI has introduced Aadhaar Face Authentication as a key biometric modality and is enabling its adoption across Point-of-Sale (PoS) devices through a dedicated Face Authentication Software Development Kit (SDK). The changes allow requesting entities to perform Aadhaar authentication for people with worn-out fingerprints from labor, aging, or other conditions.

This SDK is designed for Android and Linux-based PoS devices and enables seamless, contactless 1:1 biometric face matching directly at retail and service delivery touchpoints.

**Key capabilities enabled by Face Authentication SDK**

**Plug-and-Play Integration**

Provide merchant application developers with clean APIs to trigger face captures and receive signed Personal Identity Data (PID) blocks with minimal coding

**Hardware Agnostic Performance**

Optimize capturing speeds and processing on budget POS terminals

**L1-Level Security Compliance**

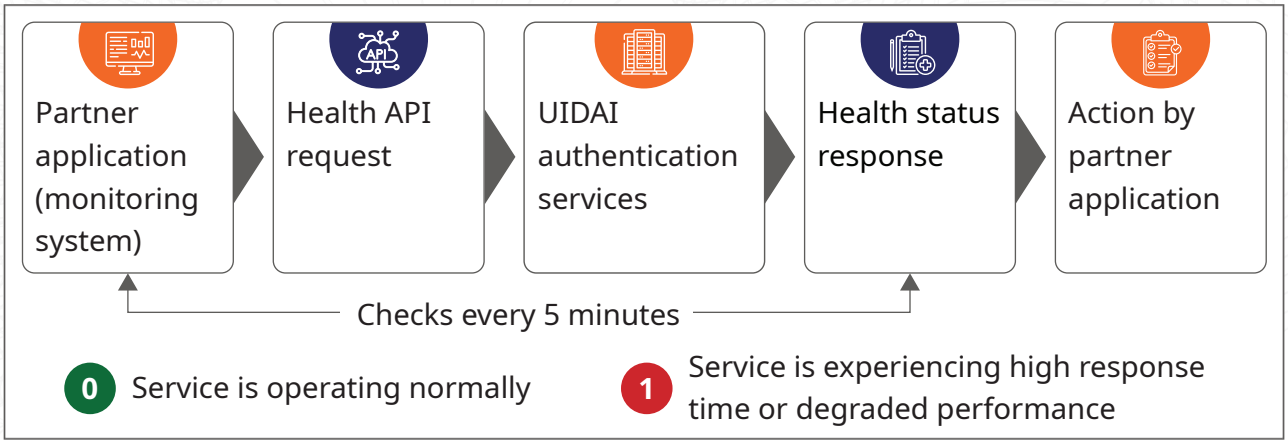
Ensure the cryptographic signing of biometric data occurs in a hardware-secured environment (TEE)

**Improved Transaction Success Rates**

Offer a touchless, high-success-rate biometric fallback option to eliminate checkout failures

## (d) Health API

UIDAI's Health API enables the requesting entities to monitor the real-time availability of Aadhaar authentication services. It provides service status updates, e.g., "0" for normal availability, and "1" for high response time or degraded performance. Fintech platforms can use these indicators to detect disruptions, trigger alerts, activate fallback mechanisms, and improve service reliability.




## (e) Aadhaar e-Sign

Aadhaar e-Sign allows user to digitally sign the documents remotely. This service ensures security through safeguards such as document hash-based signing, one-time private keys, protection of biometric information, and signature invalidation upon document modification, enabling faster and trusted digital experiences.

**Aadhaar e-Sign: Authenticated, consent-based, secure, paperless digital signature**

| | | | |
|---|---|---|---|
| Consent based digital sign of document from remote location | User is authenticated through Aadhaar authentication | ESP digitally signs the document after authentication | Digitally signed document delivered |

## (f) Multi-mode authentication

Multi-mode authentication refers to the UIDAI's ecosystem's support for more than one channel of demographic, OTP based, biometric and multi-factor combination of these. Requesting entities can choose the mode or combination of modes, best suited to their transaction device capability and citizen's context.

| | | | | | | |
|---|---|---|---|---|---|---|
| Aadhaar No | + | OTP | + | Demographic | | |
| Aadhaar No | + | OTP | + | Biometric: Face or Finger or Iris | | |
| Aadhaar No | + | Demographic | + | Biometric: Face or Finger or Iris | | |



# 6 What are the key use cases?

Aadhaar authentication is enabling expanding use cases across BFSI, fintech, and other sectors, helping entities build secure, seamless, and scalable future-ready digital services.

## (a) BFSI sector use case

**Challenges**

**Co-operative Bank**

Manual KYC & re-KYC

**Digital Lending**

Complex customer verification

**Insurance**

Difficult renewal and claim servicing

**Aadhaar authentication – Enabling secure, paperless and trusted journeys across BFSI sector**

1. Account opening/Loan application/Insurance policy purchase & renewals
2. Secure identity verification using Aadhaar (OTP/Biometric authentication)
3. Accurate data capture reduces manual entry and verification time
4. Seamless Re-KYC, renewals, nominee updates




**Applicable onboarding route**

| | AUA/KUA | Sub-AUA/ Sub-KUA | SWIK | e-KYC Setu | Sub-AUA (LITE) |
|---|---|---|---|---|---|
| Cooperative Bank | ✓ | ✓ | ✗ | ✓ | ✓ |
| Digital Lending | ✓ | ✓ | ✗ | ✓ | ✓ |
| Insurance | ✓ | ✓ | ✗ | ✓ | ✓ |

## (b) Aadhaar-enabled biometric attendance system (AeBAS) use case

**Challenges**

How can organizations ensure accurate, real-time attendance and visibility of employee presence?



**Authenticate the employee using Aadhaar**

1. Employee consents to use Aadhaar authentication for marking attendance
2. Aadhaar authentication (Biometric authentication)
3. Attendance marked instantly




**Applicable onboarding route**

| | AUA/KUA | Sub-AUA/ Sub-KUA | SWIK | e-KYC Setu | Sub-AUA (LITE) |
|---|---|---|---|---|---|
| AeBAS | ✓ | ✓ | ✓ | ✗ | ✓ |

## (c) Matrimony/matchmaking/dating platforms use case

**Challenges**

How can users trust that profiles represent genuine individuals without fake, duplicate or impersonated identities?




**Trusted profile verification through Aadhaar**

1. Entity captures basic details during registration on the platform
2. User completes Aadhaar authentication (OTP / Biometric authentication)
3. Show Aadhaar-authenticated indicator on user's profile




**Applicable onboarding route**

| | AUA/KUA | Sub-AUA/ Sub-KUA | SWIK | e-KYC Setu | Sub-AUA (LITE) |
|---|---|---|---|---|---|
| Matrimony/ dating | ✓ | ✓ | ✓ | ✗ | ✓ |

## (d) Pension/credit bureau/securities market broker use case

### Challenges

**Pension registration**

Slow & Manual onboarding

**Credit Bureaus**

Duplicate or inaccurate identity records

**Securities/ Market Brokers**

Identity fraud risk

### Aadhaar authentication – Enabling secure, paperless and trusted journeys across sectors

1. Pension registration/Jeevan Pramaan/Demat account opening/Credit information verification
2. Secure identity verification using Aadhaar (OTP/Biometric authentication)
3. Aadhaar-verified details captured through e-KYC
4. Requested service successfully completed




### Applicable onboarding route

| | AUA/KUA | Sub-AUA/ Sub-KUA | SWIK | e-KYC Setu | Sub-AUA (LITE) |
|---|---|---|---|---|---|
| **Pension** | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Credit Bureaus** | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Securities Market Brokers** | ✓ | ✓ | ✓ | ✓ | ✓ |

## (e) Taxi, ride share, and delivery platform use case

### Challenges

How can I prevent profile misuse and ensure only authenticated workers serve customers?



### Authentication of Drivers/Delivery partners

1. Driver/Delivery partner consents
2. Authenticate via OTP / Biometric authentication
3. Platform verifies Driver/Delivery partner identity and assigns ride/delivery




**Applicable onboarding route**

| | AUA/KUA | Sub-AUA/ Sub-KUA | SWIK | e-KYC Setu | Sub-AUA (LITE) |
|---|---|---|---|---|---|
| Ride-share/ delivery platform | ✓ | ✓ | ✓ | ✗ | ✗ |



# Contact Us

### Onboarding activities

dir2.auth-hq@uidai.net.in

dd2.auth-hq@uidai.net.in

onboarding@uidai.net.in

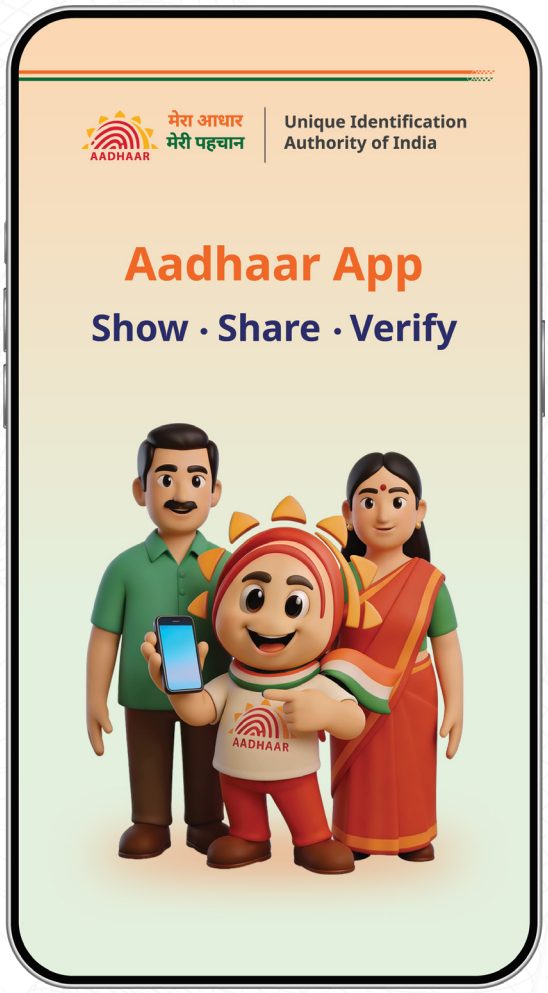
### Audit and compliance activities

dir1.auth-hq@uidai.net.in

dd1.auth-hq@uidai.net.in

auth.audit@uidai.net.in

**Have query?**
**Scan the QR Code**

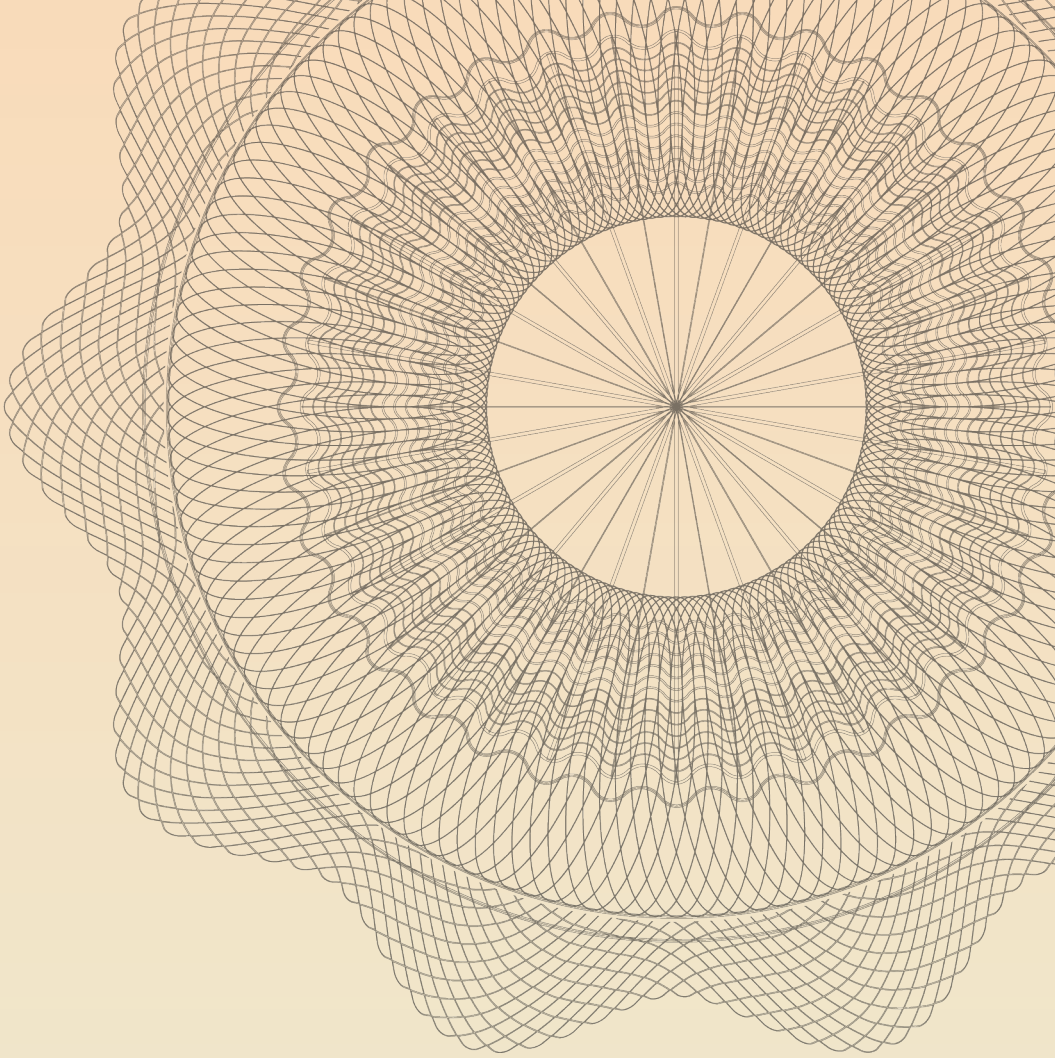



**Acknowledgement:**

This playbook was developed with support from our knowledge partner, MSC (MicroSave Consulting).

**Disclaimer:**

This handbook is provided solely for informational and reference purposes.



मेरा आधार
मेरी पहचान
AADHAAR

Unique Identification
Authority of India

**UIDAI Head Office**

Bangla Sahib Road, Behind Kali Mandir, Gole Market, New Delhi - 110001

For more information, please contact us at help@uidai.gov.in

Follow us on: