मेरा आधार
मेरी पहचान

Unique Identification
Authority of India

Aadhaar offline verification

Handbook

January 2026

Table of contents

About this handbook

This handbook provides a comprehensive overview of Aadhaar offline verification, a secure, convenient, and privacy-friendly mechanism that enables identity verification of Aadhaar number holders without connection to the UIDAI's Central Identities Data Repository (CIDR). The handbook aims to support Offline Verification Seeking Entities (OVSEs), policymakers, technology providers, and other ecosystem players in understanding the offline verification, types of offline verification, offline verification using the new Aadhaar App and practical use cases of offline verification. By consolidating information on offline verification, the handbook aims to encourage responsible and lawful adoption of Aadhaar offline verification by the ecosystem.

- Overview of Aadhaar offline verification
- Types of Aadhaar offline verification
- Aadhaar App and verifiable credentials
- Aadhaar offline verification ecosystem
- Use cases of Aadhaar offline verification

This handbook is intended for entities who want to register as Offline Verification Seeking Entities (OVSEs) to carry out offline verification of Aadhaar Number Holder (ANH).

The intended audience includes:

- Government ministries, departments, and agencies
- Public institutions seeking identity verification
- Private sector organizations seeking identity verification
- System integrators and solution providers

1 Aadhaar offline verification: An overview

Understanding Aadhaar offline verification

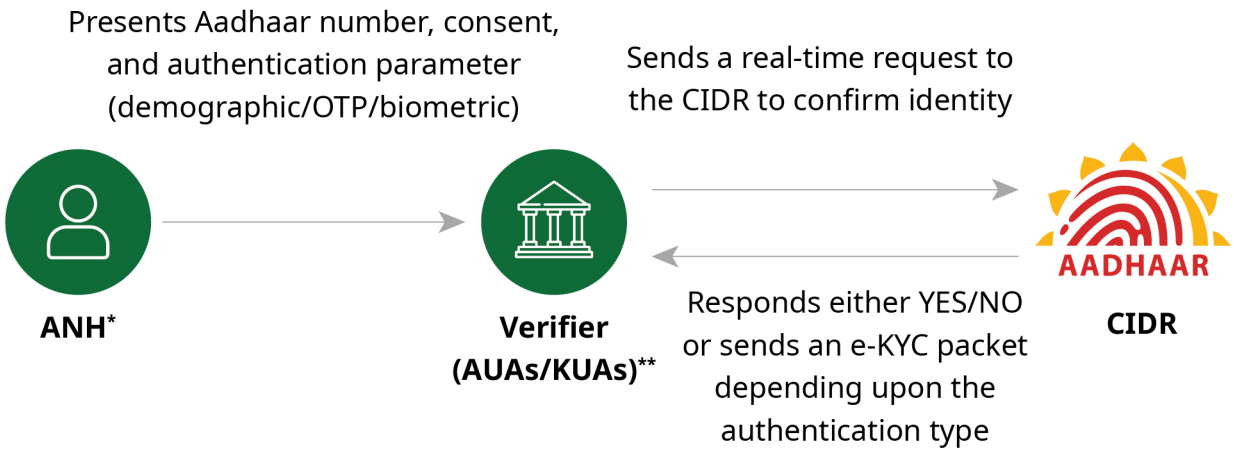
Aadhaar offline verification can be understood as identity verification of Aadhaar Number Holder (ANH) without sending request to and receiving a response from the UIDAI's Central Identities Data Repository (CIDR). The organizations that conduct offline verification are referred to as Offline Verification Seeking Entities (OVSEs).

Definition as per the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016:

Offline verification means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations

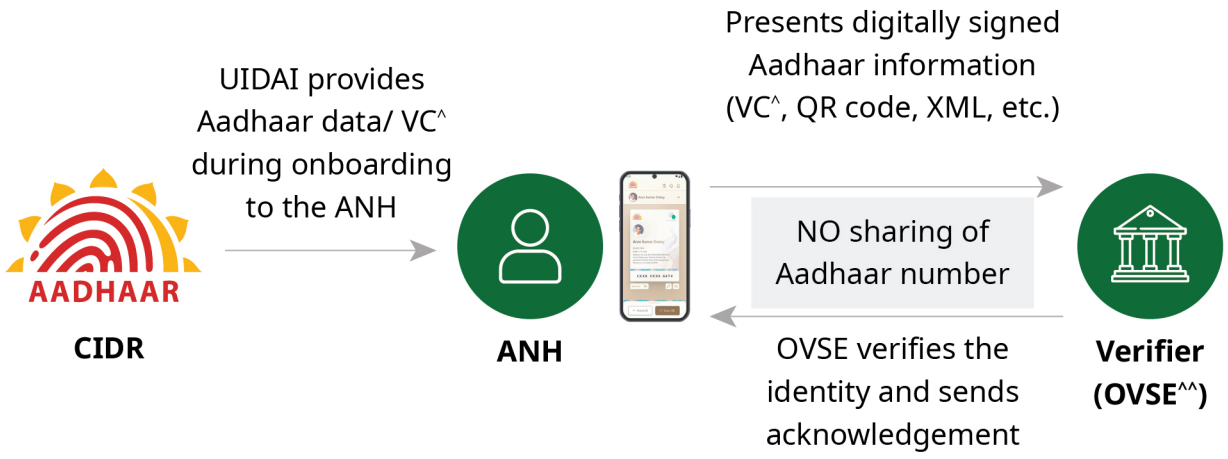
Flows in online authentication and offline verification:

Online authentication



In online authentication, a real-time request is sent to UIDAI's CIDR with the Aadhaar number and authentication parameters (demographic, OTP, biometric), and CIDR responds in real time with Yes / No or a e-KYC packet

Offline verification



In offline verification, the ANH directly provides digitally signed Aadhaar information to the OVSE instead of the OVSE receiving it from CIDR

*ANH: Aadhaar Number Holder

**AUA: Authentication User Agency; KUA: e-KYC User Agency

^Aadhaar verifiable credential (VC) stored locally on ANH's device

^^OVSE: Offline Verification Seeking Entity

Evolution

Evolution of Aadhaar offline verification

2009 — The Unique Identification Authority of India (UIDAI) was established in 2009, laying the foundation for Aadhaar.

2016 — The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, established the statutory framework for Aadhaar use and governance.

2018 — UIDAI introduced the 'Aadhaar Secure QR Code,' and 'Aadhaar paperless offline e-KYC (offline XML)' that contained demographic data and a photograph, digitally signed by UIDAI.

2019 — Aadhaar offline verification legal framework incorporated under the Aadhaar and Other Laws (Amendment) Act, 2019.

2021 — UIDAI notified the Aadhaar (Authentication and Offline Verification) Regulations, 2021, setting out the governance framework for offline verification.

2025 — UIDAI launched an early-access version of the new Aadhaar App.

2025 — UIDAI notified the Aadhaar (Authentication and Offline Verification) Amendment Regulations, 2025.

2026 — UIDAI launched the new Aadhaar App.

Benefits of Aadhaar offline verification

Aadhaar offline verification is driven by its ability to provide privacy and greater control to ANH of their Aadhaar data, ensuring the integrity and security of Aadhaar information through digital signatures, reducing compliance burdens for OVSEs, and enabling identity verification without connectivity to UIDAI's CIDR.

Privacy-preserving and user control: Aadhaar offline verification enables the ANH to share digitally signed, selective, and minimum information required for verification, thereby reducing the risk of data leakage and identity theft.

Digitally signed information: The core feature of offline verification is the digital signature used by UIDAI. The shared offline Aadhaar data is digitally signed by UIDAI, enabling service providers to verify its integrity and ensuring that the information cannot be tampered.

Less compliance burden: As Aadhaar offline verification does not require the collection, transmission, or storage of the full Aadhaar number, it significantly reduces the compliance burden on OVSEs.

No connectivity to CIDR required: Aadhaar offline verification does not require a connection to the CIDR for verifying the identity of ANH.

Real-world example: Need for Aadhaar offline verification

Scenario:

Akanksha arrives at the hotel front desk for check-in, where the staff requests her to submit the proof of identity.

Case 1: Without Aadhaar offline verification

She gives her Aadhaar card as proof of identity, following which the staff makes a photocopy and retains it. The photocopy exposes the Aadhaar number and associated personal details in full, leaving her little control over how her data is stored, shared, or reused. Akanksha's data may be sold/shared with any other entity without her consent. The hotel also faces difficulty in establishing the authenticity of the Aadhaar card since visual inspection alone does not confirm whether the document is genuine or not.

Case 2: With Aadhaar offline verification

The hotel, acting as an OVSE, obtains consent from Akanksha. She shares her verifiable credentials using Aadhaar App. This approach reduces risk of data leakage and identity theft, while verifiable credentials enables the hotel to establish the integrity of data.

2 Types of Aadhaar offline verification

Primarily, Aadhaar offline verification may be carried out through four types: Aadhaar secure QR code verification, Aadhaar paperless offline e-KYC verification, e-Aadhaar verification, and Aadhaar verifiable credential (VC) verification.

Aadhaar secure QR code verification

UIDAI provides the Aadhaar secure QR code in the Aadhaar letter, PVC card, e-Aadhaar, mAadhaar and the new Aadhaar App. The secure QR code holds demographic information and photograph of the ANH, which is secure and tamper proof, as it is digitally signed by UIDAI.

OVSE may use an Aadhaar application, such as the new Aadhaar App, Aadhaar QR scanner and mAadhaar, to read the QR code and subsequently validate the digital signature present in the QR code, confirming the authenticity and integrity of the shared document without connecting to the CIDR.

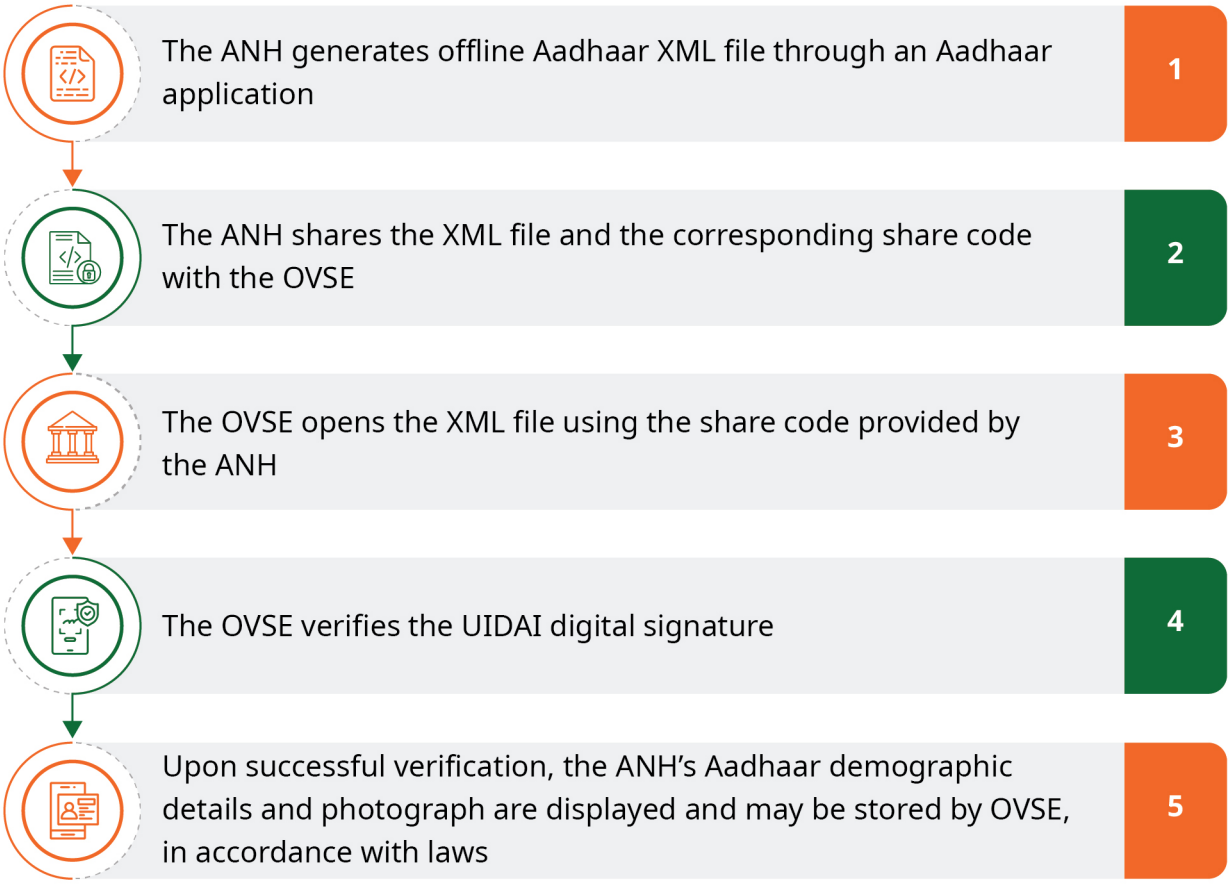
Process flow of Aadhaar secure QR code verification

1. The ANH presents an Aadhaar document (physical or digital) containing the Aadhaar secure QR code, or displays the QR code through an Aadhaar application
2. The OVSE scans the QR code using a QR scanner on an Aadhaar application
3. The Aadhaar application verifies the UIDAI digital signature embedded in the QR code
4. Upon successful verification, the ANH's demographic details and photograph are displayed, but the details are not savable

Aadhaar paperless offline e-KYC verification

Aadhaar paperless offline e-KYC is a digitally signed, shareable document provided by UIDAI to ANH that enables ANH to share their identity information with service providers. The document (XML file) has demographic information and a photograph of the ANH. ANH can download Aadhaar paperless offline e-KYC through an Aadhaar application and share the same along with 'share code' with OVSEs for identity verification.

Process flow of Aadhaar paperless offline e-KYC verification



e-Aadhaar verification

e-Aadhaar is a digitally signed, password-protected digital version of the Aadhaar letter, issued by the UIDAI. It is legally valid and equivalent to the physical Aadhaar letter. e-Aadhaar enables ANH to carry and present their Aadhaar details in digital form for lawful purposes, including offline verification. e-Aadhaar also contains an Aadhaar secure QR Code, providing an additional mechanism for offline verification.

Process flow of e-Aadhaar verification

1. The ANH downloads the e-Aadhaar from UIDAI's official website or mobile application after OTP-based verification
2. The downloaded e-Aadhaar PDF is accessed using the prescribed password
3. The OVSE opens the e-Aadhaar document using a compatible PDF reader
4. The OVSE checks the UIDAI digital signature embedded in the document to confirm that it is genuine and untampered
5. Optionally, the Aadhaar secure QR code within the e-Aadhaar may be scanned using an Aadhaar application
6. Upon successful signature validation or QR code verification, the Aadhaar details are verified locally

See this video to understand the digital signature validation in e-Aadhaar

Aadhaar verifiable credential verification

Aadhaar Verifiable Credential (VC) verification is the latest type of offline verification introduced by UIDAI to enhance user control, selective disclosure, and digital portability. VCs are digitally signed and are issued to the ANH through the Aadhaar App. These credentials may include Aadhaar attributes such as demographic information and a photograph. Aadhaar VC is stored securely on the Aadhaar App of the ANH and may be shared fully or partially, based on the requirements of the verification request and with the approval of the ANH.

Process flow of Aadhaar verifiable credential verification

1. The ANH onboards on the Aadhaar App after SIM binding and face authentication. Upon successful onboarding, Aadhaar VC issued by UIDAI is stored locally on the ANH's Aadhaar App
2. The OVSE requests specific Aadhaar attributes required for offline verification
3. The ANH reviews the request and either approves or rejects it
4. If OVSE requires, an optional face verification may be performed on the ANH's device to establish proof of presence
5. The requested verifiable credentials are shared with the OVSE through the Aadhaar App
6. The OVSE verifies the UIDAI digital signature to ensure integrity of data

3 Use of the Aadhaar App for offline verification

This chapter provides the details on the newly launched Aadhaar App by UIDAI and its utility in the Aadhaar offline verification.

An overview of the Aadhaar App

UIDAI has released the Aadhaar App to enable seamless access to Aadhaar-related services. The Aadhaar App is a key tool for OVSEs to complete the offline verification through Aadhaar Verifiable Credentials (VC).

The Aadhaar App allows the Aadhaar Number Holder (ANH) to access Aadhaar-related services such as Aadhaar detail update, authentication history logs, one-click biometric lock/unlock, etc.

The flagship features of the Aadhaar App are:

The Aadhaar App-Key features and capabilities

Show · Share · Verify

Sharing of verifiable credentials	• VCs are digitally signed, tamper-proof, and verifiable without requiring access to the CIDR • VCs can be shared through cross-device QR scanning, app-to-app intent, web-to-app intent, or self-share
Selective data sharing	• Enables selective sharing of Aadhaar data attributes such as name, address, date of birth, or photograph
Face verification for proof of presence	• Face verification can be performed locally, without connection to the CIDR • Convenient verification anywhere, anytime
Savable, digitally signed outputs	• For registered OVSEs, the app enables generation of a digitally signed VC which can be stored in compliance with UIDAI regulations

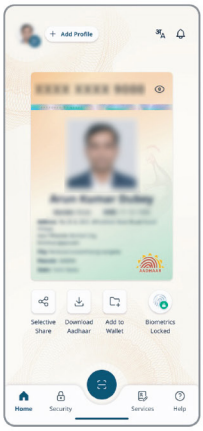
Illustrative flows of identity verification using the Aadhaar App

The Aadhaar App supports multiple offline verification flows using Aadhaar verifiable credentials, depending on the use case and assurance requirements.

The Aadhaar App flows are defined as follows:

1. Show : Simple show of digital Aadhaar on phone for verification

In the Show flow, Aadhaar details are displayed on ANH's Aadhaar App for visual verification by the verifier, without any credentials being digitally shared or transferred



ANH displays the Aadhaar data on Aadhaar app

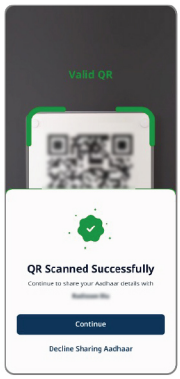
Verifier visually verifies the Aadhaar data

2. Share: Sharing of Aadhaar VC through Aadhaar app

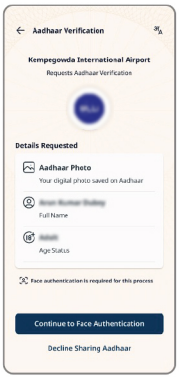
Aadhaar VC is shared digitally through the Aadhaar App with an OVSE, based on approval from ANH. If an OVSE requires higher assurance, it can implement an additional assurance layer through offline face verification

(i) QR-based sharing

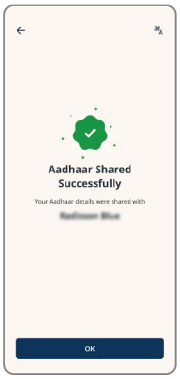
Aadhaar VC is shared through QR code scanned via the Aadhaar App and verified locally by the OVSE



ANH scans the QR code presented by OVSE



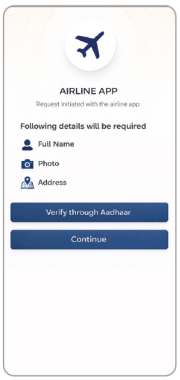
ANH approves sharing of data requested by OVSE



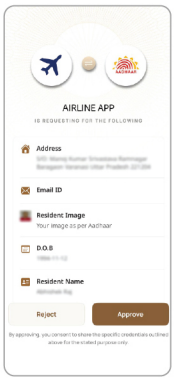
OVSE receives the data & validates digital signature

(ii) App-to-app and Web-to-app intent

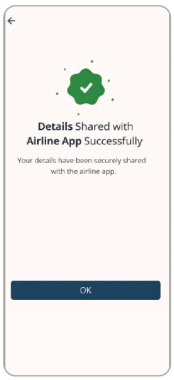
Aadhaar VC is shared securely from the Aadhaar App to the OVSE's application using app-to-app intent mechanisms, or to the OVSE's web portal using web-to-app intent mechanism



ANH initiates a verification request from OVSE's app or web portal, which redirects to ANH's Aadhaar app



ANH approves credentials requested by OVSE



OVSE app/ web-portal receives the verifiable credentials

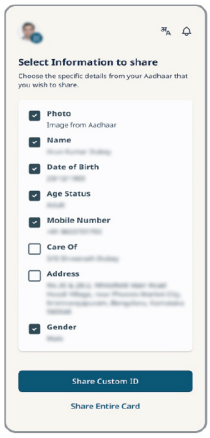
What is app-to-app and web-to-app intent?

App-to-app intent in the Aadhaar flow is a secure handoff where a requesting app invokes the Aadhaar App via a system intent to perform consent-based identity verification and receives a signed response back from the Aadhaar App in verifiable credential format.

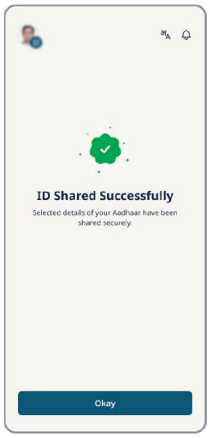
Web-to-app intent in the Aadhaar flow is a secure handoff where a web application redirects the user to the Aadhaar App using a deep link to complete consent-based identity verification and receives a signed response back in verifiable credential format.

(iii) Selective self-sharing

ANH shares the Aadhaar VC selectively with the OVSE



ANH selects data fields in the Aadhaar app



ANH shares the selected data with the OVSE

Offline face verification using the Aadhaar App

If an OVSE requires proof of presence, it can implement an additional assurance layer through offline face verification

1

Request Stage

App-to-App/ web-to-app sharing: After ANH initiates the verification request, the OVSE requests to the ANH's Aadhaar App through its app or web-portal

Cross-Device QR sharing: OVSE displays a QR code that the ANH scans via the Aadhaar App to share VCs

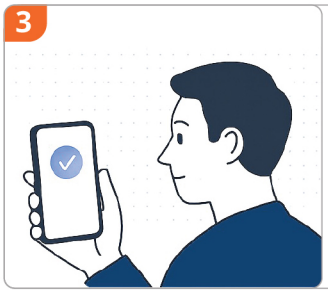
2

Face Verification Stage

If face verification is required, the Aadhaar App initiates the face capture journey

The Aadhaar App captures a live face image and performs local face match with the photograph stored in the ANH's Aadhaar App

3



Upon successful match, the Aadhaar App generates a digitally signed VC as per request

4

The Aadhaar App shares the VC with the OVSE through a callback URL specified by the OVSE

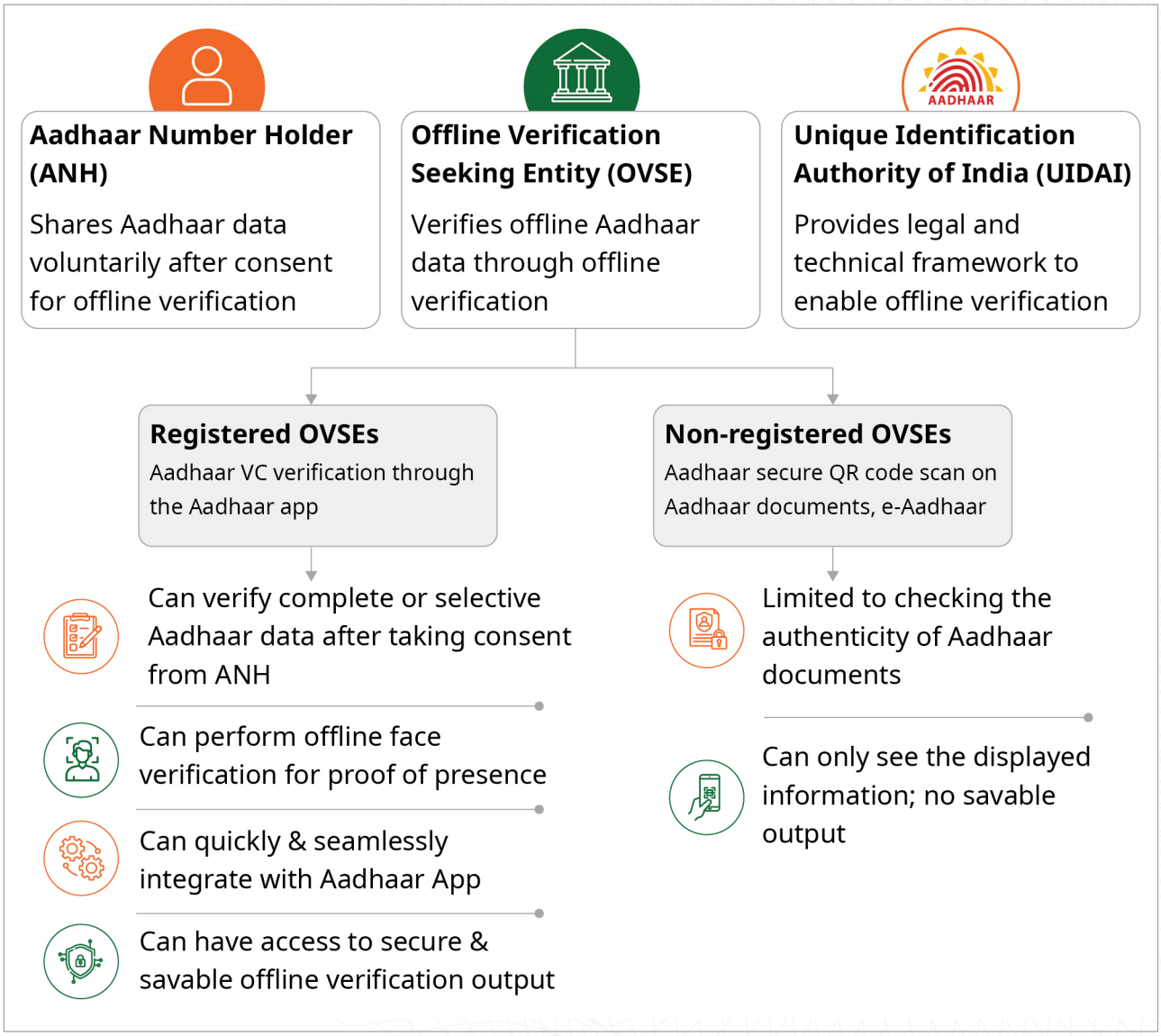
OVSE uses the UIDAI public key to verify the digital signature in the VC

4 The Aadhaar offline verification ecosystem

This chapter provides an overview of the Aadhaar offline verification ecosystem including the key stakeholders in the ecosystem and details the process of becoming an Offline Verification Seeking Entity (OVSE).

Key stakeholders in the Aadhaar offline verification ecosystem

There are three key stakeholders in the offline verification ecosystem: Aadhaar Number Holder (ANH), who needs to avail some service using Aadhaar, Offline Verification Seeking Entity (OVSE), which seeks identity verification of the ANH, and the UIDAI, which provides a platform to enable offline verification.



1) Aadhaar Number Holder (ANH)

The ANH is the primary and central stakeholder in the Aadhaar offline verification ecosystem. Aadhaar offline verification is voluntary, and an ANH can use it to establish their identity. The ANH may present Aadhaar information through an Aadhaar secure QR code, Aadhaar paperless offline e-KYC, or Aadhaar app–based verifiable credentials, depending on the type of offline verification being used.

A key feature of offline verification is informed consent. OVSE must seek the ANH's consent before any Aadhaar data is shared or verified. The ANH also retains the ability to selectively disclose information, sharing only those attributes that are necessary for the intended purpose.

2) Offline Verification Seeking Entity (OVSE)

Any organization that has a requirement to perform identity verification using ANH Aadhaar App may use Aadhaar offline verification to avail services. Such organizations, desirous of undertaking offline verification of ANH, are called offline verification seeking entities (OVSEs). OVSEs may include government departments, service providers, institutions, or other entities that require identity verification.

OVSEs play the role of verifiers in the offline verification ecosystem, verifying the integrity of Aadhaar data presented by the ANH through digital signature validation. As offline verification does not involve the transmission or storage of the Aadhaar number, OVSEs face less compliance burden.

To participate in the ecosystem, entities are required to follow UIDAI's prescribed processes and standards. As per the Aadhaar (Authentication and Offline Verification) Amendment Regulations, 2025, entities desirous to undertake Aadhaar verifiable credential verification through the Aadhaar App may register with UIDAI. Registration enables OVSEs to seamlessly integrate with the Aadhaar App, verify complete or selective Aadhaar data, perform offline face verification for proof of presence, and access digitally signed, savable, offline verification data. Notably, registration is not mandatory for entities using the Aadhaar secure QR code-based offline verification or e-Aadhaar verification, which are limited to document authenticity checks and display-based verification.

3) UIDAI

UIDAI serves as the anchor of the Aadhaar offline verification ecosystem. While UIDAI does not participate in individual offline verification transactions, it enables and governs the system by providing a platform (Aadhaar App) and by registration of entities as OVSE.

UIDAI defines the legal and regulatory framework for offline verification through the Aadhaar Act and the Aadhaar (Authentication and Offline Verification) Regulations, 2021. It also specifies the technical standards, data formats, and cryptographic mechanisms that allow offline Aadhaar data to be verified. Central to this framework is UIDAI's use of digital signatures, which enables OVSEs to confirm that Aadhaar VC shared by ANH using the Aadhaar App is genuine and has not been tampered.

Registration of entities as Offline Verification Seeking Entity (OVSE)

Entities desirous of undertaking offline verification using the Aadhaar Verifiable Credential (VC) verification through the Aadhaar App may apply to the UIDAI for registration to become OVSE. The requirements for registration is anchored in the Aadhaar (Authentication and Offline Verification) Regulations, 2021, as amended by the Aadhaar (Authentication and Offline Verification) Amendment Regulations, 2025.

Application and review process:

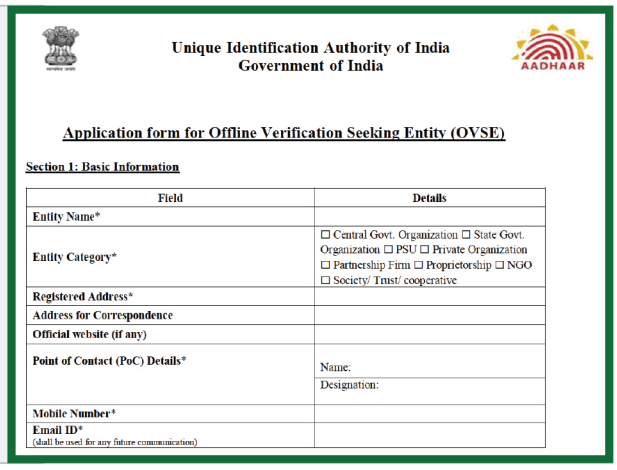
The registration process follows a structured, step-by-step workflow:

1. **Application for OVSE registration** — The entity applies to UIDAI in the prescribed form and manner. The application includes organizational details, intended use cases, and other information specified by UIDAI
2. **Verification of details by UIDAI** — UIDAI may seek additional information or clarification from the applicant entity and may independently verify the information submitted
3. **Processing and approval decision** — Based on the information provided by the entity & assessment, UIDAI may approve or reject the application. Approval is granted only where UIDAI is satisfied that the entity meets the prescribed terms and conditions which are available alongside the application form
4. **Technical integration and onboarding** — Once approved, entity is registered as OVSE with UIDAI, and further initiates technical integration with support from UIDAI in accordance with the applicable specifications and standards

A glimpse of OVSE application form

Link to the application form

For more details, reach out to ovse.support@uidai.net.in



Unique Identification Authority of India
Government of India

AADHAAR

Application form for Offline Verification Seeking Entity (OVSE)

Section 1: Basic Information

Field	Details
Entity Name*	
Entity Category*	☐ Central Govt. Organization ☐ State Govt. Organization ☐ PSU ☐ Private Organization ☐ Partnership Firm ☐ Proprietorship ☐ NGO ☐ Society/ Trust/ cooperative
Registered Address*	
Address for Correspondence	
Official website (if any)	
Point of Contact (PoC) Details*	Name: Designation:
Mobile Number*	
Email ID* (shall be used for any future communication)	

A summary of requirements for entity to apply for OVSE registration

S.No.	Parameter	Description
1	Documentation requirement	• PAN • Certificate of Incorporation / Registration, Registration number- CIN, NGO Darpan ID, etc • Company profile • Self-declaration confirming adherence to the Aadhaar Act, compliance with UIDAI regulations, lawful purpose of use, and related requirements • Technical infrastructure details: ○ Registered domain name ○ Callback/redirect URL ○ Class 3 public certificate ○ OVSE logo in SVG format (<10kb) ○ Public certificate with validity of 2 years
2	Application submission	Applications shall be submitted through the online registration portal (to be made live soon). In the interim, the filled application form, along with the required documents, may be sent to ovse.registration@uidai.net.in
3	Technology integration	OVSE to integrate based on selected pathway – cross device QR, app to app intent, web-to-app intent
4	Compliances	• Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and Regulations framed thereunder • Information Technology (IT) Act, 2000, and Digital Personal Data Protection (DPDP) Act, 2023 and rules thereunder • Local state laws, as applicable

5 Use cases of Aadhaar offline verification

This section outlines few of the potential use cases of Aadhaar offline verification across public and private sector.

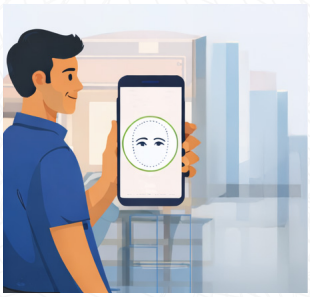
Access control

Aadhaar offline verification is well-suited for access control in environments such as data centers, educational campuses, government buildings, etc. Traditionally, such environments have relied on manual identity document inspection at entry points. Aadhaar offline verification offers a quick and secure identity verification for both institutions and visitors.

Further, wherever required, optional offline face verification can establish proof of presence, strengthening assurance without compromising privacy.

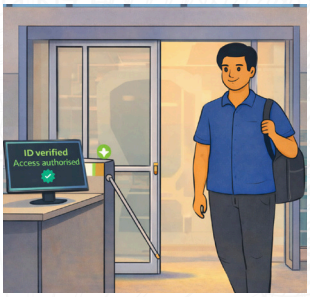
Use case: At the security gate of the official premises

Employee/visitor arrives at the office premises and scans the QR code through Aadhaar App



Employee/visitor approves the requested data and performs face verification to establish proof of presence

Aadhaar verifiable credentials shared with office security for verification



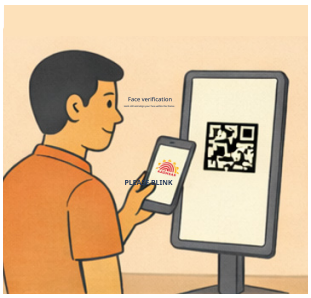
Upon successful verification, the employee/visitor enters the office premises

Residential access and community management

Aadhaar offline verification can serve as an effective mechanism to regulate entry in residential societies. It can be used to support entry management mechanisms for guests, domestic workers, and delivery executives. Traditional methods of verifying domestic workers, delivery executives largely rely on visual inspection of identity cards, making it difficult to verify the identity presented.

Use-case: Security gate at societies- only verified visitors can enter

Delivery executive reaches the society gate



Delivery executive scans the QR through Aadhaar App at the entry of the society

Security personnel can see the details shared

Delivery executive is allowed inside the building

Employee and workforce verification

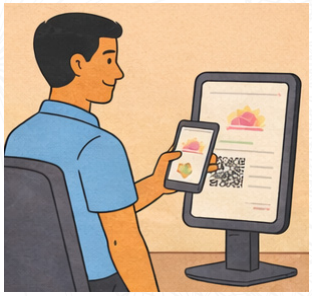
Offline verification is particularly relevant for distributed or gig-based workforce, such as:

- Cab and mobility aggregators
- Food and delivery platforms
- Facility management staff
- Contractual and temporary workers

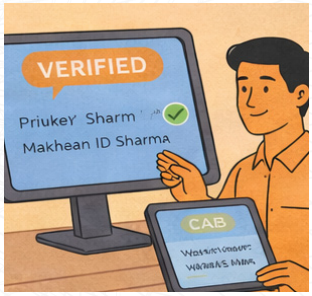
In such cases, offline verification can be used during onboarding or periodic checks to establish identity in an easy, secure, and convenient manner. This is especially useful where verification is required across multiple locations or during field operations.

Use-case: Gig worker identity verification

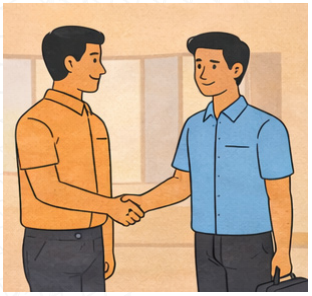
Cab company initiates driver verification during onboarding



Driver shares Aadhaar verifiable credentials through Aadhaar App



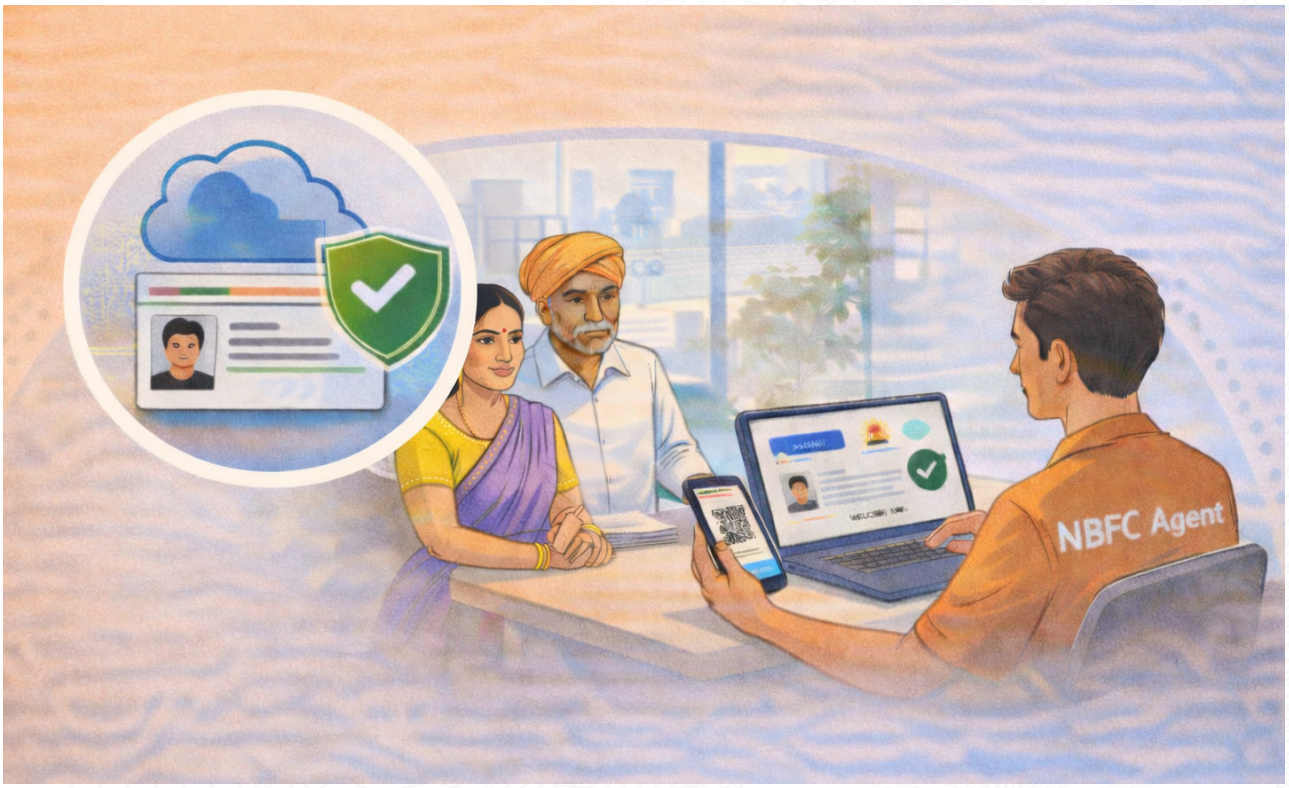
Digitally signed information verified by cab company



Driver onboarded to the company after successful verification

Non-banking financial companies (NBFCs) – customer verification

Aadhaar offline verification can be highly useful for NBFCs-MFIs in doing identity verification of customers. Traditionally, NBFCs-MFIs rely on Aadhaar as the primary KYC document and supplement it with another identity document, such as a voter ID or PAN card. They often use optical character recognition (OCR) to extract details from Aadhaar cards or other submitted documents. Aadhaar offline verification enables NBFCs-MFIs to conduct customer due diligence securely and efficiently, with assurance of data integrity backed by UIDAI's digital signature.



The use cases of Aadhaar offline verification listed above are not exhaustive, but rather indicative. Aadhaar offline verification, especially using the Aadhaar App, will open up more use cases across diverse sectors.

6 Way forward

Aadhaar offline verification using the Aadhaar App offers immense opportunities for the public and the private sector to implement innovative use cases. By enabling consent-based, locally verifiable identity checks without reliance on connection with the UIDAI's CIDR, offline verification can support scalable adoption across various sectors. The introduction of Aadhaar VCs and structured verification flows through the Aadhaar App further strengthens the potential for paperless, seamless, and ANH-controlled identity interactions.

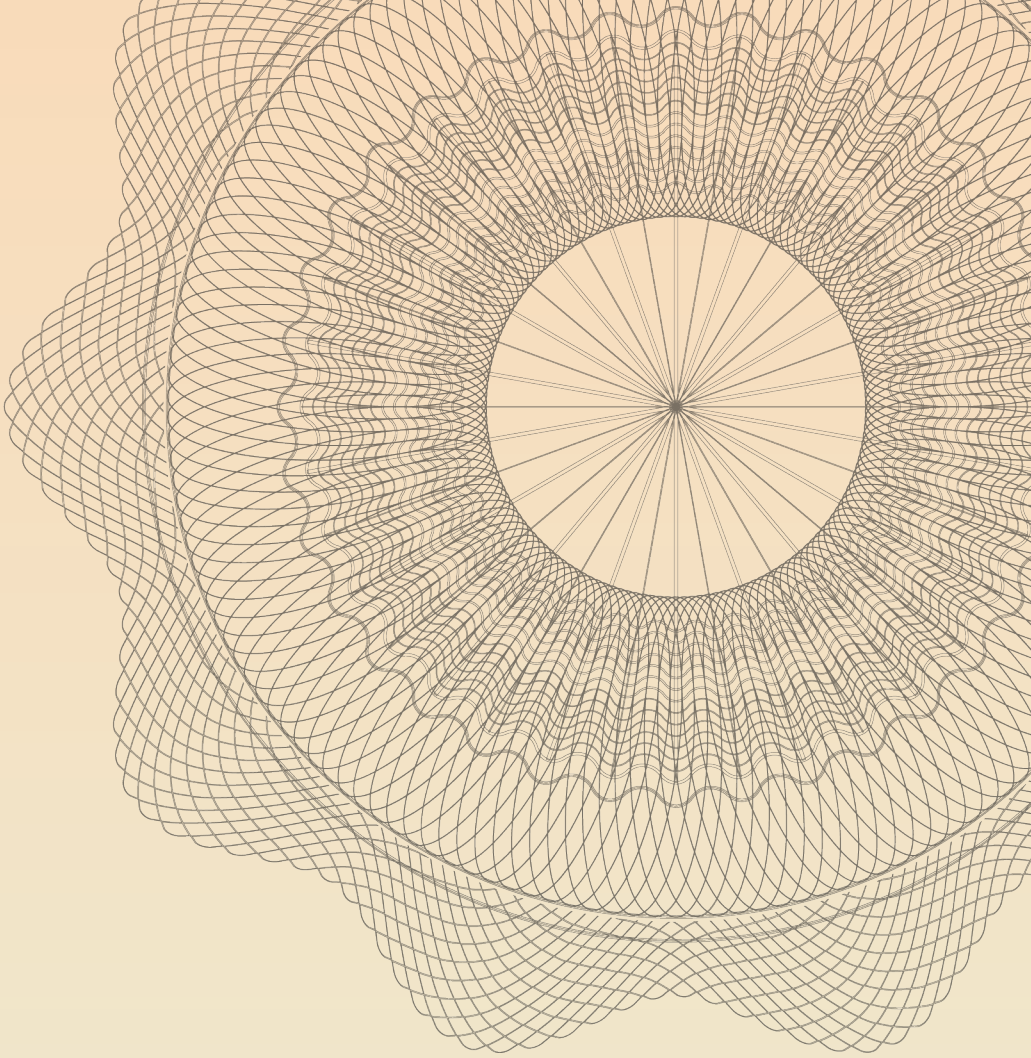
Looking ahead, the Aadhaar offline verification framework can evolve to support greater interoperability with emerging digital identity ecosystems, and, where appropriate, cross-border use cases aligned with legal and regulatory frameworks. Continued outreach, awareness-building, and capacity development among OVSEs will be critical to ensuring correct adoption and responsible use.

Acknowledgement:

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

Disclaimer:

This handbook is provided solely for informational and reference purposes. OVSEs must refer to UIDAI's T&C as updated from time to time.



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: