Ultimate Solution Provider

Easy Document Management Solutions Private Limited.

AADHAAR BASED KYC

E-KYC SOLUTIONS

What is KYC

- Know Your Customer – KYC enables banks to know/understand their customers and their financial dealings to be able to serve them better and prudently manage the risks of Money Laundering and Financing of Terrorism.

- Banks are mandated by RBI to carry out customer due diligence and KYC before onboarding a new client.

What is KYC

- It is a process by which banks obtain information about the identity and address of the customers and helps to ensure that banks' services are not misused
- Banks are also required to periodically update their customers' KYC details
- It enables banks to know / understand their customers and their financial dealings so as to be able to serve them better.
- Know your customer (KYC) policy is an important step developed globally to prevent:
  - ✓ Identity theft
  - ✓ Financial fraud
  - ✓ Money laundering and
  - ✓ Terrorist financing

When is KYC needed in Banking?

- Opening an account in a bank
- Applying for a Credit card or Loan
- Opening a subsequent account
- Opening a Locker facility
- While investing in a Mutual fund
- Financial institutes may ask for a mandatory KYC process in other instances too
- When there are not enough documents with the Bank in existing account
- When there are changes in Signatories, Beneficial owners, etc
- When the bank feels it necessary to obtain additional information from existing customers based on conduct of the account

What KYC process entails?

- Name matching against lists of known parties
- Collection and analysis of basic identity information ('Customer Identification Program' or CIP)
- Creation of an expectation of a customer's transactional behavior
- Determination of the customer's risk in terms of propensity to commit money laundering, terrorist finance or identity theft
- Monitoring of a customer's transactions against their expected behavior and recorded profile as well as that of the customer's peers

Why e-KYC?

Traditional KYC methods rely on paper based documentation received from customers, verifying the authenticity of the documents and/or conversion of the received documents into digital form for storage/ storage and warehousing of the documents in physical form.

This process is costly, inefficient, requires a lot of manual work and thus also exposing banks to risks of fraud.

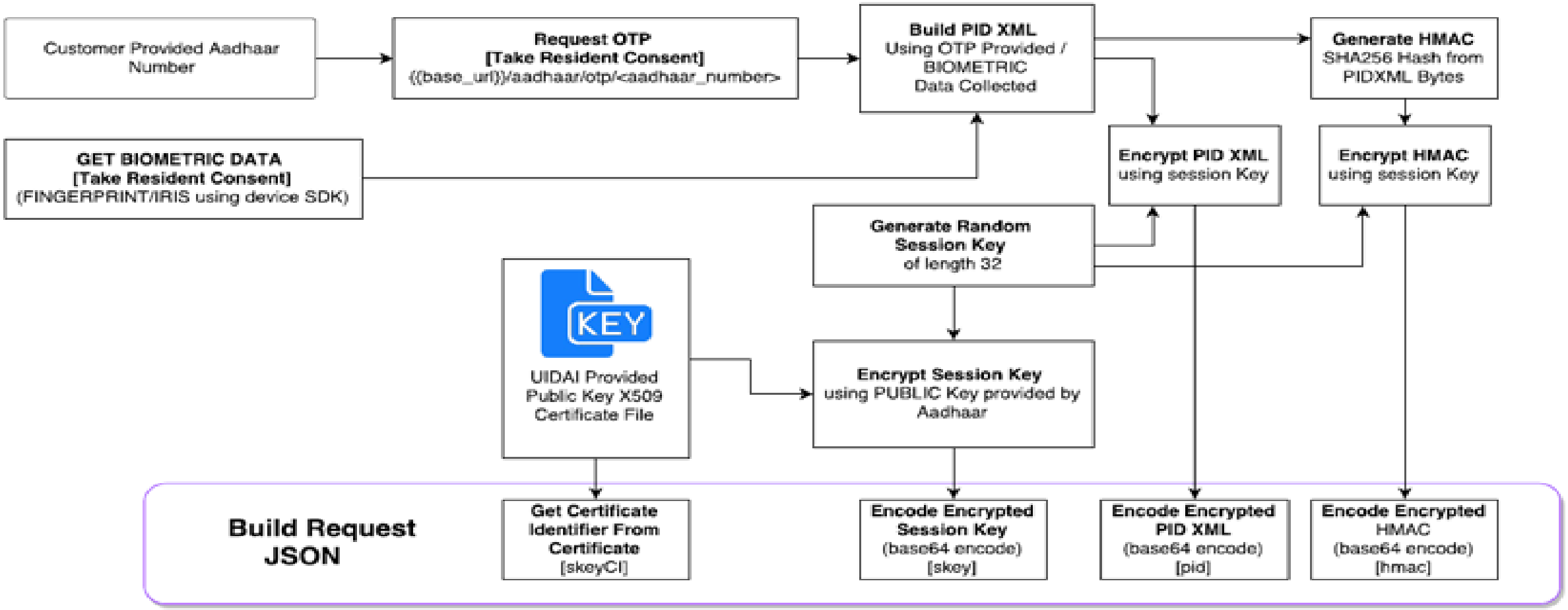
A typical KYC journey takes from couple of weeks to about a month to complete. This elongated wait leads to customer dissatisfaction, complaints/enquiries raised at helpdesk leading to additional cost and effort being spent, at times adding to poor customer experience.

Today's digitally connected world looks for experiences, frictionless journeys.

EKYC provides instant KYC based on prospect's Aadhaar card number by connecting to the UIDAI database and proving real-time authentication.

All this while, bring the cost of KYC per customer to an all-time low.

How e-KYC works?



Reference : https://aadhaarapi.com/api-reference/

How e-KYC works?

- Organizations wanting to use e KYC service will have to get approval and authorization by the UIDAI. When availing for e-KYC service, individuals have to authorize the Unique Identification Authority of India (UIDAI), by explicit consent, to release identity or address through biometric authentication to the bank.
- The UIDAI then transfers the data comprising name, age, gender, and the photograph of an individual, electronically to the bank. Information thus provided through the e-KYC process is permitted to be treated as an ‘Officially Valid Document' under PML Rules and is a valid process for KYC verification.
- Note that information will be pulled from UIDAI only with the consent of the customer. Authentication will be done through the OTP sent on the registered mobile number. UIDAI server will send OTP to customer's registered mobile.
- On submitting correct OTP and successful authentication by UIDAI server, the details will be shared. Now, banks may accept e- Aadhaar downloaded from UIDAI website as an officially valid document.

EKYC - Benefits

- **Paperless** : The service is fully electronic, enabling elimination of KYC document management Consent based Data is shared by the resident consent through Aadhaar authentication, thus protecting resident privacy.
- **Secure and compliant with the IT Act** : Data transfer are secured through the use of encryption and digital signature as per the Information Technology Act, 2000 making e-KYC document legally equivalent to paper documents.
- **Non-repudiable** : The use of resident authentication for authorization, the affixing of a digital signature by the service provider originating the e-KYC request, and the affixing of a digital signature by UIDAI when providing the e-KYC data makes the entire transaction non - repudiable by all parties involved.
- **Instantaneous** : The service is fully automated, and KYC data is furnished in real-time, without any manual intervention.
- **Regulator friendly** : The service providers can provide portal to the Ministry/Regulator for auditing all e-KYC requests. **RBI, IRDA, PFRDA & SEBI have accepted UIDAI's e KYC service as a valid KYC.**

Aadhaar Authentication - Modes

- **Address and Demographic Verification:**
  - Address verification - Address verification, which is a key requirement for providing services like telephone connection, banking products, could be done through Aadhaar- authentication. This is expected to reduce the cost of KYC & at the same time provide a reliable verification mechanism.
  - Demographic data verification - Demographic data like age and gender can be verified through Aadhaar authentication.
- **Aadhaar Authentication Offerings**
  - **Type 1 Authentication** - Through this offering, service delivery agencies can use Aadhaar Authentication system for matching **Aadhaar number and the demographic attributes** (name, address, date of birth, etc)of a resident.
  - **Type 2 Authentication** - This offering allows service delivery agencies to authenticate residents through **One-Time-Password (OTP)** delivered to resident's mobile number and/or email address present in CIDR.
  - **Type 3 Authentication** - Through this offering, service delivery agencies can authenticate residents using one of the **biometric** modalities either iris or fingerprint.
  - **Type 4 Authentication** - This is a 2-factor authentication offering with OTP as one factor and biometrics (either iris or fingerprint) as the second factor for authenticating residents.
  - **Type 5 Authentication** - This offering allows service delivery agencies to use OTP, fingerprint & iris together for authenticating residents

Technology

- **Aadhaar Number**

The Unique Identification (Aadhaar) Number, which identifies a resident, will give individuals the means to clearly establish their identity to public and private agencies across the country. Three key characteristics of Aadhaar Number are:

1. Permanency (Aadhaar number remains same during lifetime of a resident)
2. 2. Uniqueness (one resident has one ID and no two residents have same ID)
3. 3. Global (same identifier can be used across applications and domains)

Aadhaar Number is provided during the initiation process called enrolment where a resident's demographic and biometric information are collected and uniqueness of the provided data is established through a process called de-duplication. Post deduplication, an Aadhaar Number is issued and a letter is sent to resident informing the details.

Technology - Authentication Flow

- Scenario 1 in the diagram is a typical authentication flow and is a case of an operator assisted transaction at a PoS terminal: a) Resident provides Aadhaar Number, necessary demographic and biometric details to terminal devices belonging to the AUA/SA (or merchant/operator appointed by AUA/SA) to obtain a service offered by the AUA/SA. b) Aadhaar authentication enabled application software that is installed on the device packages these input parameters, encrypts, and sends it to AUA server over either a mobile/broadband network using AUA specific protocol. c) AUA server, after validation adds necessary headers (AUA specific wrapper XML with license key, transaction id, etc.), and passes the request through ASA server to UIDAI CIDR. d) Aadhaar authentication server returns a "yes/no" based on the match of the input parameters. e) Based on the response from the Aadhaar authentication server, AUA/SA conducts the transaction.
- Scenario 2 below depicts the resident conducting assisted/self-service transactions with Aadhaar authentication on his/her mobile or on the Internet. a) In this case, transaction data is captured on the mobile/Internet application provided by AUA/SA to residents b) Resident provides necessary demographic data long with OTP (fingerprint/iris is also possible although not yet common on mobiles or PCs) in addition to AUA specific attributes (account number, password, PIN, etc.) c) Step c, d, and e are same as in scenario 1 above.
- Scenario 3 : is a slight variant of 2nd scenario where AUA also plays the role of ASA and has direct connectivity to UIDAI data centers.
- Scenario 4 is how AUAs and application developers can test Aadhaar authentication using the public URL.

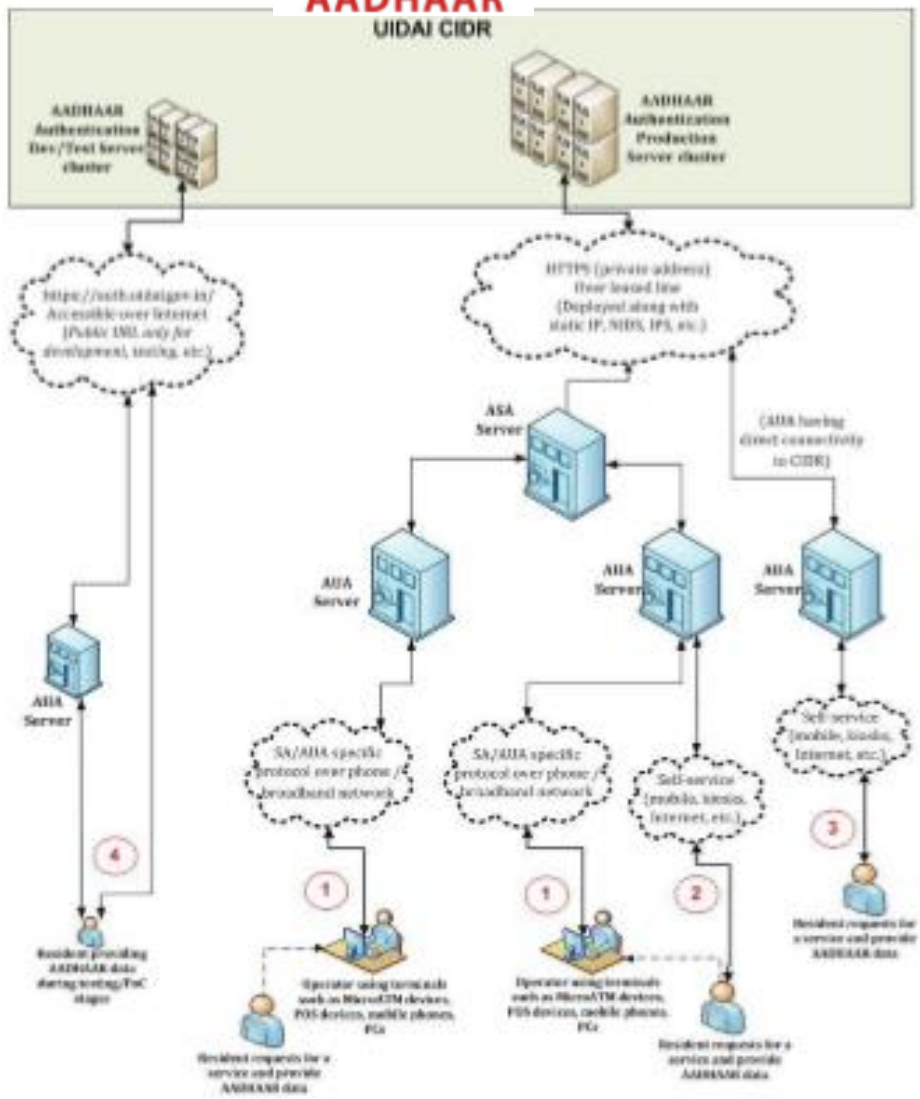


Figure 1: Aadhaar authentication flow under various scenarios

Technology - Security

- PID block data should be encrypted with a dynamic session key using **AES-256 symmetric algorithm** (AES/ECB/PKCS7Padding). Session key, in turn, is encrypted with **2048-bit UIDAI public key** using asymmetric algorithm (RSA/ECB/PKCS1Padding). Session key must not be stored anywhere except in memory and should not be reused across transactions. Only re-use of session key that is allowed is its use as seed key when using synchronized session key scheme. To increase assurance multi-factor authentication using one-time pin (OTP) could also be used in conjunction with biometrics

The encryption flow is as defined below:

1. Aadhaar Number, demographic, and biometric details as required by the application are entered into the device along with other factors such as OTP if it is used. If OTP is used, the request for OTP is sent to Aadhaar server along with Aadhaar Number (see "Aadhaar OTP Request API 1.5" specification). Aadhaar Authentication server sends the OTP back to the resident's registered mobile phone as an SMS and to the registered Email address.

2. AUA/Sub-AUA application generates a one-time session key.

3. The authentication "Data" XML block is encrypted using the one-time session key and then encoded (base 64).

4. The session key is then encrypted with the UIDAI public key.

5. AUA application on the device sends the encrypted block along with HMAC data to AUA server.

6. AUA server forms the final authentication XML input for API including license key, transaction reference ("txn" attribute), and sends the data to Aadhaar authentication server through an ASA network.

7. Aadhaar authentication server decrypts session key with the UIDAI private key. The data block is then decrypted using the session key.

How we can help?

- End to End registration with the Regulator.
- Development of the EKYC module using micro services based architecture and integrating with the existing core banking system. This ensures minimal changes will be required in the existing Banking software.
- Services being exposed as APIs will mean it will be channel agnostic and can be called from Branch banking software, Internet, Mobile or Tablet app.
- Comprehensive documentation, to ensure seamless support for internal support teams post production go live.
- We take care of end-to-end environment build and setup. We also provide Preproduction environment, which will be similar to production, and can be used for real-time debugging.

Thank You!

For More Information get in touch with us

Easy Document Management Solutions Pvt. Ltd.

Mr. Amol Ranshinge.
AVP – Sales & Services
+91 – 9167999052/9869653134.

Email Id – sales@easydocmanagement.com