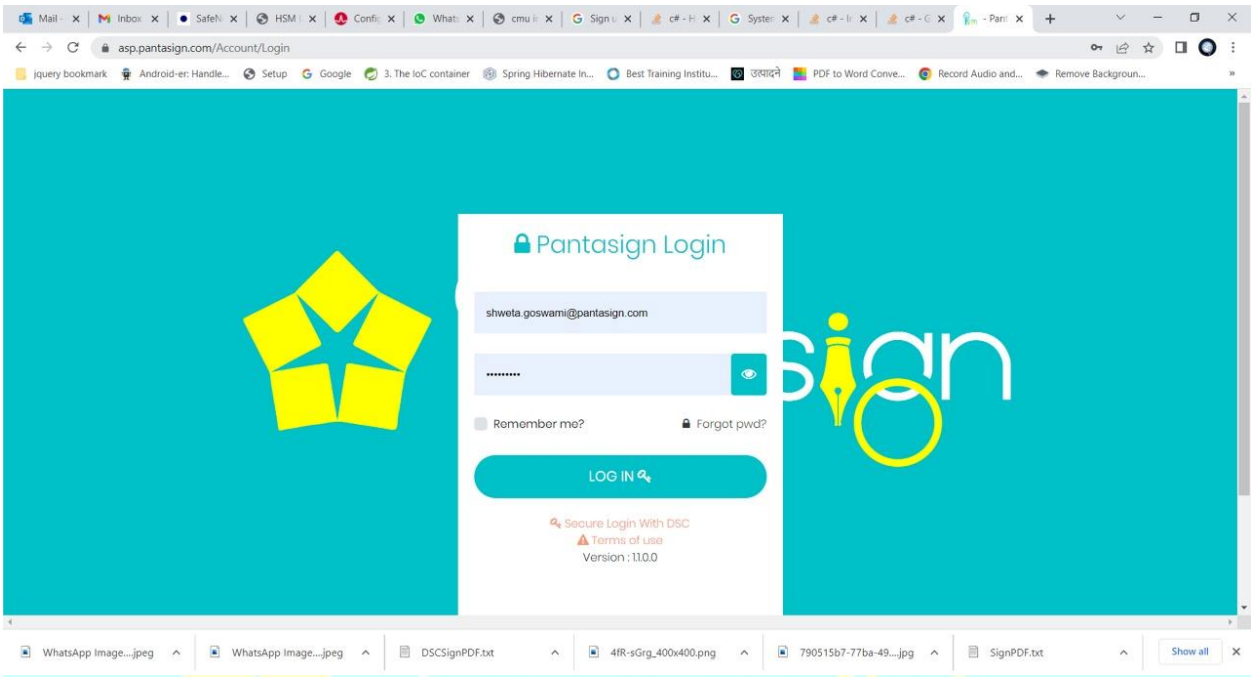
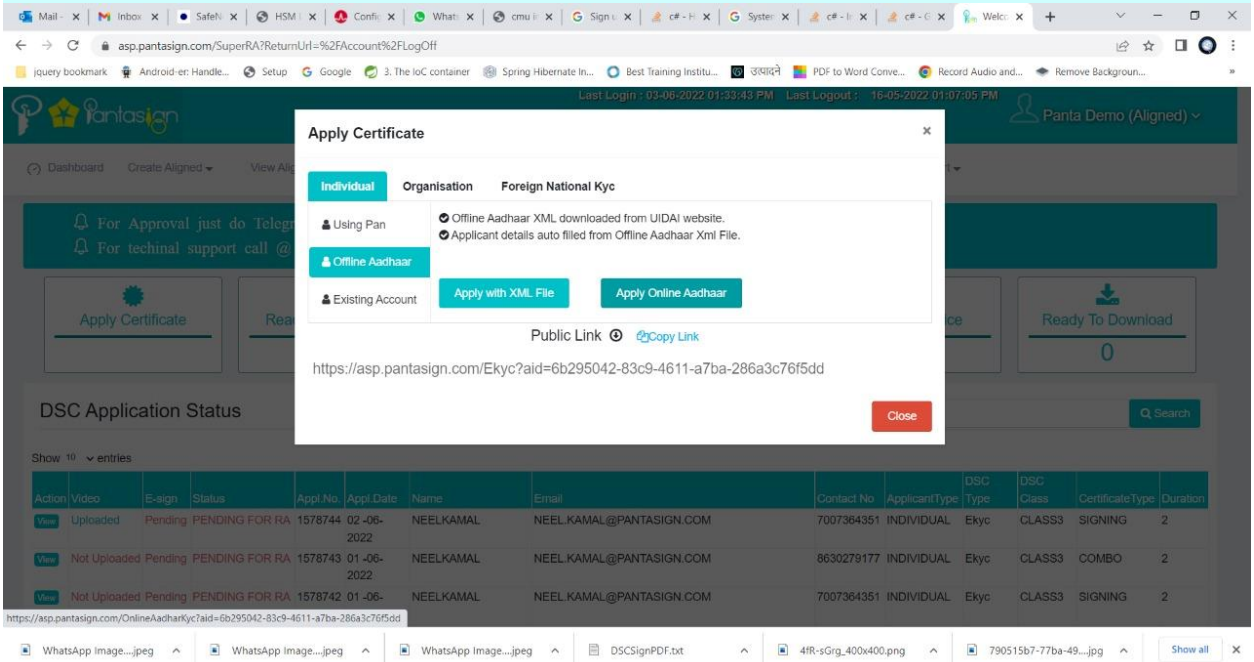
Aadhaar Operator Login

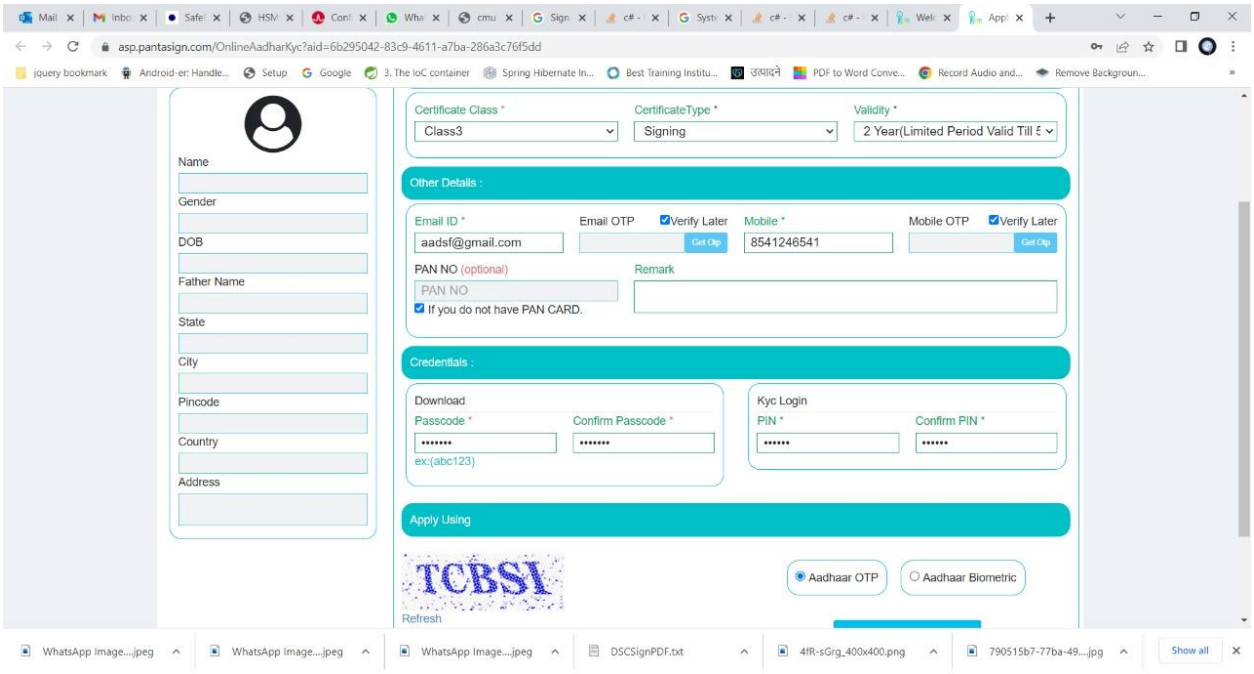
Operator login with username and password in portal.



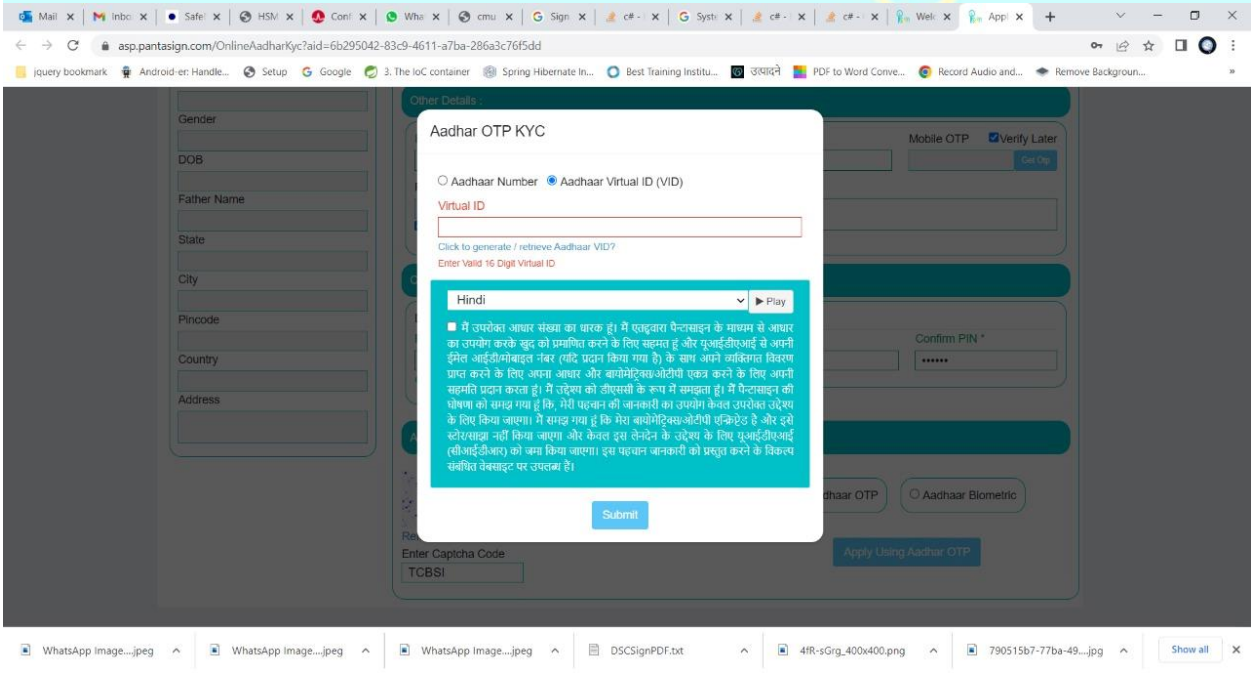
After Successful Login Operator apply DSc using Online Aadhaar Option .



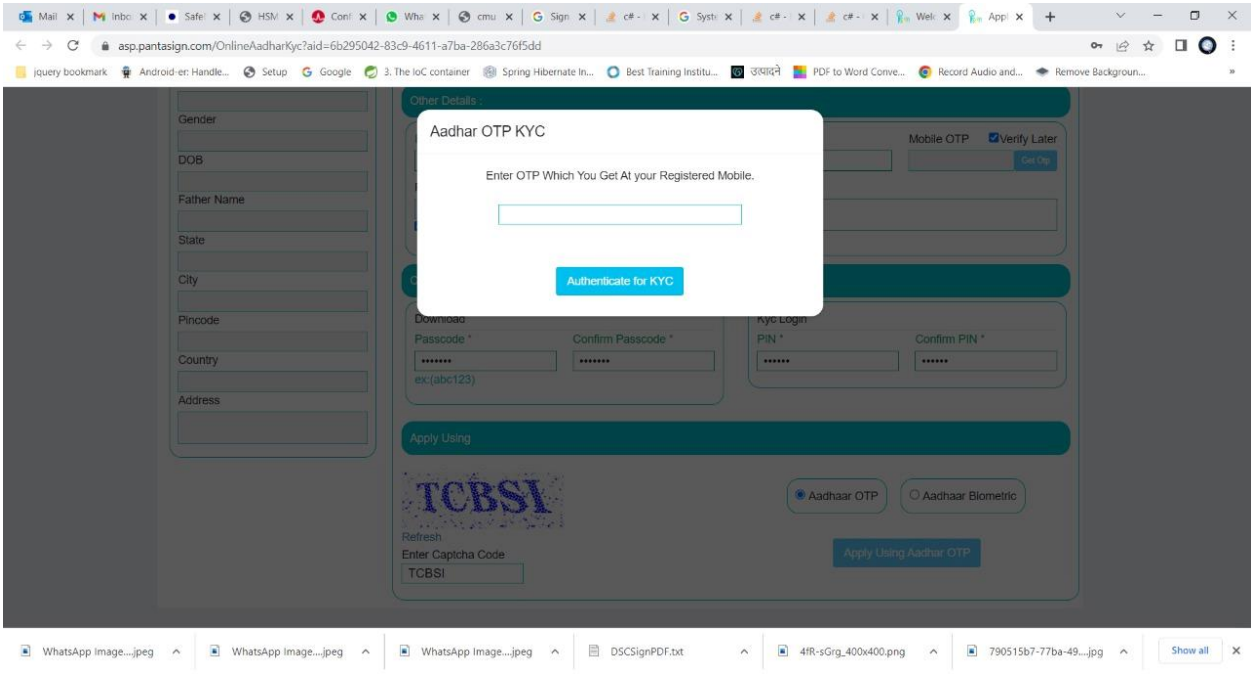
Operator Fill the Form with Required Details for Apply DSC and choose option for get User Kyc Authentication using Aadhaar OTP OR Biometric Device.



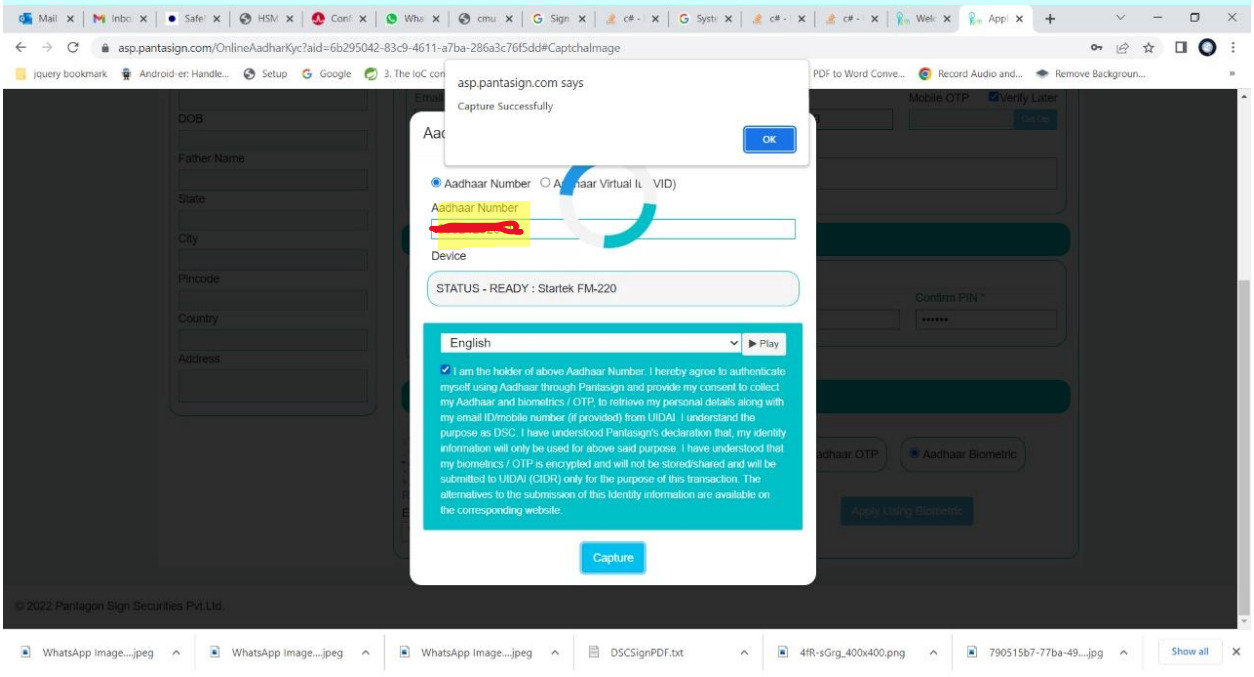
Operator enter Aadhaar No Or Virtual Id of resident and read and show the consent for resident's approval .

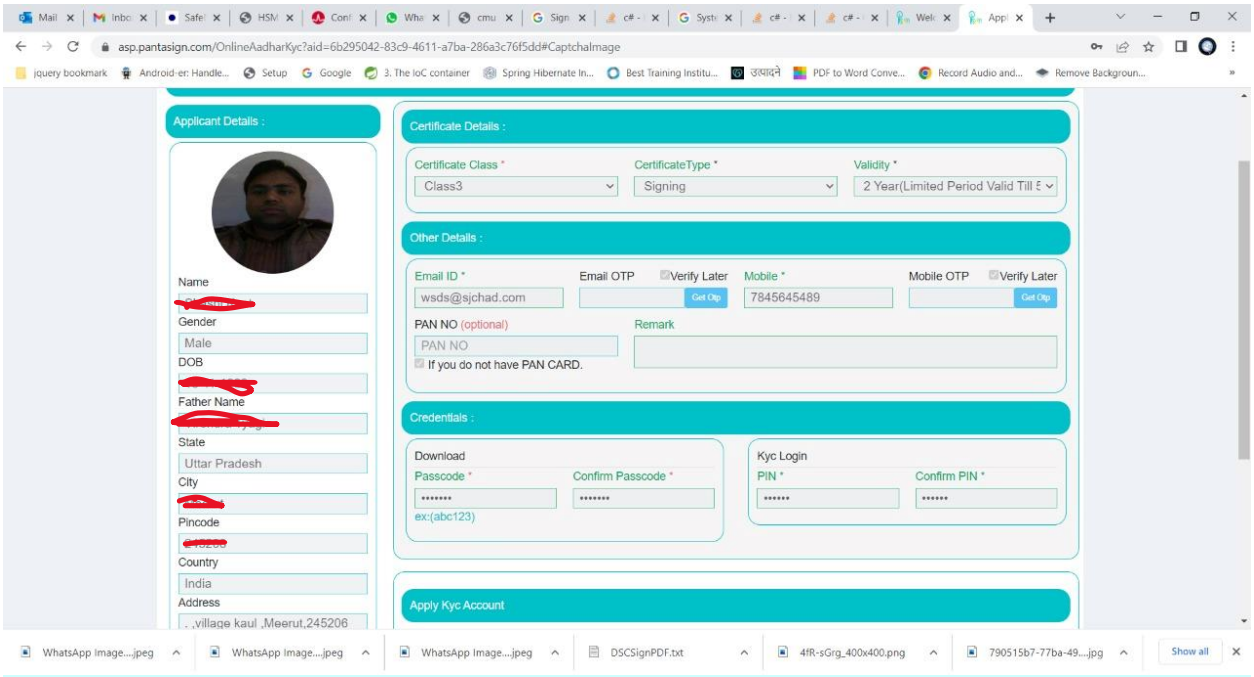


If user Select online Aadhaar OTP Option than show this Window for enter OTP which is send to Resistdent's mobile no.



If operator select Online Aadhaar Biometric option than first of you have to install rd service of any one device Star Tex FM220, ARATEK A600,Morpho, MANTRA MFS 100, registered device with STQC certification and install RD Service of the Devive.





Features of Aadhaar

What Aadhaar is	What Aadhaar is not
✓ Random 12-digit number	X Just another card
✓ Unique ID number issued to an individual shall not be re-assigned to any other individual	X One per family
✓ Enables resident's identification subject to successful Authentication	X Aadhaar will replace all other IDs
✓ Collect and record demographic and biometric information (Exception Handling for people with disability)	X Will collect profiling information such as caste, religion, language
✓ Given to resident of India, irrespective of existing documentation (Head of the Family and Introducer based Enrolment)	X Aadhaar can be used as Proof of Citizenship
✓ UIDAI enables universal identity infrastructure that any ID-based application like ration card, passport and so on can use	X An individual can obtain multiple Aadhaar numbers
✓ Aadhaar uses photograph of the face, demographic information, fingerprints and Iris to identify a resident	X Aadhaar collects financial information of residents

ABOUT AUTHENTICATION

What is Aadhaar Authentication?

Aadhaar Authentication means the process by which the Aadhaar number along with the demographic information or biometric information of a Aadhaar number holder is submitted to the Central Identities Data Repository (CIDR) for its verification and such repository verifies the correctness, or the lack thereof, on the basis of the information available with it.

Overview

The Aadhaar number or the authentication thereof shall not, by itself, confer any right of, or be proof of, citizenship or domicile in respect of an Aadhaar number holder.

Several requesting entities (or service providers) require individuals to submit their identity proofs that serve as an enabler for providing consumer services, subsidies or benefits. While collecting such identity proofs, these service providers face challenges in verifying/validating the correctness of identity information documents or proofs submitted by individuals.

The purpose of Aadhaar Authentication is to provide a digital, online identity platform so that the identity of Aadhaar number holders can be validated instantly anytime, anywhere.

UIDAI offers Aadhaar-based authentication as a service that can be availed by requesting entities (government / public and private entities/agencies). This service from UIDAI can be utilized by the requesting entities to authenticate the identity of their customers / employees / other associates (based on the match of their personal identity information) before providing them access to their consumer services / subsidies/ benefits / business functions / premises.

Modes of Authentication

- **An authentication request shall be entertained by the Authority only upon a request sent by a requesting entity electronically in accordance with these regulations and conforming to the specifications laid down by the Authority.**
- **Authentication may be carried out through the following modes:**
    - **Demographic authentication: The Aadhaar number and demographic information of the Aadhaar number holder obtained from the Aadhaar number holder is matched with the demographic information of the Aadhaar number holder in the CIDR.**
    - **One-time pin based authentication: A One Time Pin (OTP), with limited time validity, is sent to the mobile number and/ or e-mail address of the Aadhaar number holder registered with the Authority, or generated by other appropriate means. The Aadhaar number holder shall provide this OTP along with his Aadhaar number during authentication and the same shall be matched with the OTP generated by the Authority.**
    - **Biometric-based authentication: The Aadhaar number and biometric information submitted by an Aadhaar number holder are matched with the biometric information of the said Aadhaar number holder stored in the CIDR. This may be fingerprints-based or iris-based authentication or other biometric modalities based on biometric information stored in the CIDR.**

- Multi-factor authentication: A combination of two or more of the above modes may be used for authentication.

- A requesting entity may choose suitable mode(s) of authentication from the modes specified in sub-regulation (2) for a particular service or business function as per its requirement, including multiple factor of authentication for enhancing security. For the avoidance of doubt, it is clarified that e-KYC authentication shall only be carried out using OTP and/ or biometric authentication.

Obtaining Aadhaar number holder's Consent for Authentication

The Central / State Government may, for the purpose of establishing the identity of individual as a condition for receipt of subsidy, benefit or service require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment of Aadhaar.

If an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of subsidy, benefit or service.

In compliance with Aadhaar Act, all requesting entities or service providers shall

- unless otherwise provided in the Act, obtain the consent of an individual before collecting his/her identity information for the purpose of authentication in such manner as mandated by UIDAI's policy and regulations.

- ensure that the identity information of an individual is only used for submission to the CIDR for authentication.

Nothing contained in this Aadhaar Act shall prevent the use of Aadhaar number for establishing the identity of an individual for any purpose, whether by the State or anybody corporate or person, pursuant by law, for the time being in force, or any contract to this effect.

Provided that the use of Aadhaar number shall be subject to the procedure and obligations under section 8 and Chapter VI of the Act.

Authentication Services

The authentication service is provided in online and real-time manner by UIDAI through its two data centres i.e. Hebbal Data Centre (HDC) and Manesar Data Centre (MDC) where online services for authentication and other services such as e-KYC are deployed in active-active mode to ensure high availability of services.

The UIDAI's Central Identities Data Repositotry (CIDR) is currently capable of handling tens of millions of authentications on a daily basis, and can be scaled up further as demand increases. Many requesting entities that provide services to Aadhaar number holders have integrated Aadhaar into their domain applications for improved service delivery anywhere in the country in a real-time, scalable, interoperable manner.

What Aadhaar Authentication will do	What Aadhaar Authentication Will Not Do
✓ Authentication against residents data in UIDAI CIDR	X Authentication against residents data in a smart card
✓ Return response to requesting agencies as	X Return personal identity information

Yes/No	
✓ Initiate request over Mobile/Landline/Broadband network	X Remain restricted to broadband network
✓ Require Aadhaar for every Authentication request, reducing transaction to 1:1 match	X Search for Aadhaar based on details provided requiring 1:N match

Aadhar Based eKYC

Aadhaar eKYC is the electronic version of the KYC which is administered by the Unique Identification Authority Of India (UIDAI).

Like the normal KYC, the idea of eKYC too is to verify the identity of an individual except that it is done online.

eKYC involves the digital KYC authentication of individuals via demographic & biometric information stored in the UIDAI database, which is retrieved after the customer verifies their identity.

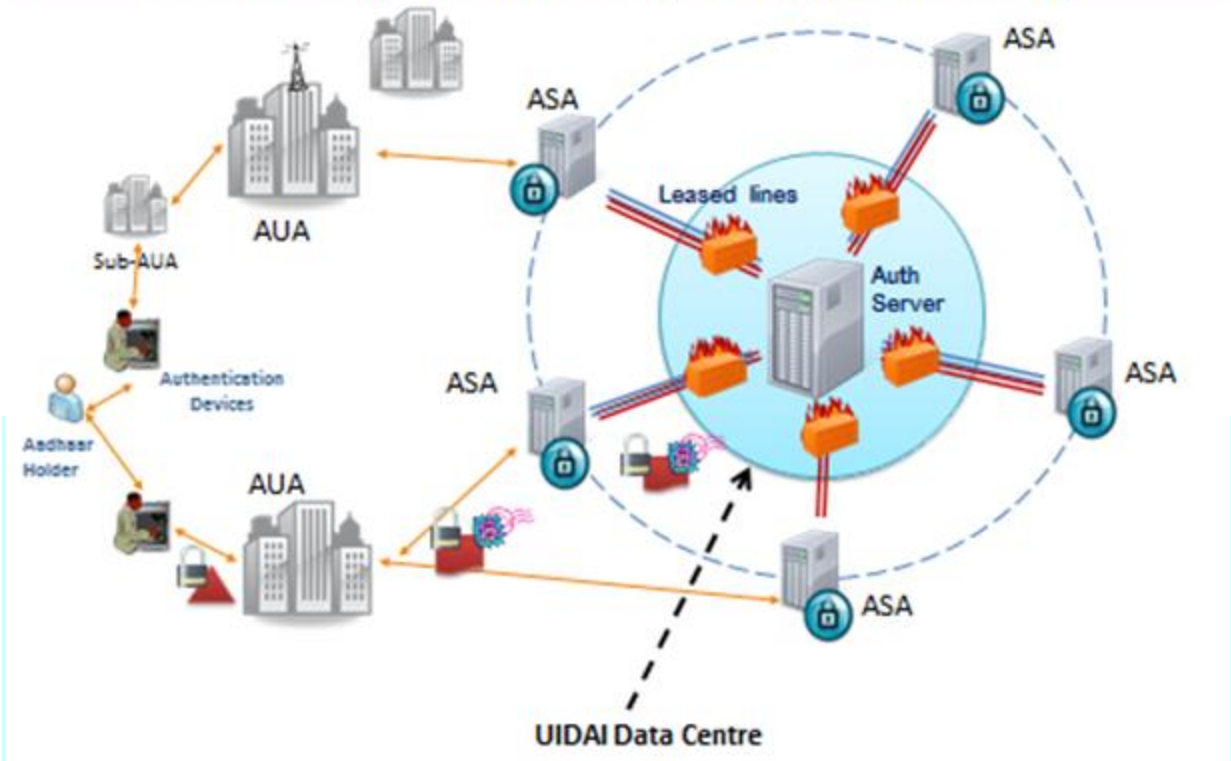
This customer identification information is collected by UIDAI during the registration process for the Aadhaar initiative.

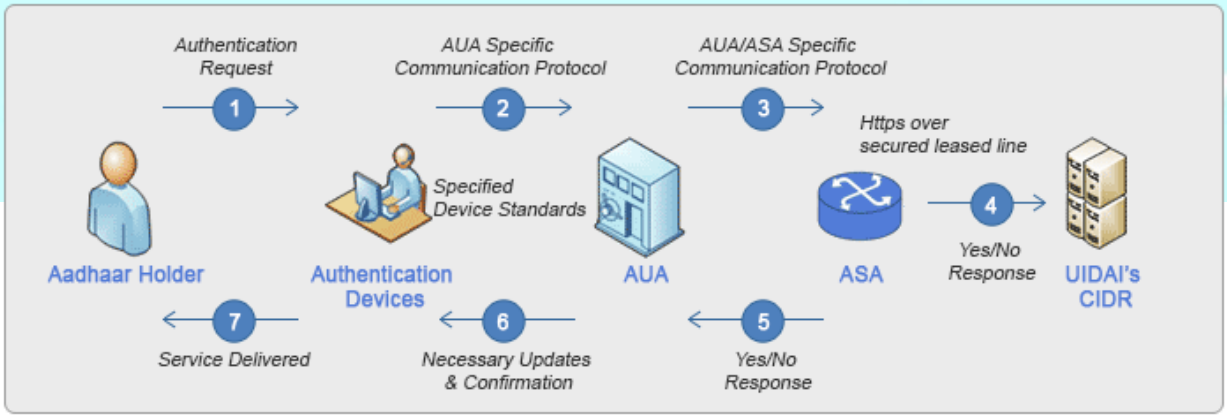
eKYC is simple to perform & completely digital. The different types of eKYC differ based on the methods used by the customer to verify his or her identity before their KYC details are retrieved from the Aadhaar database.

Online eKYC can be conducted either via OTP or biometric authentication. In these cases, an OTP is sent to the customer's Aadhaar-registered mobile number to authenticate Aadhaar, or a scanner is used to read the customer's fingerprints and retina & these readings are authenticated with the biometric information recorded for that individual in the UIDAI database.

Aadhaar Authentication Ecosystem

Authentication Ecosystem (Overview)





Introduction to UIDAI and Aadhaar

The Unique Identification Authority of India (UIDAI) is a statutory authority established under the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act 2016") on 12th July 2016 by the Government of India, under the Ministry of Electronics and Information Technology (MeitY). Prior to its establishment as a statutory authority, UIDAI was functioning as an attached office of the then Planning Commission (now NITI Aayog) vide its Gazette Notification No.-A-43011/02/2009-Admn.I) dated 28th January, 2009. Later, on 12th September 2015, the Government revised the Allocation of Business Rules to attach the UIDAI to the Department of Electronics and Information Technology (DeitY) of the then Ministry of Communications and Information Technology. UIDAI was created with the objective to issue Unique Identification numbers (UID), named as "Aadhaar", to all residents of India that is: (a) Robust enough to eliminate duplicate and fake identities, and (b) Can be verified and authenticated in an easy, cost-effective way Under the Aadhaar Act 2016, UIDAI is responsible for Aadhaar enrolment and authentication, including operation and management of all stages of Aadhaar life cycle, developing the policy, procedure and system for issuing Aadhaar numbers to individuals and perform authentication and also required to ensure the security of identity information and authentication records of individuals.

Important Definitions

Act - Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 published on 25th March 2016.

Regulations - The Aadhaar (Enrolment and Update) Regulations, 2016 published on 12th September 2016 and other amendments issued thereafter.

Central Identities Data Repository (CIDR) - A centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto.

Resident - An individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days (182) or more in the twelve months immediately preceding the date of application for Aadhaar enrolment

Demographic Information - Information relating to the name, date of birth, address and other relevant information of an individual, as specified by regulations for the purpose of issuing an Aadhaar number. Note: This information shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history

Biometric Information - Photograph, finger print, Iris scan, or such other biological attributes of an individual as specified by regulations

Aadhaar Letter - A document for conveying the Aadhaar number to a resident

Aadhaar Data Vault (ADV) means a separate secure database/vault/system where the entities mandatorily store Aadhaar numbers and any connected data such that it will be the only place where the said data will be stored. Reference: Point number (a) Circular No. 11020/205/2017 – UIDAI (Auth-I), dated 25.07.2017

Anonymization in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which an individual cannot be identified, which meets the standards of irreversibility. Reference: Section 3 (2) of the Personal Data Protection Bill 2019

Authentication means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it. Reference: Section 2(c) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

Authentication Service Agency or "ASA" shall mean an entity providing necessary infrastructure for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication using the authentication facility provided by the Authority. Reference: Regulation number 2(f) of the Aadhaar (Authentication) Regulations, 2016

Authentication User Agency or "AUA" means a requesting entity that uses the Yes/ No authentication facility provided by the Authority. Reference: Regulation number 2(g) of the Aadhaar (Authentication) Regulations, 2016

Authority means the Unique Identification Authority of India established under subsection (1) of section 11 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016. Reference: Section 2(e) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

Consent means the consent referred to in section 11 of PDP bill 2019 Reference: section 11 of PDP bill 2019 (given below)

1. **The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing.**

2. **The consent of the data principal shall not be valid, unless such consent is-**

    a. **free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;**

    b. **informed, having regard to whether the data principal has been provided with the information required under section 7;**

    c. **specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;**

    d. **clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and**

    e. **capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.**

3. In addition to the provisions contained in sub-section (2), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained-

    a. after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal;

    b. in clear terms without recourse to inference from conduct in a context; and

    c. after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing.

4. The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.

5. The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary.

6. Where the data principal withdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal.

De-identification means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal; Reference: Section 3(16) of the Personal Data Protection bill 2019

Demographic information includes information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history. Reference: Section 2(k) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

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. Reference: Regulation number 2(l) of the Aadhaar (Authentication) Regulations, 2016

Identity information in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information. Reference: Section 2(n) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

Limited KYC means the service that does not return Aadhaar number and only provides an agency specific unique UID Token along with other demographic fields that are shared with the Local AUAs depending upon its need. Reference: Point number 3 (II) and 9(b) of - Circular No. 1 of 2018, F. No. K-11020/217/2018-UIDAI (Auth-I), dated 10th January 2018

PID Block means the Personal Identity Data element which includes necessary demographic and/or biometric and/or OTP collected from the Aadhaar number holder during authentication. Reference: Regulation number 2(n) of the Aadhaar (Authentication) Regulations, 2016

Personal data means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling; Reference: Section 3(28) of the Personal Data Protection bill 2019

Personnel means all the employees, staff and other individuals employed/contracted by the requesting entities; Reference: Regulation number 2 (1) (f) of Aadhaar (Data Security) Regulations 2016

Processing in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction; Reference: Section 3(31) of the Personal Data Protection bill 2019

Reference Key means an additional key which is mapped with each Aadhaar number stored in the Aadhaar data vault. Reference: Point number (c) Circular No. 11020/205/2017 - UIDAI (Auth-I), dated 25.07.2017

Requesting Entity means an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the Central Identities Data Repository for authentication. Reference: Section 2(u) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

Sensitive personal data or information means such personal information which consists of information relating to -

- **password;**
- **financial information such as Bank account or credit card or debit card or other payment instrument details;**
- **physical, physiological and mental health condition; iv. sexual orientation;**
- **medical records and history;**
- **Biometric information;**
- **any detail relating to the above clauses as provided to body corporate for providing service; and**
- **any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise;**

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules. Reference: Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

UID Token means a 72-character alphanumeric string returned by UIDAI in response to the authentication and Limited KYC request. It will be unique for each Aadhaar number for a particular entity (AUA/Sub-AUA) and will

remain same for an Aadhaar number for all authentication requests by that particular entity. Reference: Point number 10 of in Circular No. 1 of 2018, F. No. K-11020/217/2018-UIDAI (Auth-I), dated 10th January 2018

Virtual ID (VID) means any alternative virtual identity issued as an alternative to the actual Aadhaar number of an individual that shall be generated by the Authority in such manner as may be specified by regulations. Reference: Section 3 (4) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 and Section 4 of the Aadhaar and Other Laws (Amendment) Act, 2019

Vision and Mission of UIDAI

Vision -

To empower residents of India with a unique identity and a digital platform to authenticate anytime, anywhere.

Mission –

- **Deliver Aadhaar numbers universally to residents with a well-defined turnaround time and adhering to stringent quality metrics**
- **Collaborate with partners to set up infrastructure, which provides convenience to residents for updating and authenticating their digital identity**
- **Collaborate with partners and service providers in leveraging Aadhaar to serve residents effectively, efficiently and equitably**
- **Encourage innovation and provide a platform for public and private agencies to develop Aadhaar linked applications Ensure availability, scalability and resilience of the technology infrastructure**
- **Build a long-term sustainable organisation to carry forward the vision and values of the UIDAI**
- **Make it attractive for the best global expertise in different fields to collaborate and provide valuable insights to the UIDAI organisation**

Core Values –

- **We value integrity**
- **We are committed to inclusive nation building**
- **We pursue a collaborative approach and value our partners**
- **We will strive towards excellence in services to residents and service providers**
- **We will always focus on continuous learning and quality improvements**
- **We are driven by innovation and provide a platform for our partners to innovate**
- **We believe in a transparent and open organisation**