UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India,
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

AADHAAR E-KYC SERVICE

NOVEMBER 2012

Table of Contents

Abbreviations

API	Application Programming Interface
ASA	Authentication Service Agency
AUA	Authentication User Agency
BC	Business Correspondent
CIDR	Central ID Data Repository
e-KYC	Electronic Know Your Customer
FI	Financial Inclusion
IT	Information Technology
KSA	KYC Service Agency
KUA	KYC User Agency
OTP	One Time PIN
RBI	Reserve Bank of India
STQC	Standardisation Testing and Quality Certification Directorate
UIDAI	Unique Identification Authority of India

1. Introduction

The Unique Identification Authority of India (UIDAI) has been established with the mandate of providing a Unique Identification Number (Aadhaar) to all residents of India[1]. The UIDAI has now issued Aadhaar to over 20 crore residents of India. During enrollment, the following data is collected:

1. Demographic details[2] such as the name of the resident, address, date of birth, and gender;
2. Biometric details[3] such as the fingerprints, iris scans[4], and photograph; and
3. Optional fields for communication of such as the mobile number and email address.

The UIDAI offers an authentication service that makes it possible for residents to authenticate their identity biometrically[5] through presentation of their fingerprints or non-biometrically using a One Time Password (OTP) sent to the registered mobile phone or e-mail address. Iris authentication[6] will soon be launched by the UIDAI.

Verification of the Proof of Identity (PoI) and Proof of Address (PoA) is a key requirement for access to financial products (payment products, bank accounts, insurance products, market products, etc.), purchasing SIM cards for mobile telephony, buying LPG, and access to various Central, State, and Local Government services. Today, customers provide physical PoI and PoA documents. Aadhaar is already valid KYC for banking[7], insurance[8], capital markets[9], telecom[10], LPG[11], Railways[12], and various Government services. In addition, the UIDAI now also proposes to provide an e-KYC service, through which the KYC process can be performed electronically with explicit authorization by resident. **As part of the e-KYC process, the resident authorizes UIDAI (through Aadhaar authentication using either biometric/OTP) to provide their demographic data along with their photograph (digitally signed and encrypted) to service providers**. The e-KYC service has the potential to revolutionize service delivery in the public and private sector, and drive innovation in the market.

[1] http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf
[2] http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf
[3] http://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf
[4] http://uidai.gov.in/UID_PDF/Working_Papers/UID_and_iris_paper_final.pdf
[5] http://uidai.gov.in/images/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf
[6] http://uidai.gov.in/images/iris_poc_report_14092012.pdf
[7] http://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=7367
[8] http://www.irda.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo1322&flag=1
[9] http://www.sebi.gov.in/cms/sebi_data/attachdocs/1344851126270.pdf
[10] http://www.dot.gov.in/as/2011/as_14.01.2011.pdf
[11] http://uidai.gov.in/images/FrontPageUpdates/aadhaar_news_release_28_june.pdf
[12] http://www.indianrail.gov.in/id_proof.doc

Service providers can provide a paperless KYC experience by using e-KYC and avoid the cost of repeated KYC, the cost of paper handling and storage, and the risk of forged documents. The real-time e-KYC service makes it possible for service providers to provide instant service delivery to residents, which otherwise would have taken a few days for activation based on the verification of KYC documents, digitization, etc.

1.1 Aadhaar enrolment ecosystem

The Aadhaar enrolment ecosystem[13] consists of Registrars appointed by UIDAI, who in turn appoint Enrolment Agencies, who in turn appoint certified operators. In co-ordination with the Registrars, the Enrolment Agencies set up enrolment centres, where residents can enrol for Aadhaar. Multiple fingerprint scanners, iris scanners, and cameras used for enrolment are certified[14] by STQC and UIDAI, and all connect to the UIDAI designed enrolment client through a standard Application Programming Interface (API)[15]. This makes it possible for Enrolment Agencies to use any certified equipment.

Appointment of multiple registrars, multiple enrolment agencies, and multiple technology providers has created an environment of healthy competition, which has brought about speed and kept costs under control in addition to providing choice. This ecosystem has enrolled over 20 crore residents for Aadhaar in a period of two years.

1.2 Aadhaar updation ecosystem

The UIDAI has published an updation policy[16], which lays the foundation for residents to update their data in the UIDAI database. Residents can update their data (such as residential address, mobile number, email for example) at a permanent updation centre, or through the website.

Given that the Aadhaar will become the foundation for service delivery in the public and private sector, residents will have the incentive to keep their data updated with the UIDAI at all times. Alignment of this incentive for efficient service delivery demanded by residents, with the need for accurate data by Government will ensure that the Aadhaar database becomes the authoritative database for service delivery.

[13] http://uidai.gov.in/registrar-link-2.html
[14] http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification
[15] http://uidai.gov.in/UID_PDF/Working_Papers/UID_Biometrics_Capture_API_draft.pdf
[16] http://uidai.gov.in/images/update_policy_version_2_1.zip

1.3 Aadhaar authentication ecosystem

The UIDAI has set up a scalable ecosystem for the purpose of instant authentication[17] of residents. The UIDAI has appointed a number of Authentication Service Agencies (ASAs), who in turn are appointing various Government and non-Government organizations as Authentication User Agencies (AUAs). The UIDAI, in partnership with STQC, has also laid down the technical standards for biometric devices, and certified[18] a number of them. Since the authentication service is provided online and in real-time, the UIDAI has also established two data centres where authentication and other online services such as e-KYC are deployed in active-active mode to ensure high availability.

The Aadhaar authentication ecosystem is capable of handling tens of millions of authentications on a daily basis, and can be scaled up further as demand increases. Banks and payment network operators have embedded Aadhaar authentication into microATMs[19] in order to provide branch-less banking anywhere in the country in a real-time, scalable, interoperable manner.

1.4 Aadhaar e-KYC ecosystem

A fundamental building block for service delivery is the KYC (Know Your Customer) process, which establishes the identity of the resident, their address, and other basic information such as their date of birth and gender. Typically, this KYC information is combined with other information at the point of service delivery to determine eligibility – either for an LPG connection, a scholarship, a loan, a social security pension, a mobile connection, etc.

The Aadhaar e-KYC service provides an instant, electronic, non-repudiable proof of identity and proof of address along with date of birth and gender. In addition, it also provides the resident's mobile number and email address to the service provider, which helps further streamline the process of service delivery. E-KYC may be performed at an agent location using biometric authentication, as well as remotely using an OTP on a website or mobile connection.

The Aadhaar e-KYC ecosystem has been designed to be scalable, just like the enrolment, updation, and the authentication ecosystems. It follows the same operating model as that of the Aadhaar authentication ecosystem.

The rest of this document describes the e-KYC service and ecosystem in detail.

[17] http://uidai.gov.in/auth.html
[18] http://www.stqc.gov.in/content/bio-metric-devices-testing-and-certification
[19] http://www.iba.org.in/Documents/MicroATM_Standards_v1.5_FINAL_Aug11_2012[1].pdf

2. Features of the Aadhaar e-KYC service

2.1 Salient Features of the e-KYC service

1. **Paperless**: The service is fully electronic, and document management can be eliminated.

2. **Consent based**: The KYC data can only be provided upon authorization by the resident through Aadhaar authentication, thus protecting resident privacy.

3. **Eliminates Document Forgery**: Elimination of photocopies of various documents that are currently stored in premises of various stakeholders reduces the risk of identity fraud and protects resident identity. In addition, since the e-KYC data is provided directly by UIDAI, there is no risk of forged documents.

4. **Inclusive**: The fully paperless, electronic, low-cost aspects of e-KYC make it more inclusive, enabling financial inclusion.

5. **Secure and compliant with the IT Act**: Both end-points of the 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. In addition, the use of encryption and digital signature ensures that no unauthorized parties in the middle can tamper or steal the data.

6. **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.

7. **Low cost**: Elimination of paper verification, movement, and storage reduces the cost of KYC to a fraction of what it is today.

8. **Instantaneous**: The service is fully automated, and KYC data is furnished in real-time, without any manual intervention.

9. **Machine Readable**: Digitally signed electronic KYC data provided by UIDAI is machine readable, making it possible for the service provider to directly store it as the customer record in their database for purposes of service, audit, etc. without human intervention making the process low cost and error free.

10. **Regulation friendly**: The service providers can provide a portal to the Ministry/Regulator for auditing all e-KYC requests. The Ministry/Regulator can establish rules for secure retention of e-KYC data (eg. storage method, period of storage, and retrieval among other things).

2.2 Compliance with the Information Technology Act, 2000

The data provided to the service provider is fully in compliance with the Information Technology Act (IT Act), 2000[20] as follows:

1. The e-KYC electronic record provided by UIDAI is equivalent to the Aadhaar letter (Section 4 of the IT Act, 2000);

2. A cryptographic hash of the KYC data is computed and attached with. The SHA-2 digital hash function algorithm is used. Hashing ensures that any tampering of the data in transit is detected (Section 3 of the IT Act, 2000);

3. The KYC data along with the computed hash are encrypted using a combination of AES-256 symmetric key and RSA-2048 PKI encryption form a secure electronic record. The encryption ensures that only the intended service provider can view the data provided by UIDAI (Section 14 of the IT Act, 2000); and

4. The encrypted data and hash are digitally signed by UIDAI using RSA-2048 PKI. The secure digital signature of UIDAI can be verified by the service provider to ensure the authenticity of the source (Section 15 of the IT Act, 2000).

The e-KYC service is compliant with the latest standards notified in the *Information Technology (Certifying Authorities), Amendment Rules 2011 – 25th October 2011(GSR 782(E) & GSR 783(E)-Standards (Hash & key Size), usage period of private keys, verification of Digital Signature Certificate*[21].

2.3 Deployment of the Aadhaar e-KYC service

The Aadhaar e-KYC API[22] can be used (only with the explicit authorization of the resident through biometric/OTP authentication) by an agency to obtain latest resident demographic data and photo data from UIDAI. The resident servicing agency is called the KYC User Agency (KUA). The KUA accesses the e-KYC service through a KYC Service Agency (KSA). The KSA provides connectivity to the UIDAI's Central ID Repository (CIDR).

[20] http://deity.gov.in/content/information-technology-act
[21] http://deity.gov.in/sites/upload_files/dit/files/GSR782_GSR783_08112011(1).pdf
[22] http://uidai.gov.in/images/aadhaar_kyc_api_1_0_170912.pdf

Broadly speaking, two scenarios under which the e-KYC service can be used:

1. **New customer/beneficiary**:
    a. The KUA captures resident authentication data and invokes the Aadhaar e-KYC API through a KSA network;
    b. The KYC data returned within the response of the e-KYC API is digitally signed and encrypted by UIDAI; and
    c. Using the resident data obtained through this KYC API, the agency can provision the service instantaneously.

2. **Existing customer/beneficiary**
    a. The KUA captures resident authentication data and invokes the Aadhaar e-KYC API through a KSA network;
    b. The KYC data returned within the response of the e-KYC API is digitally signed and encrypted by UIDAI;
    c. Since the resident is already a customer/beneficiary, the KUA can use a simple workflow to approve the Aadhaar linkage by comparing data retrieved through the e-KYC API against what is on record (in paper or electronic form); and
    d. Once verified, the existing customer/beneficiary record can be linked to the Aadhaar number.

The Aadhaar e-KYC API returns data along with a unique transaction code. The fact that the data is digitally signed by UIDAI and that every transaction has a unique code makes it possible to perform an electronic audit at a later point in time for any particular transaction.

The Aadhaar e-KYC service does not compromise security for inclusion, and instead offers a solution that is secure as well as inclusive and protects data privacy by eliminating paper trail on the field.

3. Aadhaar e-KYC operating model

The Aadhaar e-KYC service has been designed as a layer on top of the Aadhaar authentication service. Thus, it uses an operating model that is very similar to that of Aadhaar authentication[23].

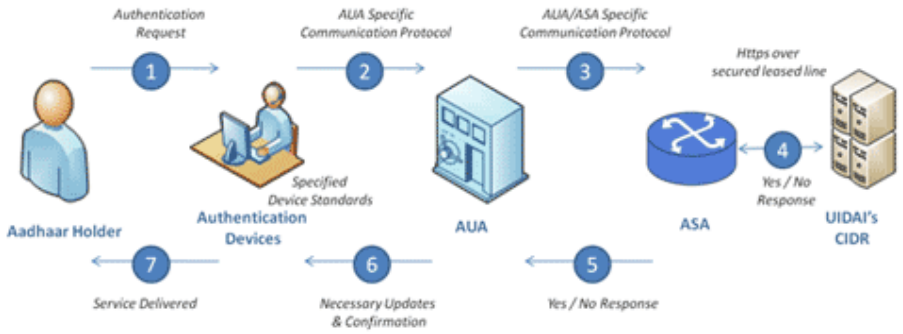
3.1 Aadhaar authentication

Aadhaar authentication is a process where the Aadhaar number, along with other attributes (demographic/biometrics/OTP) are submitted to UIDAI's Central Identities Data Repository (CIDR) for verification. The CIDR verifies whether the data submitted matches the data available in CIDR and responds with either a yes or a no.

3.2 Stakeholders

The UIDAI authentication ecosystem consists of a number of stakeholders, which also holds true for the e-KYC ecosystem:

Figure 1: The Aadhaar authentication ecosystem



1. **Unique Identification Authority of India (UIDAI):** UIDAI is the overall regulator and overseer of the Aadhaar authentication system. It owns and manages the Central Identities Data Repository (CIDR) that contains the personal identity data (PID) of all Aadhaar-holders.
2. **Authentication Service Agency (ASA):** ASAs are entities that have secure leased line connectivity with the CIDR. ASAs transmit authentication requests to CIDR on behalf of one or more AUAs. An ASA enters into a formal contract with UIDAI.

[23] http://uidai.gov.in/images/authDoc/d3_1_operating_model_v1.pdf

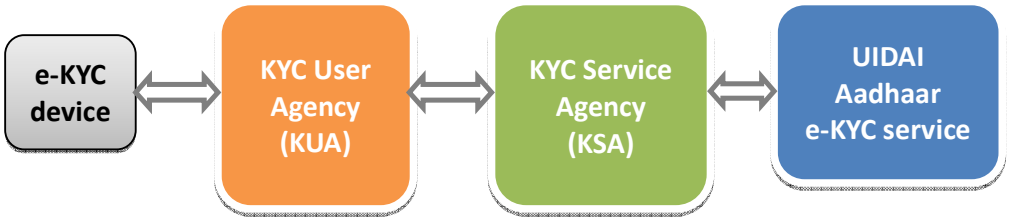
3. **Authentication User Agency (AUA):** An AUA is any entity that uses Aadhaar authentication to enable its services and connects to the CIDR through an ASA. An AUA enters into a formal contract with UIDAI.
4. **Sub AUA:** An entity desiring to use Aadhaar authentication to enable its services through an existing AUA. Examples: (i) The IT Department of a State/UT could become an AUA and other departments could become its Sub AUAs to access Aadhaar authentication services. (ii) A Hoteliers Association becomes an AUA and several hotels could access Aadhaar authentication as its Sub AUAs. UIDAI has no direct contractual relationship with Sub AUAs.
5. **Authentication Device Technology Service Provider:** These are the devices that collect PID (Personal Identity Data) from Aadhaar holders, transmit the authentication packets and receive the authentication results. Examples include PCs, kiosks, handheld devices etc. They are deployed, operated and managed directly by the AUA/Sub AUA, or through a Technology Service Provider.
6. **Aadhaar holders:** These are holders of valid Aadhaar numbers who seek to authenticate their identity towards gaining access to the services offered by the AUA.

The key stakeholders could engage with each other in multiple ways. For example, an AUA could choose to become its own ASA, an AUA could access Aadhaar authentication services through multiple ASAs for reasons such as business continuity planning, an AUA transmits authentication requests for its own service delivery needs as well as on behalf of multiple Sub AUAs, .

Similarly, it may also be possible to use a single authentication device for servicing multiple AUAs. For example, the authentication device at a fair price shop may also be used for carrying out financial transactions for banks.

3.3 e-KYC data flow

Currently, all ASAs and AUAs are approved by the UIDAI to access the e-KYC service. Hence, every ASA is also a KYC Service Agency (KSA), and every AUA is also a KYC User Agency (KUA). The following diagram depicts the relationship between various entities in the e-KYC transaction. The operating model for e-KYC is the same as that for authentication.



The data flow for an e-KYC is as follows:

1. The e-KYC front-end application captures Aadhaar number along with the biometric/OTP of resident and forms the encrypted PID block;
2. The KUA forms the e-KYC XML by encapsulating the PID block, affixes the digital signature and sends it to the KSA (the digital signature step can be delegated by the KUA to the KSA);
3. The KSA forwards the e-KYC XML (affixing the digital signature if delegated by the KUA to the KSA) to UIDAI's Aadhaar KYC service;
4. The Aadhaar KYC service authenticates the resident. If the authentication is successful, it responds back with a digitally signed and encrypted demographic and photograph in XML format;
5. The demographic data and photograph in response is encrypted by default with the KUA's encryption key. Upon the KUA's request, this may be instead encrypted with the key of the KSA; and
6. The KSA sends the response back to KUA, which interprets the result for service delivery.

3.4 Pricing of e-KYC transactions

E-KYC Services are offered free of cost as of now, till a pricing policy decision is announced.

4. Instant service delivery with e-KYC

The Aadhaar e-KYC service can help drive instant service delivery in the following ways:

1. Instant service provisioning on the basis of e-KYC in the public and private sector;
2. Enable the use of Aadhaar as a payment address; and
3. Enable combination product offerings at one location, which would have otherwise required the resident to make multiple trips to multiple locations.

4.1 Instant service provisioning

The Aadhaar e-KYC service can be used for instant service provisioning wherever KYC details are required. In some cases, the KYC requirements are regulatory, whereas in other cases, the KYC requirements are for the purpose of getting basic customer data for service provisioning.

4.1.1 Government applications

The Aadhaar e-KYC service can help speed up the realization of the goals of the Electronic Service Delivery Bill[24]. A key application of e-KYC in Government applications is the seeding of Aadhaar in the various Government Schemes for service delivery.

The Budget Speech 2012-13 (Paragraph 124)[25] identified the need for Aadhaar-based payments for MGNRES wages, old age, widow, and disability pensions, and various education scholarships. The Prime Minister has recently constituted a National Committee on Direct Cash Transfers[26] under his chairmanship and an Executive Committee on Direct Cash Transfers to give a thrust to roll out a cash transfer programme across the country, leveraging the Aadhaar platform. The Task Force on Direct Transfer of Subsidy for Kerosene, LPG, and Petroleum[27], the Task Force on an IT Strategy for PDS[28], and the Task Force on an Aadhaar-enabled Unified Payment Infrastructure[29] have given a detailed roadmap for the implementation.

The e-KYC service can be deployed for linking existing beneficiary records with Aadhaar numbers based on the process outlined in Section 2.3. Examples include linkage of existing Ration Cards, pension accounts, scholarships, etc. with Aadhaar. This has the

[24] http://deity.gov.in/sites/upload_files/dit/files/DraftEDSBill_11042011.pdf
[25] http://indiabudget.nic.in/ub2012-13/bs/bs.pdf
[26] http://pmindia.gov.in/press-details.php?nodeid=1528
[27] http://finmin.nic.in/reports/Interim_report_Task_Force_DTS.pdf
[28] http://finmin.nic.in/reports/IT_Strategy_PDS.pdf
[29] http://finmin.nic.in/reports/Report_Task_Force_Aadhaar_PaymentInfra.pdf

twin benefit of achieving de-duplication and elimination of fakes and ghosts, while ensuring that the benefits reach the targeted beneficiaries.

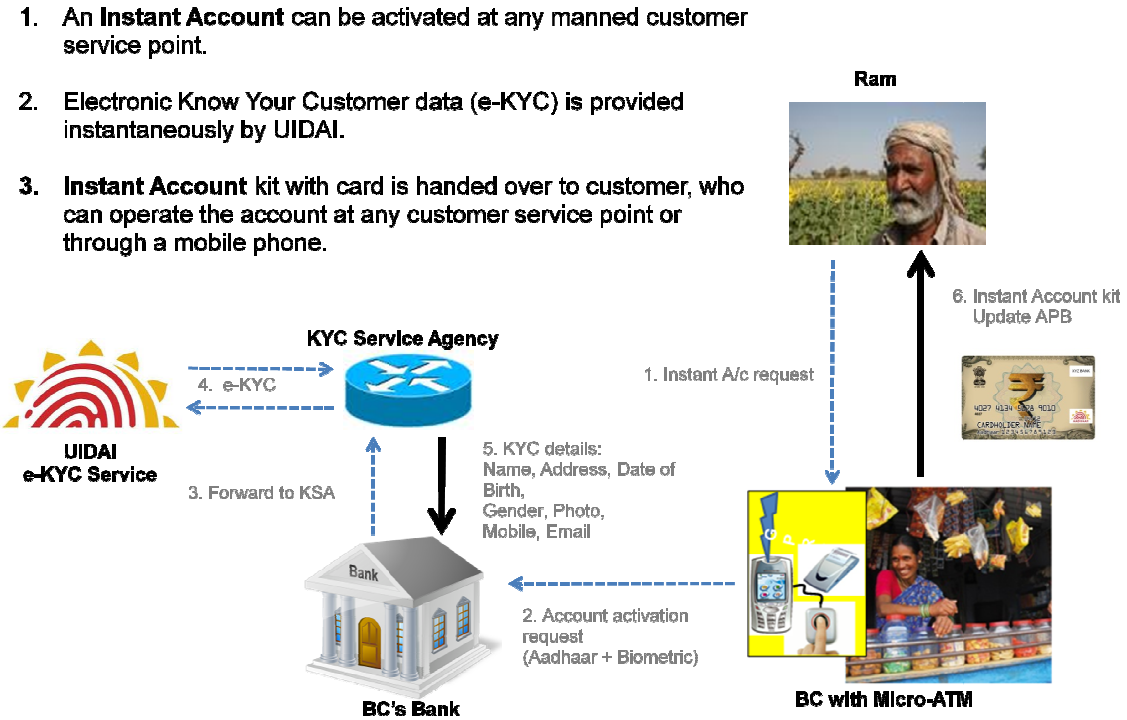
In cases where residents are applying for various Government-issued documents such as a Ration Card, Drivers' license, Caste certificate, Passport, Birth certificate, etc., the e-KYC service can be used for efficient service delivery, based on quick and accurate identification of the person.

4.1.2 Other applications

The e-KYC service can greatly reduce the KYC risk in the financial and telecom sectors.

The PMLA Rules, 2005 have been amended in 2010 vide Government of India, Gazette Notification GSR 980 (E) dated 16th December 2010. This amendment includes the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number in the list of officially valid documents. This has been followed by notifications from the sector regulators accepting Aadhaar as a valid KYC document. The Aadhaar e-KYC service is in full compliance with the provisions of the IT ct, 2000 and later amendments (Section 2.2).

Figure 2: Instant Account opening



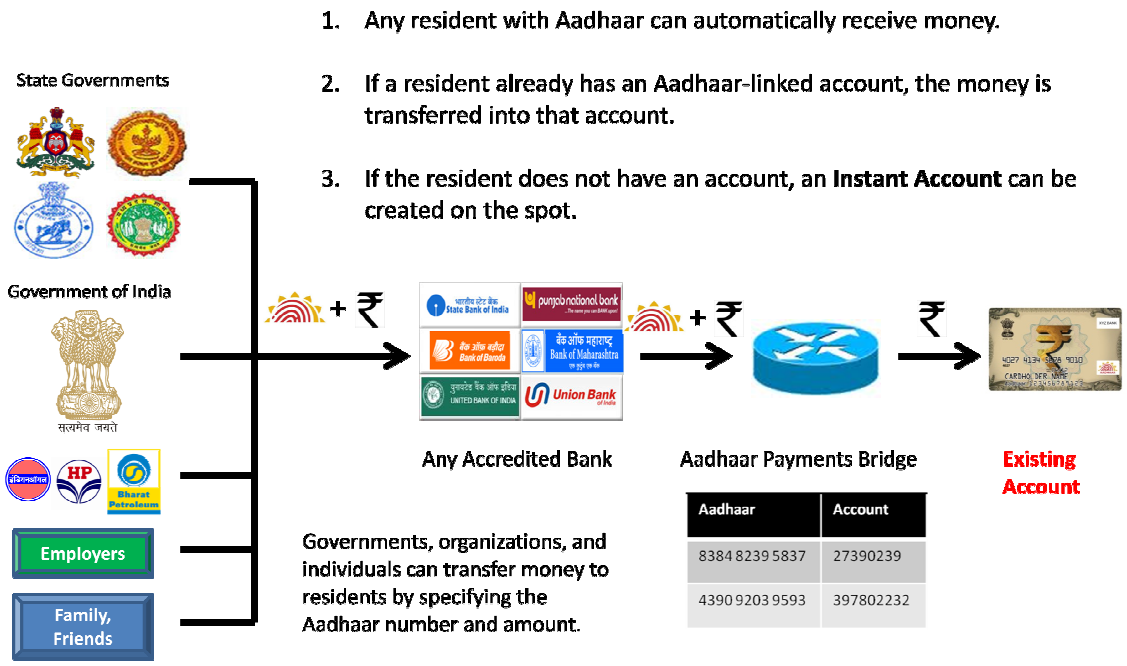
Banks can simplify the process of opening a bank account using the Aadhaar e-KYC service. Similarly, obtaining an insurance policy, purchasing capital market products such as mutual funds, and buying pension products, all can be greatly simplified through the use of the Aadhaar e-KYC service.

In the telecom industry, KYC has been an ongoing concern. The Department of Telecommunications has already notified Aadhaar as KYC for obtaining a mobile connection. A roadmap for the adoption of Aadhaar in the telecom sector is described in *Leveraging Aadhaar in the Telecom Sector*[30].

4.2 Aadhaar as a payment address

The Aadhaar number has the property of being a globally unique address for every resident of India, for life. This property makes it attractive to use Aadhaar as a payment address. The Aadhaar Payments Bridge has been recommended by the Task Force on an Aadhaar-enabled Payments Infrastructure, as a system that can route money to any resident on the basis of the Aadhaar number.

Figure 3: Aadhaar as a payment address



[30] http://uidai.gov.in/images/leveraging_aadhaar_telecom_sector_ver10_090412.pdf

With e-KYC, an Instant Account can be provided to anyone. The combination of Aadhaar as a Payment Address and e-KYC for an Instant Account can be used to create innovative products. For example, money can be sent to anyone with an Aadhaar number, irrespective of whether they have a bank account. If the receiver has an Aadhaar-enabled bank account, money can be transferred into it. If the receiver does not have an Aadhaar-enabled bank account, an Instant Account can be created on the basis of the Aadhaar number, with a debit freeze. Money transferred is credited into the Instant Account. The Instant Account can be activated during the first withdrawal on the basis of e-KYC.

5. Conclusion

The UIDAI is ready to offer the e-KYC service in a scalable, robust, and secure manner at scale. The Aadhaar e-KYC service can revolutionize service delivery in the public and private sector. It does not trade-off security for convenience and inclusion, and instead provides a solution that is secure, convenient, and inclusive.