Mapping Digital Identity Systems

India

Shared under
Creative Commons Attribution 4.0 International license

CONCEPTUALIZATION
Saumyaa Naidu and Pooja Saxena

RESEARCH
Shruti Trikanad, Yesha Tshering Paul, and Saumyaa Naidu

MAPPING
Akash Sheshadri and Saumyaa Naidu

TEXT
Saumyaa Naidu and Shruti Trikanad

REVIEWING AND EDITING
Pooja Saxena

With inputs from Amber Sinha, Divyank Katira, and Anubha Sinha

OMIDYAR NETWORK

THE CENTRE FOR internet & society

Digital Identities: Design and Uses
A project of the Centre for Internet and Society, India supported by Omidyar Network

Overview / Digital Identity System in India

This series of research maps, based on our global survey of digital identity systems, is for India. Read together with our glossary of core concepts and processes, these maps provide a coherent view of digital identity in India. They shine a light on the pervasiveness of digital identity, as well as dissect digital identity systems in a way that brings attention to the actions of key stakeholders, and to kinds of data and how they are shared. Designed as stepping stones to further research, the maps facilitate the identification of points of accountability and intervention.

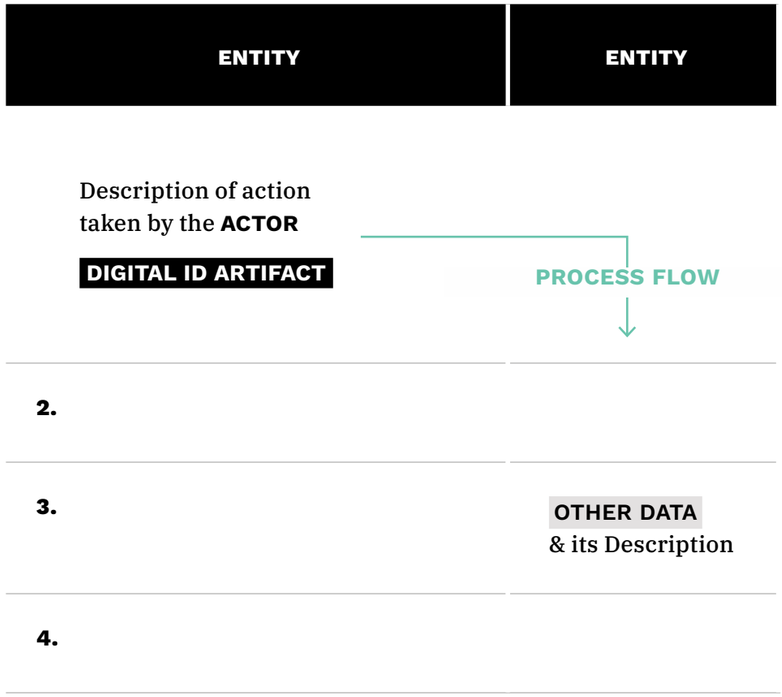
The Digital ID system in India, Aadhaar was launched in 2010, with the primary aim to improve the Public Distribution System in the country. It is managed by the Unique Identification Authority of India (UIDAI). The Digital ID system includes the Unique Identification (UID) numbers, called 'Aadhaar,' which can be assigned to all residents of India. The Aadhaar number is a random 12-digit number issued by the UIDAI after a verification process. The enrollment and authentication processes are conducted by the UIDAI. The enrolment process includes capturing demographic and biometric data from residents.

Aadhaar is currently used for identity verification in several private and public services by linking the Aadhaar numbers of residents with their mobile SIM cards, bank accounts, and a large number of welfare schemes. Other key digital services that have been planned are in the healthcare and finance sectors. While Aadhaar is envisioned to be used by state and private hospitals for registration and appointments, and for identification in other government healthcare schemes, there is also the proposed National Health Stack, which will include an identifier for beneficiaries. It is not yet confirmed if this identifier will be Aadhaar number itself or a new unique ID. In the finance sector, a set of Application Program Interfaces (APIs) for provision of financial infrastructure for governments, businesses, startups, and developers called India Stack has been created. IndiaStack currently includes the following APIs — are DigiLocker, e-KYC, e-Sign, Aadhaar Auth, and UPI.

Process Maps / Identification and Authentication

The core processes within each digital identity system are being mapped in order to evaluate the existing technological and policy decisions. These process maps bring forward the advantages and barriers in the mechanisms of identification, authentication, and authorisation. These maps follow the Swim Lane Model to capture these processes. The use of this technique helps to read the processes with clarity, and also points out the multiple possibilities at different steps.

The Swim Lane Model represents a process as a sequence of steps, and places the entities in different lanes (or columns) to show who is responsible for taking those steps. Each column shows the action taken by the respective entity. The numbered rows establish the sequence of steps. The arrows connect the end of each step to the beginning of the next one. *Refer to the key on the right to navigate the process maps.* They also indicate multiple routes that can be taken within a step. Additionally, these process maps highlight the data being collected and digital identity artifacts being used in various steps.



Identification

AADHAAR

The enrolment process is carried out by the UIDAI through registrars and enrolment agencies.
Enrolment centres are set up to collect demographic and biometric data. The biometric data captured includes photograph, fingerprint scans, and iris scans. The data is stored in a centralised database, and a unique Aadhaar number is generated upon verification of captured data. Residents can also update their data online through the UIDAI.

Sl.	RESIDENT	ENROLING AGENCY	ENROLMENT OPERATOR	REGISTRAR	UNIQUE IDENTIFICATION AUTHORITY OF INDIA (UIDAI)	CENTRAL IDENTITIES DATA REPOSITORY (CIDR)	PRINT AND LOGISTICS PARTNERS
1.	AADHAAR ENROLMENT **Resident** visits **Enrolment Centre**						
2.	Fills out the ENROLMENT FORM						
3.	Submits PROOF OF IDENTITY (POI), PROOF OF ADDRESS (POA), AND DATE OF BIRTH (DOB) documents. If unavailable, a Certificate of Identity, and Certificate of Address with photo, issued by Gazetted Officer/Tehsildar on letterhead is also accepted. IF POI AND POA ARE UNAVAILABLE OR If the **Head of family (HOF)** possesses the POI and POA, and has been enrolled through them, the resident can be enrolled. They need to provide a PROOF OF RELATIONSHIP (POR) , and SUPPORTING DOCUMENTS (NAME OF HOF, RELATIONSHIP, HOF'S AADHAAR NUMBER, ONE MODALITY OF BIOMETRIC INFORMATION OF HOF) should record the same address for the **Resident** and the **Head of Family**.	**Introducers** are available at the enrolment centre. **Introducer** verifies information filled, fills up their name and AADHAAR NUMBER , and affixes their signature or thumb impression on the enrolment form.		**Introducers** are identified and notified by the **Registrar** or regional offices of **UIDAI**.			
4.		**Enrolment Operator** captures DEMOGRAPHIC (NAME, DOB, GENDER, RESIDENTIAL ADDRESS) and BIOMETRIC DATA (FACIAL IMAGE; ALL 10 FINGERPRINTS; SCANS OF BOTH IRISES) . MOBILE NUMBER and EMAIL ADDRESS are collected at the option of the **Resident**. For **Children** below 5 years, NAME, DOB, GENDER, ENROLMENT ID OR AADHAAR NUMBER OF ANY ONE PARENT (PREFERABLY MOTHER), OR GUARDIAN, ADDRESS, FACIAL IMAGE OF THE CHILD, BIOMETRIC INFORMATION OF ANY ONE PARENT/ GUARDIAN, PROOF OF RELATIONSHIP (POR) DOCUMENT are captured. For **Residents** who are unable to provide fingerprints, only IRIS SCANS are collected.		For **Residents** who are unable to provide any biometric information, **UIDAI** shall provide for handling of such exceptions in the enrolment and update software.		
5.	**Resident** reviews details provided and asks for corrections if required.						
6.		After the information is successfully recorded, an ACKNOWLEDGEMENT SLIP is generated by the **Enrolment Operator**					
7.		The ACKNOWLEDGEMENT SLIP containing the ENROLLMENT ID and other ENROLMENT DETAILS signed by the **Enrolment Operator** is provided to the **Resident**.					
8.	**Resident** can visit the **Enrolment Centre** with the ACKNOWLEDGEMENT SLIP for correction in the enrolment data within 96 hours of enrolment.						
9.		AADHAAR GENERATION **Enrolment Agencies** upload the ENROLMENT PACKET to **CIDR (Central ID Repository)** using the upload client provided by **UIDAI**. The ENROLMENT PACKET gets encrypted after completion of enrolment in the upload client itself. (RECORDS of uploaded packets is maintained in the client software to avoid duplicate uploads)		**Registrars** also upload the ENROLMENT PACKET to **CIDR** using the upload client provided by **UIDAI**.			
10.					Each ENROLMENT PACKET is checked for validity in the **CIDR DEMILITARIZED ZONE (DMZ)** using automated process. In **CIDR**, all packets are archived.		
11.				Automated data validation is done, followed by Demographic De-duplication, manual quality checks, and biometric de-duplication. **Automated Biometric Identification System (ABIS)** includes providing the **Vendor** with ANONYMISED BIOMETRICS along with a REFERENCE NUMBER . **ABIS** searches for duplicates, if any.			
12.				IF DUPLICATE FOUND Duplicates are sent to manual adjudication module. IF DUPLICATE CONFIRMED If it is found to be a duplicate by the module, the enrolment will be rejected. IF DUPLICATE NOT FOUND If it was marked as duplicate due to an error by **ABIS**, the error is corrected by manual checking. Then the **Resident** will be assigned an AADHAAR NUMBER . IF DUPLICATE NOT FOUND AADHAAR NUMBER is allotted after the checks. It is also sent to the authentication systems.		
13.				AADHAAR NUMBER may also be communicated to **Residents** in electronic form (available for download through the **UIDAI's** website or through SMS).	After Aadhaar generation, data is shared with **Print Partner**, who prints the letter and delivers it to **Logistics Partner**. The **Logistics Partner (India Post)** delivers the physical letter (Aadhaar Letter) to the **Resident**. AADHAAR CARD and NUMBER are sent after 60-90 days after receipt of resident data packets in **CIDR**.	

Identification

UPDATING AADHAAR

Sl.	RESIDENT	ENROLING AGENCY	ENROLMENT OPERATOR	REGISTRAR	UNIQUE IDENTIFICATION AUTHORITY OF INDIA (UIDAI)	CENTRAL IDENTITIES DATA REPOSITORY (CIDR)	PRINT AND LOGISTICS PARTNERS
1.	**Resident** visits **Enrolment Centre** and places the DEMOGRAPHIC/BIOMETRIC UPDATE REQUEST OR UPDATING ADDRESS ONLINE **Resident** logs in to **UIDAI** portal using AADHAAR NUMBER and REGISTERED PHONE NUMBER. They are authenticated using OTP on their registered phone number. They select fields to be updated, enter data, submit form. UPDATE REQUEST NUMBER (URN) is generated. They select Business Process Outsourcing (BPO) for review of update, and upload the SUPPORTING POA DOCUMENTS.		**Enrolment Operator** biometrically authenticates the **Resident**, collects AADHAAR NUMBER, IDENTITY INFORMATION that is to be updated, and DOCUMENTARY EVIDENCE. **Operator** gives the **Resident** an ACKNOWLEDGEMENT RECEIPT with UPDATE REQUEST NUMBER (URN) which can be tracked.	A convenience fee may be charged by the **Registrars** to update the information.	Documents are verified against requested data by a **Verifier** at **UIDAI**'s Update back-office (at the time of placing the Update request for physical mode).		

CANCELLATION OF AADHAAR

Sl.	RESIDENT	ENROLING AGENCY	ENROLMENT OPERATOR	REGISTRAR	UNIQUE IDENTIFICATION AUTHORITY OF INDIA (UIDAI)	CENTRAL IDENTITIES DATA REPOSITORY (CIDR)	PRINT AND LOGISTICS PARTNERS
1.					If it is established that more than one Aadhaar numbers have been issued to the same person, then **AADHAAR NUMBER** from the earlier enrolment is retained, and all subsequent ones are cancelled. If the **AADHAAR NUMBER** has been generated in violation of prescribed guidelines, it is cancelled. Upon cancellation, services that are provided by **UIDAI** to the **Resident** are disabled permanently.		

DEACTIVATION OF AADHAAR

Sl.	RESIDENT	ENROLING AGENCY	ENROLMENT OPERATOR	REGISTRAR	UNIQUE IDENTIFICATION AUTHORITY OF INDIA (UIDAI)	CENTRAL IDENTITIES DATA REPOSITORY (CIDR)	PRINT AND LOGISTICS PARTNERS
1.					If the photograph, biometric and demographic data is not correctly captured, the **AADHAAR NUMBER** is deactivated. Upon deactivation, services are discontinued temporarily. **Resident** is informed of the omission or deactivation of their **AADHAAR NUMBER** along with reasons through SMS, registered e-mail ID, tele-calling, letter. Any complaint regarding omission or deactivation is addressed through the grievance redressal mechanism set up by **UIDAI**.		

Resident updates or rectifies the information

IN CASE OF A COMPLAINT

DIGILOCKER IDENTIFICATION IN INDIASTACK

DigiLocker is a platform for issuance and verification of digital documents & certificates. On creating a DigiLocker account, residents get a dedicated cloud storage space that is linked to their Aadhaar number. Organizations that are registered with DigiLocker can add digital copies of documents and certificates directly into the residents' accounts. Residents can also upload scanned documents and use e-Sign to add a digital signature to them. The identification process during signing up on DigiLocker is done through Aadhaar Number and biometrics or OTP, or directly through the website using biometrics.

Sl.	RESIDENT	DIGILOCKER WEBSITE
1.	**Resident** visits the **DigiLocker Website**, and clicks on the 'Sign Up' button.	
2.	**Resident** enters their **MOBILE NUMBER** and clicks on the 'Continue' button.	
3.		**DigiLocker Website** sends an **OTP** on the **Resident's** **MOBILE NUMBER** .
4.	**Resident** enters the **OTP** on the Website and clicks on 'Verify'.	
5.		Upon verification, **DigiLocker Website** asks to set a **USERNAME** and **PASSWORD** .
6.	**Resident** enters the **USERNAME** and **PASSWORD** .	
7.		**VERIFICATION USING AADHAAR**: **DigiLocker Website** asks for **AADHAAR NUMBER** verification through OTP or Thumbprint **VERIFICATION WITHOUT USING AADHAAR**: **DigiLocker Website** allows option to continue without Aadhaar verification.
8.	**USING OTP**: **Resident** enters their **AADHAAR NUMBER** and clicks on the 'Submit' button. **USING FINGERPRINTS**: **Resident** enters their **THUMBPRINT** using a fingerprint device. **Resident** chooses the 'continue without Aadhaar' option and directly logs into their **DigiLocker** account.	
9.		**DigiLocker Website** sends an **OTP** to the Aadhaar registered **MOBILE NUMBER** . Upon successful validation of **THUMBPRINT** , the registration process is completed.
10.	**Resident** enters the **OTP** and clicks on the 'Validate OTP' button.	
11.		Upon successful validation of **OTP** , the registration process is completed.

Identification

UPI IDENTIFICATION IN INDIASTACK

Unified Payment Interface (UPI) allows residents with bank accounts to make financial transactions using their mobile phones instantly. During the identification process, UPI requires users to create a Virtual Payment Address (VPA) and link it to any bank account. The resident then creates a UPI Pin for transactions.

Sl.	RESIDENT	PAYMENT SERVICE PROVIDER (PSP)	UNIFIED PAYMENT INTERFACE (UPI)	ISSUER BANK
1.	**Resident** visits the **PSP App**, using a mobile number registered with their bank account, and initiates the configuration process.			
2.			Sends an **ENCRYPTED SMS** automatically from the **Resident's** mobile number to the **PSP**.	
3.	Registers and logs into the **PSP App** by setting up a **PASSWORD/PATTERN/ FINGERPRINT** to access the App itself.			
4.	Selects the **Issuer Bank** and links the bank account.			
5.		Sends SMS to the registered phone number for verification.		
6.			Sends the **ACCOUNT NUMBER** + **IFSC** registered for that mobile number in a masked format to **UPI**.	
7.			Sends **ACCOUNT NUMBER** + **IFSC** to the **PSP**.	
8.		PSP stores the **ACCOUNT NUMBER** + **IFSC** in its database. This database includes information such as **MOBILE NUMBER, VIRTUAL ADDRESS, NAME OF RESIDENT ON PSP APP AND ACCOUNT NUMBER, ACCOUNT & IFSC MAPPED TO THE ADDRESS, DEVICE ID ETC.**		
9.	Selects a **UPI PIN** for making transactions.			

Authentication

AADHAAR

The UIDAI conducts the authentication process through the Authentication Service Agencies (ASAs) and Authentication User Agencies (AUAs) which have been appointed from various Government and non-Government organisations. When the resident submits their Aadhaar number and biometric data or OTP to a requesting entity, it is encrypted and sent to the Central Identities Data Repository (CIDR). On successful validation by the CIDR, a Yes/No response is sent back to the requesting entity.

Sl.	RESIDENT	REQUESTING ENTITY (RE)	AUTHENTICATION SERVICE AGENCY (ASA)	CENTRAL IDENTITIES DATA REPOSITORY (CIDR)	UNIQUE IDENTIFICATION AUTHORITY OF INDIA (UIDAI)	SERVICE PROVIDER
1.		**Requesting Entity (RE)** informs the **Resident** of nature of information that will be shared, its uses, and alternatives to submission of identity information. **RE** obtains consent of **Resident** in physical or preferrably electronic form, and maintains log of it.			**UIDAI** offers two types of authentication facilities; Yes/No authentication using OTP and/or Biometrics, and Multi-factor modes e-KYC authentication using OTP and/or biometrics	
2.	**Resident** submits **AADHAAR NUMBER** along with **BIOMETRIC AND/OR DEMOGRAPHIC INFORMATION, OR OTP**					
3.		**RE** captures **BIOMETRIC INFORMATION** of the **Resident**, and encrypts and secures it.				
4.		Client application packages and encrypts these **INPUT PARAMETERS** into Personal Identity Data (PID) block before any transmission, and sends it to the server of the **RE** using secure protocols. After validation, the **RE** server sends the **AUTHENTICATION REQUEST** to **CIDR**, through the server of the **Authentication Service Agency (ASA)**.				
5.			The **AUTHENTICATION REQUEST** is digitally signed by the **RE** and/or **ASA.**			
6.				**CIDR** validates the **INPUT PARAMETERS** with the data stored therein, and returns a digitally signed Yes/No response, or a digitally signed e-KYC response with encrypted e-KYC data along with other technical data related to authentication transaction to the **ASA.**		
7.					**Resident** is notified of the authentication through the **REGISTERED EMAIL OR MOBILE NUMBER** .	
8.					**UIDAI** stores and maintains **AUTHENTICATION TRANSACTION DATA** (authentication request data received including PID block, authentication response data sent, meta data related to the transaction, any authentication server side configurations) for 6 months. The stored transaction data is available on the **UIDAI** website for **Residents** to view. After this the data is archived for 5 years and is no longer available for viewing to **Residents**.	
9.	**Resident** can access their **AUTHENTICATION RECORDS** under specific conditions, and for payment of fees, within period of data retention (6 months). They can also access digitally signed **E-KYC DATA** through biometric or OTP authentication, upon payment of fees.					

Authentication

OFFLINE AADHAAR DATA VERIFICATION

Sl.	RESIDENT	REQUESTING ENTITY (RE)	AUTHENTICATION SERVICE AGENCY (ASA)	CENTRAL IDENTITIES DATA REPOSITORY (CIDR)	UNIQUE IDENTIFICATION AUTHORITY OF INDIA (UIDAI)	SERVICE PROVIDER
1.	**Resident** visits **UIDAI** resident portal. **Resident** enters **AADHAAR NUMBER**, **SECURITY CODE** mentioned on the portal, and asks for **OTP**. **OTP** is received on the **REGISTERED MOBILE NUMBER**. **Resident** enters **OTP** and submits it. **Resident** enters **NAME, PIN CODE,** (Postal Code as registered in Aadhaar) **SECURITY CODE** mentioned on the portal and asks for verification.					
2.					**IF VALIDATION IS SUCCESSFUL** **Resident** will be redirected to the next screen. **IF NOT** **Resident** will be redirected to the previous page with an error message asking them to check the details entered.	
3.	**Resident** selects the required details that they want to download, enters the desired **SHARE CODE** with required parameters as indicated, enters the **SECURITY CODE** and submits it. A **SHARE CODE** is a password that the **Resident** will create in this step, that can be used to open the zip file containing the data they are downloading.					
4.	A zip file containing the digitally signed XML file is downloaded to the device. **Resident** then extracts the file using the given password (**SHARE CODE**).					
5.	**Resident** shares zip file along with the **SHARE CODE** with the **Service Provider**.					
6.						**Service Provider** extracts the XML file using the **SHARE CODE**. XML file contains **NAME, DOB, GENDER, AND ADDRESS** in plain text; **ENCODED PHOTOGRAPH**; one way hashed **EMAIL ADDRESS AND MOBILE NUMBER**.
7.						**Service Provider** collects **EMAIL ADDRESS AND MOBILE NUMBER** from **Resident** and validates the hash.
8.						**Service Provider** validates the XML file using the signature and public key available on the **UIDAI** website.

Authentication

AADHAAR AUTHENTICATION IN INDIASTACK

In addition to the larger process of authentication for Aadhaar shown above, this process map shows the use of the Point-of-Sale (POS) machine, or the resident's own device during the authentication process.

Sl.	RESIDENT	APPLICATION SOFTWARE ON POS DEVICE	AUTHENTICATION USER AGENCY (AUA)	AUTHENTICATION SERVICE AGENCY (ASA)
1.	**USING POS SERVICE** **Resident** provides **AADHAAR NUMBER** or **AUA/SUB-AUA SPECIFIC IDENTIFIER, NECESSARY DEMOGRAPHIC & BIOMETRIC DETAILS** to terminal devices belonging to the **AUA/Sub-AUA** to obtain a service offered by them. **USING RESIDENT'S OWN DEVICE** **Resident** provides **NECESSARY DEMOGRAPHIC DATA ALONG WITH OTP** (Fingerprint/Iris scan is also possible, if available on the device) in addition to **AUA** specific attributes (**ACCOUNT NUMBER, PASSWORD, PIN** , etc.).			
2.		Aadhaar authentication enabled **Application Software** that is installed on the device, packages these input parameters, encrypts, and sends it to **AUA** server over a mobile/broadband network using **AUA** specific protocol.	Transaction data is captured on the mobile/Internet application provided by **AUA/Sub-AUA**.	
3.			**AUA** server, after validation, adds necessary headers (**AUA SPECIFIC WRAPPER XML WITH LICENSE KEY, SIGNATURE** , etc.), and passes the request through **ASA** server to **UIDAI CIDR**.	
4.				Aadhaar authentication server returns a "Yes"/"No" based on the match of the input parameters.
5.			Based on the response from the Aadhaar authentication server, **AUA/Sub-AUA** conducts the transaction.	

Authentication

DIGILOCKER AUTHENTICATION IN INDIASTACK

The authentication process in DigiLocker is carried out through Aadhaar Number and OTP, or through a username and password created during identification, or through Facebook ID validation.

Sl.	RESIDENT	DIGILOCKER WEBSITE
1.	**Resident** visits the **DigiLocker Website**, and clicks on the 'Sign In' button.	
2.		**DigiLocker Website** offers 3 options to login
3.		USING AADHAAR NUMBER AND OTP: **DigiLocker Website** asks for **AADHAAR NUMBER** USING USERNAME AND PASSWORD: **DigiLocker Website** asks for the **USERNAME** and **PASSWORD** created during Identification. USING FACEBOOK ID VALIDATION: **DigiLocker Website** asks to Sign In with Facebook.
4.	**Resident** enters their **AADHAAR NUMBER**. **Resident** enters the **USERNAME** and **PASSWORD** and clicks on the 'Sign In' button. **Resident** enters the **FACEBOOK ID** and **PASSWORD** and clicks on Log In.	
5.		**DigiLocker Website** sends an **OTP** to the Aadhaar registered **MOBILE NUMBER**. **DigiLocker Website** takes the **Resident** to the Dashboard. **DigiLocker Website** takes the **Resident** to the Dashboard.
6.	**Resident** enters the **OTP** and clicks on the 'Verify OTP' button.	
7.		Upon seccessful verification, **DigiLocker Website** takes the **Resident** to the Dashboard.
8.	**Resident** clicks on Uploaded Documents, and then clicks on Upload, to add documents to their DigiLocker Account.	
9.	**Resident** selects the files and clicks on the Open button.	
10.		**DigiLocker Website** shows the files on the Uploaded Documents page.

Authentication

E-KYC AUTHENTICATION IN INDIASTACK

e-KYC is a digital Know Your Customer (KYC) process, which involves the verification of the identity and address of a resident using a service through Aadhaar authentication. The authentication process in e-KYC can only be done by a KYC User Agency (KUA).

Sl.	RESIDENT	KYC USER AGENCY (KUA)	E-KYC FRONTEND APP	KYC SERVICE AGENCY (KSA)	AADHAAR E-KYC SERVICE
1.	**Resident** enters their **AADHAAR NUMBER** + **BIOMETRIC/OTP** in the **e-KYC Frontend App**.				
2.			**e-KYC Frontend App** captures **AADHAAR NUMBER** + **BIOMETRIC/OTP** of **Resident** and forms the encrypted **PID BLOCK (PERSONAL IDENTITY DATA BLOCK)** .		
3.		**KUA** sends the encrypted **PID** to **KSA**			
4.				**KSA** sends **PID** to **Aadhaar e-KYC Service**	
5.					**Aadhaar e-KYC service** authenticates the **Resident**
6.					Upon successful authentication, sends encrypted and digitally signed by UIDAI **ELECTRONIC AADHAAR LETTER** with latest demographic and photograph information to **KSA**.
7.				**KSA** sends **ELECTRONIC AADHAAR LETTER** to **KUA**	

Authentication

E-SIGN AUTHENTICATION IN INDIASTACK

The eSign service allows a resident with Aadhaar to electronically sign a form/ document. The authentication of the resident is carried out using Aadhaar e-KYC services, and the digital signature on a document is carried out on a backend server of the e-Sign provider.

Sl.	RESIDENT	REQUESTER	APPLICATION SERVICE PROVIDER (ASP)	CERTIFYING AUTHORITY (CA)
1.	**Resident** uploads document on **ASP** and clicks on e-Sign link.	**Requester** uses **ASP** for getting Digital Signature on a document.		
2.			**ASP** asks for the **BIOMETRICS/OTP** from the **Resident**.	
3.	USING BIOMETRICS: **Resident** enters their **BIOMETRICS** using a fingerprint device, and clicks on e-Sign button. USING OTP: **Resident** enters **OTP** received on registered mobile number, and clicks on e-Sign button.			
4.			**ASP** sends the **BIOMETRICS/OTP** and required document attributes to the **CA** for identity authentication.	
5.				Upon authentication, the **CA** returns a unique **DIGITAL CERTIFICATE**
6.			**ASP** embeds the unique **DIGITAL CERTIFICATE** into the original document.	
7.			**ASP** sends the document with the **E-SIGNATURE** to the **Requester.**	

Authentication

UPI AUTHENTICATION IN INDIASTACK

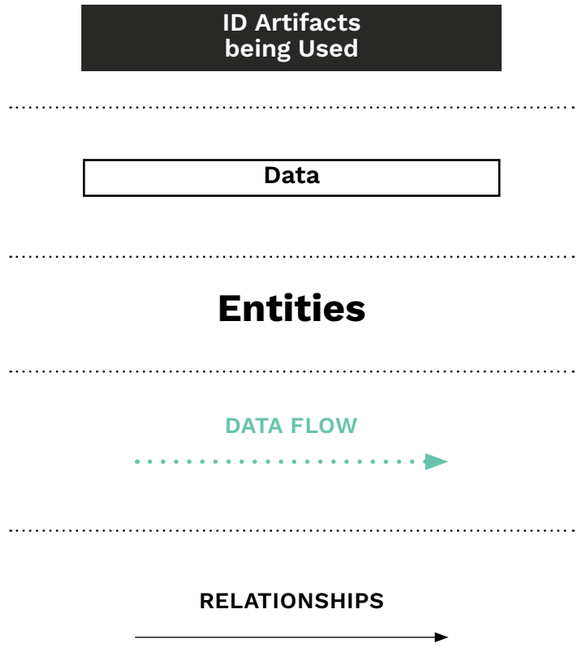
In the UPI authentication process, the login password and further the UPI Pin are validated by the issuer bank. Upon successful validation, the transaction is carried out based on the VPA provided for the receiver.

Sl.	RESIDENT	USER DEVICE	ISSUER BANK
1.	**Resident** visits the **PSP App**.		
2.	Uses **PASSWORD/PATTERN/FINGERPRINT** that was created during the identification process, to log into the app. **FINGERPRINT** can be used when that option is available on the device. The **PSPs** usually give an option.		
3.		Validates the **PASSWORD/PATTERN/FINGERPRINT** locally	
4.	Enters the **PHONE NUMBER/VIRTUAL PAYMENT ADDRESS (VPA)** of the receiver.		
5.	Enters the **UPI PIN**		
6.			Validates the **UPI PIN**

Systems Maps / Sectoral Uses

As part of the systems thinking approach, sectoral use cases have been mapped to understand how the digital identity system in the UK has been conceptualised and implemented. Studying these sectors allows a closer look at the various purposes of the digital identity, and how the residents, and state and private actors interact with it. The ERAF technique of systems mapping has been used for these maps to give a holistic view of the system and connections within it. It is an analytical tool rather than a representational tool. The ERAF model helps to place the various constituents involved in the system and divides them into entities, relationships, attributes, and flows. This technique of mapping reveals missing connections and flows in a system, and leads to the identification of specific leverage points where a small shift can produce a big impact on the system[1].

In the ERAF model, entities are the key components. These could be individuals, institutions, laws, places, etc. Relationships describe the way in which different entities are connected to each other. Attributes are characteristics that describe the entities. These could be duration, dimensions, costs, etc. The Flows show the direction of action between entities. This includes transaction of data and resources. Data and its flow within the system, and digital identity artifacts have been highlighted in these maps.

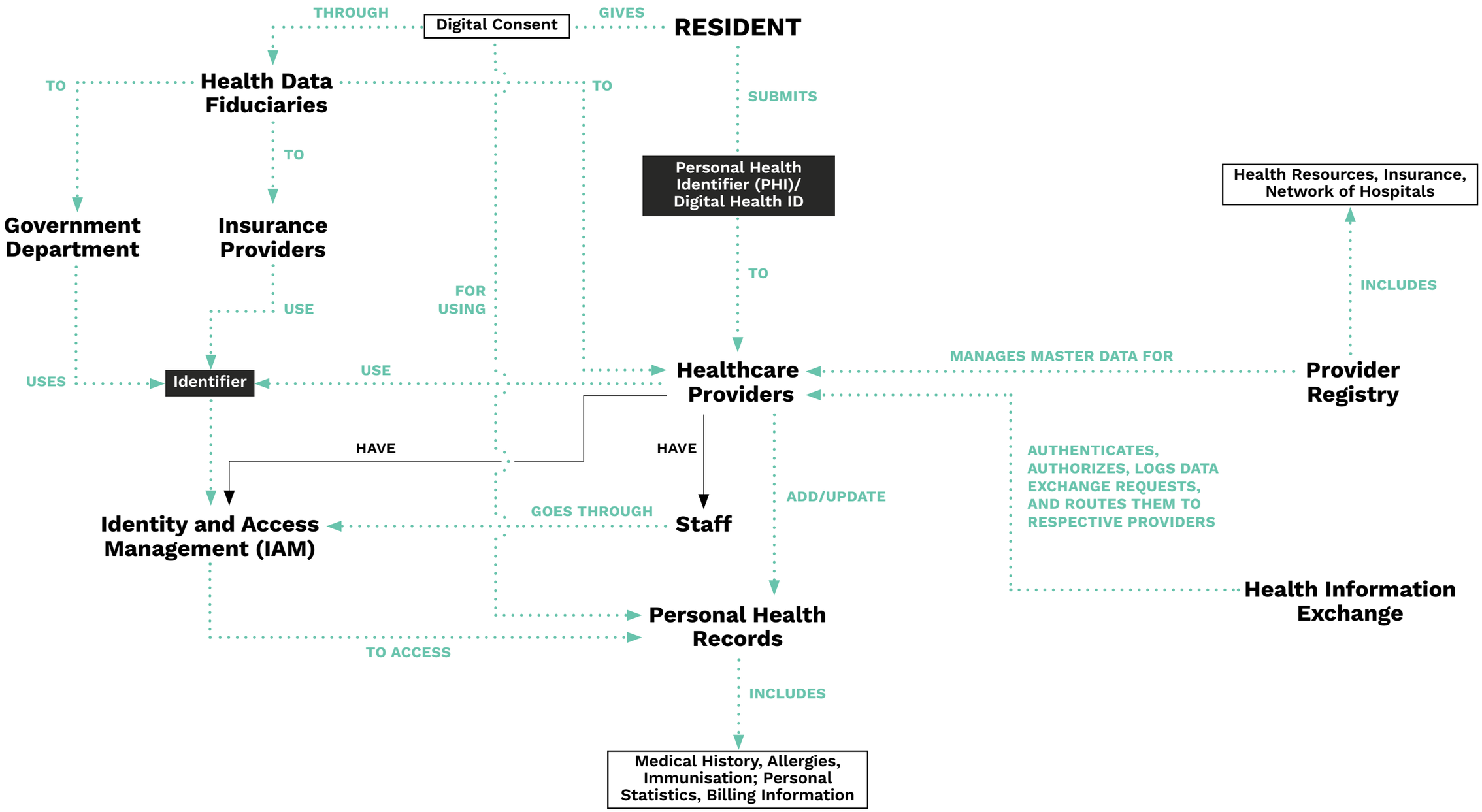


1 *http://donellameadows.org/archives/leverage-points-places-to-intervene-in-a-system/*

Healthcare

AADHAR

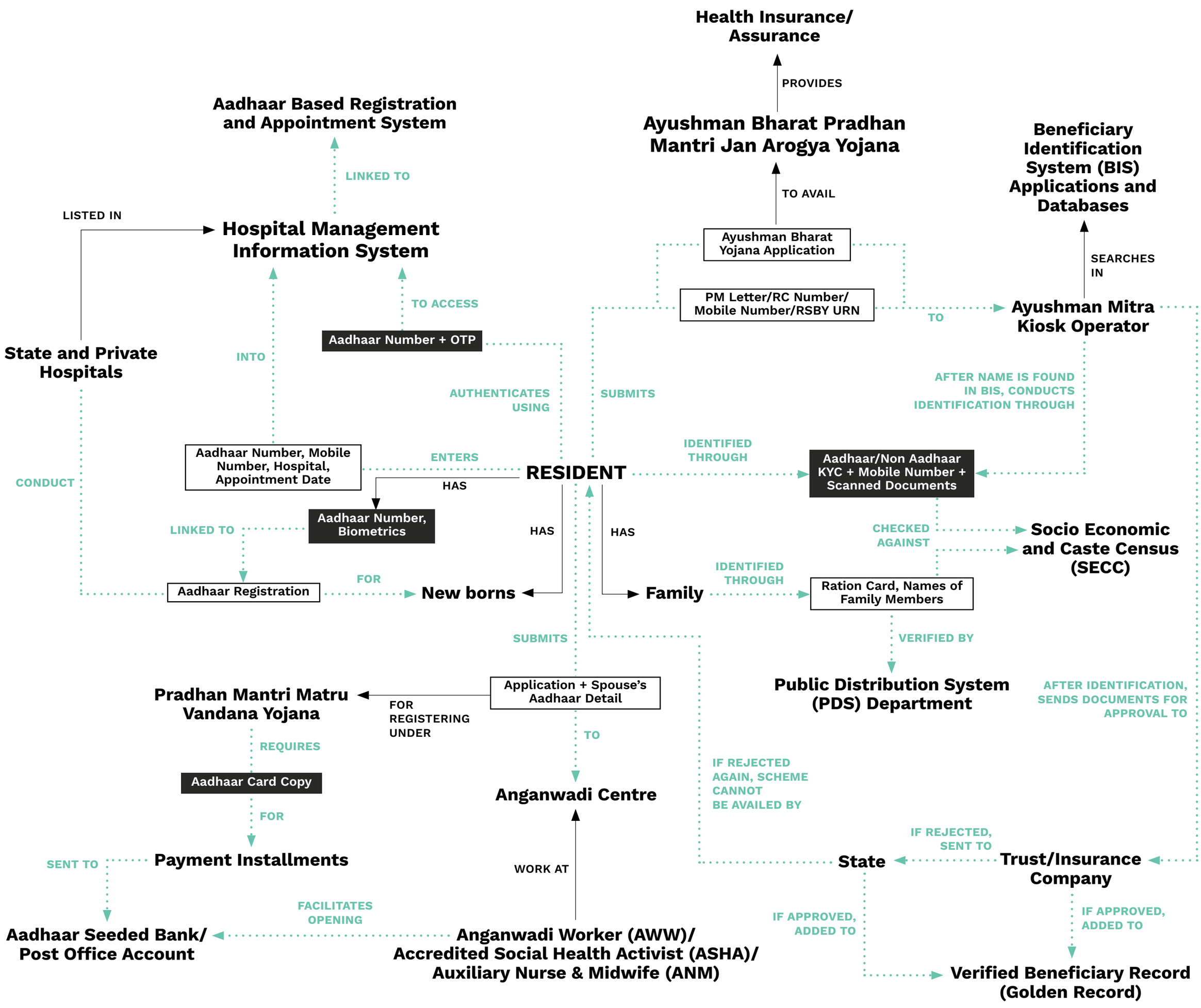
It is envisioned that the healthcare system will use Aadhaar number based registration and appointment system, for both state and private hospitals. Services and schemes such as insurance and maternal health, are also provided based on Aadhaar authentication.



Healthcare

NATIONAL HEALTH STACK

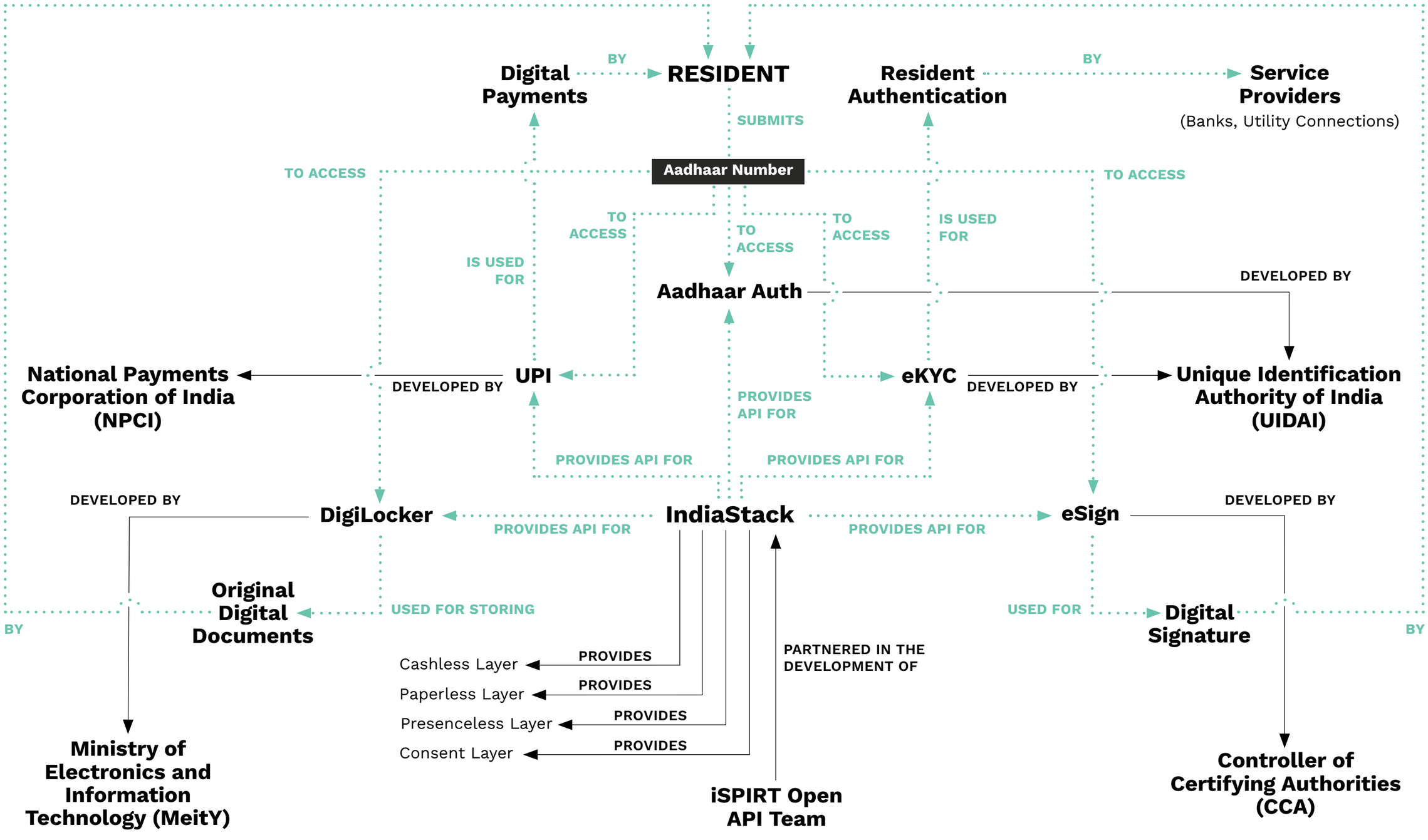
The NITI Aayog in India has proposed a blueprint for the digital health system in the country. The National Health Stack has been envisioned to be a shared digital infrastructure that will facilitate existing and future health initiatives, both private and public. It seeks to have digital personal health records and service provider records on cloud-based services. It also proposes a digital ID for all beneficiaries, an identity and access management system for healthcare staff, and a single registry of health resources and network of hospitals.



Finance

INDIASTACK

The IndiaStack is a set of digital tools on the basis of which digital infrastructure can be built by governments, businesses, and developers. This can be used to build digital services for people with the aim of a paperless, cashless, and presence-less service delivery. It also seeks to provide a consent technological layer.



Stakeholders

Unique Identification Authority of India (UIDAI)
The Unique Identification Authority of India (UIDAI) is a statutory authority that was established with the objective to issue Unique Identification numbers (UID) to all residents of India. UIDAI is responsible for Aadhaar enrolment and authentication, including operation and management of all stages of the Aadhaar life cycle, developing the policy, procedure and system for issuing Aadhaar numbers to individuals and performing authentication, and the security of identity information and authentication records of individuals.

Registrars
Registrar is an entity authorised or recognized by UIDAI for the purpose of enrolling individuals. They are primarily various state governments, central ministries, banks and public sector organizations who have signed MOUs with the UIDAI for enrolment of residents.

Enrolment Agencies
Enrolment Agencies are appointed by Registrars, and are responsible for collecting demographic and biometric information of individuals during the enrolment process by engaging certified Operators and Supervisors.

Central Identities Data Repository (CIDR)
The Central Identities Data Repository (CIDR) is a centralised database containing all Aadhaar numbers issued to residents along with the corresponding demographic, biometric and other information of the Aadhaar Number holders.

Requesting Entities, or Authentication User Agencies (AUAs)
Authentication User Agency is an entity that provides Aadhaar Enabled Services to a resident with an Aadhaar number, using authentication as facilitated by the Authentication Service Agency (ASA). An AUA may be a government, public or private legal agency registered in India, that sends authentication requests to enable its services or business functions.

Authentication Service Agencies (ASAs)
Authentication Service Agencies have secured connectivity with the CIDR, which are compliant with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to requesting entities (such as AUAs/KUAs) and transmit their authentication requests to CIDR.

KYC User Agencies (KUAs)
KYC User Agencies (KUAs) are requesting entities, which are eligible for Aadhaar e-KYC authentication of a resident with an Aadhaar number, from KSAs.

KYC Service Agencies (KSAs)
KYC Service Agencies (KSAs) are ASAs that are eligible to provide access to the e-KYC service through their network.

NITI Aayog
The NITI (National Institution for Transforming India) Aayog is a policy think tank of the Government of India which designs strategic and long term policies and programmes for the Government of India. It also provides relevant technical advice to the Centre and States.

Pradhan Mantri Matru Vandana Yojana
Pradhan Mantri Matru Vandana Yojana is a maternity benefit program run by the government of India, and implemented by the Ministry of Women and Child Development. It is a conditional cash transfer scheme for pregnant and lactating women of 19 years of age or above for the first live birth. It also provides a partial wage compensation to women for wage-loss during childbirth and childcare and to provide conditions for safe delivery and good nutrition and feeding practices.

Anganwadi Centre
An Anganwadi centre provides basic health care in a village as part of the Indian public health care system. The basic health care activities at a centre include contraceptive counseling and supply, nutrition education and supplementation, as well as pre-school activities.

Anganwadi Worker (AWW)
Workers at the Anganwadi centre are responsible for showing community support and actively participating in executing this program.

Accredited Social Health Activist (ASHA)
An accredited social health activist is a trained female community health worker instituted by the government of India's Ministry of Health and Family Welfare as a part of the National Rural Health Mission.

Auxiliary Nurse & Midwife (ANM)
Auxiliary nurse midwife is a village-level female health worker in India who is known as the first contact person between the community and the health services.

Public Distribution System (PDS) Department
The Public Distribution System (PDS) in the country facilitates the supply of food grains and distribution of essential commodities to a large number of poor people through a network of Fair Price Shops at a subsidized price on a recurring basis.

Socio Economic and Caste Census (SECC)
Socio Economic and Caste Census (SECC) is a study of socio economic status of rural and urban households that allows ranking of households based on predefined parameters.

Ayushman Bharat Yojana
Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (AB PM-JAY) is a flagship scheme of the Indian government's National Health Policy which aims to provide free health coverage at the secondary and tertiary level to its bottom 40% poor and vulnerable population.

Ayushman Mitra Kiosk Operator
A Pradhan Mantri Arogya Mitra is a certified frontline health service professional who is to be present at each of the Empanelled Health Care Providers (EHCP) and serve as a first contact point for beneficiaries.

iSPIRT
Indian Software Products Industry Round Table (iSPIRT), is a think tank for the Indian software products industry.

Controller of Certifying Authorities (CCA)
The Controller of Certifying Authorities (CCA) provides the required legal sanctity to digital signatures based on asymmetric cryptosystems. CCAs license and regulate the working of Certifying Authorities.

Certifying Authority (CA)
Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users.

Ministry of Electronics and Information Technology (MeitY)
The Ministry of Electronics and Information Technology (MeitY) is a standalone ministerial agency responsible for IT policy, strategy and development of the electronics industry.

National Payments Corporation of India (NPCI)
National Payments Corporation of India (NPCI) is an umbrella organisation for operating retail payments and settlement systems in India. It is an initiative of Reserve Bank of India (RBI) and Indian Banks' Association (IBA) for creating a robust Payment & Settlement Infrastructure in India.

Bibliography

Identification

1. UIDAI, "The UIDAI Ecosystem," Unique Identification Authority of India, last accessed May 29, 2020, *https://uidai.gov.in/ecosystem/uidai-ecosystem.html*.
2. UIDAI, "About Your Aadhaar," Unique Identification Authority of India, last accessed June 9, 2020, *https://uidai.gov.in/my-aadhaar/about-your-aadhaar/aadhaar-enrolment.html*
3. UIDAI, "Aadhaar (Enrolment And Update) Regulations, 2016," Unique Identification Authority of India, September, 2016: 26, *https://uidai.gov.in/images/regulation_1_to_5_15092016.pdf*
4. UIDAI, "Regulations," Unique Identification Authority of India, last accessed June 9, 2020, *https://uidai.gov.in/about-uidai/legal-framework/regulations.html*
5. Vidushi Marda, "Data Flow in the Unique Identification Scheme of India," The Centre for Internet and Society, September 3, 2015, last accessed June 9, 2020 *https://cis-india.org/internet-governance/blog/data-flow-in-unique-identification-scheme-of-india*

Authentication

1. UIDAI, "Operation Model," Unique Identification Authority of India, last accessed May 29, 2020, *https://uidai.gov.in/ecosystem/authentication-ecosystem/operation-model.html*.
2. UIDAI, "Aadhaar (Authentication) Regulations, 2016," Unique Identification Authority of India, September, 2016: 54, *https://uidai.gov.in/images/regulation_1_to_5_15092016.pdf*
3. UIDAI, "Aadhaar (Data Security) Regulations, 2016," Unique Identification Authority of India, September, 2016: 70, *https://uidai.gov.in/images/regulation_1_to_5_15092016.pdf*
4. UIDAI, "Regulations," Unique Identification Authority of India, last accessed June 9, 2020, *https://uidai.gov.in/about-uidai/legal-framework/regulations.html*
5. UIDAI, "Offline Aadhaar Data Verification Service," Unique Identification Authority of India, *https://uidai.gov.in/images/Offline-Aadhaar-Data-Verification-Service_v1-23082018.pdf*
6. UIDAI, "Aadhaar Generation," Unique Identification Authority of India, last accessed June 9, 2020, *https://uidai.gov.in/my-aadhaar/about-your-aadhaar/aadhaar-generation.html*

Sectors

HEALTH STACK

1. National Health Stack, NITI Ayog, July 2018, *https://www.niti.gov.in/writereaddata/files/document_publication/NHS-Strategy-and-Approach-Document-for-consultation.pdf*
2. National Digital Health Blueprint, MoH&FW, 2019, *https://www.nhp.gov.in/NHPfiles/National_Digital_Health_Blueprint_Report_comments_invited.pdf*
3. Trisha Jalan, "Summary: National Digital Health Blueprint proposes new body for digital health mission, health data exchanges and registries," Medianama, August 6 2019, *https://www.medianama.com/2019/08/223-summary-national-digital-health-blueprint-2019/*
4. India Today Web Desk, "India is getting its first public healthcare record system to track the health of all citizens," India Today, July 16 2018, *https://www.indiatoday.in/education-today/gk-current-affairs/story/india-getting-first-public-healthcare-record-system-html-1284914-2018-07-16*
5. Electronic Consent Framework Technology Specifications version 1.1, Digital Locker Authority, *http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf*
6. Electronic Health Standards 2016, MoH&FW, December 30, 2019, *https://main.mohfw.gov.in/sites/default/files/EMR-EHR_Standards_for_India_as_notified_by_MOHFW_2016_0.pdf*
7. Omprakash V. Nandimath, "Consent and medical treatment: The legal paradigm in India," 25(3) Indian Journal of Urology, 343–347 (2009).
8. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, *https://ijme.in/articles/the-indian-medical-council-professional-conduct-etiquette-and-ethics-regulations-2002/?galley=html*
9. "Data Empowerment and Protection Architecture Explained – Video," ISpirit, last updated June 23, 2019, *https://pn.ispirt.in/data-empowerment-and-protection-architecture-explained-video/*

INDIA STACK

UPI

1. United Payment Interference Procedural Guidelines Version 1.7, NPCI, January 2016, *https://www.npci.org.in/sites/default/files/UPI-PG-17_01_31_RBI_Final%20version%201.7.pdf*

2. Aadhaar Authentication API Specification Version 2.0, UIDAI, February 2017, *https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf*

3. Digital Payments Step by Step Instructions, NITI Aayog, *https://niti.gov.in/writereaddata/files/Step-by-step_presentation_on_digital_payments-English.pdf*

E-sign

1. E-authentication Guidelines for e-Sign Version 1.6, CCA, May 2019, *http://cca.gov.in/sites/files/pdf/esign/CCA-EAUTH.pdf*

2. "E-sign- Online Electronic Signature Service," CCA, last accessed May 31, 2020, *http://cca.gov.in/eSign.html*

Digilocker

1. "Digilocker Registration Process: An Ultimate Digilocker App Guide," Digilocker- Create Digital Locker Account, last accessed May 31, 2020, *https://www.digilocker.info/digilocker-registration-process/*

2. Digilocker User Manual, DeiTY, *https://digilocker.gov.in/assets/img/DigiLocker-User-Manual.pdf*

EKYC

1. Aadhaar Authentication API Specification Version 2.0, UIDAI, February 2017, *https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf*