E-ID in India

Indukumar Vellapillil-Hari

21 Mar 2023

Table of contents

What is Aadhaar?

- 12 digit unique biometric ID system established in 2009
- ID linked to photo, 10 fingerprints and 2 iris scans
- Voluntary; available for all citizens and non-citizens with residence in India for at least 6 months
- World’s largest biometric ID system - 1.35 billion IDs
- Managed by a dedicated government department - Unique Identification Authority of India (UIDAI)

Why Aadhaar?

- Many specific purpose ID documents - but not guaranteed to be unique per person
  - Ration card for food security
  - Voter ID card to exercise voting rights in elections
  - Passport
  - PAN card for income tax compliance
  - Driving license
- Aadhaar is unique ID by design; linking of the different IDs to Aadhaar improve reliability (e.g. Voter IDs)

Benefits - Poverty Alleviation

- Rajeev Gandhi, Indian prime minister (1980s): “*For every 1 rupee target towards poverty alleviation, only 15 paise (0.15 rupee) reached the intended beneficiary*”
  - High leakages due to very high levels of corruption and administration expenses
  - Fake or duplicate ration cards created by organised crime syndicate

- Aadhaar based Direct Benefit Transfer - subsidies are directly transferred to bank accounts of the beneficiary
- Aadhaar linked ration cards reduced duplication, and resulted in savings

Benefits - eKYC

- Previously: no consensus among financial institutions on list of ID documents that are acceptable for KYC
- Getting loans for marginalised group was complex due to need for multiple documents for KYC compliance

- Aadhaar card with mobile OTP based authentication - possible over internet (e.g video + UIDAI signed KYC XML)
- Aadhaar simplified Know Your Customer (KYC) process, reducing hassle of loan application processes

Benefits - Ease of Living

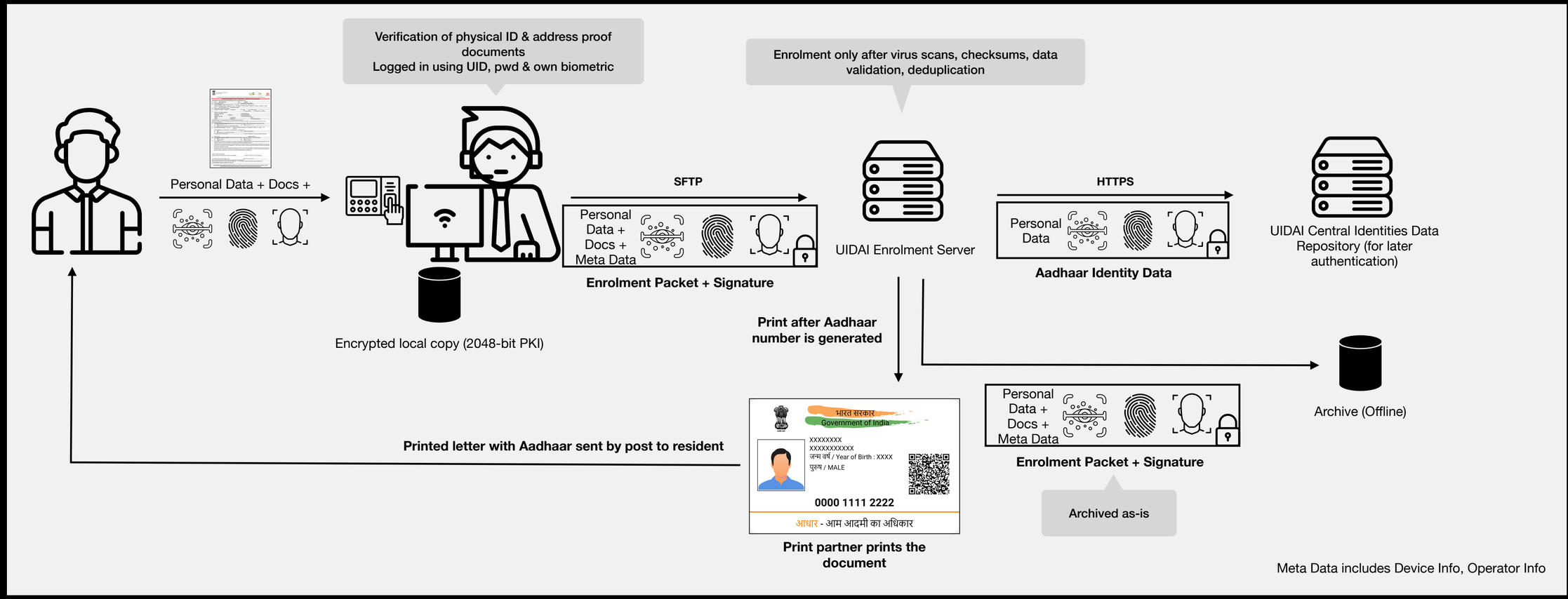
- Ration Card - not portable; need to go through complex process of de-registration and re-registration
- Multiple documents had to be shared manually with different government departments

- One Nation One Card - Aadhaar linked ration card; instrumental in supporting migrant workers during Covid
- DigiLocker - A free of cost Aadhaar enabled digital vault for documents and certificates for Indian residents; supports e-signature, auto updates

Challenges

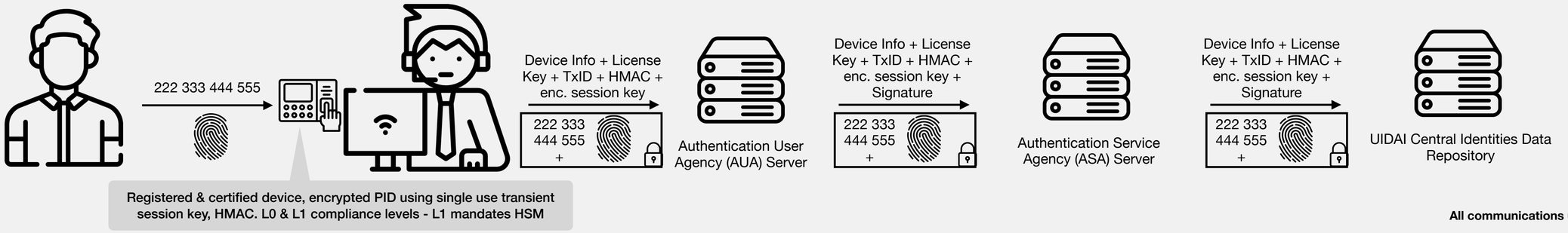
- Bedridden residents get scanning kits at home for enrolment
- Physically challenged residents have exemption process where only one biometric input is taken in addition to photograph (1% of enrolment)
- With population of 1.4 billion, there are still high amount of edge cases not thought of before
- Potential to become tool of mass surveillance - needs vigilance by citizens
    - Though UIDAI itself does not have the linked documents/information

Enrolment process



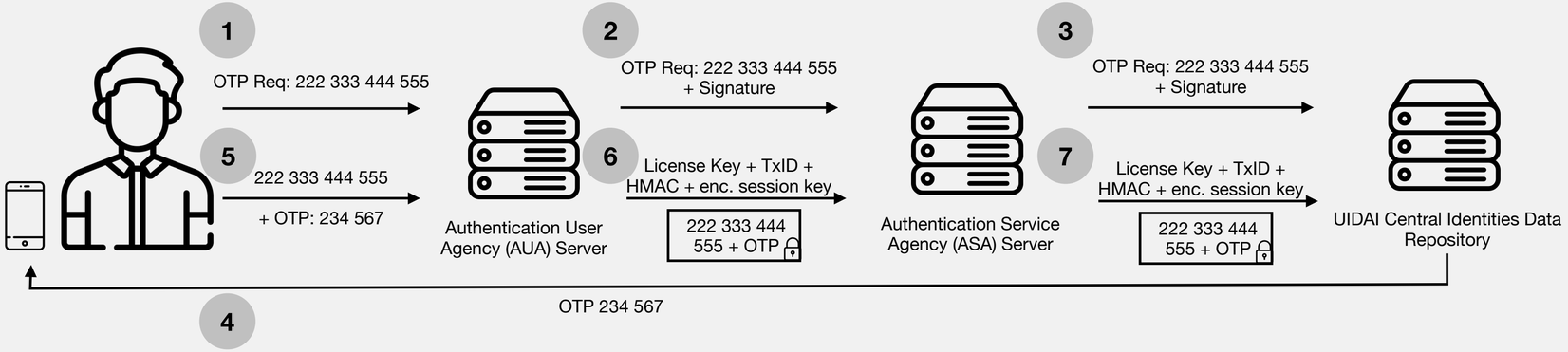
Authentication process

In-person authentication



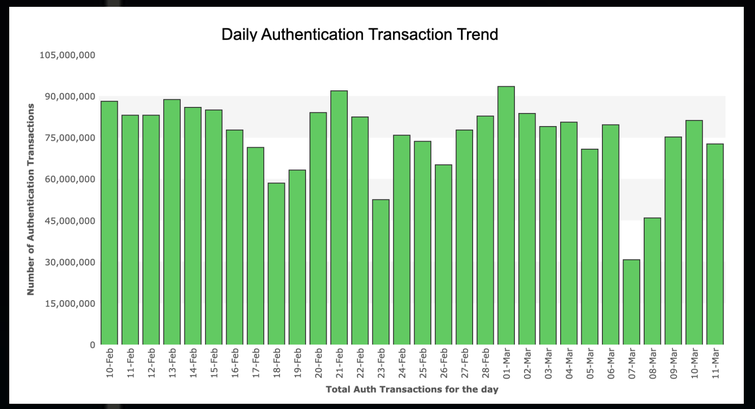
All communications using HTTPS

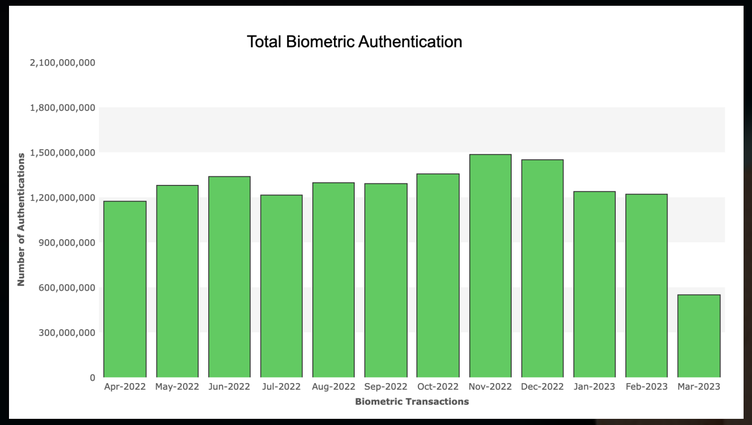
Self-service authentication

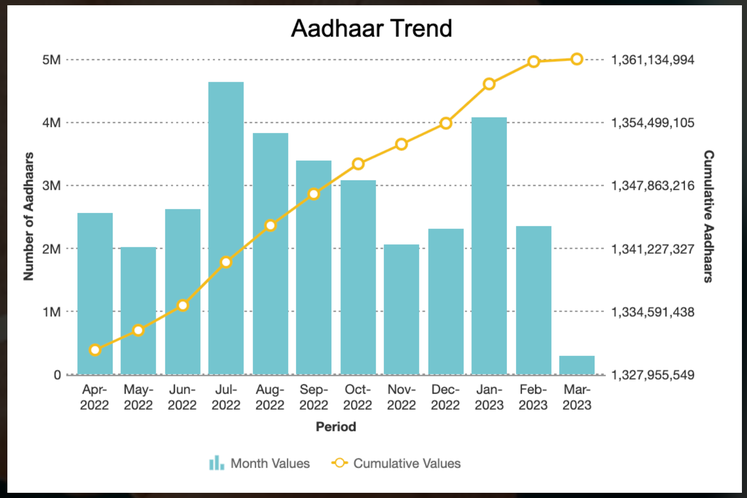


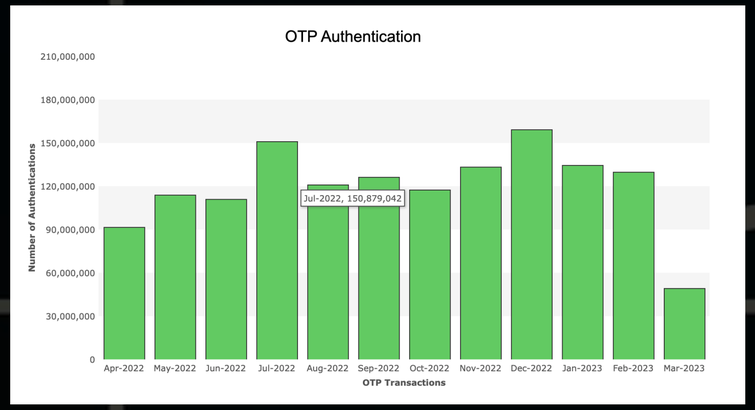
All communications using HTTPS

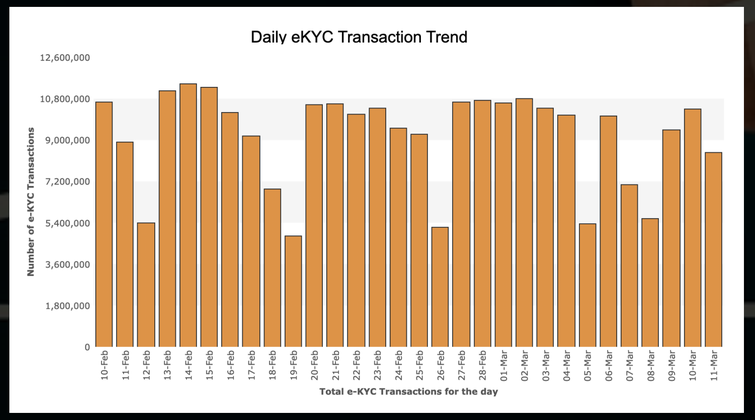
Statistics from Aadhaar Dashboard











Technical Architecture

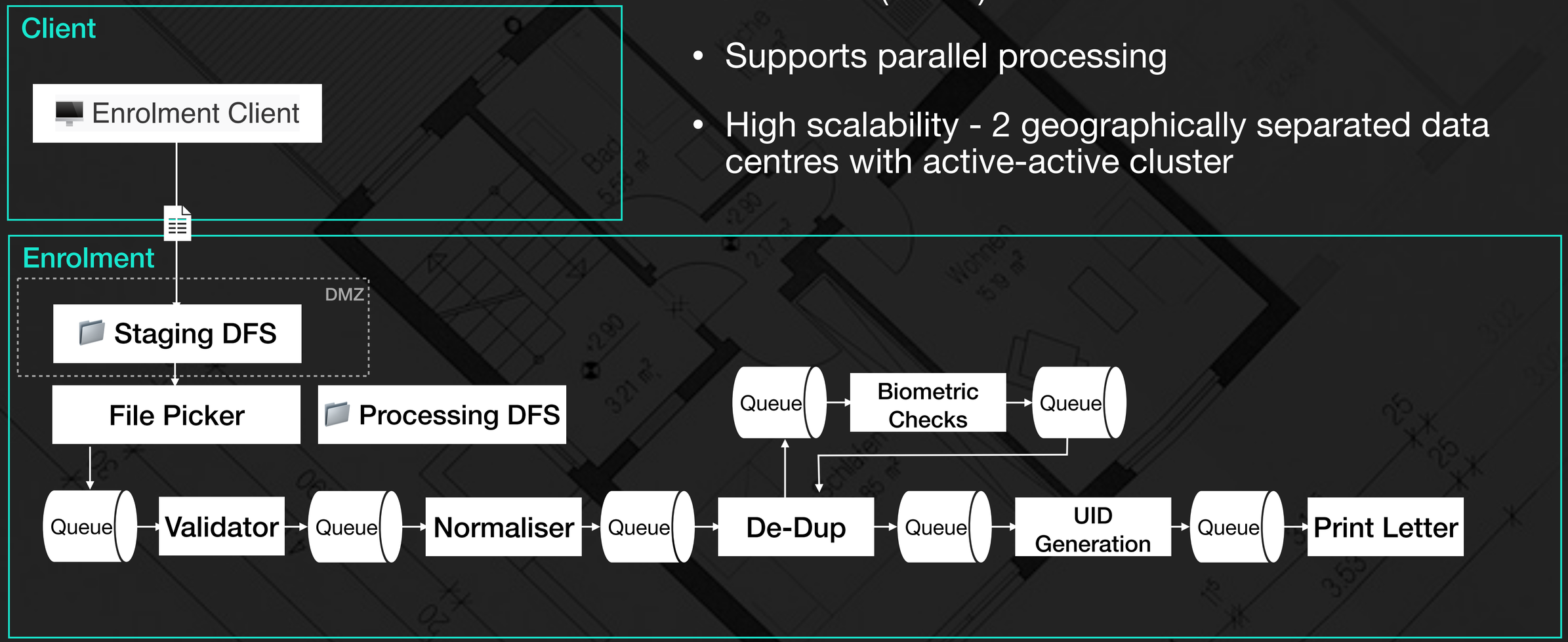
Technology

- Open & vendor neutral
  - Standards, Open Source, APIs, commodity hardware
- Tech Stack
  - Linux, Java+Spring, MySQL, MongoDB, Mule ESB, Apache Tomcat, HDFS, RabbitMQ, XML, JSON, AMQP, HTTP
- Security
  - PKI 2048, Hardware Security Module, physical, & network security, access controls, audits & monitoring, encryption in transit & at rest

Technical Architecture

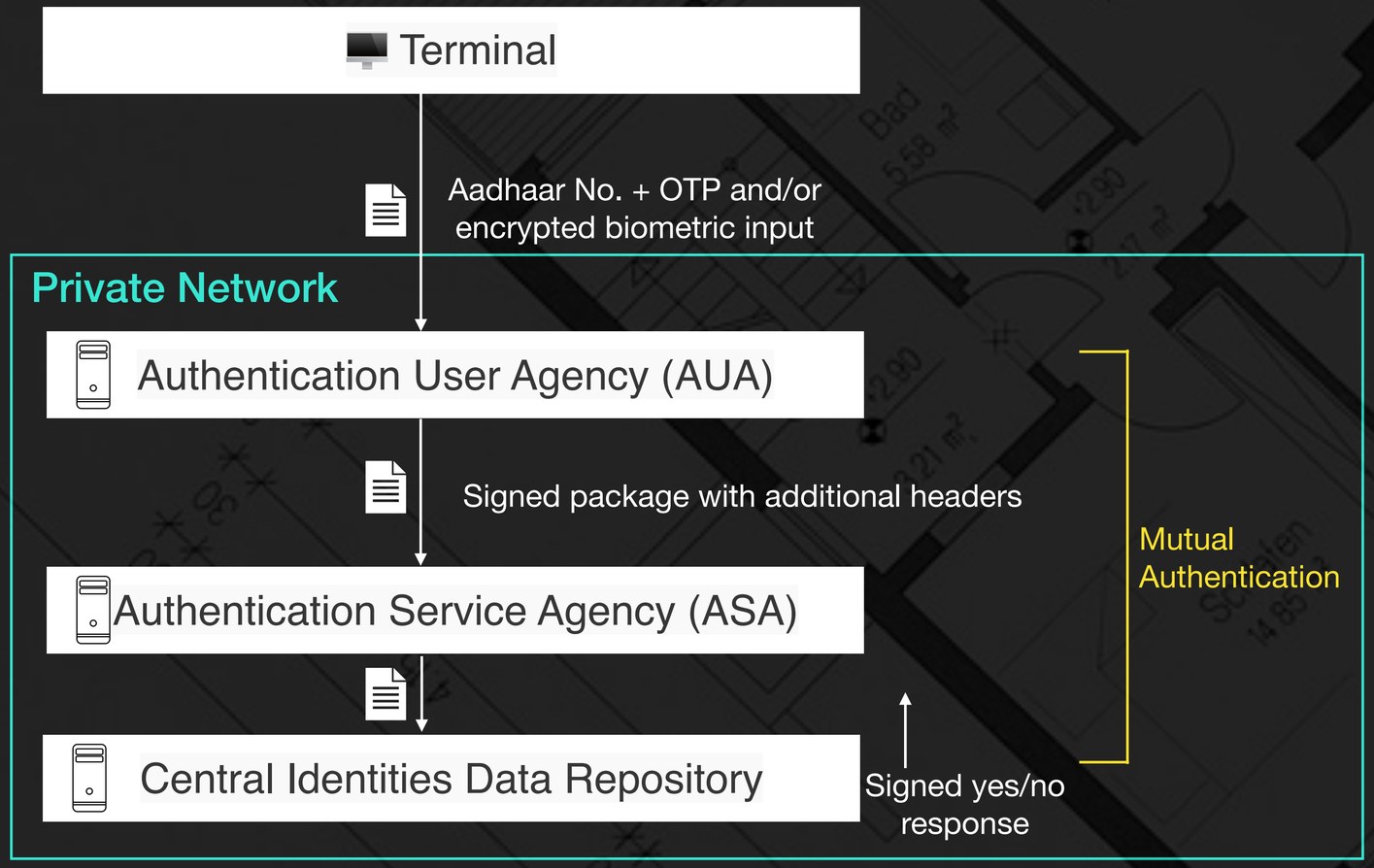
Enrolment Architecture

- Defined as per principles of Staged Event Driven Architecture (SEDA)
  - Supports parallel processing
  - High scalability - 2 geographically separated data centres with active-active cluster



Technical Architecture

Authentication Architecture

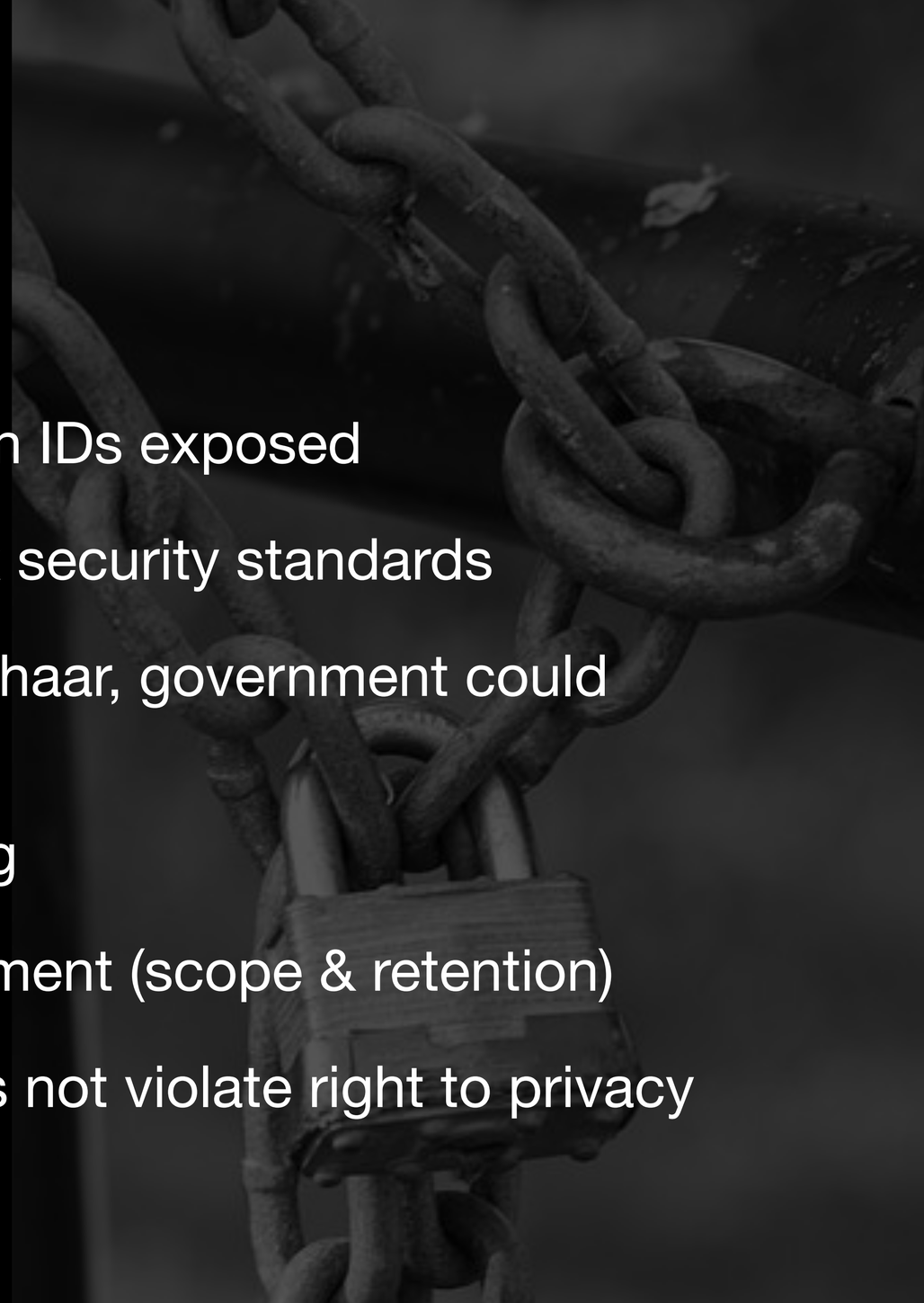


- REST APIs with XML payload over an encrypted channel
- Production servers are within a secure private network and are mutually authenticated
- The input payload is encrypted
- Response is only a “yes/no”

Security & Privacy (1/3)

- Aadhaar captures: Biometrics, Photograph, Name, Gender, DoB, Address, and optionally Mobile & E-Mail
  - No other data is stored or linked within the Aadhaar database itself
- Authentication using OTPs (6digits, 10m) with registered mobile number
- Consent/Authorisation checks before the Aadhaar data is shared with 3rd parties
  - However, 3rd parties may use the data for purposes other than the consent
- One-time use Virtual Aadhaar IDs to avoid sharing of actual Aadhaar IDs
- By legislation Aadhaar is voluntary - but practically a necessity

Security & Privacy (2/3)



- Security breaches in the past - up to 150 million IDs exposed
- Many authorised private organisations have lax security standards
- As more and more services are linked with Aadhaar, government could potentially conduct mass surveillance
- Strong data protection legislation is still missing
  - Currently under consideration by the government (scope & retention)
- Supreme Court judgement 2018: Aadhaar does not violate right to privacy

Security Issues (3/3)

- Replay attacks - previously allowed devices that stored unencrypted biometric data (now fixed with mandatory use of registered devices with transient encrypted biometric data - 2018)
- Biometrics is not a secret - can be forged/spoofed - 440 people defrauded recently (UIDAI now introducing liveness checks)
- SMS is not secure - messages can be intercepted and SMS is prone to SIM card scams
- UIDAI is reactive - many security features added only after occurrences of real world frauds

DigiLocker

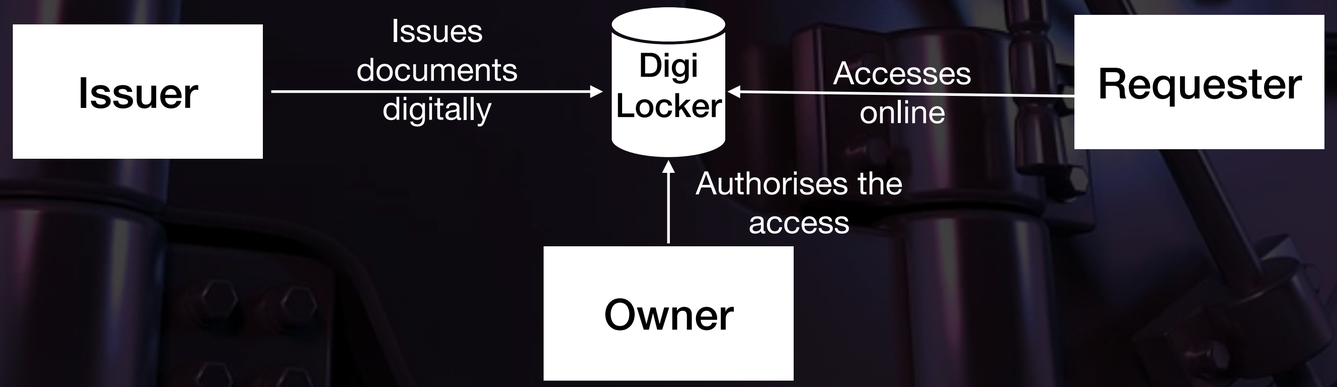
Vision

- Provide shareable private space on a public cloud
- Digitise all documents and records of the citizens and make them available on a real-time basis
- Facilitate process reengineering through paperless processes
- With due authentication, consent, audits, and other security best practices

DigiLocker

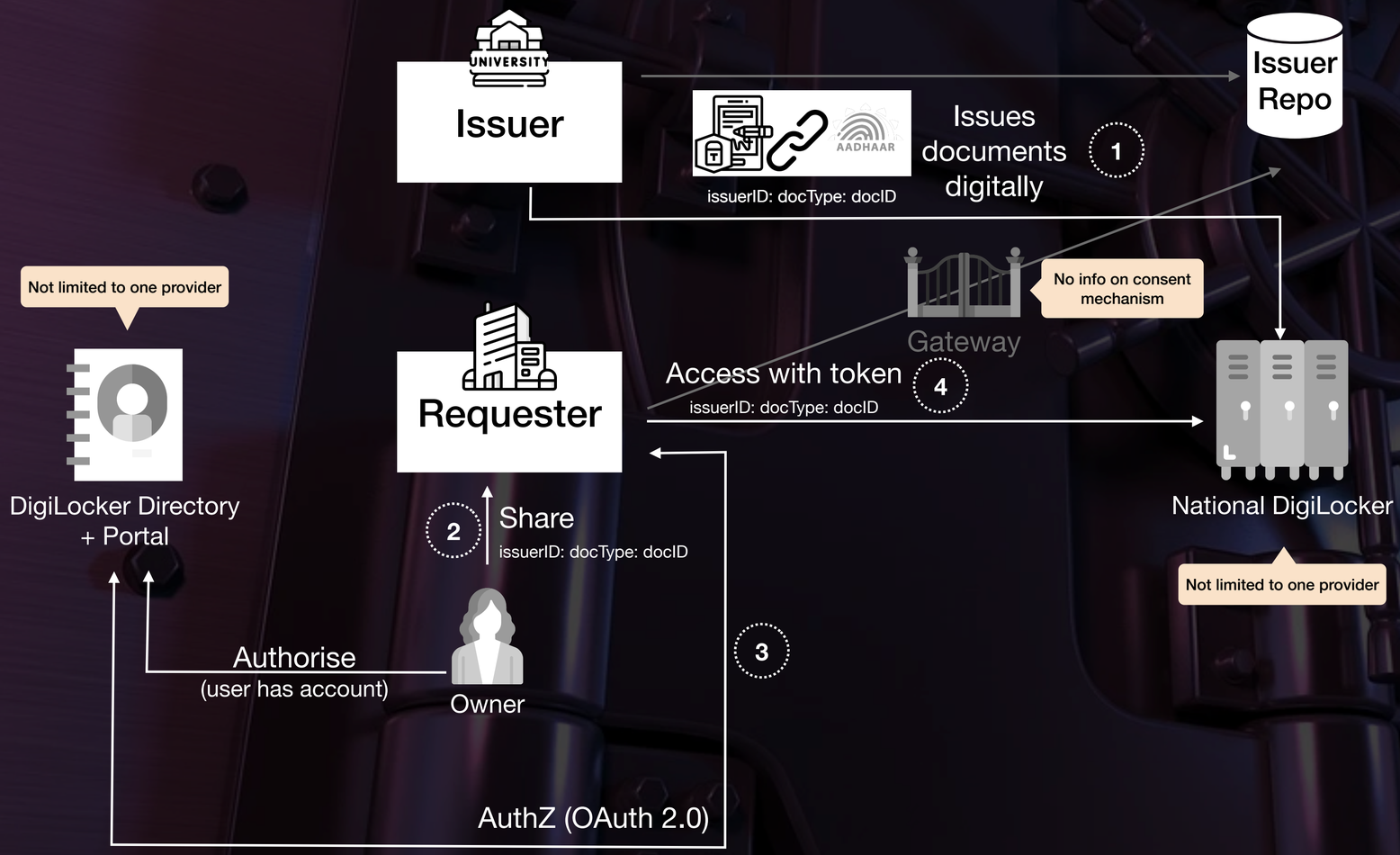
What it provides

- Open and interoperable architecture for creating a multi-provider ecosystem providing choice to the issuers, requesters, and individuals
  - Federated architecture: No centralised single document repository
- E-Sign capability
- Secure access to various government issued documents



DigiLocker

How it works (simplified)



- REST APIs (HTTPS)
- APIs accessed with API Key + Signature
- E-Document (XML)
  - Two references: Machine Readable (e.g. XML) and/or Printable (e.g. PDF)
  - Digitally Signed
  - Owner consent required for documents classified as private/ secure
  - Unique document URI (IssuerID::DocType::DocID)

Appendix

References

- Aadhaar Design
  - https://ia800108.us.archive.org/17/items/Aadhaar-Technology-Architecture/AadhaarTechnologyArchitecture_March2014.pdf
  - https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf
  - https://uidai.gov.in/images/resource/aadhaar_otp_request_api_2_5.pdf
  - https://uidai.gov.in/images/resource/Aadhaar_Registered_Devices_2_0_4.pdf
  - https://uidai.gov.in/images/resource/User_manulal_QR_Code_15032019.pdf
  - https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar/aadhaar-generation.html
- Aadhar Security
  - https://www.jisasoftech.com/what-goes-into-making-aadhaar-safe/
  - https://eprint.iacr.org/2022/481.pdf
- DigiLocker
  - https://partners.digitallocker.gov.in/assets/img/Digital%20Locker%20Authorized%20Partner%20API%20Specification%20v1.8.pdf
  - https://www.dla.gov.in/sites/default/files/pdf/DigitalLockerTechnologyFramework%20v1.1.pdf
  - https://img1.digitallocker.gov.in/assets/img/technical-specifications-dlts-ver-2.3.pdf
  - https://img1.digitallocker.gov.in/assets/img/issuer_api/Digital%20Locker%20Issuer%20API%20Specification%20v1.12.pdf
  - https://www.livemint.com/money/personal-finance/all-you-need-to-know-about-digilocker-and-how-to-use-it-11612943898102.html
- News
  - Confusion on documents: https://theleaflet.in/indian-citizenship-law-a-mess-proving-citizenship-even-messier/
  - DBT: https://vikaspedia.in/social-welfare/direct-benefit-transfer/overview-of-direct-benefit-transfer
  - Voter-ID Linking: https://www.financialexpress.com/opinion/linking-voter-id-to-aadhar-can-make-voting-portable/1681304/
  - Data center: https://www.businesstoday.in/latest/policy/story/aadhaar-safety-where-is-uidai-13-feet-high-5feet-thick-wall-246996-2018-03-23
  - Only registered devices: https://www.livemint.com/Politics/FgXy2gorgyXaGVvpkl4yKN/From-1-Mar-only-registered-devices-to-be-used-to-authentica.html
  - Reduction in KYC costs: https://www.procivis.ch/post/lessons-from-the-worlds-largest-e-identity-program-indias-aadhaar
  - Data protection bill: https://www.gadgets360.com/cryptocurrency/news/digital-personal-data-protection-bill-india-parliament-provisions-safeguards-3844077
  - Fake ration cards: https://timesofindia.indiatimes.com/city/dehradun/fake-ration-cards-duped-over-rs-10cr-during-lockdown-allege-locals-in-kichha/articleshow/81260500.cms
  - Rajeev Gandhi Quote: https://www.hindustantimes.com/india-news/only-15-paise-reaches-the-needy-sc-quotes-rajiv-gandhi-in-its-aadhaar-verdict/story-I8dniDGXF6ksulggTDgb9L.html
  - One Nation One Ration Card: https://newsonair.com/2022/06/22/india-achieves-another-milestone-with-one-nation-one-ration-card-now-fully-portable/
  - Biometric fraud: https://www.deccanchronicle.com/nation/crime/110223/kadapa-police-bust-money-swindling-fingerprint-cloning-gang.html

Special thanks to Flaticon (https://www.flaticon.com/free-icons/), Pixabay for the icons and images