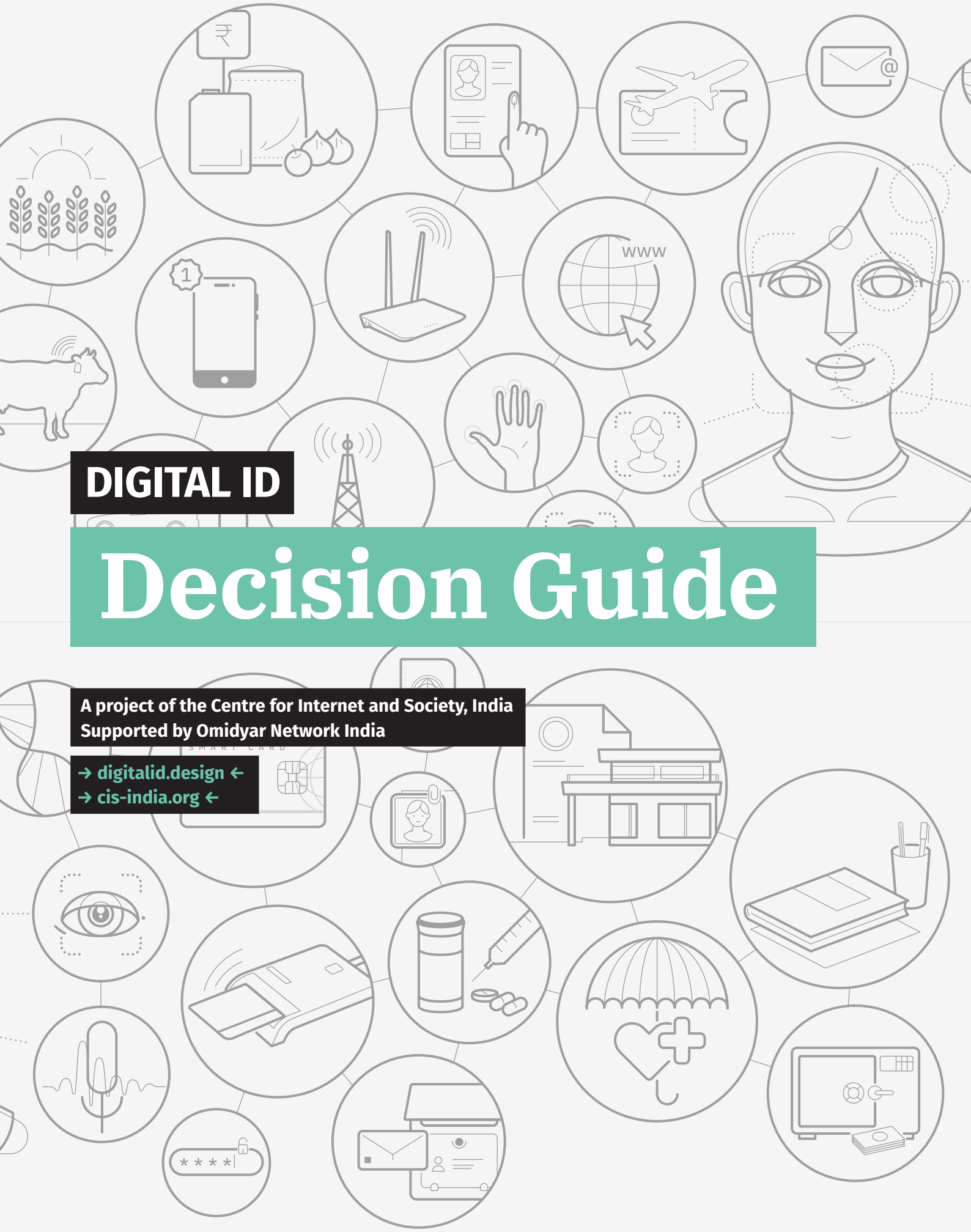


DIGITAL ID

Decision Guide

A project of the Centre for Internet and Society, India
Supported by Omidyar Network India

→ digitalid.design ←
→ cis-india.org ←

RESEARCH & WRITING

Amber Sinha, Anubha Sinha, Divyank Katira, Shruti Trikanad, Yesha Tshering Paul

REVIEW & EDITING

Yesha Tshering Paul

DESIGN

Akash Sheshadri, Pooja Saxena, Saumyaa Naidu

COVER ILLUSTRATION

Akash Sheshadri

LAYOUT

Saumyaa Naidu

THE CENTRE FOR internet & society

Contents

This guide seeks to serve as a comprehensive toolkit to enable different parties to make informed decisions around proposed digital ID systems.

Who is this guide for?

POLICYMAKERS

To help inform policy and technological decisions around digital ID systems.

VENDORS

To lay out the range of technological choices available, and shift focus to more inclusive, privacy enhancing and open technologies.

CIVIL SOCIETY

To enable civil society to ask the right questions of, and make appropriate policy recommendations for digital ID systems.

RESEARCHERS & ACADEMIA

To facilitate further scholarship on digital ID systems that builds upon this Decision Guide.

JUDICIARY

To empower future litigants and courts to analyse questions of fact, necessity and proportionality, and best practices for digital ID systems.

Understanding Digital ID

Research by **Shruti Trikanad and Amber Sinha**
Conceptualization by **Pooja Saxena and Amber Sinha**
Illustrations by **Akash Sheshadri and Pooja Saxena**

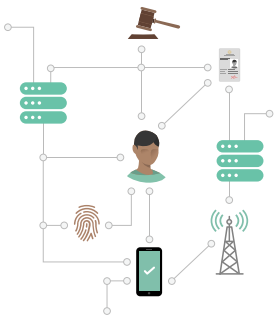
This Decision Guide seeks to serve as a valuable resource when making decisions about a proposed digital ID system. For this, we need a shared vocabulary to understand and critically analyse all aspects of digital ID systems. Through a preliminary study of existing identity systems, we have arrived at this core set of concepts and processes that mark a digital ID system.

When we embarked on this research project, we began with the primary questions of what constitutes a digital identity system. In the last few years, with the rise in national digital identity projects, there has been significant academic and media attention to the idea, benefits and risks of a digital identity system. However, there have been relatively few attempts to critically look at what makes an identity system digital, and what are its defining elements and characteristics. Through a preliminary study of existing identity systems, we have arrived at these core set of concepts and processes that mark a digital identity system. In arriving at this list, we have relied upon and referred to the works by Dave Birch et al, World Bank's ID4D initiative, Mawaki Chango, Kaliya Young and Kayode Ezike.

By publishing this, we hope to arrive at a shared vocabulary to discuss and critically analyse digital identity systems, both within our team and in engagements with other stakeholders. This illustrated glossary can serve as an easy reference for anyone seeking an introduction to the core aspects of digital identity. Even though this is essentially a list of definitions with examples, it does not follow an alphabetical order like most glossaries, but the logical flow of concepts as they build upon each other in a working identity system. We have paid special emphasis to the core processes of Identification and Authentication, elucidating them through diagrams.

1. **Individual**: Identity Systems are created in order to provide means of identification to an identified set of population, such as residents, citizens, individuals above a certain age etc. In the context of an Identity System, an individual is someone eligible to enroll within it.

2. **Identity**: Identity refers to a set of attributes of an Individual that can be used to identify them individually or as part of a group of individuals.



3. **Identity System**: An identity system comprises all the databases, processes, technologies, infrastructure, credentials, and legal frameworks associated with the collection, use, and management of personal identity data for the purpose of identifying individuals.

    a. **Foundational Identity System**: A foundational identity system is a core Identity System created to manage identity information for the general public, and to provide identity proof for a wide variety of public and private services. National ID systems such as Aadhaar in India or the e-ID scheme in Estonia, and population registries, are common examples of foundational identity systems.

    b. **Functional Identity System**: A functional identity system is designed to meet the needs of an individual sector, and is not designed for other purposes or in other sectors, although in some cases, it may be used as such. For instance, a voter ID designed specifically for use by the Individual for the purpose of proving their Identity while voting, just as a Tax ID number (or registration number) is designed for use while dealing with tax related matters. The National Health Service in the UK has its own digital ID System to identify patients and keep records of their treatment.

    c. **Unique Identity System**: A unique identity system is one that uniquely identifies individuals within a population, such that no one person may enrol multiple times in the system, and that each Identity Artifact is associated with only one person. For instance, the Aadhaar scheme in India has ensured that each Unique Identification Number in the system is only associated with one individual, through the process of de-duplication.

    d. **Centralised Identity System**: A centralised identity system is one in which there is a single recognised

agency or body which is tasked as the issuer of identity. The e-ID system in Estonia or the NADRA in Pakistan, for instance, entails one government agency responsible for providing identification and authentication services for individuals, without the Individual being able to choose which entity to enroll with.

e. **Federated Identity System**: Under a Federated Identity System, multiple digital ID providers, who may be public or private, are endorsed by the Identity System. Here, individuals can choose between these digital providers, and use the issued credentials for a wide range of services through an identity hub or a gateway that facilitates authentication across multiple platforms. In a Brokered Identity Provider model, identification and authentication are carried out by multiple digital ID providers, but with the additional presence of a central hub through which data is exchanged. An example of this is the Gov.UK Verify ID system in the UK, which allows individuals to choose between several different certified private identity providers to access a range of public and private services.

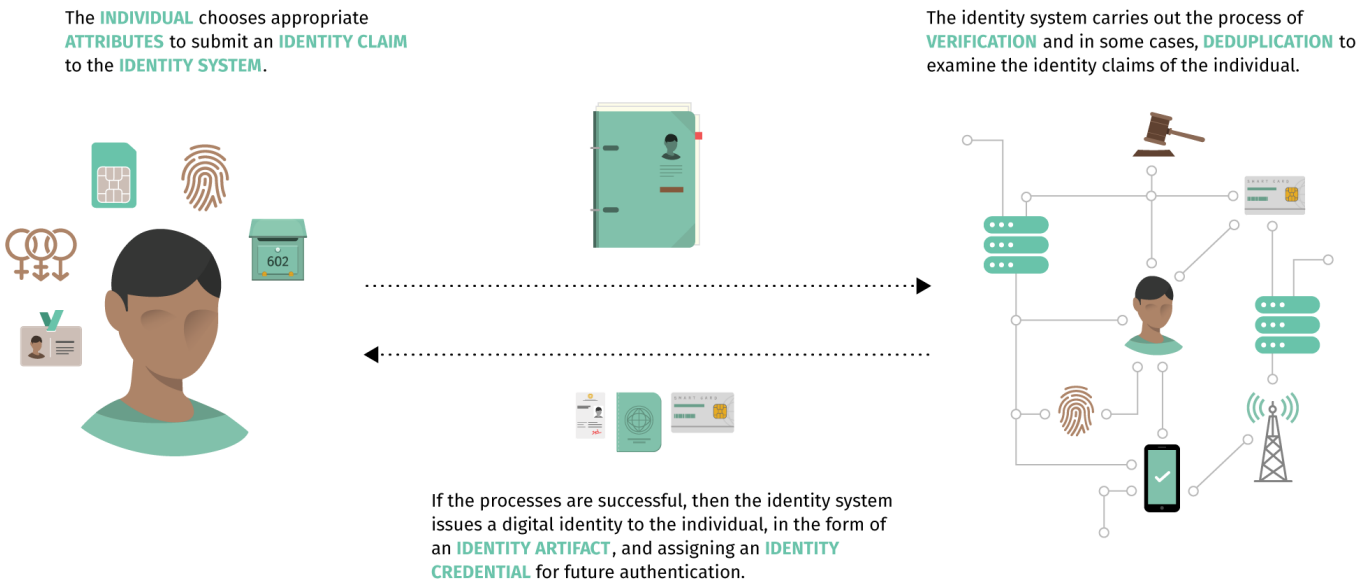
f. **Open Market Identity System**: In an open market system, public and private organizations create, use, and manage their own digital IDs according to a self-regulated framework. Here, there is no central scheme, and the digital IDs can be used to access government services only where there are agreements between the government agency and the identity services provider.

g. **Self Sovereign Identity System**: In a self sovereign identity system, each Individual or entity can be empowered to create unique, digital and portable identities on their own which can rely on decentralised technologies such as shared ledgers for use, but do not rely on any centralised authority, rendering them irrevocable by any third party.

4. **Interoperability**: Interoperability is the ability of different functional units—e.g., systems, databases, devices, or applications—to communicate, execute programs, or transfer data in a manner that requires the user to have little or no knowledge of those functional units. An interoperable system is one whose interfaces are understood, to work with other products

or systems, present or future, without restrictions.

5. **Identification**: Identification is the process of establishing the digital identity of an Individual and ascertaining information about them, by verifying corroborating documents, testaments, and other forms of proof of the Individual's claimed Identities and Attributes. In the context of a digital ID System, this may involve individuals first claiming certain Attributes (such as their name, sex, date of birth etc) and having them recorded, then presenting requisite documents or testaments to validate their Identity Claim. Finally, they are issued certain credentials (such as PINs, ID Cards etc) or their Attributes are accorded the status of ID credentials (such as biometrics) which can be digitally used to control or assert the established digital ID.



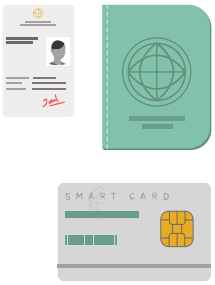
a. **Attribute**: An attribute is any property, characteristic, or quality, that is inherent to or ascribed to an Individual, and can be associated with them in a stable or reliable manner. Examples: name, age, sex, place of birth, address, fingerprints, signature etc.

b. **Identity Claim**: During the process of Identification, Individuals enrolling into the Identity System are often required to produce supporting documents which serve as proofs or identity, address etc. In some cases, Identity

Claim may also be made through testimonials or certificates from other entities, or through self-assertion in the form of an affidavit or some other means. Based on the priorities of the Identity System such as fraud reduction, inclusivity etc., the standard for what is an acceptable Identity Claims could vary.
Examples: Existing Civil Registration document, Testimonials, Self-asserted affidavits.

c. **Verification**: Verification is the process followed during Identification to check the Identity Claims of an Individual, and ensure that they are the true owner of the claimed Identity and the related evidence/documents. This could include inspecting breeder documents such as a birth certificate to verify the date of birth claimed by the entity, or examining a photo ID card to verify other attributes of appearance, name, sex, etc., by the enrolling agent during the Identification process.

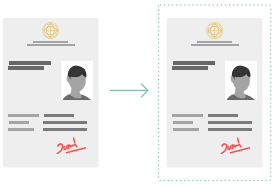
d. **Deduplication**: Deduplication is a process undertaken during Identification in some Identity Systems to establish the uniqueness of individuals. It typically involves digitally comparing biographic or biometric data submitted by Individuals against previously enrolled records to determine if there is already a record of the Individual.



e. **Identity Artifact**: An identity artifact is a document or object, which can be both physical or digital, that is issued to an Individual at the end of the process of Identification, and facilitates in establishing their Identity. The Identity Artifact will usually involve a registration number assigned to the Individual.
Examples: Smart Identity Card, Registration Number, Paper Identity document.

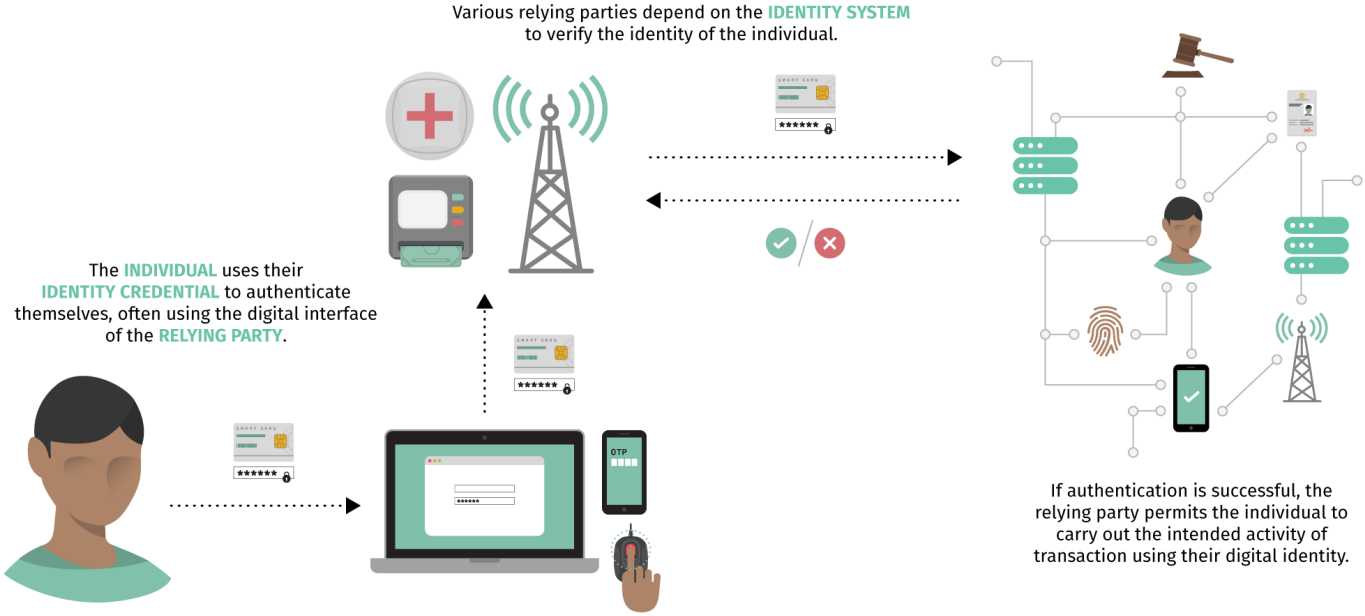
6. **Identity Assurance**: Identity assurance is the ability to determine, with some level of certainty or assurance, that a claim to a particular identity made by an Individual can be trusted to actually be the claimant's true identity. The mapping of this assurance in terms of its overall level, derived from both the quality of the identification process and the strength of the authentication credential used when asserting the identity, is termed its Level of Assurance (LOA).

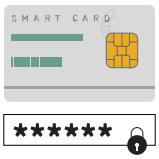
7. **Seeding**: Seeding is the mapping of identity records in



an existing database with those in another database, typically through a unique identifier. For instance, in India, Aadhaar numbers of residents are being seeded into the service delivery database of public and private service providers.

8. **Authentication**: Authentication is the process of establishing confidence that an Individual is who they claim to be. This involves using an Identity Credential, that was bound to the Identity during the process of Identification (such as fingerprints, a password, a smartcard, etc) to assert that it is within the control of the Individual whose identity is being asserted. This is done through a process established within the Identity System to digitally check the Identity Credential usually against the Identity Artifact.





a. **Identity Credential**: An identity credential is any document, object, or data structure that can digitally affirm the Identity of an Individual through some method of Authentication in an Identity System. There are several kinds of factors that could be used as Identity Credentials. Examples: Smartcards, Biometrics, Passwords, OTPs, etc.

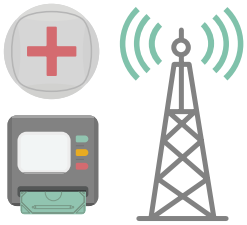
b. **Knowledge Factors**: In some Identity Systems, the process of authentication is carried by testing for information that the Individual is expected to know. These include Identity Credentials such as passwords and PINs.

c. **Possession Factors**: In some Identity Systems, the process of Authentication is carried out through the use of an object that is supposed to be in the possession and control of the Individual. It includes a card, or mobile phone on which they receive an OTP, or a token device on which they receive a code.

d. **Inherence Factors**: These factors rely on the use of physical attributes of the Individual that are digitally measurable for Authentication such as fingerprints, iris scans, facial recognition etc.

e. **Behavioral Factors**: These factors rely on measurements of behavioral aspects of an individual such as gait, voice patterns for Authentication.

f. **Multi-Factor Authentication**: A system workflow that requires more than one factor for the Authentication of the Individual. In Estonia, the use of both the card and PIN is an example of multi-factor authentication.



g. **Relying Party**: A relying party is an entity that uses the Authentication mechanism provided by an Identity System to verify the Identity of an Individual, in order to process a transaction or grant access to a system, or information, or a service. Based on the nature and purpose of the Identity System, relying parties can be both government bodies or private actors.

9. **Authorisation**: Authorisation is the act of the Individual determining what actions may be performed on their behalf, or if their personal data may be accessed, based on the asserted and authenticated Identity. The process of authorisation involves the use of the digital ID to undertake activities and transactions (both financial and otherwise). It is this aspect of digital ID which leads to both its oft-mentioned benefits such as ease of doing business, cost effectiveness and speedy transactions; as well as its prominent risks such as profiling, digital trail connecting disparate activities and discriminatory effects.

Designing Digital ID

Digital ID solutions are often vendor-driven, where a particular vision of technological specification dominates the process of designing the identification system. This is not ideal as it treats the identification system, or rather a pre-decided version of the identification system itself, as the end goal.

The process of designing a digital ID system must begin with its objectives. It must analyse the existing identification system and the desirable purposes it does not adequately meet. All these identified purposes for the use of the identification system must correspond to a legitimate aim identified in the valid law.

Some of the key objectives of a digital ID system are discussed below.

Objectives

Research and Writing by **Yesha Tshering Paul & Anubha Sinha**

1. Legal identity

The World Bank estimates that approximately 1 billion persons lack official proof of identity[1], with these undocumented populations being disproportionately concentrated in sub-Saharan Africa and South Asia, and amongst marginalised and vulnerable communities within these regions in particular. This is often due to many such countries having weak legacy systems for civil registration, a history of political turbulence that has resulted in civil registration records being destroyed or misused, or the State excluding certain classes of persons on the basis of religion, refugee status, or sexual or gender identity.

Digital ID has been posited as a way to address this, by providing proof of identity by modernising existing identity infrastructure and addressing the lack of a foundation of trust and accountability between the government and its citizens. Digital ID promises to provide a reliable and trustworthy identity to all, help overcome barriers to political and economic participation, and provide access to entitlements.

It is important, however, to delineate our understanding of a "legal" identity from a "digital" identity. While a technological solution promises seemingly obvious benefits, particularly to countries with large undocumented populations and limited resources, it cannot itself address the underlying political and structural issues that have actually caused these gaps in identification (in fact, it poses the danger of escalating them instead). Moreover, the sensitive data collected and stored by digital ID systems raises concerns around privacy and surveillance, and a potentially adverse impact on civil liberties. Many national digital ID programmes have been observed to resort to the collection of biometrics and other unnecessary data points[2], which bring about their own security issues and fear of misuse. These result in databases that are potential targets for cyberattacks, amplify exclusions, or aid in the targeting of already vulnerable communities.

Therefore, it is critical to reconsider whether digital ID should be pushed as the first-line solution to these issues. It is crucial to allow for multiple forms of identification (including non-digital), particularly keeping in mind infrastructural, political and other factors that may prevent persons from enrolling for digital ID or successfully authenticating their identities, and the adverse outcomes that have arisen from being locked out of these systems or databases being misused.

2. National Population Registers and determination of citizenship

1 Global Identification Challenge by the Numbers (2018), https://id4d.worldbank.org/global-dataset/visualization.

2 While challenging the introduction of the Huduma Namba system before the High Court of Kenya, the Petitioners argued that the expanded definition of 'biometrics' (which includes 'unique identifiers or attributes including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and Deoxyribonucleic Acid in digital form') and GPS coordinates were intrusive and unnecessary. Similarly, Ghana collects more than 30 data points about an individual *(Akuetteh Falconer & Odoru-Morfo, 2021)*, and Lesotho collects around 23 *(Pule, 2021)*.

While the stated aim of many digital ID system is to include undocumented populations and provide them access to government entitlements, many countries have witnessed these systems being weaponised to determine citizenship, resulting in exclusion of stateless persons, or those who do not have access to the required citizenship documents.

In Kenya, a major concern raised by the Huduma Namba system was that evidence of citizenship would be tied to the new system, raising concerns among border communities, refugees and ethnic minorities who have not been able to obtain proof of citizenship due to systemic barriers in obtaining identification.[3]

In India, the controversial National Register of Citizens (NRC) and National Population Register (NPR) are built on existing Aadhaar infrastructure[4] despite assurances to the contrary by the Ministry of Home Affairs.[5] The forceful eviction of nearly 2 million persons who have resided in the border state of Assam for generations but did not have the required documentation[6] is just one example of the adverse impacts of determining citizenship on this basis.

3. Welfare

The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act was passed in 2016. The Supreme Court in its Aadhaar judgment held that the aim of the Act was legitimate, noting that it was "aimed at offering subsidies, benefits or services to the marginalised sections of the society for whom such welfare schemes have been formulated from time to time" and "the objective of the Act is to plug the leakages and ensure that the fruits of welfare schemes reach the targeted population, for whom such schemes are actually meant."[7]

The implementation of digital ID systems for this purpose is meant to increase inclusion and access to entitlements, while also tackling welfare fraud. However, making a digital ID the sole means of accessing basic services disregards the many barriers that hamper enrollment and authentication, and the difficulties in obtaining ID by persons for whom these welfare schemes are often intended. In the absence of alternative forms of identification, this has resulted in beneficiaries being locked out of basic entitlements.

The use of digital ID to tackle corruption in these systems has also been contested, on the basis that it assumes that the biggest source of corruption is through claims by people who don't exist, or by people who have enrolled twice and therefore claim more than they are entitled to. Digital ID fails to address other major forms

3 Digital Identity in Kenya: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa (November 3, 2021), https://digitalid.design/RIA%20docs/CIS_DigitalID_RIA_Kenya_31.10.21.pdf.

4 Srinivas Kodali, "Digital India on Steroids: How Aadhaar Infra Enables the NPR and the NRC", *The Wire*, December 24, 2019, https://thewire.in/tech/aadhaar-infra-npr-nrc.

5 Dheeraj Mishra, "Exclusive: Official File Notings on NPR and Aadhaar Contradict Home Ministry Assurances", *The Wire*, January 16, 2020, https://thewire.in/government/exclusive-npr-aadhaar-home-ministry.

6 "India excludes nearly 2 million people from Assam citizen list", *Al Jazeera*, August 31, 2019, https://www.aljazeera.com/news/2019/8/31/india-excludes-nearly-2-million-people-from-assam-citizen-list.

7 (2019) 1 SCC 1, paras 314, 373.

of fraud within welfare systems, such as quantity fraud.[8] While estimates vary, one survey concluded that as much as 88% of ration cards that were deleted because they were not seeded with Aadhaar belonged to genuine non-ghost households.[9] This highlights the high exclusion costs in pursuit of plugging leakages in welfare delivery systems.

4. Access and onboarding to private services

In addition to accessing public services, many digital ID systems are being adopted by private actors (including essential services such as banking and telecommunications) for purposes such as KYC and anti-money laundering. Digital ID is seen as a way to provide verification and authentication to a high degree of assurance, ensure uniqueness of each customer, and ensure that the customer provides individual consent, their privacy is protected, and they maintain complete control over their personal data. Industry estimates project that it could have the potential to help countries unlock a value equivalent to 3 to 13 percent of GDP by 2030.[10]

A survey of digital ID systems across 10 countries in Africa has found that most digital ID systems have few regulatory controls over access to data by private actors, allowing sensitive data to be accessed without any oversight.[11] In addition to this, there are concerns about digital ID being made mandatory to access these services.[12] Being locked out of accessing basic banking and telecom services denies persons the opportunity to participate meaningfully in the economy, since these are essential for their daily existence as well.

5. Voter fraud concerns

Attempts to combat voter fraud involve making voter ID requirements increasingly strict. However, this has been shown to disproportionately affect minority communities, often as a deliberate attempt to systematically exclude certain sections of the population from voting.

In India, almost 3 million voters had their names struck off electoral rolls in the state of Telangana in 2015 after the then chief electoral officer of the state began linking Aadhaar data with election photo identity card (EPIC) or voter ID under the

8 Reetika Khera, "Impact of Aadhaar in Welfare Programmes", September 29, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3045235.

9 Karthik Muralidharan et al., "Identity Verification Standards in Welfare Programs: Experimental Evidence from India", Working Paper 26744, NBER Working Paper Series (2021), https://www.nber.org/papers/w26744

10 Digital identification: A key to inclusive growth, April 17, 2019, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

11 Towards the Evaluation of Socio-Digital ID Ecosystems in Africa: Comparative analysis of findings from ten country case studies, November 2021, https://digitalid.design/RIA%20docs/CIS_DigitalID_RIA_Comparative%20Report_5.11.21.pdf.

12 Digital Identity in Lesotho: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa (November 3, 2021), https://digitalid.design/RIA_Lesotho.html.

Digital Identity in Uganda: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa (November 3, 2021), https://digitalid.design/RIA_Uganda.html.

National Electoral Roll Purification and Authentication Programme (NERPAP), in order to weed out duplicate and bogus voters. This also highlighted that the state government had collected sensitive data such as caste and religion under the State Resident Data Hub (SRDH), which is an Aadhaar-seeded repository of information consolidated from multiple government databases.[13] Despite this, the Election Commission of India recently mooted a proposal to link Aadhaar records with voter IDs and faced widespread criticism on the grounds that this would actually cause mass disenfranchisement and increase voter fraud (with self-reported errors in Aadhaar higher than that in the voter ID database). The additional introduction of biometric authentication for voting would cause additional exclusions, and linking of these two databases would result in demographic information from Aadhaar being linked to the voter database, increasing the likelihood of voter profiling and violating the fundamental right to privacy. This is illustrative of the need to keep databases separate, and allow for different forms of ID for different purposes.

6. National security

Because of the high levels of assurance for identity verification and authentication that it claims to provide, digital ID has also been touted as a solution to address national security concerns - to prevent cyberattacks, ransomware attacks and identity fraud by adversaries.[14]

However, this requires a comprehensive regulatory and accountability framework to govern the use of personal data, strict identity checks at the time of enrollment, robust security features, and transparency in the role of foreign players in the ecosystem. Many of these conditions are often not met, resulting in digital IDs in many countries not being conclusive proof of identity, residence or citizenship. Moreover, data protection laws usually grant an exemption in cases of 'national security', but the term itself is often broadly or not at all defined in statutory law. This opens up major avenues for abuse of sensitive personal data in the absence of any oversight, accountability or means for recourse. As with all such surveillance and profiling in the name of national security, this will inevitably impact the fundamental freedoms of communities that are considered to be 'threats' by the State.

7. Handling COVID-19

The COVID-19 pandemic and the ensuing difficulties in claiming benefits, receiving vaccinations, the need for digital payment solutions and e-services, and the push for digital vaccine passports to resume international travel resulted in a worldwide push for various forms of digital ID.[15]

13 Yunus Y. Lasania, "Telangana voter deletion: Activists seek details of Aadhaar-Voter linkage", *Mint*, February 25, 2019, https://www.livemint.com/politics/news/telangana-voter-deletion-activists-seek-details-of-aadhaar-voter-id-linkage-1551093961654.html.

14 "Digital Identity is a National Security Issue", War on the Rocks, last accessed November 12, 2021. https://warontherocks.com/2021/04/digital-identity-is-a-national-security-issue/.

15 Mohamed Dabo, "Digital ID systems take centre stage as the world shuns physical contact", *Electronic Payments International*, September 15, 2020, https://www.electronicpaymentsinternational.com/news/digital-id-systems-take-centre-stage-as-the-world-shuns-physical-contact/.

The shortage of vaccines faced by many countries in the global south was exacerbated by enrollment for vaccination programmes sometimes being completely digital, and often linked to possession of a national digital ID. This led to many sections of the population without documentation or access to the internet being denied access to vaccines in a critical situation that required as many people to be vaccinated as quickly as possible.

In India, despite Aadhaar not being mandatory in order to get vaccinated, many patients have complained that hospitals have rejected other official forms of identification and demanded Aadhaar for registration instead.[16] India also witnessed many instances of patients in need of critical COVID care being denied admittance to hospitals in the absence of an Aadhaar card.[17]

16 Sunitha Rao R, "Bengaluru: Why hospitals insist on Aadhaar to register citizens for vaccination", *The Times of India*, April 4, 2021, https://timesofindia.indiatimes.com/city/bengaluru/why-hospitals-insist-on-aadhaar-to-register-citizens-for-vaccination/articleshow/81895866.cms.

17 "Bengaluru hospitals demand Aadhaar details, patient dies", *The New Indian Express*, August 18, 2020, https://www.newindianexpress.com/cities/bengaluru/2020/aug/18/bengaluru-hospitals-demand-aadhaar-details-patient-dies-2184858.html.

Appropriate Roles of Actors

Roles of the State

THE STATE AS THE SINGLE ID PROVIDER

THE STATE AS ENDORSING OTHER ID PROVIDERS

THE STATE AS BROKER OF ID PROVIDERS

Models of Creation

SERVICE AGREEMENT

BUILD OPERATE TRANSFER/ CONCESSION AGREEMENT

Vendor Lock-in and Interoperability

INTEROPERABILITY

OPEN STANDARDS APPROACH

OPEN SOURCE APPROACH

Research and Writing by **Amber Sinha & Shruti Trikanad**

A factor that characterises a digital ID system is the actors that are involved in developing and managing it, and the role the State plays in this process. In this section, we discuss different roles assumed by States in ID systems around the world, the models of creation they have employed, and the policy consequences of these decisions. As part of this, we also address achieving interoperability through design of the system, and some common issues such as that of vendor-lock in.

A key policy issue that surrounds digital ID discourse is the role played by the state in the development, design and implementation of the digital ID system. This raises questions about what the appropriate role of the state is, to what extent must it intervene not just in regulation but also the development of identity systems, and how best to determine suitable sites of intervention. As opposed to private firms which invest in innovation with the expectation that this activity will generate profit for the company, states are meant to be driven by public interest motives.

A private firm will ordinarily focus on four primary questions:

- Is the technology a solution, or a better solution, to a market need? (Right technology)
- Is the market for the technology large enough? (Right market size)
- Is the cost of bringing the technology to market sufficiently low? (Right cost of commercialization)
- Is the technology performance, market, and commercialization cost certain enough? (Right market certainty).[18]

On the other hand, appropriate roles for the government in deployment of technology include "any actions that will assist the private sector in meeting public good objectives that cannot be accomplished, or will not be accomplished, by the private sector alone without government participation or leadership."[19] Ensuring the above requires multiple steps, some of which are listed below:

1. A consultative process to arrive at the definition of public good outcome. These need to be debated and decided by the legislative and executive branches and established as basic mission requirements of government agencies. Further, they need to involve significant public consultation and take into account views of different stakeholders. Within any democratic setup, a specific desired public good outcome is defined through adequate debate and consensus building.

2. Legislative and executive branches should not arbitrarily eliminate specific deployment tools or mechanisms from consideration, but rather focus on ensuring broad stakeholder collaboration to select the appropriate tools for each circumstance and then insist on getting the desired results out of the tools used.

3. Narrow down the set of steps that require the state's intervention to meet the

18 Jon Pietruszkiewicz, "What are the Appropriate Roles for Government in Technology Deployment? A White Paper with Author's Response to Comments", *NREL* (1999), https://www.nrel.gov/docs/gen/fy00/26970.pdf

19 Jon Pietruszkiewicz, "What are the Appropriate Roles for Government in Technology Deployment? A White Paper with Author's Response to Comments", *NREL* (1999), https://www.nrel.gov/docs/gen/fy00/26970.pdf

public good objectives, and restrict state intervention to only those steps.

4. Ideally, the state should restrict itself to pre-competitive activities leaving competitive activities for the private sector, unless required otherwise by competition regulators.[20]

5. Public funding must be evaluated appropriately for the following categories of activities:[21]

   - Technologies developed entirely for government use
   - Technology requirements imposed by regulatory agencies
   - Technologies having compelling societal benefits
   - Technologies that advance commerce

In the case of digital ID, arguments for state funding are often made on the basis of the third criteria above. While there are multiple factors at play in determining the societal benefits of identity technologies, it must be acknowledged that they have immense power, both in enabling constructive engagement between citizen and state, and as a potential tool to cause harm in the hands of the state.[22] The fourth criterion of the potential of identity technologies to advance commerce is also provided, and this must be evaluated carefully to ensure that broad classes of consumers should benefit, directly or indirectly, from the deployment of the technology.

1. Roles of the State

Below we list some examples of roles assumed by the state.

1.1. The State as the single ID provider

In India, the digital ID project, Aadhaar, has a single identity provider, the Unique Identity Authority of India and falls within the "classic hierarchical, centralised, command-and-control paradigm."[23] Such identity systems are marked by concentration of power in the hands of one entity controlled by the state. It is also marked by single points of failure and inadequate preparedness for contingencies.

20 Frist, B.; Domenici, P.; Lieberman, J.; Rockefeller, J. Letter Attachment Statement of Guiding Principles for the Science and Technology Caucus. Washington D. C.: United States Senate, January 28, 1998.

21 Environmental Engineering Division of the Council on Engineering of the American Society of Mechanical Engineers (ASME), "Position Statement on the Role of Federal Government in Environmental Technology Development." in Jon Pietruszkiewicz, "What are the Appropriate Roles for Government in Technology Deployment?", https://www.nrel.gov/docs/gen/fy00/26970.pdf

22 Kaliya Young, "Key Differences Between the U.S. Social Security System and India's Aadhaar System", *New America*, 2019, https://www.newamerica.org/fellows/reports/anthology-working-papers-new-americas-us-india-fellows/key-differences-between-the-us-social-security-system-and-indias-aadhaar-system-kaliya-young/.

23 Sunil Abraham, "Building Trust: Lessons from Canada's Approach to Digital Identity", *Observer Research Foundation*, June 5, 2020, https://www.orfonline.org/research/building-trust-lessons-from-canadas-approach-to-digital-identity-67360/.

Several critical processes rely on the operability of the digital ID infrastructure, while some of the systems may rely on the ID exclusively. The result of such an approach is effectively a state-enforced market monopoly of identity providers, which leads to classic anti-competitive and anti-consumer outcomes.

1.2. The State as endorsing other ID providers

In Estonia, Smart ID and Mobile ID are provided by private entities.[24] Mobile ID requires a special SIM card to be inserted into the user's smartphone; and one needs a smartphone or tablet to use the Smart ID application.

Digilocker, a document storage service provided by the Indian government, adopted a mechanism to identify users and allow them to authenticate using the Facebook Login service.[25,26] However, this option was later discontinued.

India's Aadhaar ID system also relies heavily on the use of One-time Passwords (OTPs) to authenticate citizens. In this case, the cell service provider, which is usually a private entity, plays the role of ID provider, as individuals are identified by their phone numbers.

1.3. The State as broker of ID providers

In the UK and Canada, we see a model where the State acts as a broker of identity systems provided by multiple public and private entities. The role of the state is in providing standards for identity verification for different levels of identity assurance, and private identity providers validate residents' identity and provide them login credentials for authentication. In order to maintain user privacy, identity providers do not know which government service the resident is attempting to access, and the government service does not know which identity provider has been used to verify residents' identity. Moreover, different government services require varying levels of identity assurance, which allows residents who may not have all the required documentation to access a wider pool of services than if all government services demanded one single high standard of identity assurance.

2. Models of Creation

Even where the State is the provider of the digital ID, it typically utilises private services in building the ID system, through public-private partnerships. As digital ID systems are technically complex to build and require significant investment, many State ID providers are delegating some of the services involved in building, operating, or managing the ID system to private companies. This may also increase the State's public service efficiency, as the expertise and services involved in operating an ID system are highly specialised, and therefore benefit from having

24 "Smart-ID", E-Identity, last accessed November 12, 2021. https://e-estonia.com/solutions/e-identity/smart-id.

25 Digilocker User Manual, https://web.archive.org/web/20210408140853/https://digilocker.gov.in/assets/img/DigiLocker-User-Manual.pdf.

26 "Facebook Login", Facebook for Developers, last accessed November 12, 2021. https://developers.facebook.com/docs/facebook-login/.

partnerships between different actors.[27] Perhaps the biggest advantage to using private services is that it removes the requirement of a big upfront investment by the government; costs are shouldered by the private investor, and typically managed over the contract period.[28]

The degree of private firm involvement varies, depending on the capacity of the State, private sector expertise and profitability. Amongst other things, the private actor can be involved in (1) designing and building identity infrastructure, (2) financing initial and ongoing capital investments, (3) key services in operating and maintaining digital IDs throughout their lifecycle, including registration, issuance, authentication, etc.[29] Public-private partnerships in the creation of an ID system can typically be categorised into one of the following:

2.1. Service agreement

Here, the government contracts with a private firm to undertake a specific role in one or more stages of the digital ID lifecycle. The firm may either receive payment from the government depending on its performance, or it may get revenue directly from consumers.

In **Nigeria**, the National Identity Management Commission (NIMC) is in charge of its National Identity Database and e-ID card, but it partnered with financial service companies to issue a smartcard (used for authentication) that is also a payment card.

In **Estonia, Finland and Norway**, the national digital ID system is operated by the State, but private entities offer and operate one mode of authentication through a mobile sim.

2.2. Build Operate Transfer/ Concession agreement

These agreements are typically for a more significant role in the ID project, entailing higher risk and investment on the part of the private actor. Here, the private actor is almost solely in charge of designing, building and operating a project, usually for a fixed concession period. The public authority typically grants the private company the right to use its assets for a fixed period, and at the end of the contract the authority recovers its assets.

Chile: In 2013, in order to modernize its national identification system, Chile's Registro Civil e Identificación (SRCeI) awarded a 10 year concession to a private firm, Morpho Chile, to upgrade, build, install, and maintain new hardware and software, integrate existing databases, train SRCeI staff, and personalize eID

27 "Public private partnership models for national identity programs", Thales, last accessed November 12, 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/public-private-partnerships.

28 "Public private partnership models for national identity programs", Thales, last accessed November 12, 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/public-private-partnerships.

29 Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation (July 2016), https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf. See pages 30-32 for more details.

smartcards. The government continues to operate the system and manage the collected data, but it was the private firm that invested significant capital for the upgrade, and is paid a fee per document issued by the government.[30]

Albania: Pursuing similar goals of modernizing its national identification system, Albania's Ministry of Interior Affairs awarded a full concession to a private firm, Aleat, to design, build, operate, and maintain an eID system. This model differed from the one seen in Chile; the firm was tasked with building an entirely new database, for which it enrolled citizens, collected and stored their data, and issued eIDs at a fee. A copy of the collected data was shared with the government, and they were also paid a portion of the fee collected.[31]

3. Vendor Lock-in and Interoperability

On building digital ID systems, a universal problem identified by governments has been that of inflexibility, caused by having to depend on select solution providers. This is often because while the identity solution uses the current best technology and is intended to meet the needs of the current population, it does not adapt to the growing needs or advancement in technology. Sometimes, these systems are developed in silos, on proprietary technologies from multiple technology partners, and struggle to operate with each other or be upgraded or replaced. In fact, the lack of provider and technology neutrality was identified by several bodies tasked with implementing national ID systems as a major concern, particularly by those countries in Africa that recently introduced digital ID systems.[32] Thus, this is a major concern to consider when conceiving a digital ID system, to ensure easy upgrades at minimum cost and operational risk. For this, there are several factors to consider.

3.1. Interoperability

"Interoperability" can be seen as: *a constantly shifting interconnection among ID users, ID providers, and ID consumers that permits the transmission of Digital ID information between them via a secure, privacy-protected channel.*[33] In this context, is the characteristic of a system whose interfaces are completely understood, to work with other products or systems, (present or future), without any restrictions.[34]

30 Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation (July 2016), https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf. Page 36.

31 Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation (July 2016), https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf. Page 35.

32 Chris Burt, "Two ideas to break down vendor lock-in in foundational biometric ID systems launch at ID4Africa 2019", *Biometric Update*, June 20, 2019, https://www.biometricupdate.com/201906/two-ideas-to-break-down-vendor-lock-in-in-foundational-biometric-id-systems-launch-at-id4africa-2019.

33 John Palfrey and Urs Gasser, "Digital Identity Interoperability and eInnovation", *Berkman Publication Series* (2007). https://cyber.harvard.edu/pubrelease/interop/pdfs/interop-digital-id.pdf

34 "Best Practices for Adopting Open Standards", Open First Whitepaper: Open Standards, last accessed November 12, 2021. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/open-source-software/open-first-whitepaper/open-first-whitepaper-standards.html#best-practices-for-adopting-open-standards.

When viewed through the perspective of its major stakeholder groups, it looks like this:[35]

1. Individuals (or users, subjects) – who want to be able to share aspects of their identity efficiently and securely regardless of the service or platform, with at least some level of ID portability;

2. Relying parties (usually providers of services individuals want to use) – who want easy and secure access to accurate, timely, and relevant information about individuals from any source to maximize the value of their trust relationships and better serve their users, while limiting their own exposure to risks of a data breach;

3. ID providers – who want effective and sustainable means to provide Digital ID services to any user and any relying party; and

4. Society as a whole – to balance convenient and secure authentication and accreditation with other social needs such as privacy.

Interoperability is an important factor to consider here, as it directly influences flexibility and vendor lock-ins. Often, different components of an ID system (such as a civil registry, authentication system, etc) are incompatible with those made by a different provider, forcing the government to rely on the same vendor, often at some cost. Similarly, ID holders may want to be able to expand the scope of the access their ID gives them, but are unable to because different components of the system are unable to communicate with each other.[36]

3.2. Open standards approach

Building an identity platform using open standards may aid in ensuring interoperability and avoiding vendor lock-in. Open standards are simply a set of rules designed to do a specific job in technology. They comprise file formats, protocols and application interfaces that can be implemented by everyone since the specifications are available at no cost, and since their development and standardization is open and transparent.[37]

This approach uses these agreed upon standards to create a framework for developers by defining the components of a system and how they interact with each other; this allows the developer a variety of choices from the market in terms of components that can be substituted for each other.[38] The fixed standards result in substitutable and compatible technical components, and the standardized

35 John Palfrey and Urs Gasser, "Digital Identity Interoperability and eInnovation", *Berkman Publication Series* (2007). https://cyber.harvard.edu/pubrelease/interop/pdfs/interop-digital-id.pdf

36 Putting government back in control: Solving vendor lock-in with open standards (2019), https://www.id4africa.com/2019/almanac/SECURE-IDENTITY-ALLIANCE-SIA.pdf.

37 Best Practices for Adopting Open Standards", Open First Whitepaper: Open Standards, last accessed November 12, 2021. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/open-source-software/open-first-whitepaper/open-first-whitepaper-standards.html#best-practices-for-adopting-open-standards.

38 Putting government back in control: Solving vendor lock-in with open standards (2019), https://www.id4africa.com/2019/almanac/SECURE-IDENTITY-ALLIANCE-SIA.pdf.

interfaces (APIs) enable these components (and any new ones that are added later) interact with each other. Thus, through this model, governments can use existing modules and components from several existing ID technology providers, and are not limited by any one vendor or hardware.

India: Aadhaar

The Aadhaar program utilises the open standards approach in its largely centralised structure, with its single ID provider (the government) and its centralised data storage system. It does this for the dual purpose of encouraging interoperability, and reducing upfront infrastructural costs. Aadhaar uses an open standards-based interoperable platform to allow easy plug-and-play for various service delivery/support systems; this is supported by defined Application Programming Interface (APIs) and standards for ecosystem partners to leverage while building their solutions.[39] This includes core authentication APIs (both biometric and OTP requests), and APIs for the plug-and-play services that can be added on. For its hardware, it has distributed commodity computing running Linux machines on open source fully parallelizable, such that processes happen concurrently on different nodes. [40]

Canada: PCIM

This approach has also been used in Canada, where the ID system is not centralised, with several ID providers, both public and private, and different credentials, authentication factors etc. The Pan-Canadian approach for identity management is an agreement of principles and standards to develop solutions for use by all Canadians. It has an overarching framework, the *Pan Canadian Trust Framework (PCTF)*, that amongst other things, sets standards that allow different platforms, services, architectures, and technologies to work interoperably to create a digital ID ecosystem. The PCTF supports the acceptance of trusted digital IDs and relationships by defining a set of agreed-upon standardized trusted processes that can be mapped to existing business processes, independently assessed using conformance criteria, and certified to be trusted and interoperable within the many contexts that comprise the digital ecosystem. The standards it sets has 2 main purposes:

1. Defining participant roles and associated identity-related functions within the ecosystem.

2. Facilitating interactions within the ecosystem by defining requirements and guidelines that establish a level of trustworthiness for functions performed by ecosystem Participants.

39 ITU document

40 Dr. Pramod Varma, "*Big Data at Aadhaar*", July 31, 2012 (Presentation), https://www.slideshare.net/regunathbalasubramanian/aadhaar-at-5thelephantv3/10-Open_APIs_Aadhaar_Services_Core.; Ambika Choudhury, "The Birth Of Aadhaar To Address Problems Of Fraud And Duplication In Individual Identities: Aadhaar Chief Architect Dr Pramod Varma", *Analytics India Magazine*, April 1, 2020, https://analyticsindiamag.com/the-birth-of-aadhaar-to-address-problems-of-fraud-and-duplication-in-individual-identities/.

3.3. Open source approach

Open source platforms, typically built with the use of open standards, is another approach to avoid the vendor lock in problem. Open source systems are designed to be publicly accessible, allowing any developer to inspect, modify or enhance them. With this, the government ID provider can build or use an existing (vendor neutral) open source platform concurrently with multiple vendors and service providers, allowing a flexible and scalable identification system.

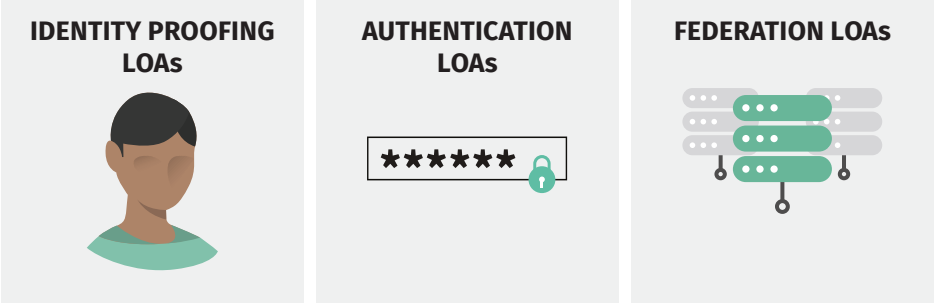
The governments of Morocco and Philippines have been using the Modular Open Source Identity Platform (MOSIP) platform to build their foundational digital ID platforms.[41] MOSIP is a modular, open source platform that countries (and other ID issuing organisations) can adopt and customize to their requirements.[42] It is designed as a core foundational identity layer, with a set of modules that can be added as per the desired design, and is completely vendor neutral. As an open-source platform, service providers can be used interchangeably, avoiding vendor lock-in.[43]

41 Chris Burt, "MOSIP open digital identity initiative partners up to enhance platform for developing countries", *Biometric Update*, October 1, 2020, https://www.biometricupdate.com/202010/mosip-open-digital-identity-initiative-partners-up-to-enhance-platform-for-developing-countries.

42 "Principles of Engagement", *MOSIP*, April 2019, https://www.mosip.io/uploads/resources/5cc84b0a08284Country%20Engagement%20Principles_v2.pdf.

43 Chris Burt, "Two ideas to break down vendor lock-in in foundational biometric ID systems launch at ID4Africa 2019" *Biometric Update*, June 20, 2019, https://www.biometricupdate.com/201906/two-ideas-to-break-down-vendor-lock-in-in-foundational-biometric-id-systems-launch-at-id4africa-2019.

Establishing Trust



Research and Writing by **Amber Sinha**

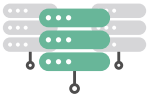
At its core, digital ID seeks to solve the trust problem—how can an individual demonstrate who they claim to be, such that verifying parties may trust them. The current models for establishing this trust are largely top-down, with the primary motive of reducing identity fraud. However, there are multiple factors at play in determining the appropriate threshold for establishing trust which should guide the design of identity systems.

1. Reconceptualising Levels of Assurance

The popular meme by Peter Steiner in The New Yorker, 'On the internet, nobody knows you're a dog,'[44] is an oft-quoted phrase in digital ID design discussions. As stated in the latest version of the Levels of Assurance technical guidelines by NIST,[45] 'when accessing some low-risk digital services, "being a dog" is just fine; while other, high-risk services need a level of confidence that the digital ID accessing the service is the legitimate proxy to the real life subject.' The most recent guidelines recognise the need for dynamic levels of assurance, retiring the 'the concept of a level of assurance (LOA) as a single ordinal that drives implementation-specific requirements' and instead suggesting combining 'appropriate business and privacy risk management side-by-side with mission need.' The essence of the guidelines are captured below:

44 Glenn Fleishman, "Cartoon Captures Spirit of the Internet", *The New York Times*, December 14, 2000, https://web.archive.org/web/20171229172420/, http://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html.

45 NIST: Digital Identity Guidelines (June 2017), https://pages.nist.gov/800-63-3/sp800-63-3.html.



Identity proofing LOAs	Authentication LOAs	Federation LOAs
IAL1	**AAL1**	**FAL1**
Attributes, if any, are self-asserted or should be treated as self-asserted; there is no proofing process.	Provides some assurance that the claimant controls an authenticator registered to the user. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.	Permits the relying party to receive a bearer assertion from an identity provider. The identity provider must sign the assertion using approved cryptography.
IAL2	**AAL2**	**FAL2**
Either remote or in-person identity proofing is required using, at a minimum, the procedures given in SP 800-63A.	Provides high confidence that the claimant controls authenticator(s) registered to the user. In order to authenticate at AAL2, claimants must prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.	Adds the requirement that the assertion be encrypted using approved cryptography such that the relying party is the only party that can decrypt it.
IAL3	**AAL3**	**FAL3**
In-person or supervised-remote identity proofing is required. Identifying attributes must be verified through examination of physical documentation as described in SP 800-63A.	Provides very high confidence that the claimant controls authenticator(s) registered to the user. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a “hard” cryptographic authenticator that provides verifier impersonation resistance.	Requires the user to present proof of possession of a cryptographic key reference to in the assertion and the assertion artifact itself. The assertion must be signed using approved cryptography and encrypted to the relying party using approved cryptography.

By introducing pseudonymous identifiers, and encouraging 'minimizing the dissemination of identifying information by requiring federated identity providers (IdPs) to support a range of options for querying data, such as asserting whether an individual is older than a certain age rather than querying the entire date of birth,' the guidelines clearly express its intent for privacy preserving decision making in the design of identity systems. However, it is limited in its view of approaching privacy and business interests are the primary competing values. This approach further continues the top-down approach in designing identity solutions by centering reduction of identity fraud. A competing value that is consistently ignored by LoA technical documents including the above, is that of inclusivity This is all the more perplexing as inclusivity has fast emerged as one of the primary rationales for digital ID systems.[46] Centering 'inclusivity' in digital ID design would entail that the interest of individuals to not be excluded from services, benefits, entitlements and exercise of rights is a driving value.

Let us consider what inclusivity may (or may not) look like through an example. One of the biggest concerns around the Aadhaar project is its exclusionary impacts.[47] The proviso to Section 7 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act states that "if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service." This is an example of a legal provision attempting to factor the need for inclusivity in the implementation of an identity system. Despite this attempt, overall, it is an inadequate measure for the following reasons. First, instead of building inclusivity into the design of the digital ID solution, it seeks to retrospectively 'fix' through law what technology has 'broken'. Second, the nature of protection it provides is limited and covers only those who have not been 'assigned' an Aadhaar Number yet. Therefore, those who have not applied for the Aadhaar Number or are unable to use the service due to technical glitches are offered recourse for inclusion.

Increasingly as digital ID solutions are used in exercise of both civil and political rights (use of identity in elections), and economic and social rights (access to essential benefits and services), the denial of services due to faulty design as well as failures of identity solutions imposes both real-life human costs as well as denial of fundamental human rights. Rather than top-down approach where the 'business' or 'state' interests of those in charge with making decisions about what level of assurance to use dictates the design of identity solutions, it is imperative that levels of assurance are designed with 'inclusivity' as its guiding principle.

2. Recommendations

2.1. Selecting LOA based on privacy, inclusivity, and reduction of fraud

The digital ID system should be designed in such a way that a Relying Party is able

46 "Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable", *World Bank*, August 14, 2019, https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable.

47 Prashant Reddy, "Aadhaar: Amid the debate about privacy, the more pressing issue of exclusion has been forgotten", *Scroll.in*, March 29, 2017, https://scroll.in/article/833080/aadhaar-amid-the-hullabaloo-about-privacy-the-more-pressing-issue-of-exclusion-has-been-forgotten.

to select levels of assurance based on consideration of privacy, inclusivity and reduction of fraud.

2.2. Drawing from proportionality standard

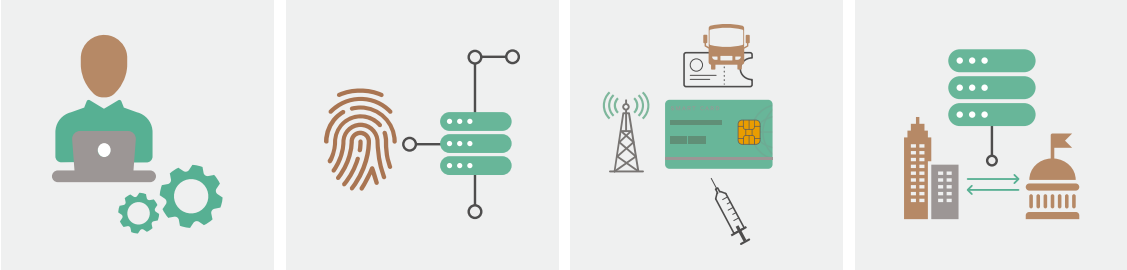
IAL is selected to mitigate potential identity proofing errors in a privacy-preserving and inclusive manner. The definition of 'privacy-preserving' ought to draw from the proportionality standard.

2.3. Non-negotiable degree of inclusivity

If we look at the Authenticator Assurance Levels under NIST's LoA, the range of choices available to individuals reduces as we go up to the levels. AAL1 requires single-factor authentication using a wide range of available authentication technologies. In AAL2, proof of possession and control of two different authentication factors is required through a secure authentication protocol. In AAL3, proof of possession of a key through a cryptographic protocol is required. An additional consideration that needs to be introduced is the degree of inclusivity that is non-negotiable. Access to civil and political rights, and social and economic rights may require the highest degree of inclusivity, and consequently, the need for a range of option of authentication technologies.

Technological Design Choices

Appropriate Use of Technology

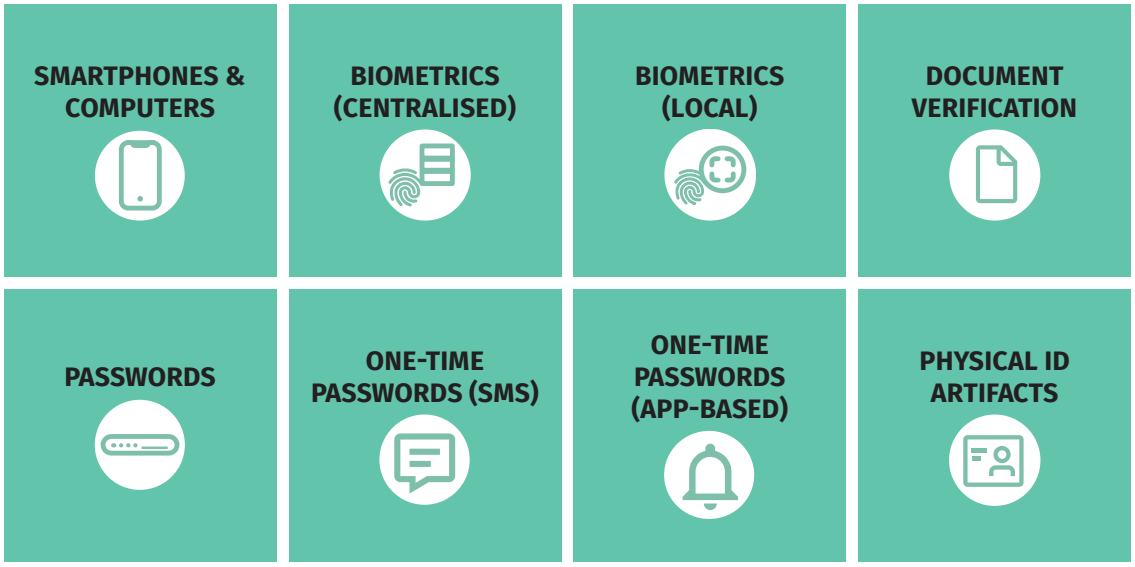


Information Architectures

SOURCE OF IDENTITY OR TRUST	STORAGE	CONTROL AND FAULT TOLERANCE	RISK OF RE-CENTRALISATION

Credentials, Identification and Authentication Factors

BIOMETRIC FACTORS	DOCUMENT VERIFICATION	PSEUDONYMOUS IDENTIFIERS	QR CODE
MICROCHIP-BASED CARDS (SMART CARDS)	CONTACTLESS CARDS	SECURITY KEYS	SMARTCARD OR SECURITY KEY WITH BIOMETRICS



Research and Writing by **Divyank Katira**

The use of digital technologies to aid the identification of individuals, the subsequent authentication of their identity, and to allow authorisation on their behalf is a common practice in emerging national ID schemes. We describe principles for the appropriate use of digital technologies in ID systems, common technical architectures that have emerged in their design, and summarise some of the key characteristics of these digital technologies.

1. The appropriate use of technology

The use of digital technologies to aid the identification of individuals, the subsequent authentication of their identity, and to allow authorisation on their behalf is a common practice in emerging national ID schemes. In this section, we present principles to achieve privacy, security, and inclusivity.

1.1. Digital technologies can supplement existing manual processes but not entirely replace them

Despite a rapid rate of advancement in recent decades, the technologies that are used to compose digital ID systems still suffer from reliability issues. Faults in software and hardware systems, gaps in network connectivity between them, and their inability to accurately and adequately represent people's identities can all lead to exclusion of individuals from benefits and services. For instance, a study found that about one-fifth of transactions in India's Aadhaar-enabled Payments System failed due to technical reasons (17.03% due to biometric mismatch, 3.71%

due to other technical issues).[48] Even large technology companies with well-funded engineering and operations teams only guarantee 99.99% uptime for their cloud offerings, which roughly translates to one hour of downtime in a year.[49] While not all of these faults will lead to denial of access to benefits or services, their outcome can be particularly grave in cases where they prevent access to essential services such as food distribution or healthcare. For this reason, it is necessary to have robust manual processes in place for when technological systems fail.

In addition to being susceptible to unintentional faults, technological solutions are also susceptible to cyberattacks. Having well-tested human-operated processes to fallback upon also makes identity infrastructure and the services that rely on it less vulnerable to cybersecurity threats.

1.2. Storing biometric data in central repositories is ill-informed and not sustainable

Another trend that we have observed in national digital ID systems is the use of biometric information, such as fingerprint or iris scans, to identify individuals and then authenticate their identity. In comparison to knowledge and possession factors, biometric factors allow for quick, cost-effective and convenient authentication as they do not require users to remember a secret password or present costly physical tokens such as smartcards or security keys at the point of authentication. They also serve as highly accurate identification factors for most people. But from a cybersecurity perspective, biometrics are weak authentication factors. They are immutable and, in most cases, publicly visible. This makes them impossible to change in case the database used to store them is breached and also prone to forgery. To understand this, we can compare them to passwords, which have served as a de-facto authentication factor on the web for the past two decades. Over this time a total of at least 8.4 billion passwords have been leaked through successive data breaches.[50] Without the invention of the mythical unhackable database, it is likely that the use of centralised biometric authentication will yield similar results over time. Leaks of biometric information are also more severe than passwords as they cannot be reset after a leak. As such, the appropriate use of biometrics is limited to local authentication i.e. when the storage and matching of biometrics takes place on an end-user device or credential such as a cellular phone, smartcard, or security key.

1.3. Foundational ID systems must ensure separation of responsibilities

Unlike Functional ID systems which are designed and built for a specific purpose, Foundational ID systems are general-purpose systems that can be used for many different purposes. They are responsible for conducting the processes of

48 Padmanabhan Balasubramanian et al., "Fintech For The Poor: Do Technological Failures Deter Financial Inclusion?", *SSRN* (2021), https://ssrn.com/abstract=3840021.

49 "Compute Engine Service Level Agreement (SLA)", *Google Cloud*, last accessed November 12, 2021. https://cloud.google.com/compute/sla; "Amazon Compute Service Level Agreement", *Amazon Web Services*, last accessed November 12, 2021. https://aws.amazon.com/compute/sla/.

50 Lance Whitney, "Billions of passwords leaked online from past data breaches", *TechRepublic*, June 9, 2021, https://www.techrepublic.com/article/billions-of-passwords-leaked-online-from-past-data-breaches/.

identification, authentication, and authorisation. However, the ease with which such systems allow processes to incorporate these mechanisms creates a potential for their misuse or overuse.

As an example, we can look at Nigeria's National Electronic Identity Card. It is a Foundational ID system that allows for the creation of 'applets' which enable its use for different purposes. One such applet is e-Transport, which allows the use of the ID card as a payment system for travel through public transportation.[51] Through such use, the National Identification Number, which is an identity-linked identifier, is collected and linked to an individual's movements as they travel through public transport — a purpose that should not require any identification documents. This is a case of misuse of identification functionality in a Foundational ID System. Since the identification and authentication mechanisms are intertwined and rely on the same identifier, the system unnecessarily identifies individuals and creates a log of their movements when the goal of the system here should only be to authenticate an individual and check whether they have loaded sufficient funds onto their card to make the journey. A workaround to this issue is to use a unique, pseudonymous identifier, which is not linked to a person's identity, for each different purpose that the ID card is used for. The Web Authentication standard supports such anonymous authentication.

Another case of conflation of responsibilities in a Foundational ID system was seen in India's Aadhaar ID program. Here, there were multiple instances where the process of authentication was used as a proxy for authorisation, leading to actions being taken on an individual's behalf without their informed consent:

- A telecom operator which also operates a payment service mistook authentication of individuals, which was required for KYC purposes, as authorisation to open an account on its payment service. This led to its users' subsidy payments being silently redirected to this new account which they did not even know existed.[52]

- Some individuals who used Aadhaar to authenticate themselves to receive vaccinations as part of the COVID-19 immunisation drive were also enrolled in a Unique Health ID program, without their consent.[53]

Foundational ID systems, owing to their expansive scope, should be carefully designed and strictly regulated through both technical and legal means to prevent such abuse. They must ensure separation of the responsibilities of identification, authentication and authorisation and only use them where necessary.

51 "Mapping Digital Identity Systems: Nigeria", Digital Identities: Design and Uses, November 03, 2020. https://digitalid.design/research-maps/nigeria.html.

52 Anand Venkatanarayanan and Srikanth Lakshmanan, "Aadhaar Mess: How Airtel Pulled Off Its Rs 190 Crore Magic Trick", *The Wire*, December 21, 2017, https://thewire.in/banking/airtel-aadhaar-uidai.

53 Mehab Qureshi, "Govt Created Health IDs Without Consent, Say Vaccinated Indians", *The Quint*, June 9, 2021, https://www.thequint.com/tech-and-auto/govt-created-uhid-without-consent-say-vaccinated-indians#read-more.

1.4. Seamless public-private interoperability increases data sharing and collection

In all of the identity systems we have encountered, Governments are the primary identity providers. From civil registration to driver's licenses and voter IDs, there are many legitimate purposes for a state to identify its citizens. Even private-sector entities that take up the role of identity provider, such as the GOV.UK Verify platform[54] or various commercial identity verification services[55, 56], still rely on verification of Government-issued IDs as the source of identity attestation. Such document verification is done either manually or automatically and both processes suffer from drawbacks — they are either labour-intensive or expensive, and inaccurate.

To streamline the sharing and verification of identity data, several industrial actors[57] are attempting to develop systems and protocols through which Governments can digitally issue identity credentials to individuals. These credentials can subsequently be shared with relying parties, who can then verify them. In addition to bringing down identity verification costs for the industry and increasing accuracy of the data collected, such systems would also benefit the individuals using them as they would no longer have to carry around multiple physical documents to prove their identity.

However, enabling streamlined access to sensitive identity data, with unprecedented levels of accuracy, will likely encourage industrial actors, who have historically collected data under meaningless, coercive notions of consent[58], to collect and retain even more private information. The adoption of such technologies must be carefully considered, and governed by strong regulatory and technical barriers to prevent unfettered commercial access to this previously inaccessible identity information.

2. Typology of Information Architectures

Over time, identity systems have evolved into three distinct informational models, namely, centralised, federated, and decentralised systems. Given the wide range of uses these systems have been applied to in both the public and private sectors, these categories are sometimes overlapping and take on different meanings in different contexts.

In this section, we attempt to explain the various meanings of these terms in the context of digital ID systems by analysing three different systems that are

54 "Mapping Digital Identity Systems: UK", Digital Identities: Design and Uses, July 10, 2019. https://digitalid.design/research-maps/uk.html.

55 "Document Verification", Onfido, last accessed November 12, 2021. https://onfido.com/solutions/document-verification/.

56 "The easiest way to verify identities", *Stripe*, last accessed November 12, 2021. https://stripe.com/identity.

57 Decentralised Identity Foundation, last accessed November 12, 2021. https://identity.foundation/.

58 "A Critique of Consent in Information Privacy", *The Centre for Internet and Society*, last accessed December 7, 2021. https://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy.

representative of these three informational models: India's Aadhaar ID system[59] with its "Central Identities Data Repository" is a centralised model, Canada's Sign-in Partner service[60] is a federated model where financial institutions play the role of Identity Provider, and the W3C standards[61,62] proposed by organisations under the Decentralized Identity Foundation[63] represent a typical decentralised model which aims to create a marketplace of Identity Providers and Relying Parties for quick and efficient data sharing.

We define the *axes*[64] of centralisation/federation/decentralisation of information in digital ID systems as follows:

2.1. Source of Identity or Trust

Any identification, authentication, or authorisation operation in a digital ID system can be thought of as a transaction between an individual, an identity provider, and a relying party.

In a **centralised** system, there is a single identity provider that serves as a source of identity or trust for one or more relying parties.

A **federated** system allows an individual to choose a single identity provider from a set of choices. These can be of two types:

- Many (identity providers) to one (relying party), for example, a website that allows Google and Facebook login.
- Many (identity providers) to many (relying parties), for example, Canada and UK's ID systems that allow online access to government services. Transactions in such systems are typically mediated by a 'broker' for ease of management so that not every relying party needs to learn about every identity provider, they simply trust the broker.

The proposed '**decentralised**' or '**self-sovereign**' ID systems also provide support for many identity providers with many relying parties, with even multiple identity providers participating in a single transaction (for added assurance). They have defined open standards with the hope of spawning a network or ecosystem of independent vendors, identity providers, and relying parties that can all interoperate with ease, for efficient data collection and sharing.

59 "Mapping Digital Identity Systems: India", *Digital Identities: Design and Uses*, October 13, 2020. https://digitalid.design/research-maps/india.html.

60 Alaca, Furkan, and Paul C. Van Oorschot. "Comparative analysis and framework evaluating web single sign-on systems." ACM Computing Surveys (CSUR) 53.5 (2020): 1-34.

61 "Decentralized Identifiers (DIDs) v1.0", *World Wide Web Consortium*, last accessed November 12, 2021. https://www.w3.org/TR/did-core/.

62 "Verifiable Credentials Data Model v1.1", *World Wide Web Consortium*, last accessed November 12, 2021. https://www.w3.org/TR/vc-data-model/.

63 Decentralised Identity Foundation, last accessed November 12, 2021. https://identity.foundation/.

64 This term was used by Vitalik Buterin, who defined the axes of decentralization for software. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

CENTRALISED SYSTEM

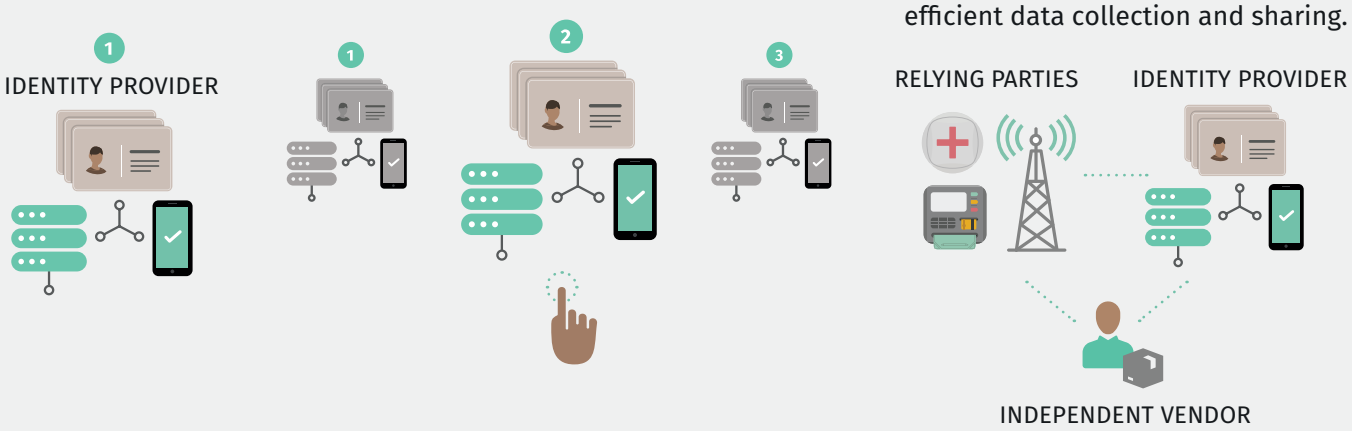
A single IDENTITY PROVIDER serves as a source of identity or trust for one or more RELYING PARTIES.

FEDERATED SYSTEM

An INDIVIDUAL can choose a single IDENTITY PROVIDER from a set of choices.

DECENTRALISED SYSTEM

A network or ecosystem of INDEPENDENT VENDORS, IDENTITY PROVIDERS, and RELYING PARTIES that can interoperate with ease, for efficient data collection and sharing.



2.2. Storage

Another important informational aspect of digital ID systems is where the vast amount of sensitive personal data and metadata handled by these systems resides. This is distributed among:

- Identity providers, who must necessarily store such data as they are responsible for issuing credentials.
- Relying parties, which may verify and discard such information or store it indefinitely, depending on their privacy policies and other incentives. It is important to note that the information architecture of the ID system does not impact the data collection or retention policies of relying parties.
- Other intermediaries, such as brokers (in federated systems) and network operators (in decentralised systems). These typically only store metadata (such as **who** accessed **what** service, **when**, and **where**), but this can also be sensitive, particularly if it is not de-identified or if there is a risk of re-identification.

In a **centralised** system, there is a large central identity provider that stores the private information of all participating individuals and metadata relating to usage of the ID. This forms a lucrative target for data breaches and presents a privacy risk as the operator of the system has insight into all activity within it.

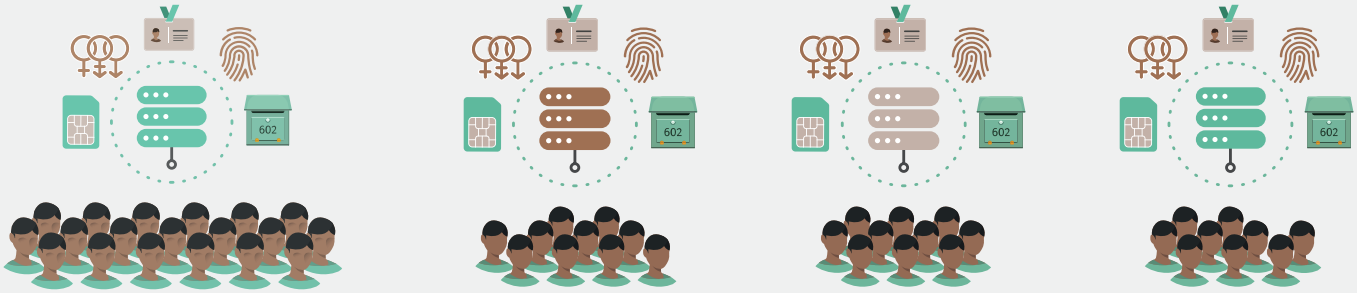
A **federated** system distributes this risk to some extent by having multiple identity providers, each of which will only store the information and metadata of a subset of users. Brokered federated systems, however, present a central trusted point through which all data passes (but is not necessarily stored) and has insight into all activity (metadata) within the system.

CENTRALISED SYSTEM

A large central IDENTITY PROVIDER stores the private information of all participating individuals.

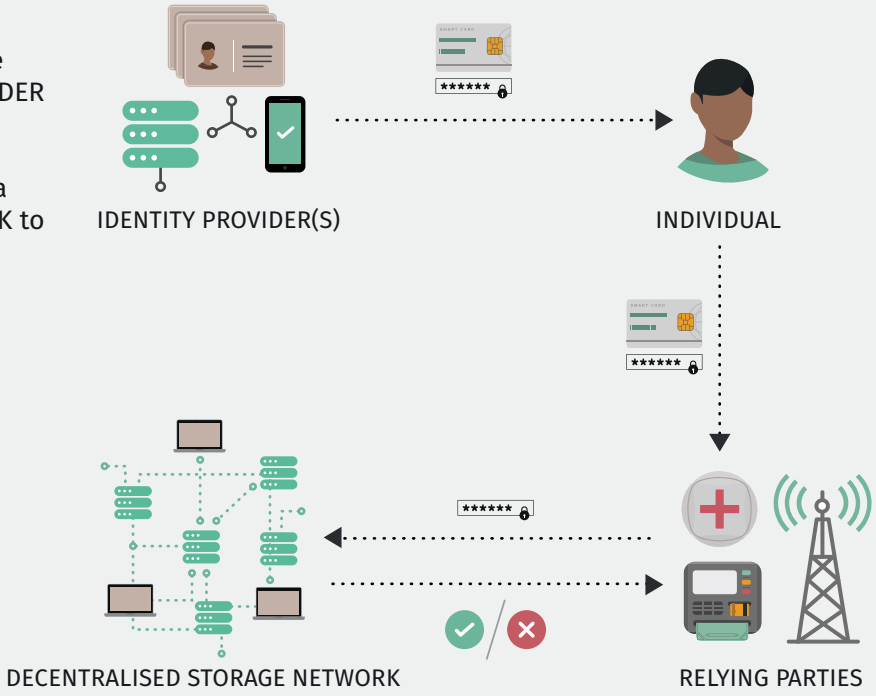
FEDERATED SYSTEM

Multiple identity providers store the information and metadata of a subset of users.



DECENTRALISED SYSTEM

Data is distributed among multiple identity providers. IDENTITY PROVIDER issues IDENTITY CREDENTIALS to the INDIVIDUAL, who shares it with RELYING PARTIES who can consult a DECENTRALISED STORAGE NETWORK to verify its authenticity.



Like federated systems, proposed '**decentralised**' or '**self-sovereign**' ID systems also distribute data among multiple identity providers. Additionally, in place of a central trusted broker, in this model an identity provider issues identity credentials to the individual, who stores it on their own device or a cloud storage solution provided by vendors of such systems. The individual, in turn, shares the credential with relying parties who can consult a decentralised storage network (typically a blockchain) to verify its authenticity. In this model, the decentralised storage network stores pseudonymised metadata about affiliations of individuals to IdPs and RPs and its operators can potentially[65] glean metadata into usage activity.

65 Halpin, Harry. "Vision: A Critique of Immunity Passports and W3C Decentralized Identifiers." International Conference on Research in Security Standardisation. Springer, Cham, 2020.

Storage of Sensitive Data Across Identity Systems

WHO SEES/STORES SENSITIVE DATA	IDENTITY PROVIDER	BROKER/ VENDOR	DECENTRALISED STORAGE NETWORK	INDIVIDUAL'S DEVICE/CLOUD STORAGE PROVIDED BY VENDOR	RELYING PARTY
CENTRALISED	✓ Single large IdP	N/A	N/A	N/A	✓
FEDERATED	✓ Multiple smaller IdPs	N/A	N/A	N/A	✓
BROKERED FEDERATED	✓ Multiple smaller IdPs	✓ Metadata	N/A	N/A	✓
DECENTRALISED/ SELF-SOVEREIGN ID	✓ Multiple smaller IdPs	N/A	✓ Metadata	✓	✓

2.3. Control and Fault Tolerance

In a **centralised** ID system, a single large identity provider is tasked with the responsibility of issuing credentials and attesting the identity of all participants. This forms a single point of failure that could go offline (say, due to technical failure) leaving users with little recourse.

A **federated** system distributes this responsibility among multiple identity providers, providing redundancy and some resilience to technical failure.

In the proposed '**decentralised**' or '**self-sovereign**' ID systems, the individual holds their own credentials or delegates this responsibility to the vendors of these systems. This allows the credential to be used even when the issuing identity provider is unavaliable/offline, as the relying party can verify its authenticity by consulting a decentralised storage network.

Additionally, while identity providers have the power to unilaterally and arbitrarily revoke credentials in all of the three models described above, the decentralised model stores a tamper-resistant record of credentials in its storage network (usually a public or permissioned blockchain), which provide some accountability in the face of abuse of power by an identity provider.

2.4. Risk of re-centralisation

Decentralisation is something that needs to be actively managed and maintained. Along each of the axes described above — source of identity, storage, and control — a decentralised or federated system can always regress to a more centralised one:

CENTRALISED SYSTEM

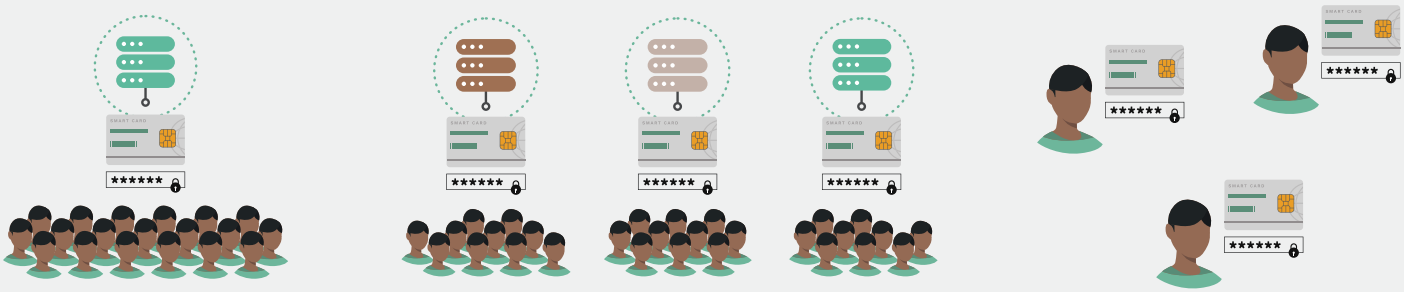
A single large IDENTITY PROVIDER is tasked with issuing credentials and attesting the identity of all participants.

FEDERATED SYSTEM

Distributes issuing credentials and attesting the identity among multiple IDENTITY PROVIDERS.

DECENTRALISED SYSTEM

The INDIVIDUAL holds their own credentials or delegates issuing credentials and attesting the identity to the vendors.



- Source of identity: One or two popular identity providers could emerge, effectively resembling a centralised system.
- Storage: The market could converge to a few popular vendors for storing credentials, creating a honeypot of sensitive data similar to a centralised system.
- Control: The decentralised storage network (usually a blockchain) must be maintained by many disparate operators. If a single operator controls a majority of nodes in the network, it would resemble a regular database controlled by a single entity, negating the tamper-resistance guarantees it provides.

3. Credentials, Identification and Authentication Factors

3.1. Choice of Identification Factors

	Privacy	Accuracy	Cost
Biometric Factors			
This refers to the use of physiological features to identify individuals.			
	LOW	**HIGH**	**HIGH**
	The immutable nature of biometrics makes it hard to place meaningful limits on their future use. Some biometric factors, such as face and gait recognition, can be deployed without an individual's consent.	Biometrics are highly accurate identification factors. However, solely relying on them leads to exclusion as they are never fully accurate.	They require the use of dedicated hardware and software.

	Privacy	Accuracy	Cost
	**Document Verification**		
	If the people being identified possess pre-existing identity documents, these can be used to identify them. Verification is either done manually or through a computer-assisted process.		
	MEDIUM	**MEDIUM TO HIGH**	**MEDIUM TO HIGH**
	The use of existing identity documents minimizes the amount of additional identifying information that is collected.	Both human and computer-assisted verification processes are prone to error. The use of security features such as holograms and microprinting can improve accuracy.	Manual processes are labour-intensive and computer-assisted processes require dedicated hardware and software.
	**Pseudonymous Identifiers**		
	Individuals can be identified by identifiers that are not linked to their identities, such as email ID, phone number or a public key.		
	HIGH	**N/A**	**LOW**
	Allows individuals to transact anonymously.		

Ratings shown are relative to each other

3.2. Choice of Identity Artifacts

	Security	Cost
	**QR Code**	
	A Quick Response (QR) code allows for convenient scanning of identity information encoded within it.	
	LOW	**LOW**
	They can be copied with ease.	These are cheap to issue and can be printed on a piece of paper.
	**Microchip-based Cards (Smart Cards)**	
	Identity attributes are encoded into an Integrated Circuit chip that is embedded into a physical document.	
	MEDIUM TO HIGH	**MEDIUM**
	The chips are typically secured by a second factor, such as a PIN.	Costlier than paper-based ID documents.

	Security	Cost
	**Contactless Cards**	
	These are similar to smart cards but can be scanned over a small distance.	
	LOW	**MEDIUM**
	They can be remotely accessed. Their use is limited to low-risk scenarios for convenient access.	Cost is similar to smart cards.
	**Security Keys**	
	A security key is a thumb drive shaped device with an embedded chip for storage of identity attributes.	
	MEDIUM TO HIGH	**MEDIUM**
	These are typically used as a second factor.	Cost is similar to smart cards and contactless cards.
	**Smart Card or Security Key with Biometrics**	
	A fingerprint scanner is embedded into a smart card or a security key.	
	HIGH	**HIGH**
	Integrating possession, biometric, and knowledge factors into a single device makes them highly secure.	Costlier than regular smart cards or security keys.
	**Smartphones & Computers**	
	A virtual credential can be issued that can be stored on a smartphone or a computer.	
	MEDIUM	**HIGH**
	Security properties are similar to smart cards and security keys. However, they are connected to the internet, making them more vulnerable.	This is only cost-effective if the intended users of the ID system already possess these devices.

Ratings shown are relative to each other

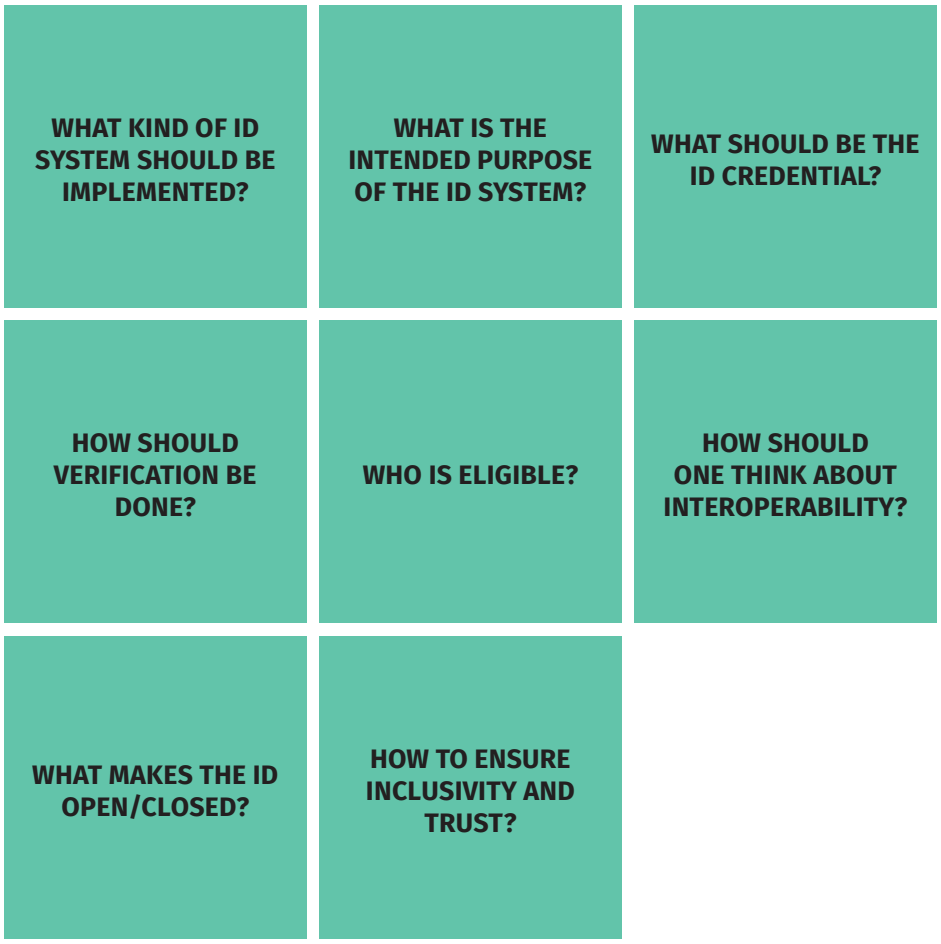
3.3. Choice of Authentication Factors

	Security	Privacy	Cost
	**Biometrics (Centralised)**		
	Biometric information is used to authenticate individuals. Centralised refers to storing many biometrics in a central database.		
	LOW	**LOW**	**LOW TO MEDIUM**
	Biometrics are immutable and, in most cases, publicly visible. This makes them prone to forgery and impossible to change in case of a breach.	Storing biometrics on a large central database makes them vulnerable to breach.	A small number of biometric readers are required at points of authentication.
	**Biometrics (Local)**		
	This refers to matching and storing of biometric information on the end-user device performing authentication, such as a smartphone or security key.		
	MEDIUM	**HIGH**	**HIGH**
	In this method, biometrics are typically used as a secondary factor.	Biometric information does not leave the device under the control of the individual.	The individual being authenticated must possess a device capable of biometric authentication.
	**Document Verification**		
	A pre-existing identity document is used to authenticate an individual. Verification can be done either manually or through a computer-assisted process.		
	MEDIUM TO HIGH	**MEDIUM**	**HIGH**
	Both human and computer-assisted verification processes are susceptible to forgery. The use of security features such as holograms and microprinting can improve security.	The physical document may have personal information printed on it — potentially revealing more data than is required for the purpose of authentication.	Manual verification is labour-intensive and automated verification requires dedicated hardware and software.

	Security	Privacy	Cost
	**Passwords**		
	An individual is authenticated on the basis of a secret piece of information.		
	MEDIUM	**HIGH**	**LOW**
	This method's reliance on individuals to choose secure passwords and not re-use or share them weakens its security.	Allows individuals to be authenticated anonymously.	Passwords are highly cost-effective authentication mechanisms.
	**One-Time Passwords (SMS)**		
	An OTP is sent to an individual over SMS.		
	LOW	**MEDIUM**	**MEDIUM**
	SMS is not considered a secure communication method.	The individual's phone number needs to be disclosed for authentication.	A cellular connection is required.
	**One-Time Passwords (App-based)**		
	In this method, after an initial registration phase, an OTP is automatically generated.		
	HIGH	**HIGH**	**MEDIUM**
	Typically used as a secondary factor, this is considered a security best-practice.	Typically used as a secondary factor, this is considered a security best-practice.	A cellular connection is not needed during authentication, but a smartphone or other device is required.
	**Physical ID Artifacts**		
	If one has been issued, it can also be used for authentication.		
	LOW TO HIGH	**MEDIUM TO HIGH**	**LOW TO HIGH**
	Depends on the artifact chosen (see above).	The physical artifact sometimes contains personal information printed on it, revealing more data than is required for authentication.	Depends on the artifact chosen (see above).

Ratings shown are relative to each other

Policy Design Choices



Research and Writing by **Shruti Trikanad, Yesha Tshering Paul and Anubha Sinha**

With the large-scale deployment of digital ID systems in the absence of appropriate safeguards, it is critical to thoroughly examine all possible policy choices before implementation of such a system. This section attempts to provide an exhaustive list of policy choices that should be considered at the planning stage of any ID system.

1. What kind of ID system should be implemented?

- **Has there been an examination of whether a digital ID system is strictly necessary (especially if a less invasive, non-digital or paper-based ID is a viable option to achieve the same stated aims)?**
- **Does it aim to be foundational, or one of multiple functional IDs?**
- **Does it aim to serve as legal identification for all citizens and residents throughout their lifetime?**
- **Does it aim to establish uniqueness within the population?**

A "legal" identity should not automatically translate into a "digital" identity without sufficient examination into whether it is strictly necessary to serve its stated purposes. There is a tendency to push digital ID as an immediate solution to provide a legal identity to undocumented populations and enable their recognition by the State. Here, we must briefly delve into the quantum of data collected, and the resulting harms that could arise. A legal identity is an officially recognised form of documentation that certifies one's identity and usually requires only basic demographic information such as name and date of birth, sex, and country of birth or residence. A digital ID, in addition to this information, usually entails the collection of further categories of sensitive information in addition to biometric data (usually fingerprints and iris scans at minimum). The quantum of data collected about an individual could lead to profiling and surveillance, and the use of biometric information introduces additional security concerns (especially since biometrics, once compromised, cannot be changed or replaced). Under these circumstances, one must examine whether a digital ID system would better serve the need for providing legal identity over traditional or existing ID systems that can instead be improved to better serve these needs.

2. What is the intended purpose of the ID system?

- **Does it intend to act as an authoritative source of basic identity information? Does it serve as a registry or a repository of data?**
- **Does it intend to provide authentication credentials for other services?**

Based on the objectives the ID is meant to serve, a broad purpose must be allotted to the ID system, that will in turn impact key choices around its model, features and identity credentials. The determination of this purpose is also necessary to identify what data to collect from users, and therefore the privacy harms and risks posed by the system.

If the intended objective is for the ID system to serve as legal identity, then it typically follows a largely centralised model, with the government as the identity provider and with minimal involvement of the private sector in verification or authentication of the identity. Several developing countries such as India, Nigeria and Kenya have created ID systems with the main goal of providing legal identity to their residents. In India, the Aadhaar system was intended to provide a reliable identity to address problems of fraud and leakages in its welfare delivery system,

and is now used pan-India as an authoritative source of identity for most Aadhaar holders. The need for a biometric digital identity was attributed to the reliability and cost-effectiveness it allows, together with the ability to deliver online services such as banking and cash subsidy deposits, amongst others.

This may be a useful purpose when there is a lack of legal identity documentation, but countries should not so easily substitute the need for a legal identity with a digital identity. This is primarily because the privacy and surveillance risk created through a digital ID system such as this is far wider than that of a traditional legal identity model. Additionally, even when the main goal is that of providing reliable legal identity to the excluded population, often it is also intended as means to access services online using the authentication offered by the ID (otherwise the need for a digital ID must be reconsidered). While it may serve a wider purpose of allowing online/remote authentication as well, there is a big cost associated with combining the purposes of legal identification and service delivery (when the State is the provider and manager of the ID) which is the case when it serves as legal identity. The access to a large body of identity information along with continuously growing data about their activities allows for extensive State surveillance. Additionally, it creates a substantial power imbalance, as the ID provider now has the means to exclude the ID holder from key services by being in control of their ID.

As a registry of information: Estonia had a population registry and an identity documents database before it introduced its digital ID system. This ID served as a means to link the information present in various databases, and give easy and safe authorization to reuse such data so that Estonian residents need not repeatedly share information they have already divulged. Improving the ease of doing business, in Estonia as well as with the rest of the EU, was the motive that initially influenced the Estonian system. As a result, its intended purpose was to act as a data registry, and to provide reliable identity credentials (for electronic signatures). The X-road interoperability platform can also be traced back to this purpose; by linking the public and private sector e-information systems, it allows seamless communication between data systems and instant information exchanges. Similarly this is why the ID is available not only to citizens and residents, but even e-residents of Estonia.

To serve as authentication attributes: In Canada, the digital ID system was intended to create an interlinked identity management system that could be easily used to access both public and private services. This is achieved through a federated system where citizens can choose from a disparate set of identity providers to create attributes. This ID system is governed largely through standards, such that private organizations that are certified to meet such standards can be ID providers. A key difference here from the other systems seen above, is that use of this digital ID is only optional, with an alternative login method remaining available for citizens.

3. What should be the ID credential?

› **What are the authentication factors assigned to the digital ID?**

› **Have authentication factors been determined keeping in mind potential exclusions due to inability to authenticate one's identity because of infrastructural and other factors, such as lack of internet connectivity or viable fingerprints?**

An identity credential is a document, object, or data structure that can digitally affirm the identity of an individual through some method of authentication in an identity system. They typically rely on six kinds of factors to authenticate: knowledge, possession, inherence, location, behavioral, multi-modal and multi-factor.[66]

Choosing the identity credential for an ID system impacts much of the functionality and use of the ID, as it can determine the level of assurance it provides to transactions, the privacy and exclusionary risk it introduces, and is the key factor in the system with which users interact. When considered at the scale of a national ID program, it also plays a large role in the cost of implementing the ID system.

Some credentials that can be adopted in an ID system are listed below:

Static Passwords: Passwords can be static passwords, passphrases, one-time passwords, and dynamic passwords. Static passwords are reusable and may or may not expire. They are usually generated by the user, and for security purposes work best when combined with another form of authentication. Static password systems with unencrypted transmission are very vulnerable to malicious actors, and can be accessed through eavesdropping, dictionary attacks, social engineering attacks and phishing.

One Time Password (OTP): An OTP is a dynamic password that remains valid for a single authentication session. This password expires once an individual has authenticated themself, or if the allotted time elapses. OTP authentication requires access to something that an individual possesses, such as an email address or a mobile phone, and optionally something only that individual knows or has access to, such as a PIN. OTPs are considered easy to use, and compatible with a wide range of devices such as mobile phones, computers and smart tokens. They can be executed through SMS or PC-based software, and can be used as both standalone authentication or as part of multifactor authentication (which is more secure). Multi-factor authentication will additionally use another form of authentication such as biometrics, PIN or contextual data. Since OTPs are easy to use and have minimal additional requirements, they are highly scalable as well as easy to adopt. They have also been widely in use for over a decade.

However, the technology provides multiple points of attack - for instance, cloning a SIM could provide someone else with illegal access to a live OTP (and consequently enable identity fraud).[67]

66 "Core Concepts and Processes", *Digital ID: Designs and Uses*, last accessed December 7, 2021. https://digitalid.design/core-concepts-processes.html.

67 "Technology Landscape for Digital Identification", *World Bank*, last accessed August 27, 2021. http://documents.worldbank.org/curated/en/199411519691370495/pdf/Technology-Landscape-for-Digital-Identification.pdf.

OTP via Mobile App: Mobile authentication apps mitigate the security risks of static OTPs by using either HMAC-based OTPs (HOTPs) or time-based OTPs (TOTPs). HMAC stands for "hash message authentication code", and HOTPs are utilised in token-based authentication. They are not time-based, and instead use a secret key and a counter. Each attempt to authenticate the counter on the token generates a new OTP. On the other hand, TOTPs are temporary and do not use a counter. Instead, the time is synchronised on both the user and the resource's end through a network time protocol. Popular mobile authentication apps use TOTPs enabling two-factor authentication. These apps are scalable and easy to adopt and use, as well as less vulnerable to circumvention by malicious actors. Two-factor authentication with biometric validation of OTP would solve the issue of stealing a token in TOTP authentication. However, app-based OTP mechanisms require individuals to possess a smartphone for authentication.

Non-electronic card: These are usually plastic cards that contain basic demographic information. They can also have a photograph, allowing them to be used as photo identity proof. Non-electronic cards used in identity systems can also contain a unique identification number linked to records in a database in order to validate identity. Barcodes and QR codes on non-electronic cards can automate the process of data-capturing and reduce errors.

Non-electronic cards provide the simplest method of identity authentication. They also have a high level of interoperability with other technologies. They are usually more affordable than other methods of authentication since they are easy to implement and do not usually require additional technology (except for barcode or QR code scanners in some instances). These factors contribute to ease of adoption, since a high level of technological literacy is not required to use them.

However, these cards pose issues of security and scalability. They do not possess electronic security features, and anyone in possession of a card can use it in the absence of biometric validation. They are not an ideal means of local biometric authentication since any biometric template encoded on the card is either not encrypted, or in case of encryption requires keys that must be distributed and secured.[68]

Contact smart card: These cards are embedded with a microchip and processing unit which work with a card reader through physical contact. Card readers contain a processor, memory and a cryptographic controller and provide high processing speeds and security. These have seen wide country adoption, and are used to access a wide array of services.

The cards allow online and offline transactions, and attempt to secure communication through built-in hashing, digital signatures, and encryption. They are versatile across purposes and scalable as they are capable of storing and transmitting increasingly large volumes of data. Other applications can be added to the card, and they can be also used as multi-application credentials to allow physical access to various facilities.

68 "Technology Landscape for Digital Identification", *World Bank*, last accessed August 27, 2021. http://documents.worldbank.org/curated/en/199411519691370495/pdf/Technology-Landscape-for-Digital-Identification.pdf.

However, these cards require a card reader in order to function, and retrieving information from them is relatively slow. While they are relatively cheaper than contactless smart cards, they can still entail high overall costs. Security issues may arise by guessing or observing the PIN or stealing biometric credentials required for authentication.[69]

Contactless smart card: These have the same features as contact smart cards with an additional radio frequency (RF) transceiver and antenna powered by electromagnetic waves emitted by the card reader. Contactless cards share similar dimensions and processor options as contact cards, but have slower data transmission rates. Documents such as electronic passports can also act as contactless cards.[70] The identity can be authenticated and verified through a password or a PIN, but this feature can also be circumvented. Cryptography implemented through an integrated circuit chip can also protect user and application information. Contactless cards are being increasingly adopted, and can be adapted for various uses because of their ability to store increasing amounts of data and perform cryptographic computations.

Contactless cards can also be expensive, making them out of reach to low-income communities. They are also subject to the same RFID tracking vulnerabilities as non-smart RFID cards.[71]

Non-smart RFID cards are a form of contactless cards that use radio frequency identification (RFID) to process the information in RFID tags. Unlike active RFID, passive RFID does not have an internal power source, and is powered by the electromagnetic energy transmitted by an RFID reader.[72] Depending on their technological specifications, non-smart RFID cards can operate at various distances. They consist of an embedded RFID tag which has a microchip that has restricted computational ability and memory, as well as an antenna. Passive RFID tags work in conjunction with a reader, and the information transmitted does not typically include personally identifiable information. To prevent unauthorised access, contactless cards should ideally be stored in an RF-blocking sleeve.

These long-range cards offer the advantage of allowing quick and efficient identification, and do not require the card to be in the line of sight of the card reader. They do not contain personally-identifiable information (PII), and also have a serial number that limits access by authorised users to information from a secured database.

However when tags are not shielded, they could be read by both authorised

69 "Technology Landscape for Digital Identification", *World Bank*, last accessed August 27, 2021. http://documents.worldbank.org/curated/en/199411519691370495/pdf/Technology-Landscape-for-Digital-Identification.pdf.

70 Machine Readable Travel Documents, Part 4: Specifications for Machine Readable Passports (MRPs) and other TD3 Size MRTDs (2021), https://www.icao.int/publications/Documents/9303_p4_cons_en.pdf.

71 "Technology Landscape for Digital Identification", *World Bank*, last accessed August 27, 2021. http://documents.worldbank.org/curated/en/199411519691370495/pdf/Technology-Landscape-for-Digital-Identification.pdf.

72 "Active RFID vs. Passive RFID: What's the Difference?", *atlasRFID*, last accessed August 27, 2020, https://www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid.

and unauthorised individuals and rogue RFID readers. This raises privacy, and surveillance, and security concerns, and individuals will not know that their information has been compromised. Overall, this is a baseline technology that requires relatively low investment to implement, but is more expensive than barcode stickers and readers (which could be a point of comparative disadvantage and an obstacle in developing countries). Scalability issues also arise because they store limited amounts of data and lack sufficient processing power.

Biometrics: When biometrics used in identification are assigned the nature of an ID credential, they usually involve matching the person's biometrics against the stored biometrics in the ID system collected during the process of Identification. Biometric technologies involve a risk of both false positives and false negatives, particularly in large populations. Biometric factors are immutable and, in most cases, visible in the public domain. This makes them impossible to change in case of breach and are susceptible to forgery.

Biometric system on card (BSoC): BSoC technology involves a smart card with a biometric sensor and matcher. After a biometric sample is captured by the sensor, its biometric features are extracted by the processor and verified against the enrolled feature set. All data remains on the card.

BSoC provides more secure authentication, since it is only performed in the presence of the cardholder and this technology is fairly resistant to circumvention. Only authentication data (and not PII) is transmitted. Since the card does not require biometric fingerprint information to be transmitted to a central server, this technology is fairly scalable. It does not require external biometric fingerprint readers which can be expensive, however this technology is more expensive than standard smart cards. While authentication accuracy is moderate, matching speed is high. If mishandled, the performance of the cards may get affected by wear and tear if mishandled.[73]

When determining the selection of an ID artifact, ID providers should take into account the following factors:

Level of technological literacy of targeted individuals, and quality of access to internet and technological infrastructures: For instance, in India, the implementation of Aadhaar has lead to a large-scale exclusions through authentication failures caused by poor internet connectivity[74] and lack of proper training of operators.[75]

Uses of the ID: The choice of ID artifact and authentication-credential should be

73 "Technology Landscape for Digital Identification", *World Bank*, last accessed August 27, 2021. http://documents.worldbank.org/curated/en/199411519691370495/pdf/Technology-Landscape-for-Digital-Identification.pdf.

74 Geeta Pillai, "Need internet to buy PDS rations? Go climb a tree," *The Times of India*, March 3, 2017, https://timesofindia.indiatimes.com/india/need-internet-to-buy-pds-rations-go-climb-a-tree/articleshow/57437975.cms.

75 "Governing ID: A Framework for Evaluation of Digital Identity", *Digital ID: Designs and Uses*, last accessed December 7, 2021, https://digitalid.design/evaluation-framework-02.html#ref73 citing "Economic Survey 2016-17", *Department of Economic Affairs* (January 2017) https://www.indiabudget.gov.in/budget2017-2018/es2016-17/echapter.pdf.

secure and support the proper exercise and enjoyment of the individual's rights.

Risks of biometric factors: Opting for biometric factors should be justifiable in terms of proportionality since biometrics create serious privacy and security risks, and may be a violation of privacy and other fundamental human rights.

4. How should verification be done?

- **What are the attributes and documentation required to verify a user's identity?**
- **In the absence of required documentation to establish identity, can a user's identity be vouched for by a reliable person?**
- **Is identity proofing based on government sources such as existing civil registration systems/ legacy identification systems?**
- **Does identity proofing involve deduplication based on biometric or biographic data?**

During the registration phase of a digital ID system, an applicant goes through the process of recording their attributes (identity claim) and verifying their data (identity proof). This verification process forms an important part of the ID system, and is often determinative of both the trustworthiness of the final identity credentials, as well as the inclusivity of the ID system. This also presents a trade-off: a process that requires comprehensive documentation or identity evidence to verify an applicant's identity might ensure reliability of the ID, but may make it less accessible to applicants who do not have these required documents or are otherwise unable to complete such a robust vetting process. It could also substantially increase the costs for the implementing country.

Typically, credentials and documents that have already been issued are used to demonstrate attributes for this stage, as prescribed by the identifying entity. This can follow several different models:

Civil Registration and Vital Statistics Systems (CRVS): Here, an applicant's identity attributes are verified by comparing it to supporting documents such as birth certificates, marriage certificates, passports, driving licenses, and death certificates. This might also involve checking the authenticity and accuracy of these documents, and that the applicant is the true owner of the claimed identity and evidence.

Vouching: In some countries, such as India and Nigeria, the verification process also allows vouching of an applicant's identity by certain individuals (such as designated 'introducers' in India) when the applicant does not possess the required identity documents. This is particularly for excluded populations that do not possess any legal identity, and is intended to minimize the inevitable exclusions that arise from insisting on specific identity documents.

Credit reference agencies: These agencies produce scores of 'credit-worthiness' of individuals based on an analysis of their credit histories, personal information,

and other factors. This score may legally be provided to various identifying entities (employers, lenders, etc.), and is widely used in countries where banking is accessible. This, among others, is used by the UK Verify service while enrolling users. It is considered fairly accurate.

Other existing databases: The use of other databases relies on the pre-existence of trustworthy documentation which can be utilised for verification. For instance, in Estonia, the Population Register containing personal information such as educational and marital records is used for verification.

Police verification: Law enforcement authorities such as police and border authorities may oversee or act as an additional step to conduct verification. Choosing the appropriate system of verification requires consideration of many factors, but would depend most on the intended purpose of the system (and therefore the level of assurance it needs to achieve) and the unique needs and particularities of the local population. Factors to consider should include:

Costs involved: The use of an existing and reliable database to conduct verification can reduce the costs involved in performing verification through other means. It may also reduce the visits that an applicant has to make to a centre for physical checks, which in itself can act as an obstacle to digital ID adoption. For instance, in the UK Verify registration process, all the steps of verification happen online, with the ID provider checking the applicant's identity against certain recognised databases.

Privacy and surveillance: On the other hand, the use of an existing identity database to generate a digital identity may increase risks of privacy and digital surveillance, particularly when carried out through seeding. The ID provider must also be wary of the additional privacy risks involved in using private actors or databases managed by private actors in the performance of this function, as it could lead to misuse of sensitive data (such as one prominent instance of an enrollment centre leaking the personal information of a famous cricketer[76]).

Exclusion and discrimination: Many exclusionary effects of digital ID arise at this stage, as applicants can be denied an ID dude to lack of documentation, errors in the verification system, or a difficult registration process that is not well adapted to the needs of the population. Sometimes this can also be discriminatory, when it affects a particular community or group that faces special challenges in obtaining these IDs. In Kenya, border communities such as the Nubian community have to undergo a special vetting process that makes it difficult to acquire basic identity documents. Since the Kenyan digital ID requires these documents to verify identity attributes, members of these communities are more likely to be excluded from obtaining these IDs.

A flexible verification policy that allows different attributes, uses diverse methods and/or infrastructure, and accounting for exceptional situations, can help mitigate these risks. The use of vouchers in India and Nigeria, where many persons do not have identity documents or the use of non-government databases such as those

76 "UIDAI blacklists for 10 years Aadhaar centre that leaked MS Dhoni's personal details", *The Hindustan Times*, March 30, 2017, https://www.hindustantimes.com/india-news/uidai-blacklists-for-10-years-aadhaar-centre-that-leaked-ms-dhoni-s-personal-details/story-pqMszfBXhFknMbrwcrI1qJ.html.

of credit agencies and mobile phone providers in UK for persons who do not have government documents[77] are good practices to address exclusionary risks.

Exclusion can also present as the costs, in both time and money, and it takes to obtain a digital ID. In Nigeria, the verification process involves 3 visits to an enrolment (or other) centres by an applicant; this may exclude that part of the population that are unable to afford such costs. Thus, a process that requires minimal physical presence (or can be conducted online if existing infrastructure allows for it), similar to ones adopted by the UK and Canada for their digital ID systems, should be prioritised.

Deduplication and seeding: Where a country intends to only issue unique identities, the verification process often involves a deduplication of the identity information provided by the applicant. In countries with strong civil registration and vital statistics systems (CRVS), this is often done by relying on existing databases. This can involve the process of seeding, where identity records in an existing database are mapped with those in another database, typically through a unique identifier. However, in other systems, where robust CRVS databases may not exist, other verification strategies have been employed, such as deduplication on the basis of biometrics or other demographic information. For instance, the Aadhaar system in India conducts de-duplication by comparing an applicant's demographic and biometric information, collected during the process of enrolment, with records in the UIDAI database to verify if the resident is already in the database or not.[78] This aims to ensure that only one Aadhaar number is generated per individual in the database.

5. Who is eligible?

› **Is the coverage of the digital ID system intended to be universal or limited in its scope?**

One of the central questions of national Identity Systems is deciding who should enrol and use the Identity System (i.e. eligibility). The choices for the who question are groups of either one or both of:

a. residents, non-residents;
b. citizens, aliens;
c. adults, minors.

In the initial stages, uses and aims of a national Identity System are typical considerations in deciding eligibility. But when ID schemes bring new aims and uses into their fold, the nexus between eligibility and the (new) uses and aims gets diluted. The cost of such an approach is high — poor choices in eligibility criteria risks the exclusion of marginalised groups including refugees, homeless people, and migrants from rightful access to entitlements and services.

77 "Digital ID in the UK: Insights from Research Mapping", *Digital ID: Designs and Uses*, last accessed December 7, 2021. https://digitalid.design/research-maps/uk-insights.html.

78 "Features of Aadhaar", *Unique Identification Authority of India*, last accessed December 7, 2021. https://uidai.gov.in/my-aadhaar/about-your-aadhaar/features-of-aadhaar.html#:~:text=The%20de%2Dduplication%20process%20compares,in%20the%20database%20or%20not.

Further, on the choice between residence, identity, and citizenship, it is not unusual for countries to revisit questions of citizenship and processes for determining it. Making citizenship as the sole eligibility criteria ignores such possibilities.

6. How should one think about interoperability?

- **Does the ID system allow or enable communication between different identity databases (domestic and international)?**
- **Is the digital ID mutually recognised with that of other countries?**
- **Can these identity databases communicate and exchange information in a timely and low-cost manner?**
- **Does the ID system have sufficient privacy and security safeguards to regulate these information exchanges and prevent data theft, fraud, or violation of rights?**

An interoperable system is one whose interfaces are understood to work with other products or systems, present or future, without restrictions. Making a digital ID system interoperable (either within the system or with other systems) has several advantages, including:

Cost: For the ID provider, the cost of adding new components or services to the system is reduced if the existing system can interoperate. By making it interoperable with an existing CRVS or identification system, it can also increase the accuracy and reliability of the system. For instance, the Aadhaar system in India was built on an open standards interoperable platform, to allow easy scalability and preclude vendor lock-in.

Utility: The ability of a foundational ID system to interoperate with other services is beneficial for both industry and individual citizens. For the former, it lowers the cost of verifying identities or collecting data, and the assurance provided by digital IDs are typically higher than previous paper based ones. The e-KYC functionality of the Aadhaar system, employed by most banks, is an example of this. For citizens, a digital ID system linked to several other services increases convenience and ease of access. The Estonian ID system has made its ID system interoperable with various databases, to help users make available the data they need when accessing a service using their e-ID.

However, these benefits come at a high cost. Allowing the linkage of the ID system to other databases, especially when these are private/commercial services, risks the exposure and security of personal identity information, with the potential for commodification of personal data. Even in instances of interoperability only between government or public services, it enables multiple facets of an ID holder's daily life to be connected to one identifier, thereby building a deep and extensive profile of the ID holder with far-reaching consequences for surveillance.

In building a system such as this, the European Interoperability Framework[79] suggests four interoperability layers that need to be defined:

1. **Legal interoperability**: Legal, policy, and regulatory frameworks define the scope of interoperability, particularly with regard to data exchange and requirements for privacy and data protection.

2. **Organizational interoperability**: For inter-organizational interoperability, federation, or mutual recognition of ID systems, organizations must define trust frameworks and process standards around the identity lifecycle (e.g., the eIDAS standards).

3. **Semantic interoperability**: To ensure that the meaning of exchanged data and information is consistent, systems must adopt the same data standards or construct data dictionaries.

4. **Technical interoperability**: To enable machine-to-machine communication, systems must adopt the same technology standards for software, physical hardware components, and systems and platforms.

Interoperability in an ID system can be looked at from different perspectives:

Subsystem interoperability: This ensures that identity databases function as efficiently as possible, as they are able to communicate with each other easily and have timely exchanges of data. This includes, for example, interoperability between fingerprints captured with a scanner device and the deduplication engine, interoperability between smartcards and readers, interoperability of biometric formats captured during registration with those captured during authentication, or interoperability between images captured by devices from different vendors. It is also an effective cost-managing measure, particularly in the long term: by having interoperable devices, software, and hardware from different vendors, identity providers can avoid vendor lock-in and allow greater choice to users.

System interoperability: Interoperability of the ID system with other domestic and international identity databases.

1. **With CRVS**: For countries with a functioning CRVS, identity databases that are built to be interoperable with it are enhanced in terms of cost, accuracy, and inclusion when keeping identity information. Amongst other things, this can perform the following functions:

    a. **Verification of identity information**: During the registration process in Estonia, an applicant's submitted biometrics and identity documents are checked against the Population Registry and Identity Documents Database to check their authenticity and accuracy before issuing their ID.

79 New European Interoperability Framework: Promoting seamless services and data flows for European public administrations (2017), https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf.

b. **Updating recording identity information**: This comes into play in cases of death, name change for instance, since these are likely to be recorded in the CRVS.

c. **Linking ID creation to birth registration**: This could include, for example, the generation of a unique identity number for a newborn by the ID system, following a notification (through a direct connection or open APIs) of a child's birth. In some cases, this UIN could then be communicated back to the civil register. By seamlessly creating a digital ID from birth during the birth registration, this process can help ensure the inclusion of people of all ages in the ID system, increase the consistency of identities over time, and help incentivise birth registration.

However, it is important to note that the use of CRVS systems, especially where they are not well developed, could exacerbate exclusions. To ensure inclusion of the entire population, states are urged to consider alternative means of identification to address those who have been left out of CRVS infrastructure.

2. **With other databases:** The Estonian ID system is built to be interoperable with other public and private databases, with the ultimate goal of allowing easy access to personal information such that an eID holder need never share the same information twice. It achieves this through an interoperability service, X-Road, which links each separate public and private sector e-information system and enables them to communicate seamlessly with each other without human intervention.[80] In India, the India Stack comprises a family of APIs, open standards, and infrastructure components that allow a user in India to demand services digitally. Here, the Aadhaar ID system sits as the "presenceless layer", serving as a foundation for many services that are built on top of it, such that these can be delivered online, without the need for the physical presence or paper documentation of the ID holder. Some services included here are Digilocker (for issuance and verification of documents and certificates), eSign (to electronically sign documents), eKYC (to perform essential Know Your Customer verification digitally) and UPI (for sending and receiving money or making payments through bank accounts).

3. **With international databases:** ID systems can be mutually recognisable with other countries so that digital ID holders in one country can access services in the other, and be able to conduct secure electronic transactions. There are many uses for this, ranging from serving as a travel document, to accessing banking services in other countries. The most common way of implementing this is to use technical and other standards along with a legal/trust framework.[81] For instance, the eIDAS regulation in the EU creates a regulatory environment comprising standards and governance mechanisms for cross-border recognition and authentication of eIDs.

80 "Mapping Digital Identity Systems: Estonia", *Digital ID: Designs and Uses*, last accessed December 7, 2021, https://digitalid.design/research-maps/estonia.html.

81 ID4D Practitioner's Guide (October 2019), https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf.

> This ensures that people and businesses can use their national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available.[82]

The risks introduced by making identity systems interoperable deserve reiteration here: they allow for sweeping surveillance, permit the system to be used for new uses (that were not originally consented to) and encourage the collection, sharing and commercialization of personal information. ID providers are encouraged to carefully consider the need for, and degree of, interoperability, and adopt a risk-based approach in implementing it. Additionally, to mitigate the risks inherently involved in this, ID providers must use privacy by design mechanisms, set fixed purposes of the ID system to avoid mission creep, restrict the actors that can access personal data, and have a robust oversight and accountability framework.

7. What makes the ID open/closed?

- **Are enrollment and use of the digital ID mandatory or voluntary?**
- **If enrollment and use of the ID are mandatory, has the identity provider identified and mitigated all legal, procedural and social factors that may prevent any person or group of persons from enrolling and using the ID?**
- **If additional fees are charged for additional services associated with the ID, are these rates reasonable and transparent?**
- **Has the identity provider made special provisions to minimise or waive costs of obtaining and using the ID for poor or vulnerable persons?**
- **Has the identity provider made efforts to remove or mitigate all indirect costs associated with obtaining a digital ID, such as travel or administrative costs?**
- **Has the identity system been designed with sufficient legal, procedural and technological safeguards to ensure that the identity system and identity data is not used to target, persecute or discriminate against any persons/ groups or persons?**
- **Does the identity system ensure last-mile access through the provision of online and offline infrastructure in remote areas?**

The lived experiences of digital ID users, particularly in the global south, have been marked by various forms of exclusion. Many forms of exclusion tend to arise from the implementation of digital ID in countries that lack the required digital infrastructure or have low levels of internet adoption, bureaucratic or administrative processes of identification, social barriers, and making digital ID either directly or indirectly mandatory to access benefits and services in combination with these factors. In the absence of mitigation measures, these risks tend to amplify existing socio-economic inequalities and disproportionately affect already marginalised communities such as refugees, immigrants, women, elderly people, transpersons, sexual, cultural and religious minorities, economically disadvantaged persons and residents of rural or remote areas.

82 "eIDAS - The Ecosystem", *eIDAS*, last accessed December 7, 2021. https://www.eid.as/.

For instance, in addition to social barriers such as not being allowed to leave the house or have their own ID cards, many women have faced obstacles in enrollment when ID systems require facial capture, consequently excluding women who may not wish to expose their faces for religious or cultural reasons (such as in the case of women being forced to remove their headscarves for Aadhaar registration[83]). Linguistic minorities have often been locked out of these systems due to inaccurate translations of names or other important details by translation software which has resulted in non-matching of identity records. Procedural barriers witnessed in areas with high rates of illiteracy could arise from having less reliable personal data, because those enrolling themselves may have trouble corroborating if their personal information is correct. In India, a large proportion of homeless and transgender persons are unable to enroll for Aadhaar despite multiple attempts to do so. Homeless persons are usually unable to furnish documentation such as proof of residence (which is a mandatory requirement). Transpersons often face bureaucratic obstacles when the gender on their existing IDs does not match with their gender identity or appearance, and are also far more likely to have errors in their recorded gender data.[84]

Many countries also lack the basic infrastructural capacity required for successful enrollment and authentication in the digital ID ecosystem due to low internet penetration rates and a lack of stable electricity (among other infrastructural challenges). This is often coupled with tedious administrative or bureaucratic processes, high travel costs for persons travelling from remote locations, fees charged for enrollment, persons with degraded biometrics and incorrect information not being enrolled successfully, and ethnic/ religious minorities being targeted on the basis of sensitive information or deliberately excluded from enrollment. Despite these adverse circumstances, many countries continue to make access to essential benefits and services dependent on identity. Uganda goes a step further to impose criminal and administrative sanctions for failure to register in the system.[85]

In addition to carrying out an impact assessment that examines exclusion risks before implementation of a digital ID system, it is imperative that countries ensure that digital ID is accompanied by analogue options to avoid or mitigate exclusion risks. This should include measures such as phasing the introduction of such approaches and allowing the use of alternative means of identification in case of failure of the digital ID.[86] Simultaneously, governments must ramp up infrastructural capacity to ensure that exclusions do not arise from failure of the system due to internet or other infrastructural constraints.

83 "Women decry decree to remove headscarves for Aadhaar photo", *The Times of India*, August 3, 2015, https://timesofindia.indiatimes.com/city/hyderabad/women-decry-decree-to-remove-headscarves-for-aadhaar-photo/articleshow/48322706.cms.

84 State of Aadhaar: A People's Perspective (2019), https://stateofaadhaar.in/assets/download/SoA_2019_Report_web.pdf.

85 Digital ID in Uganda: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa (2021), https://digitalid.design/RIA%20docs/CIS_DigitalID_RIA_Uganda_31.10.21.pdf.

86 Towards the Evaluation of Socio-Digital ID Ecosystems in Africa: Comparative Analysis of findings from ten country case studies (2021), https://digitalid.design/RIA%20docs/CIS_DigitalID_RIA_Comparative_Report_5.11.21.pdf.

8. How to ensure inclusivity and trust?

- Is the identity system governed by a robust legal and regulatory framework?
- Does the ID system contain sufficient safeguards to ensure that the ID provider can be trusted to manage and protect user data, and held accountable if not?
- Is the identity information collected and stored by the digital ID accurate and safe from fraud and tampering?
- Has the ID provider ensured high coverage of the ID by making it accessible to every section of the population, including traditionally underserved areas?
- Are individuals able to correct or update their personal information easily and at no cost, incentivising them to keep their personal information up-to-date?
- Have proofing requirements for updates by individuals been determined keeping in mind the potential disincentives from updating and potential exclusions that may arise from very strict requirements?
- Does the identity provider effectively engage with the public and relying parties to correct errors and address grievances?
- Does the identity provider effectively engage with civil society organisations for critical feedback on the identity system?
- Has the identity system incorporated privacy and security by design at every stage of the project?
- Is the digital ID recognised as authoritative proof of identity by the government?
- Has the identity provider actively worked to ensure user literacy about the ID, and minimise potential information asymmetries?

Digital ID systems involve the collection and storage of vast swathes of sensitive personal data that infringe on the privacy of individuals, and are inherently restrictive to the fundamental rights of privacy and free speech. Any such restriction on these rights must therefore be legal, backed by a legitimate aim, narrowly tailored in scope and application, accountable, and explicitly prevent mission creep. The implementation of such a system must only be carried out within a rule of law framework that exists to govern the use of digital ID and ensure sufficient deliberation before a digital ID system is implemented for both public and private actors. Moreover, it is important that these laws must be accessible and foreseeable to the public. This is an issue highlighted in Lesotho, where the governing Act is written only in English (which is spoken by a small minority in the country). Moreover, no digital copy of the Act is available, and a copy can only be bought at one official government printing office. The high travel costs involved in

trying to obtain a copy make this even more inaccessible to the general public.[87]

The legislative framework within which such a system operates must consist of both a digital ID and data protection law deliberated upon and enacted by parliament, and should not be a result of excessive delegation through an executive order. This law must also have a clearly defined and legitimate aim that clearly outlines and limits the purposes for which the digital ID is to be used, and the public and private actors that operate within the system and have access to its databases. It has been observed that digital ID systems in many global south countries allow access to private parties with few controls, either directly or through the respective government entity. In Tanzania, for instance, the ID authority (NIDA) gives both public and private entities access to sensitive data through data sharing agreements. However, these agreements are not available in the public domain and it is unclear whether private entities can access the entire database or can only use it for verification.[88] To further ensure accountability, such a system must have adequate and accessible grievance redressal mechanisms to enable users to seek justice in case of misuse of their data, and independent regulators and rigorous systems to ensure transparency hold all public and private actors accountable. While most countries have some form of redressal mechanism, it is not always possible for the user to directly approach the relevant authority if the law does not provide for it, the process is onerous, or if they are not aware of their rights. Redressal mechanisms are also essential in case a user's registration is suspended or withdrawn, as are provided in Kenya, Tanzania and Uganda.[89]

The privacy violations that can arise through mandatory collection of sensitive personal data, risk of surveillance and profiling, or the lack of robust access control mechanisms require that there must be a determination of whether they are necessary and proportionate to achieve the legitimate aim. Data minimisation should be enforced by placing strict limitations on what categories of data can be collected, how it is stored and for how long it is retained. The law must also clearly delineate the public and private actors who have access to this data, and how it may or may not be used. Any potential harms (such as exclusion, privacy and discriminatory harms) that may arise must be accounted for through both ex-ante and ex-post preventative and mitigation measures to minimise them as much as possible. This approach to privacy requires that the system be examined against tangible risks to individuals, allowing the administrator to prioritise risks in order of severity and respond accordingly. The risk level arising out of a digital ID is measured in terms of severity and likelihood. These harms must then be proportionately addressed by law. Threats to the ID system can be analysed based on its uses, with a wider number of uses resulting in a higher level of risk. If the

87 Digital ID in Lesotho: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa (2021), https://digitalid.design/RIA%20docs/CIS_DigitalID_RIA_Lesotho_31.10.21.pdf.

88 Digital ID in Tanzania: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa (2021), https://digitalid.design/RIA%20docs/CIS_DigitalID_RIA_Tanzania_31.10.21.pdf.

89 Towards the Evaluation of Socio-Digital ID Ecosystems in Africa: Comparative Analysis of findings from ten country case studies (2021), https://digitalid.design/RIA%20docs/CIS_DigitalID_RIA_Comparative_Report_5.11.21.pdf.

risks arising from the system are demonstrably high, mechanisms to restrict use must be employed until mitigating factors are introduced. Mitigating strategies would include notifications in case of breach, having a tested business continuity plan and increased capacity building. The choice of strategies depends on the design of the ID system and its reliance on private entities for different functions.

Finally, it is critical that the identity provider and relevant authorities actively engage with proposed ID holders and civil society through every stage of the implementation process. This should begin from incorporating feedback from civil society in the planning stage itself, and should continue to ensuring that ID holders are educated about the implications of the planned ID, how to access their information and correct it if necessary, and their right to approach the relevant authority in case of grievances such as misuse of their data or failure of the ID. The cost of obtaining an ID should be free or as low as possible, and ID holders should not be charged for seeking to access or correct their information (as this will act as a disincentive and result in an inaccurate and unreliable identity database).

Governance Framework

Research and Writing by **Yesha Tshering Paul**

As governments implement new and foundational digital ID, or modernize existing ID programs, there is an urgent need for more research and discussion about appropriate uses of digital ID systems. This also raises concerns about privacy, surveillance and exclusion harms caused by state-issued digital IDs in several parts of the world. Given the sweeping range of considerations required to evaluate Digital ID projects, it is necessary to formulate a framework for evaluation that can be used for this purpose.

This framework provides tests that can help evaluate the governance of digital ID across jurisdictions, as well as determine whether a particular use of digital ID is legitimate. Through three kinds of checks — Rule of Law tests, Rights based tests, and Risks based tests — this scheme is a ready guide for evaluation of digital ID.

Rule of Law Tests

The use of digital ID by state and private actors requires a rule of law framework to prevent its misuse. Digital ID systems must aim to meet basic rule of law parameters, and any potential infringement of an individual's rights must be sanctioned by a statutory law passed by the appropriate legislative body and not merely an executive instruction. This law must be accessible to all persons who may be impacted, and precise enough to limit discretion and prevent executive abuse. It must have a legitimate aim, to which all the purposes of the digital ID must correspond. All actors and purposes that arise from this legitimate aim must be clearly identified, as well as how it applies to State and private actors. Potential mission creep should be mitigated by clearly expressed purpose limitations backed by law, to ensure that the executive authority cannot use the digital ID for unspecified purposes without a proper legislative or judicial examination of additional uses, or fresh consent from users. The law must also provide ex-ante and ex-post accountability measures.

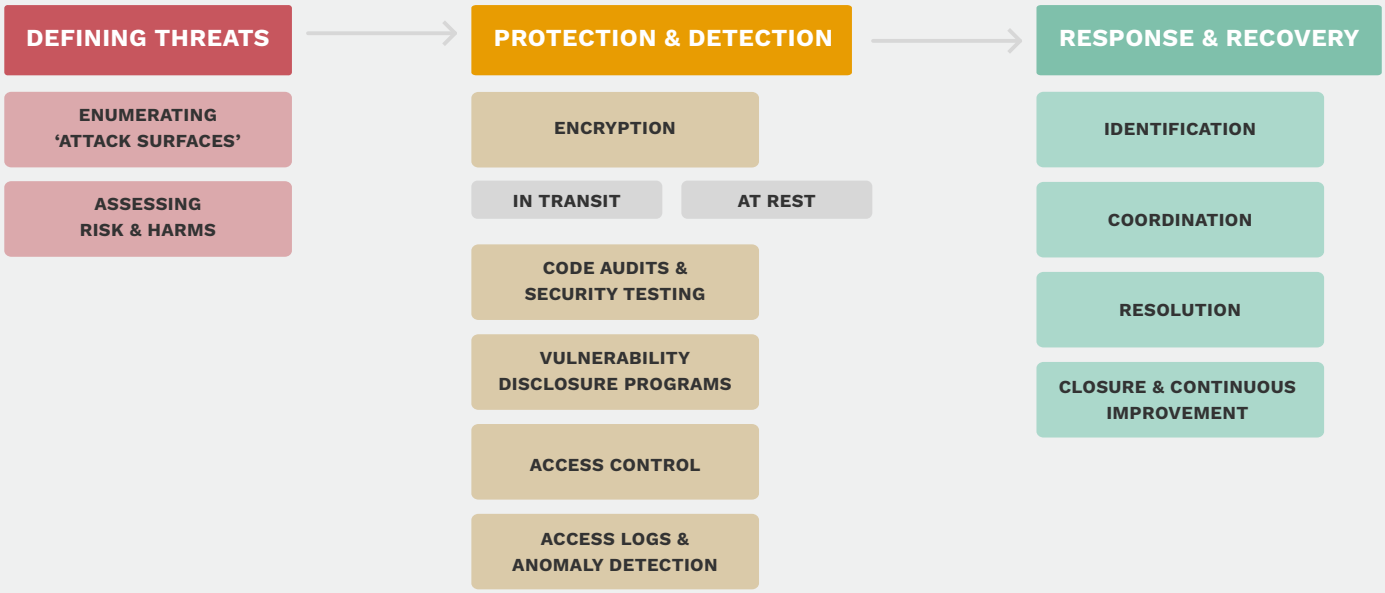
Rights Based Tests

Any digital ID will inherently infringe on certain fundamental rights. At every stage of implementation, the identity framework must be examined against the rights it may violate, and if these violations are necessary and proportionate to any potential benefits. Such an examination is critical because failure or absence of identification can lead to exclusions from basic entitlements. Principles of data minimisation must clearly dictate the amount and nature of data to be collected and stored. Access control mechanisms that regulate access to data by different actors must be laid out in the surrounding legal framework and enforced through strict civil and criminal penalties for any violations. Exclusions arise out of not only poor implementation, but also design flaws in the system. If the intended use of ID can lead to denial of services, mechanisms must be employed to ensure that individuals are not deprived. Most importantly, digital ID must not be mandatory to access benefits, and multiple alternative identification mechanisms should be provided. An opt out option that does not restrict access to the service, and mandatorily erases collected information must also be provided.

Risk Based Tests

A digital ID system must account for any potential harms. This approach to privacy requires that the system be examined against tangible risks to individuals, allowing the administrator to prioritise risks in order of severity and respond accordingly. These risks can be classified into privacy harms, exclusion harms and discriminatory harms. A differentiated approach to governance would involve categorising various uses of digital ID as *per se* harmful (which can be prohibited outright), *per se* not harmful (which can avoid regulation), and sensitive (where regulation is based on various factors). The risk level arising out of a digital ID is measured in terms of severity and likelihood. These harms must then be proportionately addressed by law. Threats to the ID system can be analysed based on its uses, with a wider number of uses resulting in a higher level of risk. If the risks arising from the system are demonstrably high, mechanisms to restrict use must be employed until mitigating factors are introduced. Mitigating strategies would include notifications in case of breach, having a tested business continuity plan and increased capacity building. The choice of strategies depends on the design of the ID system and its reliance on private entities for different functions.

Responding to Cybersecurity Threats and Failures



Research and Writing by **Divyank Katira**

A key consideration in the adoption of any technological solution, particularly one that is intended for use as public infrastructure, is the design of safeguards to prevent or minimize the impact of cybersecurity threats and failures.

In this section, we summarise key cybersecurity practices from both government and industry, primarily collected from the NIST Cybersecurity Framework[90] and Google's Infrastructure Security Design Overview paper[91]. These serve as an introduction to the steps that need to be taken to define and protect against threats, detect incidents when they occur, and respond to and recover from them.

90 Matthew P. Barrett, Framework for improving critical infrastructure cybersecurity (National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep, 2018).

91 "Google Infrastructure Security Design Overview", *Google Cloud*, last accessed November 12, 2021. https://cloud.google.com/security/infrastructure/design.

1. Defining Threats

The first step towards defining threats is threat modelling. It is the process of enumerating potential risks to security in order to develop appropriate safeguards against them[92]. In the context of digital ID systems, this entails:

Enumerating 'Attack Surfaces': Defining the various points of potential compromise, or the 'attack surface', of a system. This can include every entity that handles personal identity information or sensitive metadata, such as the various points of enrollment and authentication, central databases where such information is stored, and the network that carries information between these points.

Assessing Risk & Harms: Assessing the risk and harms associated with compromise implies adopting security measures that are proportionate to the harm that a data breach may cause. For instance, compromise of a large centralised database would have a larger impact than compromise of a single enrolment centre that serves a small number of individuals.

2. Protection and Detection

It is necessary to put in place mechanisms to protect against cyber attacks and detect incidents. The key considerations are:

Encryption in transit: implies encryption of information while it travels from one point to another over a network. This includes private links between infrastructural entities as well as over public networks such as the Internet.

Encryption at rest: refers to the encryption of data while it is stored. This protects data from attacks or flaws in the storage infrastructure, such as an untrusted storage device or unauthorised physical access to the storage disks.

Code audits and security testing: is the implementation of both manual and automated processes to attempt to identify vulnerabilities before they are exploited by malicious actors.

Vulnerability disclosure programs: provide safe harbor for security researchers to responsibly identify and disclose flaws in digital infrastructure[93]. This reduces the potential for misuse by malicious actors.

Access control: is the process of setting policies that ensure entities can only access data when they are authorised to do so.

Access logs and anomaly detection: is the process of maintaining and monitoring records about what data was accessed, when, and by whom. In the context of digital ID systems, this information can be sensitive in nature, so access logs

92 Adam Shostack, Threat modeling: Designing for security (John Wiley & Sons, 2014).

93 Improving the Processes for Disclosing Security Vulnerabilities to Government Entities in India (January 23, 2019), https://cis-india.org/internet-governance/resources/Improving%20the%20Processes%20for%20Disclosing%20Security%20Vulnerabilities%20to%20Government%20Entities%20in%20India.pdf.

should be maintained in aggregate or de-identified forms.

3. Response and Recovery[94]

Responding to a cybersecurity incident entails ascertaining what data is breached and what services are affected, removal of any ongoing unauthorised access, and restoring data and services impacted by the incident. Broadly, the steps involved in incident response are:

Identification: An incident can be identified either through the manual or automated processes put in place for detection beforehand, or by observation of the effects of the incident.

Coordination: of the various operational and technical activities, such as triage, mitigation, and restoration of services.

Resolution: involves finding the root cause of the issue, limiting its impact, implementing identified fixes and restoring all data and services affected. An important aspect of resolution is notifying the individuals impacted by the breach.

Closure and Continuous Improvement: is the process of documenting and understanding failures, and putting in place processes to avoid future incidents.

94 "Data incident response process", *Google Cloud*, last accessed November 12, 2021. https://cloud.google.com/security/incident-response.

Case Studies

Exploratory Research Maps are a result of our global survey of digital ID systems. These maps provide a coherent view of digital ID in each country. They shine a light on the pervasiveness of digital identity, and dissect digital ID 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.

NIGERIA 

INDIA 

UK 

ESTONIA