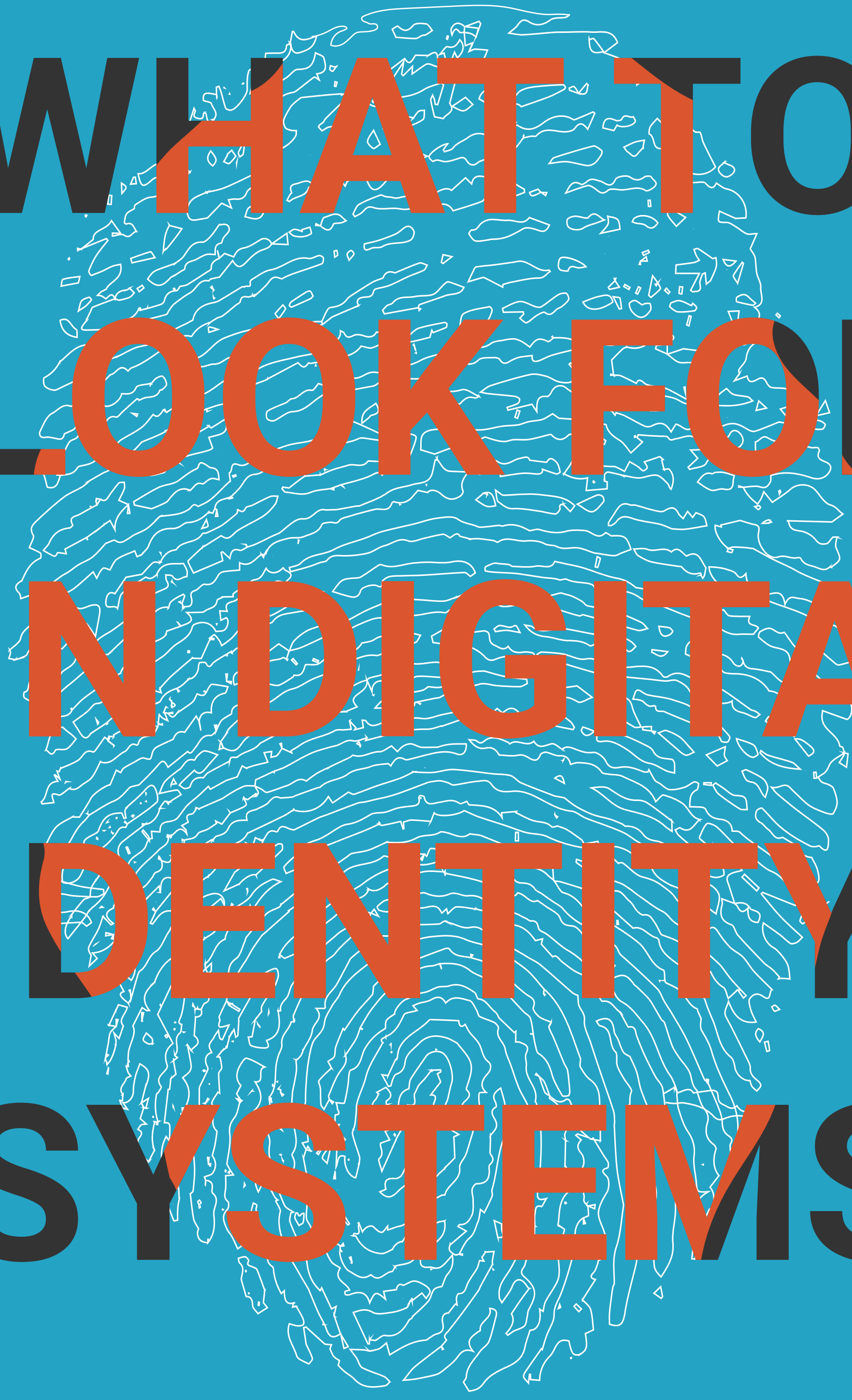
WHAT TO LOOK FOR IN DIGITAL IDENTITY SYSTEMS



A Typology Of Stages

This typology is based on research conducted by The Engine Room, with support from Omidyar Network, Open Society Foundations and Yoti Foundation from October 2018 to October 2019.

Researchers: Sharid Bin Shafique, Chenai Chair, Kittima Leeruttanawisut, Koliwe Majama, Chuthathip Maneepong, Precious Ogbuji, Berhan Taye

Writing: Sara Baker, The Engine Room

Review and editing: Zara Rahman, Laura Guzmán, Madeleine Maxwell, Sivu Siwisa, The Engine Room

Translation: Global Voices

Layout design: Julie Saw, Little by Little Studios

THE ENGINE ROOM

Project background

In late 2018, The Engine Room began a project to understand people's experiences with digital identity systems. For the purposes of this project, we defined digital identity systems as state or humanitarian systems collecting and using digital data, often including biometric data such as fingerprints and iris scans, to identify citizens, residents and beneficiaries.

We worked with in-country researchers in five locations, focusing on national systems in Nigeria, Zimbabwe and Thailand, as well as humanitarian systems in Rohingya refugee camps in Bangladesh and refugee camps in Ethiopia. To better understand the broader digital identity ecosystem, the project included a literature review that extended well beyond the five sites to explore systems in other parts of the world.

This typology of stages is the first of our findings from the project. Further reflections, including a global report and case studies, are forthcoming.

How to use this typology

This typology outlines the stages of digital ID system planning, development, implementation and maintenance as identified through our field studies and desk research. It is intended for civil society, activists and journalists aiming to build their understanding of these systems or to educate or advocate around them[1].

This tool will help you:

- Identify what stage a digital ID system is in
- Understand what to expect from each stage
- Develop advocacy strategies to influence developers and decision makers

Each stage lists key activities that may be undertaken by system creators, but not all of the systems we examined included every activity.

Each activity is followed by a list of **questions to ask** about the digital ID system in your community, and each stage includes a brief advocacy case study.

The planning and development stages also list **key documents** to review. These are documents typically produced by the developers of the digital ID system that can shed more light on their motivations, plans and goals.

More information on some of the subjects mentioned can be found in the references at the end of the document.

Stage 1 Planning

In this stage, creators of the ID system are laying the foundation by pointing to problems the system is meant to solve and creating necessary frameworks. Key questions to be asked focus on digging deeper into the arguments presented in support of a digital ID system and building an understanding of the legal and policy underpinnings that could support it.

Strategy development: Identifying the need for digital ID

Questions To Ask

- What problem is this digital ID system aiming to solve? Is this a real and significant problem? Is there evidence to demonstrate that digital ID will solve the problem at hand?
    - Common arguments from states include:
        - Enhanced national security
        - Improved service and entitlement delivery
        - Financial inclusion
    - Common arguments from humanitarian organisations[2] include:
        - Quicker, more efficient aid distribution
        - Decreased fraud
- Who benefits most from this system? Do the benefits outweigh the risks?
- Has the developer conducted meaningful consultations with a variety of stakeholders?

Policy development and legislation: Creating regulatory frameworks for the implementation of digital ID

Key Documents

- Data protection legislation
- Digital identification bill (or another law that mandates the existence of a national system)

Questions To Ask

- What existing laws enable or prevent the collection of data, such as biometric data, through this system?
- What related bills are legislators considering? Do these bills include a public comment period?
- Are there any data protection laws in place already?[3] How–if at all–will they affect the planned digital ID system? Do they address such issues as data sharing and data retention?

Case Study

Legal advocacy can be an effective method of pushing back against potential privacy violations and other problems. When the general secretary of the People's National Party filed a lawsuit alleging Jamaica's proposed digital ID system was unconstitutional, the Jamaican Supreme Court ruled[4] in his favour and the system was scrapped. While India's similar lawsuit failed to stop their own national system (Aadhaar) prior to the Jamaican case, Indian efforts had a critical impact on Jamaica, where the judges relied heavily on Indian Supreme Court Justice DY Chandrachud's dissenting opinion.[5]

Stage 2 Development

In this stage, developers are working with partners to define the parameters and infrastructure of the digital ID system. Key questions to be asked examine the nature of these partnerships and the protection of user data.

Procurement: Finding and contracting with a private sector partner to develop, and possibly maintain, a digital ID system

Key Documents

- A request for proposals and/or terms of reference for a third-party contractor
- A data-sharing agreement between host governments and aid organisations

Questions To Ask

- Is there a procurement process, and is it open and transparent?[6]
- Who is the commercial provider and how do they benefit?
- What data can the commercial provider access and what will they do with it?
- Does the commercial provider have ties to domestic or international intelligence and law enforcement communities?
- If an organisation like the UNHCR is implementing a system on behalf of a host government, is any data shared with refugees' countries of origin?

Design and planning: Creating the architecture and associated protocols of a digital ID system

Key Documents

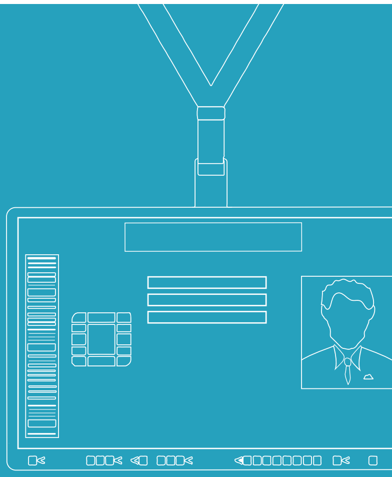
- Architecture diagram or other description outlining how the system will work
- Processes governing consent, registration, data retention, etc.
- Risk assessment or privacy impact assessment

Questions To Ask

- Does the design of the system's architecture follow increasingly recommended practices such as privacy by design,[7] human-centred design[8] and participatory design?[9]
- Are registration and consent processes designed with input from vulnerable groups?
- Which identity documents will be used for the registration process? Does everyone already possess these documents? Who might be left out?
- Where will data be stored? Is the database centralised? Who will have access?
- Are there appropriate security policies and protocols based on risk assessments?
- Are there data retention policies?

Case Study

When Tunisia proposed a biometric identity card, there was no information on where personal data would be stored or who would have access to it, and the commercial contractor was never named.[10] Civil society convinced lawmakers to adopt data protection amendments that would safeguard the biometric database.[11] In a stunning victory, once the amendments passed, the Ministry of the Interior dropped the bill entirely. It seemed they could not move forward without giving the unnamed company access to citizen data.



Stage 3 Implementation

This stage involves digital ID system roll-out and function. Key questions to be asked emphasise the importance of public outreach and seek to understand people's experiences with the system.

Awareness campaigns: Informing the population about the purpose, function and registration process of a digital ID system

Questions To Ask

- How have developers engaged the public?
    - Common tactics include:
        - › Media outreach
        - › Community leader engagement
        - › Announcements in refugee camps
- Has there been outreach with vulnerable groups?
- Do people have enough information to support and engage with digital ID systems or effectively advocate for critical changes?
- Are people able to connect data privacy to other urgent issues such as poverty and discrimination?

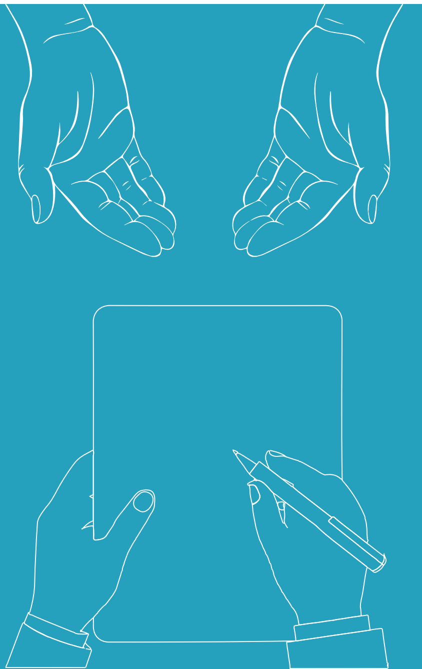
Registration and use: Enrolling users in a digital ID system and enabling services

Questions To Ask

- Have marginalised communities been consulted in order to avoid registration barriers?
    - Common barriers include:
        - Lack of accessible registration locations for people with disabilities and people in rural areas
        - Discrimination against transgender and non-binary people (e.g., lack of appropriate gender options on forms, failure to recognise gender transitions)
        - Lack of literacy in the languages or digital tools used
        - Failure to recognise cultural norms (e.g., requiring women in conservative communities to register independently)
        - Costs associated with obtaining or fixing initial identity documents
- Have humanitarian organisations considered the impact of trauma on newly registering refugees?
- Are all populations experiencing the same benefits? Are any experiencing more harm than others?

Case Study

In Thailand, civil society is doing the work of helping migrants navigate ID registration. This close connection to both migrant workers and the government's migrant ID offices creates a valuable opportunity for advocacy. Civil society organisations have unique insight into the needs of migrants as well as the barriers and risks they face, which can enable organisations to push for changes that benefit this marginalised population.



Stage 4 Maintenance

In this stage, the entities tasked with running a digital ID system manage ongoing use and related problems. While registration typically gets the most attention, maintenance is critical to the long-term success of a digital ID system. Questions to be asked focus on how people's struggles with the system are addressed and how seriously these entities approach the heavy security burden.

Updates: Addressing life changes and registration errors in a digital ID system

Questions To Ask

- What is the process for updating or fixing errors in the data?
- Is there evidence of the effectiveness or failure of this process? For instance, are there people who have been unable to make necessary changes and has this caused denial of service, aid or the ability to exercise their rights?
- How are false positives and false negatives handled?[12]

Grievance reporting: Submitting and addressing complaints about a digital ID system

Questions To Ask

- How can people lodge complaints about the system? Is the process easy, intuitive and accessible?
- Are people treated fairly and respectfully when reporting grievances?

- Do people have trust in the departments tasked with responding to grievances?
- Is there a need for independent oversight?

Security: Protecting digital ID system data over time

Questions To Ask

- Is the developer following the policies and protocols designed to prevent security incidents?
- Are there clear, viable protocols for handling data leaks, breaches and failures?
- Is the developer transparent about the volume and harms of security incidents?
- Are there ways for people to seek redress from harm stemming from security incidents?

Case Study

When complaints are not addressed, collective action may have an impact. In Bangladesh, with few ways to assert power, Rohingya refugees staged a strike to protest smart cards that labeled each person as a “forcibly displaced Myanmar national” rather than Rohingya and to demand that authorities refuse to share refugee biometric data with the government of Myanmar.[13]

Notes

1 For digital ID best practices, consider the Good ID movement (https://www.good-id.org/en/), CIS's evaluation framework (https://digitalid.design/evaluation-framework-01.html), ITU's roadmap (https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/ITU_eID4D_DIGITAL%20IDENTITY_ROAD_MAP_GUIDE_FINAL_Under%20Review_Until-05-10-2018.pdf) and the World Bank's principles (http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf).

2 The Engine Room and Oxfam. (2018). Biometrics in the Humanitarian Sector. https://www.theengineroom.org/wp-content/uploads/2018/05/Oxfam-Report-May2018.pdf

3 KJ Dearie's article on transparency, accountability and user control in privacy laws offers examples of strong data privacy laws. https://www.good-id.org/en/articles/new-age-data-privacy-3-core-concepts-privacy-laws-around-world/

4 Robinson v. Attorney General of Jamaica, JMFC Full 04 (Supreme Court, 2019). https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf

5 Bhatia, G. (2019, April 15). The afterlife of Aadhaar dissent: The Jamaican Supreme Court strikes down a national biometric identification. Medianama. https://www.medianama.com/2019/04/223-the-afterlife-of-the-aadhaar-dissent-the-jamaican-supreme-court-strikes-down-a-national-biometric-identification-gautam-bhatia/

6 Learn more about open contracting for procurement at https://standard.open-contracting.org/infrastructure/latest/en/

7 See more on privacy by design at https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/

[8] For more on human-centred design, see https://www.ideo.org/tools

[9] Sinni, G. (2017). Participatory Design for Public Services: Innovation in Public Administration. The Design Journal, 20(1), S3368-S3379, https://doi.org/10.1080/14606925.2017.1352841

[10] Mzalouat, P.H. (2018, March 22). Carte d’identité biométrique : Chronique d’un project de loi avorté. Inkyfada. https://inkyfada.com/fr/2018/03/22/carte-identite-biometrique-tunisie/

[11] Sayadi, E. (2018, January 11). Biometric ID vs. privacy: Tunisians win on privacy! But it’s not over yet.
https://www.accessnow.org/biometric-id-vs-privacy-tunisians-stood-privacy-not-yet/

[12] False positive: when the system identifies a match where it should not. False negative: when the system fails to identify a match where it should.

[13] Islam, M. N. (2018, November 26). Bangladesh faces refugee anger over term ‘Rohingya’, data collection. Reuters.