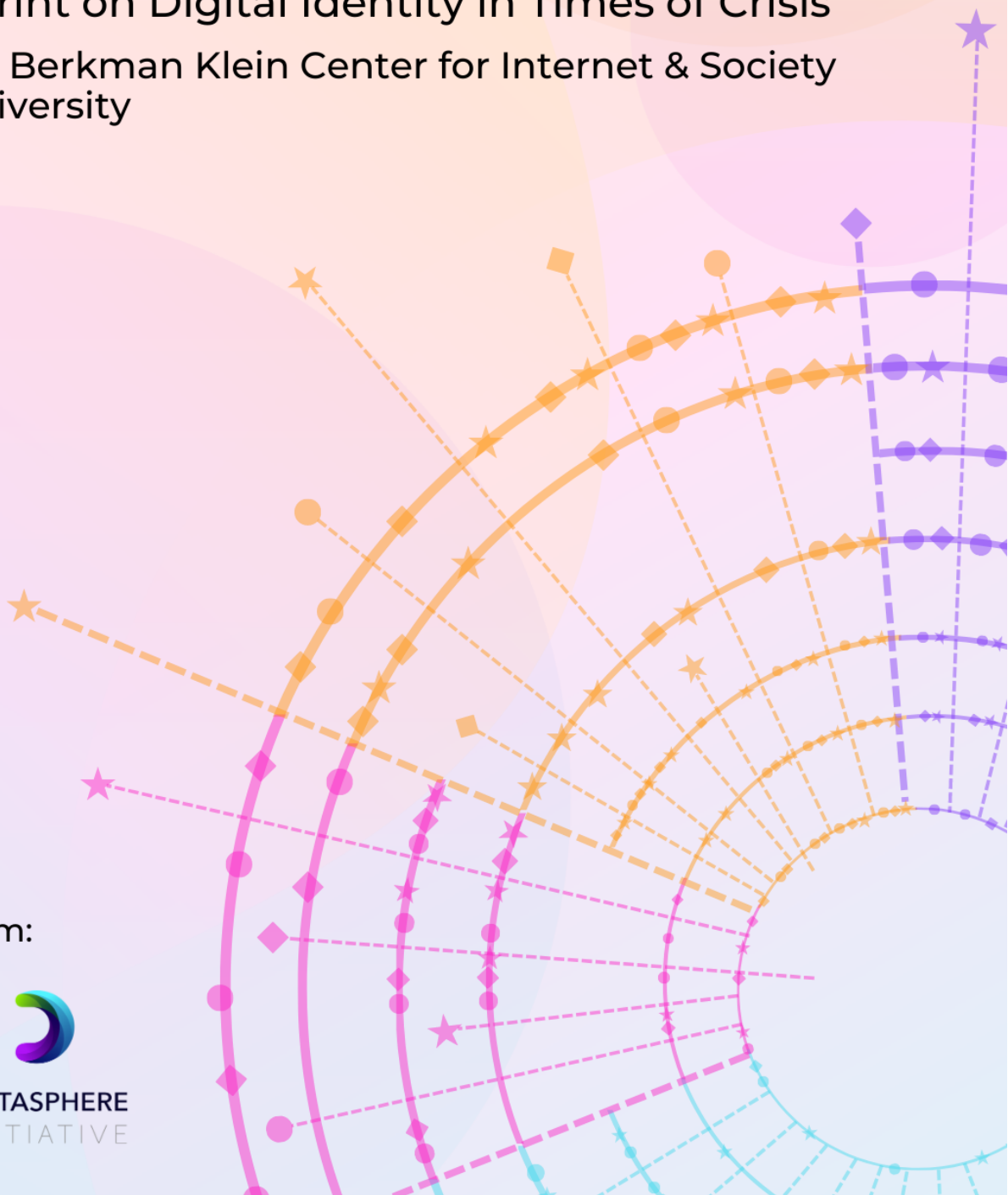
Enhancing Inclusion in Digital Identity Policies and Systems

An Assessment Framework

Final Policy Output

Research Sprint on Digital Identity in Times of Crisis

Hosted by the Berkman Klein Center for Internet & Society at Harvard University



With support from:

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY
AT HARVARD UNIVERSITY

DATASPHERE
INITIATIVE

Acknowledgements

Developed by **Mariana Rozo-Paz**, **Jack Smye**, and **Sourav Panda**; participants of the Research Sprint on Digital Identity in Times of Crisis.

The team wants to thank **Santiago Uribe**, from the Edgelands Institute, who navigated this challenging and inspiring sprint with them and guided them to frame their ideas and projects. The team is grateful to the Datasphere Initiative team, for their support, including **Carolina Rossini**, Director of Policy and Research, who contributed with invaluable suggestions for this paper's framing, narrative and impact, **Natalia Longou**, who designed and edited the cover page and graphics of the report, and **Lorrayne Porciuncula**, Executive Director, and **Sophie Tomlinson**, Director of Partnerships and Communications, who reviewed the final output. They thank the **Berkman Klein Center for Internet & Society at Harvard University** for organizing this research sprint, particularly **Valerie Gómez, Lis Sylvan, Ellen Willemin, Mawish Raza, You Jeen Ha, Madeline McGee and Adam Nagy.** They also thank the organizations co-hosting this research sprint, namely **Access Now, Edgelands Institute and MetaLab at Harvard University** for bringing together an amazing group of speakers and researchers to spark thoughts and conversations for over two months. They are grateful to the **research cohort of the fall 2022 research sprint** for bringing new perspectives to the table and opening their minds to new realities and needs.

Team backgrounds

Mariana Rozo-Paz is a Research Associate at the Datasphere Initiative, an organization that seeks to responsibly unlock the value of data for all. A lawyer and public policy professional, she graduated summa cum laude with minors in international studies and political science from Universidad de los Andes in Colombia. She has studied AI and digital policy, data for policy and international law at Sciences Po, University of Chicago, and American University.

Jack Smye is a lead technologist working with Research Casting International focused on developing frameworks for open science. He holds a Master's degree in Political Economy where he wrote his thesis on digital identity and he is currently working through a degree in computer science with a focus on systems of digital democracy.

Sourav Panda is a joint degree candidate pursuing MBA from CEIBS, and MA in Law and Diplomacy from The Fletcher School, where his focus is on Technology Policy. Sourav has worked

for the State Bank of India, the United Nations, The World Bank, and European venture capital funds. He plans to work with international organizations to continue helping build inclusive societies.

Report citation and copyright

Rozo-Paz, M., Smye, J., Panda, S. (2023). *Enhancing Inclusion in Digital Identity Policies and Systems: An Assessment Framework*. Berkman Klein Center for Internet & Society at Harvard University.

Table of Contents

EXECUTIVE SUMMARY

Systems of digital identity are emerging in nearly every part of the world as a means of transitioning societies into a digital future – there is an ere of inevitability to it and it seems almost certain that these systems will impact nearly every person on the planet. While there is without question significant benefits that can be had by these developments, it should be stated very clearly that these benefits are far from certain for everyone. Indeed, one of the most important questions we must continuously ask is with the way these systems are being developed, who will truly benefit and who will be excluded; though it should also be explicitly stated that the process of exclusion inevitably exacerbates discrimination and the exploitation of vulnerable populations.

Our team wanted to address this question directly by developing a framework of recommendations for good practices that ensure systems of digital identity are developed with an inclusive mindset with the benefits of digital identity being accessible by all. But rather than creating our own set of recommendations, we chose to explore and synthesize what has already been created by a variety of individuals and organizations (some of whom are doing incredible work). We analyzed over 50 guidelines, policy recommendations, manifestos, white papers, and everything in between from International Governmental Organizations, Academics, Non-Governmental Organizations/Civil Society, States, and the Private Sector. While these guidelines varied greatly in their scope and intended audience, we focused exclusively on the principles associated with inclusion and exclusion.

We acknowledge that our search methodology has limitations. As we needed our dataset to be manageably sized; we put together a sample limited in number but representative in terms of stakeholder groups and geography. We are also aware of our language limitations, as searches were carried out only in English, French, Portuguese, and Spanish, as well as those limitations provided by the very functioning of the search tools we used. However, as this paper aims only to further the conversation on this often-overlooked topic within digital ID discussions, we believe our methodology has served its purpose.

Based on the mapping of guidelines, principles, and practices developed by various groups of stakeholders, we developed the Inclusion Assessment Framework - a tool we propose to evaluate inclusion in digital identity systems and policies. The tool was developed based on synthesizing

what stakeholders are already designing as part of digital ID systems. In this paper, we propose such an assessment framework and highlight a series of examples of practices developed by key actors that could elucidate its application. While we do not apply the framework to any case studies, we believe that this could be the next logical step to take.

With all of these caveats, we would say that the most prominent theme that presented itself again and again with regards to inclusion was the need for meaningful and transparent consultation with all of the communities that the system hopes to reach; this aspect made itself well-known in all of the common practices that we identified for an inclusive digital identity system. In addition to this, many of the organizations recognize the need for strong and legitimate legal frameworks for managing potential abuses, and most of them also declared the need for independent and transparent auditing for wrongdoing and misuse. Further, it was asserted many times that these systems should absolutely not be rolled out without these legal frameworks in place (of which, again, consultations should be made on the ground level).

With regards to our process, our team developed an analytical lens for conceptualizing all of the practices, which includes ensuring that communities are ***aware*** of all of the systems and potentials, that they have easy ***access*** to all of the different benefits, and that they are ***integrated*** in a way that allows for them to control and determine their own way forward. While we initially identified 17 key aspects during our mapping exercise that examined the 50+ sets of guidelines, we synthesized them into **7 Good Practices to Foster Inclusion**:

- **Mandatory Accessibility**
- **Informed Consent and Free Choice Between Multiple Identity Systems**
- **Acknowledged Information Asymmetries, Various Literacy Levels, and Mitigated Technology Gaps with a Clear Plan for Dissemination**
- **Control Over Data and Changing Identity**
- **Eliminating Discrimination and Managing Unintended Consequences**
- **Integration for Policy-Making, Advocacy Efforts, and Democratic Participation**
- **Specific Integration of Communities and Groups: Inclusion by Design**

Throughout our research, it became more and more clear to us that an inclusive identity system goes far beyond digitally storing one's identity attributes. Indeed, the development of digital identity should be recognized as monumental social change, and most of the Non-Governmental

Organizations argued in favor of a human-rights based approach (though a concrete indication on how to do that was somewhat absent). We also identified a concept that is more prevalent in the Web 3.0 space having to do with 'Digital Personhood' as opposed to digital identity. We believe this to be a far stronger representation of an inclusive system – where systems are more-so thought of as networks for individuals to interact with communities in a form of self-realization while simultaneously serving as a foundation upon which to build social trust and reciprocity. Additionally, we would again state the importance of community in inclusive development and how the involvement of community leaders and civil society members is absolutely essential. It is our hope that this document is therefore read somewhat as a mandate to governments, policy-makers, and institutions to open these developments to the communities that will most be impacted by them. And as for the individuals and community members that come across this, we hope you read this as an invitation to get involved and help ensure that these systems will be beneficial for all.

I. INTRODUCTION

Impulsed by the call set on Sustainable Development Goals (SDGs) – goal 16.1 determines the objective of having legal identity for all by 2030 – and the Covid-19 pandemic that pushed for various public and private services moving online, digital identity systems are currently underpinning the digital transformation of countries worldwide.[1][2] The benefits they promise are various, including the transformation of financial schemes, fostering inclusion (e.g., by promoting greater access to goods and services), and increasing formalization (e.g, reducing fraud, protecting rights, increasing transparency and promoting digitization).[3] Many countries around the world have therefore introduced technologies that support digital ID systems that allow for an individual's identity attributes to be digitally available as a means of 'leapfrogging' more traditional

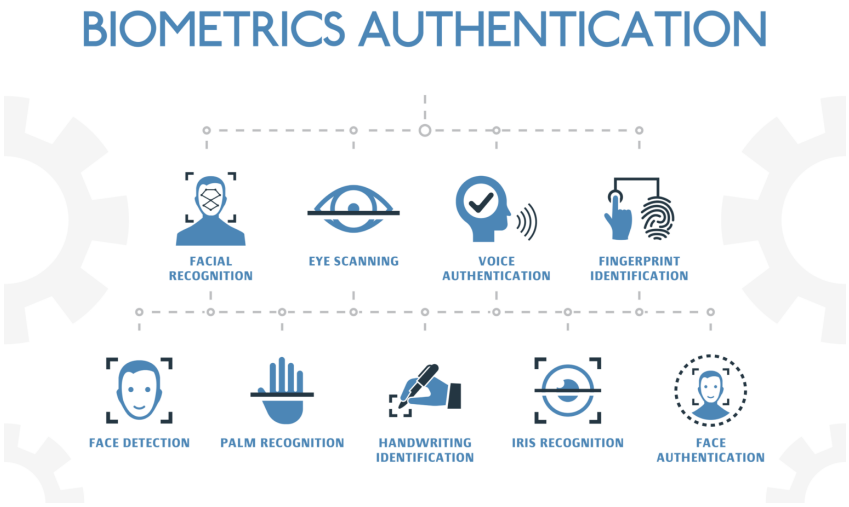
[1]United Nations Statistics Division, "SDG Indicators: Metadata Repository," Sustainable Development Goals, Nov. 2022,https://unstats.un.org/sdgs/metadata/?Text=&Goal=&Target=16.1

[2]World Bank, "Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable," The World Bank, Aug. 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

[3] McKinsey Global Institute. (2019). *Digital Identification: A key to inclusive growth*. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

paper-based systems.[4] Systems based around a user's physical data are known as biometrics and these systems can include everything from fingerprints to eye scans and sometimes even behavioral data.[5] Overall, these technologies promise to bring a series of benefits for societies and aim to support SDG 16.1.

Figure 1. Biometrics Authentication Services



Retrieved from Gatekeeper.

Nevertheless, digital identity technologies and systems pose a variety of risks and challenges. If these are not overcome, benefits will hardly be unlocked for all. Digital identity systems could potentially increase the risk of exclusion of already marginalized groups, especially because of lower levels of digital literacy and lack of access to electronic devices, vulnerability of certain communities, data protection challenges, privacy risks and even power imbalances.[6] Risks range from infrastructure to rights and trust issues.

The profound digital and data gap in infrastructure, technology, and skills, especially in the Global South, poses an additional level of complexity for digital ID systems.[7] In countries where there is a

[4] World Bank, *Technology Landscape for Digital Identification* (Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO [CC BY 3.0 IGO] 2018); Identity 2020 Systems, *The Need for Good Digital ID is Universal* (2019); World Bank Development Report, *Enabling Digital Development: Digital Identity* (2016).
[5] Jain, Anil and Pankanti, Sharath, *The Essential Guide to Image Processing (Second Edition)* (Academic Press, 2009), 649-676 https://doi.org/10.1016/B978-0-12-374457-9.00023-8
[6] Theodorou, Y. (2022). *On the Road to Digital ID Success in Africa: Leveraging Global Trends.* Tony Blair Institute for Global Change. https://institute.global/policy/road-digital-id-success-africa-leveraging-global-trends
[7] Handforth, Calum and Lee, Kendrick. "How Digital can close the 'identity gap.'" *UNDP Blog. United Nations Development Program.* May 19 2022. https://www.undp.org/blog/how-digital-can-close-identity-gap

significant gap with regards to access to services between rural and urban communities, there is already a challenge when it comes to accessing legal identity services; connectivity, infrastructure and literacy gaps only deepen the divide and the challenge of implementing digital ID systems. Further, this is only one aspect of the challenges.[8]

Communities around the world have expressed their concern with regards to the data that is being collected by these systems and what it is being used for.[9] Many have even expressed fear of the technologies that are being implemented in their countries and are unwilling to trust any form of digital tool that contains their ID.[10]

The rapid push for digital identity in times of crisis only exacerbates the gaps and the challenges. Specific communities are more vulnerable to the threats posed by these technologies and the risk of exclusion is on the rise. Migrants and refugees,[11] for instance, are being excluded from many digital ID systems since their constant mobility stops them from settling in one place and acquiring an ID. Some of them – as they are not nationals of their host countries – do not classify to obtain a digital ID, many arrive in a country without physical documentation, and many are simply not willing to obtain a digital ID because of the uncertainty of what governments might do with the data they collect. Other vulnerable communities to digital identity policies and services include women and girls,[12] LGBTQI+ communities (trans people in particular),[13] children and youth,[14] indigenous communities,[15] among other groups.

---

[8] *ID4D Practitioner's Guide (English).* Identification for Development Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide

[9] Hernandez, Marianne D. "Digital identity: Our five calls to action for the World Bank." *AccessNow Blog. AccessNow.* Sept. 28 2022. https://www.accessnow.org/digital-identity-world-bank/

[10] Bogle, Ariel; Workman, Michael; Karagic, Dung. "Minor parties spread 'big brother' fears as they ramp up campaign against proposed digital ID laws," ABC Investigations, May 1 2022. https://www.abc.net.au/news/2022-04-26/minor-parties-campaign-against-digital-id-proposals/101014152

[11] United Nations High Commissioner for Refugees, *UNHCR Strategy on Digital Identity and Inclusion* (UNHCR, n.d.) https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf

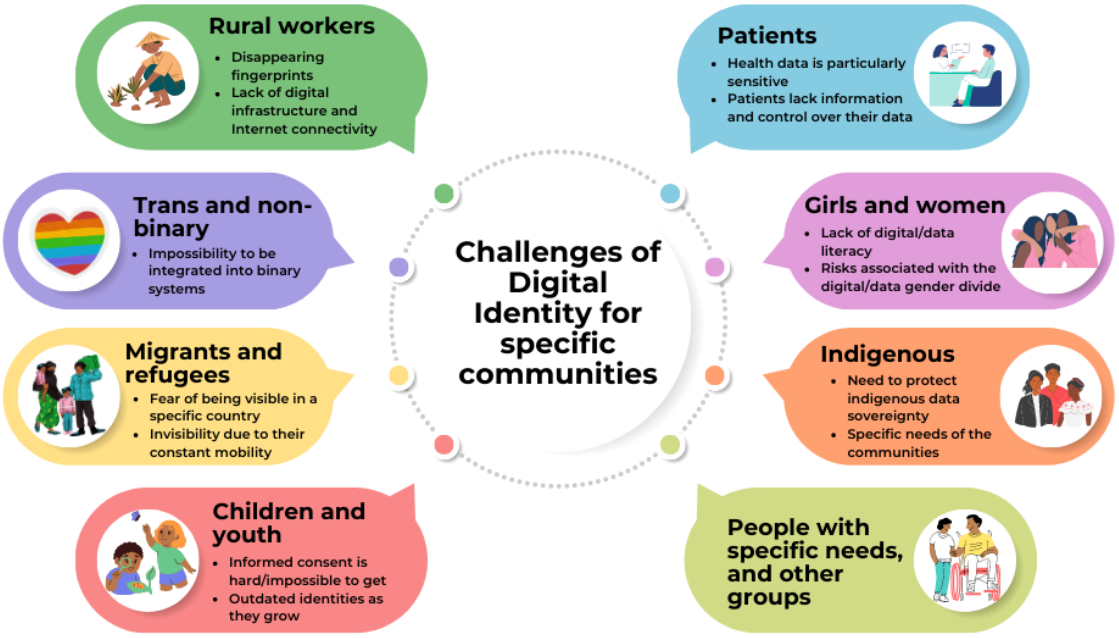
[12] Hanmer, Lucia and Dahan, Mariana. "Identification for Development: Its Potential for Empowering Women and Girls." *World Bank Blogs. Digital Development.* Dec. 2 2015. https://blogs.worldbank.org/digital-development/identification-development-its-potential-empowering-women-and-girls

[13] Os Keyes. 2018. "The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition," (Proc. ACM Hum.-Comput. Interact. 2, CSCW, Article 88 , Nov. 2018) https://doi.org/10.1145/3274357 https://ironholds.org/resources/papers/agr_paper.pdf

[14] Bailur, Savita and Smertnik, Helene. "Identification and identity for children in the digital age." *Caribou Digital Blog. Medium.* June 4 2020. https://medium.com/caribou-digital/identification-and-identity-for-children-in-a-digital-age-2409dc633ffa

[15] The World Bank, *International Bank For Reconstruction And Development Project Appraisal Document On A Proposed Loan In the Amount of US$ 225 Million To The United Mexican States For A Mexico National Digital Identity System to Facilitate Inclusion [Report No. PAD4044]* (IBRD + IDA World Bank Group 2020).

Graph 1. Risks and Challenges of Digital Identity Systems for Some Communities



Developed and designed by Mariana-Rozo Paz

The consequences of not actively including these communities in digital identity systems and policies range from the risks of discrimination and exclusion – not only from accessing the system but from benefiting from the advantages of being part of the system – to misrepresentation and perpetuation of existing gaps. Not fully incorporating communities in the systems could deepen digital and data gaps, as well as inequality. This could also lead to individuals and groups being directly harmed by the systematic lack of access and exclusion from public and private services.

To address communities' concerns and views, digital identity policies and systems need to incorporate elements of both protection and of inclusion.[16] Elements of protection include measures related to data protection, privacy, cybersecurity, and overall security by design. With that said, it is safe to say that protection elements have been incorporated in the majority of the recently released policies and systems for digital identity. Elements of inclusion, on the other hand, imply taking into consideration the needs of specific communities and groups as well as the

https://documents1.worldbank.org/curated/en/657131611543704157/pdf/Mexico-National-Digital-Identity-System-to-Facilitate-Inclusion-Project.pdf

[16] This was an ongoing discussion during the Research Sprint on Digital Identity. It was particularly discussed during the fifth session by Fabro Steibel.

existing disparities in a given context. This means looking out for tools that enable consent, avoid misuse of data, are inclusive by design, and so on.

While elements of protection are generally highly incorporated into digital identity systems and policies, elements of inclusion have often been forgotten or overlooked; policies and systems tend to stop once they have incorporated a measure to tackle privacy and security. This only increases the risk of deepening exclusion and leaving several groups and communities behind. **That is why several organizations and groups of stakeholders have started publishing guidelines, good practices, and principles that aim to enhance inclusion elements for digital identity policies and systems.**

This policy paper seeks to dive deeper into those practices around inclusion to showcase the different organizations working on the matter. Based on a non-exhaustive mapping of those stakeholders' practices around inclusive digital identity, it aims to propose a **useful assessment tool – the Digital Identity Enhancing Inclusion Tool –** for policymakers and technicians to design and evaluate inclusive digital identity systems and policies and ensure that their value is unlocked for all.

On a broader scope, several assessment tools have been developed in the past years to ensure policies' efficacy. For example, various assessment frameworks are currently being implemented to evaluate the level of digital maturity in a company or country.[17] Human rights impact assessments[18] have also been utilized to evaluate policies and contexts in developing countries. Within that same line of thought, the goal of this research project was to reflect around the ways in which digital identity policies and systems could be assessed. While there are innumerous ways of approaching this challenge, we focused on the inclusivity aspect as it tends to be forgotten in digital ID systems. By analyzing and comparing initiatives from different groups of stakeholders, we built – and hereby propose – an inclusion framework that could serve to evaluate these systems in practice. We expect that this first step will contribute towards building more inclusive and comprehensive digital identity systems.

[17] For more information, visit: https://digitalmaturity.org/
[18] For more information, visit: https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox#:~:text=Human%20rights%20impact%20assessment%20

With this goal in mind, this paper includes the following sections. Section II will dive deeper into the methodology that was followed to build the inclusion framework. Then, Section III will venture into the components of the framework. Section IV will explain the visualization developed to display the initiatives mapped and the elements of inclusion that they incorporate. Finally, Section V will provide the key measures that should be assessed at each 'level' or component of the framework. Following this, Section VI will delineate the steps ahead and draw some conclusions.

II. METHODOLOGY

This project started with the intention to bring stakeholders together to build better digital identity systems. With that intention in mind, we had originally decided to create the *Digital Identity Living Hub*, a space (or platform) where different stakeholders could come together to share the good practices that they were developing for digital identity systems and policies, and where civil society and other groups could also share their concerns with regards to these systems and the challenges they were facing in their contexts. Nonetheless, realizing the complexity of building such a platform and the restricted sprint's timeline, we spurred into the development of a tangible and valuable output that could potentially support the creation of the *Digital Identity Living Hub* in the future. **With this in mind, we decided to work towards building a tool for policymakers and practitioners that could guide the development (and potential revision or assessment) of more inclusive digital identity policies and systems based on the good practices that were already being created by stakeholders around the world**. To that end, our methodology followed four phases which are explained below.

Phase I: Mapping of relevant stakeholders

The first phase of the project was developed throughout the research sprint. We all contributed to a collaborative database of organizations and initiatives working on digital identity. Then, based on individual preference, each team member was assigned one group of stakeholders for which they had to map the most relevant actors and their initiatives related to digital identity. We targeted documents being produced by these actors and which they classified as "principles", "guidelines", or "good practices" for digital identity. The groups of stakeholders were: international non-governmental organizations, private sector, States (or government-led initiatives), academia, and civil society organizations (including non profits). This mapping was consolidated in a

spreadsheet database in which the principles, guidelines and practices were summarized and linked. We mapped over 50 guidelines, principles and practices, and then we selected 42 to undergo deeper content analysis and review based on the information we were able to ascertain; some organizations did not provide details on the documents or guidelines they were developing or there was not sufficient information to move forward with the analysis.

Phase II: Content Analysis

The content analysis phase started once the relevant organizations were identified and the principles, guidelines and practices they have developed were pinpointed. Throughout the sprint, we had reflected about the lack of inclusion elements in digital identity systems (e.g., gender lens, participatory approaches, perspectives that considered the different digital literacy levels, etc.) while elements of protection (e.g., cybersecurity, data protection and privacy) were usually present in the systems and policies. This is why we decided to analyze the compiled guidelines, principles and practices from an inclusion lens.

The content analysis thus consisted of reviewing the mapped documents in detail and marking if elements promoting inclusion were present or not in a specific set of guidelines, principles or practices. Based on the conversations with participants and speakers from the research sprint, we were able to delineate a series of categories or inclusion practices that could enable inclusion in digital identity. Some of these elements included informed consent, the consideration of different literacy levels (and gaps), the possibility to select between digital ID systems, the needs of specific communities, among others. As we dived deeper into the guidelines, principles and practices, we identified and created 17 categories of items that actively promoted inclusion in digital identity systems and policies. Details of these 17 categories, their definitions and examples can be accessed in the Annex.

Phase III: Framework Development

To better support the 17 categories extracted from the mapping and content analysis phases, we decided to build a more comprehensive framework that could not only contain these categories, but also give room for more categories to be created and added as stakeholders innovate in digital identity systems and policies. Thanks to the work throughout the sprint and previous work on inclusion, we created three levels that could be fundamental to assess inclusion, and where these

17 elements of inclusion could serve as examples of practices that could materialize such inclusion levels. The three levels of the framework are: awareness, access, and integration. Through a series of collective brainstorming sessions, we defined how each element could portray either one, two or even the three levels of assessment. More details of the proposed framework and how the 17 elements were classified in it can be found in Section III.

Phase IV. Development of the Good Practices to Foster Inclusion

Thanks to the detailed mapping of principles, guidelines and practices developed by different groups of stakeholders, we were able to identify commonalities between their approaches and extract the 17 elements of inclusion. From there, we worked to synthesize these elements into more comprehensive practices and extract a series of valuable findings by identifying similarities in all of the different actors' approaches.

As the mapping process unfolded, it became very apparent that an inclusive identity system is not simply storing one's identity attribute in a protected way. Rather, it is a monumental social change worthy of such recognition and deserving of a human-rights based approach. With this, we also recognized that nearly every piece we scanned emphasized the importance of community in inclusive development and how the involvement of community leaders and civil society members is absolutely essential.

Based on the commonalities between them, we grouped the 17 elements of inclusion into seven categories in order to facilitate analysis and visualization. The groups compile the measures that are intrinsically interrelated and should be analyzed jointly.

- **Mandatory Accessibility**: this category groups practices or measures related to the obligation that governments or companies have of ensuring that all individuals and communities have access to the digital identity system.
- **Informed Consent and Free Choice Between Multiple Identity Systems**: this category groups both the need to ensure that individuals and communities give their informed consent to be part of a system, and at the same time are given the chance to select the system they wish to be a part of, or change systems (and thus their consent sometimes).
- **Acknowledged Information Asymmetries, Various Literacy Levels, and Mitigated Technology Gaps with a Clear Plan for Dissemination**: this category groups the elements

related to the profound existing digital gaps in terms of information, literacy, and infrastructure, as well as a solution to some of these gaps - such as the importance of clear dissemination plans and information campaigns to ensure that everyone is included.

- **Control Over Data and Changing Identity**: this group refers to effective integration of individuals and communities into a group and brings together the need to have control over one's data and the possibility within a system for an identity to change and evolve as time (or transitions) pass.
- **Eliminating Discrimination and Managing Unintended Consequences**: these two elements were brought together into a group since the fight against discrimination implies that there are also measures put in place to manage unintended consequences and repair if harm is inflicted by a digital identity system.
- **Integration for Policy-Making, Advocacy Efforts, and Democratic Participation**: this group is integrated by the elements related to high-level impact, such as the importance of improving policy decisions based on the insights of a specific digital ID system, the fundamental role of advocacy that many stakeholders highlighted, and how democratic participation is key to build inclusive digital identity systems.
- **Specific Integration of Communities and Groups: Inclusion by Design**: this category brings together the efforts that many stakeholders are deploying to effectively include communities such as women and girls, LGBTIQ+, rural workers, elder people, migrants and refugees, among others to the very design of the systems. This implies adopting gender and non-discriminatory lenses.

This grouping effort resulted in the seven groups of "good practices to foster inclusion" in digital identity. These practices will be explained in detail – leveraging examples from the mapped principles, guidelines and practices – in Section V.

Once these seven categories were set, we developed a second content analysis phase by reviewing if each set of principles, guidelines or practices incorporated elements of awareness, access, and/or integration per group. For example, for the World Bank's Principles on Identification for Sustainable Development, we reviewed if the group of *Informed Consent and Free Choice Between Multiple Identity Systems* was contemplated as part of the principles, and at which level(s): awareness, access, or integration.

Inspired by the work of previous research sprinters,[19] we realized that a visualization to portray and display the results of the research could be valuable for policymakers and for everyone curious to *see* the conclusions that we had reached. That is how we ventured into the visualization alternatives that we had available to display our work. Based on the second round of content analysis and updated database, we came up with a visualization that will be explained in more detail in Section IV.

Other Considerations

Finally, we acknowledge that our search methodology has limitations. We are aware of and would like to emphasize the non-exhaustive character of our mapping of organizations and their guidelines, principles and practices. We aimed to provide a preliminary mapping and cataloging of initiatives as a sort of synthesis; how similar or different they are and what are the core issues they called attention to in order for digital identity efforts to be more inclusive.

As we needed our dataset to be manageably sized, we put together a sample limited in number but representative in terms of stakeholder groups and geography to the best of our ability. We are also aware of our language limitations, as searches were carried out only in English, French, Portuguese, and Spanish, as well as those limitations provided by the very functioning of the search tools we used. However, this is only one contribution to the conversation between different groups of stakeholders that aim to not only build safe digital identity policies and systems, but also inclusive ones that unlock their value for all. As this paper aims only to further the conversation on this often-overlooked topic within digital identity discussions, we believe our methodology has served its purpose.

[19] See *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI* at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482

III. INCLUSION ASSESSMENT FRAMEWORK

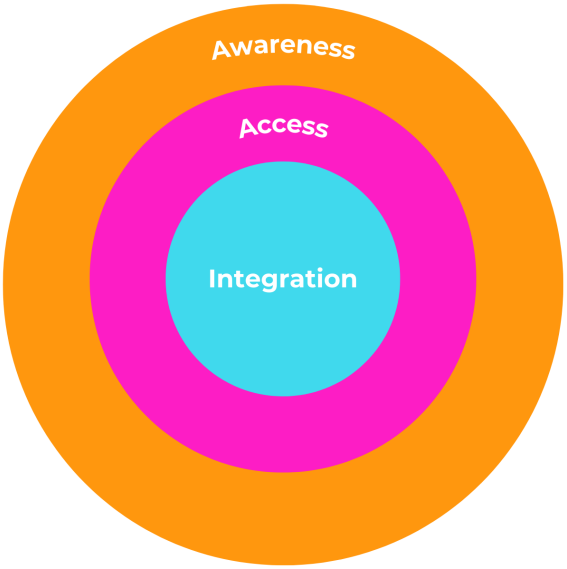
In the past years, assessment and evaluation tools have been developed to ensure that policies and systems are efficient in achieving the goals for which they were developed. From digital maturity[20] to human rights protection,[21] assessment frameworks are on the rise, especially thanks to data-driven decisions and the importance of evidence-based decisions and policy making. Similar types of assessment tools could be beneficial for digital identity systems and policies. As we learned throughout the research sprint, protection elements related to cybersecurity and data protection are usually incorporated into digital identity systems, but inclusion elements tend to be forgotten. An inclusion assessment framework could not only support policymakers and practitioners to assess the systems they have designed and/or implemented, but it could also provide them with solutions, ideas and innovations around enhancing inclusion in digital identity.

Based on the sprint's reflections and on the work of our team analyzing and comparing initiatives from different groups of stakeholders, we built – and hereby propose – an inclusion framework that could serve to evaluate these systems in practice. We expect that this first step will contribute towards building more inclusive and comprehensive digital identity systems.

The layered model displayed in Graph 2 below is composed of three levels from which systems and policies could be assessed. It was built based on the mapping of principles, guidelines and practices that enhance inclusion, developed by different groups of stakeholders. The Inclusion Assessment Framework is composed of three levels that could be measured: 1) Awareness, 2) Access, and 3) Integration.

[20] For more information, visit: https://digitalmaturity.org/
[21] For more information, visit: https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox#:~:text=Human%20rights%20impact%20assessment%20

Graph 2. Inclusion Assessment Framework



Developed by Mariana Rozo-Paz and designed by Natalia Loungou.

The proposed Inclusion Assessment Framework seeks to support the assessment of digital identity systems and policies at three levels. Definitions of what each level of assessment could imply are found below:

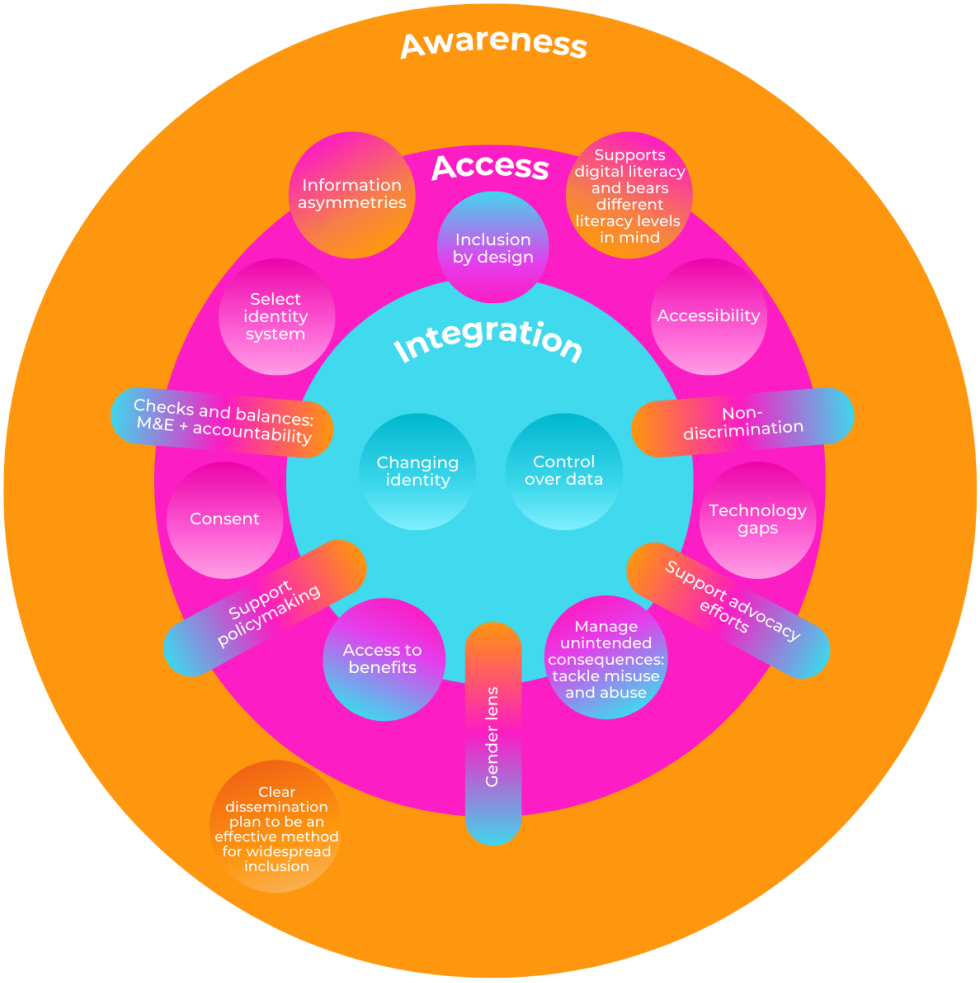
- **Awareness** refers to the extent to which individuals, communities, and actors *know* and *are aware* that either a digital identity policy or tool is being developed or is being implemented in their country. This level of analysis is fundamental when it comes to fostering inclusion precisely because it implies that knowledge and information is shared widely and is publicly available for people to understand the benefits and risks of such systems and all of their implications (e.g. interactions with public services). Awareness also relates to the need for digital and data literacy, and overall for access to information. Governments and public entities are often the ones in charge of disseminating information and potentially skills, and ensuring that citizens know about the policies and systems being put in place, the benefits of using them (e.g., accessing services), the risks of adopting these services (e.g., explaining how their data will be collected and used and what type of information they might be sharing by adhering to a digital identity system), and the potential implications of lack of adoption.

- **Access** or accessibility relates to the *availability* of the system and the *possibility of accessing* the system and its benefits by all individuals and communities. This level of analysis is connected to the possibility that people have of selecting the digital identity system they want to be a part of and of being able to access any system of their preference based on clear information on the benefits, risks and other implications. It also relates to the possibility of people giving their consent to be part of these systems – which requires having full information and thus full "Awareness"– and how governments and people are able to deal with technology gaps to ensure equal access and inclusion.

- **Integration** refers to the *effective inclusion* of an individual or community into a digital identity system and the different possibilities that derive from being part of that system. One element bound to this analytical level is, for instance, the understanding that identities change because people change and communities evolve. Integration elements enable individuals' identities to change over time, and are open for the system to adapt. In that regard, another element of integration is the possibility that people have of controlling their data, and deciding if they want it to be used for certain purposes or not. This means allowing for different waves of adoption, and due to such personal choices by individuals or the different awareness and access levels that they have, contingency plans might need to be put in place as well as potential exceptions, so individuals and communities are not excluded. If somebody opts out, the consequences – which could indeed include being denied some service – need to be acknowledged. This is fundamental, as the provision of public services tends to be tied with human rights' protection.

Furthering the Framework beyond its three core layers and as a means of deepening analysis, we mapped our proposed "17 inclusive aspects" onto the Framework to demonstrate the interconnected nature of Awareness, Access, and Integration and how the aspects in themselves look through this analytical lens. They represent core expected actions that, based on our mapping of principles, guidelines, and practices, could support a more inclusive digital identity system or policy. Graph 3 depicts how these 17 inclusive aspects interact with the Inclusion Assessment Framework at three different levels.

Graph 3. Elements of the Inclusion Framework



Designed by Natalia Loungou.

The 17 inclusive aspects interact at the three levels of the Inclusion Assessment Framework. For instance, *"Clear dissemination plan to be an effective method for widespread inclusion"* is an expected action that in principle falls under the Awareness layer as it implies that people know about the system. Adopting a *non-discrimination* lens is, on the contrary, a transversal element that should be incorporated at all levels (from Awareness, to Access, to Integration). Another example is that of "*managing unintended consequences"*, which is a shared element at the Access and Integration levels; it requires, for instance, that misuse of data and other undesirable consequences are tackled both when people access the systems and when they are integrated into them. A detailed description of the elements proposed in Graph 3 are available in the Annex.

IV. VISUALIZATION: DIGITAL IDENTITY INITIATIVES ENHANCING INCLUSION

The **Digital Identity Initiatives Visualization** was designed by Natalia Loungou based on the proposed Inclusion Assessment Framework. It is arranged like a wheel and seeks to provide stakeholders with a preliminary and non-exhaustive mapping of the guidelines, good practices, and principles that different groups of stakeholders have developed to promote inclusion in digital identity policies and systems.

Documents (containing principles, guidelines or practices around digital identity) are arranged around the wheel, and color-coded depending on the issuing stakeholder: intergovernmental organizations are orange, academics are pink, State-level actors are blue, civil society organizations and non-profit organizations are green, and private and tech sectors are purple.

As mentioned in Section II (Methodology), the 17 inclusive aspects that had been identified as categories through which inclusion was being promoted in digital identity systems were synthesized into seven groups of "good practices". That is why inside the wheel are seven rings, which represent the seven groups of practices to foster inclusion in digital identity systems. The level of the framework (awareness, access, integration) at which each group is present in each document is indicated by: a circle for awareness, a rhombus for access, and a start for integration. We suggest that comparisons are made within a given theme and across documents (and hence stakeholders), but not between themes.

Once again, we would like to acknowledge that this does not intend to be an exhaustive mapping of stakeholders or initiatives around digital identity. With this visualization we aim to provide a preliminary mapping and cataloging of initiatives as a sort of synthesis of the core aspects they are incorporating to unlock the benefits of digital identity for all. The Inclusion Assessment Framework in which this visualization is based is a suggestion of how to leverage these guidelines, principles and practices to build more inclusive digital identity systems and policies for all.

Mapping Digital Identity Initiatives

How to read

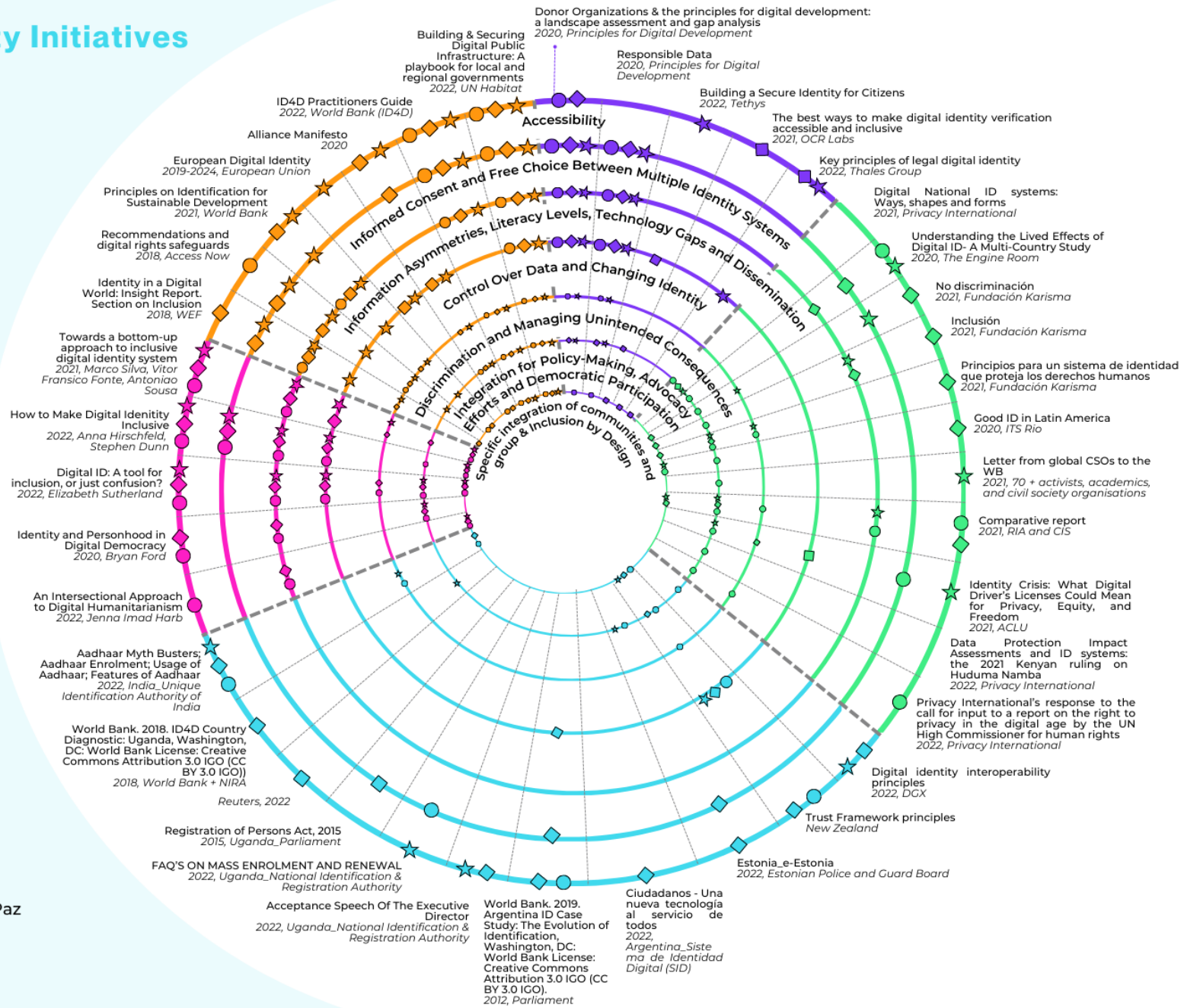
Name of guidelines
Year, Issuer

Elements to foster inclusion

- Awareness
- Access
- Integration

Types of stakeholders

- Intergovernmental Organizations (IGOs)
- Academia
- State
- Civil society organizations & NGOs
- Private-Tech



Framework developed by Mariana Rozo-Paz
Designed by Natalia Loungou
With support from:

DATASPHERE INITIATIVE

V. PRACTICES TO FOSTER INCLUSION

This section compiles the seven main groups of practices to foster inclusion extracted from the mapping of principles, guidelines and practices of different groups of stakeholders. These are examples of practices that stakeholders are developing to enhance inclusion. The groups of practices below could guide the application of the Inclusion Assessment Framework, since they could be considered as core expected actions to foster more equitable, inclusive and participatory digital IDs. While non-exhaustive, they provide further relevant insights for policymakers on how to ensure that inclusion elements are borne in mind and incorporated into digital identity policies and systems.

A. Mandatory Accessibility

One of the primary considerations with regards to the needs for accessibility in digital identity has to do with the meaningful consultation of all communities in a transparent and inclusive manner.[22] At the level of conceptualization, consideration must be given to the disproportional impact on people with disabilities, LGBTQI+ communities, and other vulnerable populations;[23] research from Uganda highlights how it may be harder for women and older persons to obtain a mobile phone, for instance.[24]

Participation in these systems must be free from discrimination and not depend on race, gender, nationality, wealth, age, privilege, or anything of the sort.[25] Systems should have multiple entry points as well as a multi-channel service delivery approach to make enrollment easy for any

[22] "National Digital Identity Programmes: What's next? - Access Now," Access Now (Access Now, May 2018), https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf.

[23]Elizabeth Sutterlin, "Digital ID: A Tool for Inclusion, or Just Confusion?," DemTools, June 22, 2021, https://dem.tools/blog/digital-id-tool-inclusion-or-just-confusion; Barker, Sara and Rahman, Zara, *Understanding the Lived Effects of Digital ID: A Multi-Country Study*, (The Engine Room, 2020) p.56-57, https://digitalid.theengineroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf

[24] Bhalla, Nita, "Uganda sued over digital ID system that excludes millions," *Technology, Media and Telecommunications (blog). Thomas Reuters Foundation.* May 15 2022. https://www.reuters.com/article/uganda-tech-biometrics/feature-uganda-sued-over-digital-id-system-that-excludes-millions-idUKL3N2X32RG.

[25]Ford, Bryan, "Identity and Personhood in Digital Democracy: Evaluating Inclusion, Equality, Security, and Privacy in Pseudonym Parties and Other Proofs of Personhood," (Swiss Federal Institute of Technology in Lausanne, 2020), https://arxiv.org/pdf/2011.02412v1.pdf; The World Bank, *Principles on Identification for Sustainable Development: Toward the Digital Age* (World Bank, 2021), https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf.

individual of any socioeconomic or demographic segment; users must not be dependent on a digital identity for access to basic human rights.[26] This means interoperability between different organizations and systems[27] as well as the meaningful, high-level participation of civil society groups and other experts in cooperation with industry and decision makers.[28]

Registration processes must be simple and free of cost, and synergies between ID, mobile communication, and financial inclusion can be used for inclusive and effective policy design.[29] Services must be multilingual and in the language of the expected users (including migrant populations), and user needs should be considered with user feedback being collected for future design and modification.[30]

Beyond this, relevant policy instruments must be translated into local languages and not written in an overly technical manner, and efforts must be made to increase usability and discoverability of

[26] World Economic Forum. *Insight Report - Identity in a Digital World: A new chapter in the social contract.* (WEF, 2018), https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf; Barbosa, Alexandre, Celina Carvalho, Cláudio Machado, and Janaina Costa. *Good ID in Latin America*: Strengthening appropriate uses of Digital Identity in the region (Instituto de Tecnologia & Sociedade de Rio, 2020). https://itsrio.org/wp-content/uploads/2020/07/Report_Good_ID_ENG.pdf; DGX Digital Identity Working Group. *Digital Identity in response to COVID-19: DGX Digital Identity Working Group. (*Digital Transformation Agency [Commonwealth of Australia] 2022) p. 20, https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf.

[27] "Estonia - We Have Built a Digital Society & We Can Show You How." e-Estonia, November 29 2022. https://e-estonia.com/.

[28] "National Digital Identity Programmes: What's next? - Access Now," Access Now (Access Now, May 2018), https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf; Privacy International, "Letter from global CSOs to the World Bank," Sept. 6 2022, https://privacyinternational.org/advocacy/4945/letter-global-csos-world-bank; Barker, Sara and Rahman, Zara, *Understanding the Lived Effects of Digital ID: A Multi-Country Study,* (The Engine Room, 2020) p.56, https://digitalid.theengineroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf

[29] Gelb, Alan and Mukherjee, Anit, *Building on Digital ID for Inclusive Service: Lessons from India,* (Center for Global Development, 2019) https://www.cgdev.org/sites/default/files/building-digital-id-inclusive-services-lessons-india.pdf; *ID4D Practitioner's Guide (English).* Identification for Development Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide.

[30]DGX Digital Identity Working Group. *Digital Identity in response to COVID-19: DGX Digital Identity Working Group.* (Digital Transformation Agency [Commonwealth of Australia] 2022) https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf; Barker, Sara and Rahman, Zara, *Understanding the Lived Effects of Digital ID: A Multi-Country Study,* (The Engine Room, 2020) p.56, https://digitalid.theengineroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf.

existing resources.[31] Systems should be transparent with users being able to understand the administrative rules, processes, and data services, and extra care should be taken to ensure this.[32] Any user with access to the internet should be able to use the system services without being dependent on the latest technology or downloading data intensive apps.[33]

B. Informed Consent and Free Choice Between Multiple Identity Systems

Inclusive digital identity should more-so focus on equal outcomes through alternative routes rather than the provision of a singular sophisticated service;[34] many individuals do not have safe and reliable access to state-based systems[35] and there could very well be a lack of trust in a mandatory single identity programme (resulting in a new form of exclusion).

Participation in the systems should be voluntary[36] and based on a user's needs, concerns, and rights,[37] and service systems should also be flexible in their acceptance of multiple identity systems (such as national and non-national, alien, refugee, etc).[38]

Digital identity should be embraced as a form of empowerment, and as such the technological, legal, and policy framework must incorporate principles of informed consent and user agency as well as the recognition of multiple forms, respect for privacy, and space for anonymity.[39]

---

[31] Anri van der, Vrinda Bhandari, Shruti Trikanad , and Yesha Tshering Paul, *Towards the Evaluation of Socio-Digital ID Ecosystems in Africa*, (Research ICT Africa, 2021) https://researchictafrica.net/wp/wp-content/uploads/2021/11/Comparative-Report_5.11.21-2.pdf; Haßler, B., Brugha, M., Muyoya, C., Mitchell, J., Hollow, D., & Jackson, A. *Donor Organizations & the Principles for Digital Development: A Landscape Assessment and Gap Analysis.* (Principles for Digital Development — Resource Development Program Asset No. 1, 2018). p. 13. [London: Jigsaw Consult. DOI: 10.5281/zenodo.1204703. License: Creative Commons Attribution-ShareAlike 4.0.] https://digitalprinciples.org/wp-content/uploads/PDD2018_interactive.pdf.

[32] *ibid.*

[33] OCR Labs (2022). Accessibility and Inclusivity at OCR Labs. https://ocrlabs.com/accessibility-&-inclusivity/

[34] Hirschfeld, Anna; Dunn, Stephen. "How to make digital identity inclusive," Public Digital, Feb. 3 2022, https://public.digital/2022/02/03/how-to-make-digital-identity-inclusive.

[35] ID 2020, "The Alliance Manifesto," 2022, https://id2020.org/manifesto (*Accessed Dec. 11 2022)*

[36] "Trust Framework Principles," New Zealand Digital government, accessed December 13, 2022, https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/trust-framework/trust-framework-principles/.

[37] World Economic Forum. *Insight Report - Identity in a Digital World: A new chapter in the social contract.* (WEF, 2018) p. 20, https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

[38] World Bank. 2019. *Argentina ID Case Study: The Evolution of Identification*, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). https://openknowledge.worldbank.org/bitstream/handle/10986/33403/Argentina-ID-Case-Study-The-Evolution-of-Identification.pdf?sequence=1&isAllowed=y; UPPC, Entebbe [Government of Uganda]. "The Registration of Persons Act, 2015." The Uganda Gazette 14 (108) 2015. https://www.ict.go.ug/wp-content/uploads/2018/06/Registration-of-Person-Act-2015.pdf

[39] AccessNow, *National Digital Identity Programmes: What's next?* (AccessNow, 2018) p. 3, https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf

With regards to informed consent, this includes aspects such as how data is collected as well as making it known that this data will not be used for any secondary purposes without additional consent.[40] This requires the development of resources to raise awareness about data and how users can address grievances while implementing values of transparency and openness.[41]

Extra consideration should also be given to the effect that power asymmetries have on informed consent and policies should be developed to offset these imbalances.[42] Finally, user's should be able to withdraw consent and opt out of a system without penalty at any time.[43]

C. Acknowledged Information Asymmetries, Various Literacy Levels, and Mitigated Technology Gaps with a Clear Plan for Dissemination

An inclusive identity system is dependent on the standards governing the system to be open and meaningfully available at all layers of society (including reasons for and the impact of).[44] Achieving this level of meaningful accessibility, however, requires a high level of civic education as a primary step in the deployment of the systems.[45] Educators and stakeholders must work to reduce the barriers that prevent individuals experiencing things such as low literacy levels or disability from accessing or using the programs, and information campaigns must be accessible as a means of ensuring that everyone has the knowledge they need to participate in the system while maintaining their control and rights.[46] Engagement with these communities at the design stage

---

[40] The World Bank, *Principles on Identification for Sustainable Development: Toward the Digital Age* (World Bank, 2021) p.18, https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf (*Accessed Dec. 11 2022)*

[41] Ibid; Principles for Digital Development, *Responsible Data*, (Pulse on the Principles, 2022) https://digitalprinciples.org/wp-content/uploads/PulseOnThePrinciples_RD.pdf.

[42]Barker, Sara and Rahman, Zara, *Understanding the Lived Effects of Digital ID: A Multi-Country Study*, (The Engine Room, 2020) p. 57, https://digitalid.theengineroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf.

[43]"Trust Framework Principles." *New Zealand Government Blog. Digital.Govt.NZ.* Jan. 18 2022. https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/trust-framework/trust-framework-principles/

[44]Sutterlin, Elizabeth. Digital ID: A Tool for Inclusion, or Just Confusion?. *DemTech Blog. DemTools.* June 22 2021. https://dem.tools/blog/digital-id-tool-inclusion-or-just-confusion.

[45] *Ibid.*

[46]The World Bank, *Principles on Identification for Sustainable Development: Toward the Digital Age* (World Bank, 2021), p.18 https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf. (*Accessed Dec. 11 2022);* Claudine Lim Manager at The Principles for Digital Development Claudine first joined the Digital Impact Alliance in October 201; " Haßler, B., Brugha, M., Muyoya, C., Mitchell, J., Hollow, D., & Jackson, A. *Donor Organizations & the Principles for Digital Development: A Landscape Assessment and Gap Analysis.* (Principles for Digital Development — Resource Development Program Asset No. 1, 2018). p. 13. [London: Jigsaw Consult. DOI: 10.5281/zenodo.1204703. License: Creative Commons Attribution-ShareAlike 4.0.] p. 9-14, https://digitalprinciples.org/wp-content/uploads/PDD2018_interactive.pdf.

should be considered as essential in ensuring that identity will meet their needs.[47] Further, it can help to demystify the systems which simultaneously contributes to higher levels of transparency and trust.[48]

Services should be available regardless of one's access to resources or connectivity and nobody should be denied these services because they lack devices, digital literacy, or digital skills.[49] Strong consideration should also be given into investing in hardware, software, and appropriate tools and resources as a global and public good,[50] and these considerations must again be addressed at the design stage; a possible way of alleviating these tensions is also offline enrollment.[51] Strategies for dissemination should involve high-impact distribution channels that reach out to as many people as possible, and possible systems of dissemination include mobile network operators, the health sector, or the energy sector – though this rollout should only occur after strong data privacy and protection practices are established.[52]

D. Control Over Data and Changing Identity

An inclusive identity system requires enforceable data privacy and protection frameworks which includes information on what data is being collected and for what reason.[53] Privacy should

---

[47] World Economic Forum. *Insight Report - Identity in a Digital World: A new chapter in the social contract.* (WEF, 2018) https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.

[48] Sutterlin, Elizabeth. Digital ID: A Tool for Inclusion, or Just Confusion?. *DemTech Blog. DemTools.* June 22 2021. https://dem.tools/blog/digital-id-tool-inclusion-or-just-confusion.

[49] The World Bank, *Principles of Identification for Sustainable Development: Toward the Digital Age* (World Bank, 2021), p. 13 https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf.

[50] Haßler, B., Brugha, M., Muyoya, C., Mitchell, J., Hollow, D., & Jackson, A. *Donor Organizations & the Principles for Digital Development: A Landscape Assessment and Gap Analysis.* (Principles for Digital Development — Resource Development Program Asset No. 1, 2018). p. 13. [London: Jigsaw Consult. DOI: 10.5281/zenodo.1204703. License: Creative Commons Attribution-ShareAlike 4.0.] https://digitalprinciples.org/resource/donor-organizations-the-principles-for-digital-development-a-landscape-assessment-and-gap-analysis/.

[51] World Economic Forum. *Insight Report - Identity in a Digital World: A new chapter in the social contract.* (WEF, 2018) p. 20, https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.

[52]Sutterlin, Elizabeth. Digital ID: A Tool for Inclusion, or Just Confusion? *DemTech Blog. DemTools.* June 22 2021.https://dem.tools/blog/digital-id-tool-inclusion-or-just-confusion; World Economic Forum. *Insight Report - Identity in a Digital World: A new chapter in the social contract.* (WEF, 2018) p. 20 https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf; Haßler, B., Brugha, M., Muyoya, C., Mitchell, J., Hollow, D., & Jackson, A. *Donor Organizations & the Principles for Digital Development: A Landscape Assessment and Gap Analysis.* (Principles for Digital Development — Resource Development Program Asset No. 1, 2018). p. 13. [London: Jigsaw Consult. DOI: 10.5281/zenodo.1204703. License: Creative Commons Attribution-ShareAlike 4.0.] https://digitalprinciples.org/resource/donor-organizations-the-principles-for-digital-development-a-landscape-assessment-and-gap-analysis/.

[53]Sutterlin, Elizabeth. Digital ID: A Tool for Inclusion, or Just Confusion?. *DemTech Blog. DemTools.* June 22 2021.https://dem.tools/blog/digital-id-tool-inclusion-or-just-confusion.

be considered as a fundamental pillar of digital identity and user's must be in control over how their data is collected, used, and shared.[54] This level of control must continue with third parties and individuals must be able to choose which aspects of their identity they share (such as certificates).[55] People should be able to obtain copies of their personal data and selectively disclose only the information needed for a particular request,[56] and individual rights should be embedded within the system relating to accuracy, rectification, and opt-out.[57] This means mechanisms allowing recovery and correction of data.[58] The data lifecycle must be transparent with clear agreements about who makes decisions about processes and what will happen with the data as well as how long it will be retained.[59]

Identity systems must also be flexible and designed in a way that allows for change; there are many aspects of identity that are fluid and not representative of how many people actually live their lives – including things such as name, address, and gender.[60] While control over data collected should be incorporated at the design stage, it must also be realized that these attributes change over time and that if they're codified as static or difficult to change, it will exclude lived realities.[61] To that end, it is critical that subjects participate in the design phases of any digital identity system. Communities should be more than aware of the existence of these systems: they need to be an active part of their design processes to fight structural inequality and ensure "collective liberation".[62]

Governments and Institutions should also practice data minimization which means not collecting data that is not necessary for the system that is being used and not holding particular data longer

[54] ID 2020, "The Alliance Manifesto," 2022, https://id2020.org/manifesto.
[55] European Commission, "Digital Identity for All Europeans: A personal digital wallet for EU citizens and residents," European Digital Identity, n.d., https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en#key-principles.
[56] The World Bank, *Principles onIdentification for Sustainable Development: Toward the Digital Age* (World Bank, 2021), p. 12 https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf.
[57] AccessNow, *National Digital Identity Programs: What's next?* (AccessNow, 2018) p. 3 https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf.
[58]Silva, João Marco; Vitor Fonte; Antonio Sousa. 2021. "Towards a Bottom-up Approach to Inclusive Digital Identity Systems" In *Proceedings of the 14th International Conference on Theory and Practices of Electronic Governances*, Athens, Greece, Oct. 6-8 2021. p.525. New York, NY. Association for Computing Machinery. https://dl.acm.org/doi/10.1145/3494193.3494317.
[59] Principles for Digital Development, *Responsible Data*, (Pulse on the Principles, n.d.) https://digitalprinciples.org/wp-content/uploads/PulseOnThePrinciples_RD.pdf
[60] Hirschfeld, Anna; Dunn, Stephen. "How to make digital identity inclusive," Public Digital, Feb. 3 2022, https://public.digital/2022/02/03/how-to-make-digital-identity-inclusive
[61] *Ibid.*
[62] Costanza-Shock, S. (2020). *Design Justice*. The MIT Press. https://designjustice.mitpress.mit.edu/

than it is needed – especially if it could pose harm if used to target certain population groups.[63] Data protection should be viewed through the auspice of 'do not harm' and seen as far more than just a compliance tick box – again, especially with regards to vulnerable populations.[64] Clear legislation should be developed regarding how data can be collected and what can be done with it as a further level of protection, and focus should also be given to protecting this information from financial exploitation and 'data colonialism'.[65]

E. Eliminating Discrimination and Managing Unintended Consequences

Identity systems must be non-discriminatory by design, which means that strong legal frameworks must be in place that ensure that data within the system cannot be used to enable or reinforce discrimination against particular groups.[66] This requires a high-level of transparency within the systems regarding how data is shared across agencies, noting that concrete harms can emerge if particular data is shared with security and immigration agencies, for instance; related to this, it should be clearly instituted that no police officer should have access to the digital identity.[67] As such, comprehensive and enforceable legal frameworks that protect human rights must be inherent to the system, which includes data protection, cybersecurity, and privacy as well as the absolute mitigation of unauthorized surveillance without due process and consent.[68]

---

[63]Holloway, Kerrie; Al Masri, Reem; Abu Yahia, Afnan, "Digital identity, biometrics and inclusion in humanitarian responses to refugee crises" ODI, Oct. 6 2021, https://odi.org/en/publications/digital-identity-biometrics-and-inclusion-in-humanitarian-responses-to-refugee-crises/

[64] *Ibid.*

[65] Sutterlin, Elizabeth. Digital ID: A Tool for Inclusion, or Just Confusion?. *DemTech Blog. DemTools.* June 22 2021. https://dem.tools/blog/digital-id-tool-inclusion-or-just-confusion

[66] The World Bank, *Principles onIdentification for Sustainable Development: Toward the Digital Age* (World Bank, 2021), https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf; Haßler, B., Brugha, M., Muyoya, C., Mitchell, J., Hollow, D., & Jackson, A. *Donor Organizations & the Principles for Digital Development: A Landscape Assessment and Gap Analysis.* (Principles for Digital Development — Resource Development Program Asset No. 1, 2018). p. 13. [London: Jigsaw Consult. DOI: 10.5281/zenodo.1204703. License: Creative Commons Attribution-ShareAlike 4.0.] https://digitalprinciples.org/resource/donor-organizations-the-principles-for-digital-development-a-landscape-assessment-and-gap-analysis/; *ID4D Practitioner's Guide (English).* Identification for Development Washington, D.C.: World Bank Group. https://id4d.worldbank.org/guide/creating-good-id-system-presents-risks-and-challenges-there-are-common-success-factors

[67] Bhatt, Riyal; Moulton, Sarah; Sutterlin, Elizabeth, *Identified but Unheard: Assessing the Impacts of Digital ID on Civic and Political Participation of Marginalized Communities*, (National Democratic Institute, 2021) https://drive.google.com/file/d/1gUESfiedxNAMXRDfoTF8EstDUbQbPf4I/view; Stanley, Jay, *Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom*, (ACLU, 2021) p. 32 https://www.aclu.org/sites/default/files/field_document/20210913-digitallicense.pdf

[68] The World Bank, *Principles onIdentification for Sustainable Development: Toward the Digital Age* (World Bank, 2021), p.18 https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf

Beyond these legal frameworks, discrimination can emerge in a myriad of ways such as technical prohibitions and internet access, so these barriers must be considered at the design stage which involves meaningful community consultation with marginalized groups prior to roll-out – a lack of this careful planning will likely exacerbate existing inequalities.[69] Mechanisms for individuals to seek redress for grievances (such as data breaches) must also be clearly incorporated within the system and accessible to all for complaints or concerns, and detailed logs should be kept when any officer accesses retained data containing who accessed the data, when, where, and for what purpose.[70] The systems should also be independently monitored and evaluated for risk assessments and stopped when these risks are heightened, and an independent framework should also be put in place to ensure that all stakeholders are complying with the set standards.[71]

F. Integration for Policy-Making, Advocacy Efforts, and Democratic Participation

Governments and institutions should involve civil society representatives at all levels of decision-making and provide consultation forums that allow feedback from the public to shape the system at the design stage and throughout implementation.[72] Further, identity should be seen less as identifying attributes and more as a system of building mutual trust, cooperation, and reciprocity for leveraging and advancing social change.[73] Gatherings should be hosted exploring

---

[69] Bhatt, Riyal; Moulton, Sarah; Sutterlin, Elizabeth, *Identified but Unheard: Assessing the Impacts of Digital ID on Civic and Political Participation of Marginalized Communities*, (National Democratic Institute, 2021) https://drive.google.com/file/d/1gUESfiedxNAMXRDfoTF8EstDUbQbPf4I/view

[70] AccessNow, *National Digital Identity Programs: What's next?* (AccessNow, 2018) p. 25 https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf; Silva, João Marco; Vitor Fonte; Antonio Sousa. 2021. "Towards a Bottom-up Approach to Inclusive Digital Identity Systems" In *Proceedings of the 14th International Conference on Theory and Practices of Electronic Governances*, Athens, Greece, Oct. 6-8 2021. p.525. New York, NY. Association for Computing Machinery. https://dl.acm.org/doi/10.1145/3494193.3494317; Gelb, Alan and Mukherjee, Anit, *Building on Digital ID for Inclusive Service: Lessons from India*, (Center for Global Development, 2019) p.9 https://www.cgdev.org/sites/default/files/building-digital-id-inclusive-services-lessons-india.pdf; AccessNow, *National Digital Identity Programmes: What's next?* (AccessNow, 2018) p.29https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf.

[71] The World Bank, *Principles onIdentification for Sustainable Development: Toward the Digital Age* (World Bank, 2021), p.20 https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf; Holloway, Kerrie; Al Masri, Reem; Abu Yahia, Afnan, "Digital identity, biometrics and inclusion in humanitarian responses to refugee crises" ODI, Oct. 6 2021, https://odi.org/en/publications/digital-identity-biometrics-and-inclusion-in-humanitarian-responses-to-refugee-crises/; Anri van der, Vrinda Bhandari, Shruti Trikanad , and Yesha Tshering Paul, *Towards the Evaluation of Socio-Digital ID Ecosystems in Africa*, (Research ICT Africa, 2021) https://researchictafrica.net/wp/wp-content/uploads/2021/11/Comparative-Report_5.11.21-2.pdf; Privacy International, "Letter from global CSOs to the World Bank," Sept. 6 2022, https://privacyinternational.org/advocacy/4945/letter-global-csos-world-bank.

[72]Sutterlin, Elizabeth. Digital ID: A Tool for Inclusion, or Just Confusion?. *DemTech Blog. DemTools.* June 22 2021. https://dem.tools/blog/digital-id-tool-inclusion-or-just-confusion

[73] Brescia, Raymond H, "Social Change and the Associational Self: Protecting the Integrity of Identity and Democracy in the Digital Age," (Penn State Law Rev. Vol. 125 2021): p. 773, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3745404

the evolving nature of collaboration with supportive environments being created for advocacy efforts, and particular attention should be given to cross-sector community conversations (especially sectors that would not otherwise interact).[74]

Regarding the system as a whole, focus should be placed on the integrity of the individual as well as the collective, and the system should be seen as a public good in itself.[75] To achieve this, an identity system should be conceptualized as a means of providing digital participation rights which include protection from identity loss, theft, coercion, or fakery while shifting the focus towards the needs of the people rather than the needs of the implementing institutions.[76] Identity systems should therefore embrace the focus on personhood and self-realization rather than that of simple identity attributes, and in doing this, it should be recognized that the self only exists in its relationship to community and political development.[77] Therefore, democratic participation rights must be embedded within the systems at the base level and should be designed in a way that more and more encourages the strengthening of democracy as a whole.

G. Specific integration of communities and groups: inclusion by design

In subsection A, under accessibility, we addressed principles and good practices to ensure citizens have multiple entry points and opportunities into the systems. But what happens to specific vulnerable groups once they are in the system?

---

[74] Haßler, B., Brugha, M., Muyoya, C., Mitchell, J., Hollow, D., & Jackson, A. *Donor Organizations & the Principles for Digital Development: A Landscape Assessment and Gap Analysis.* (Principles for Digital Development — Resource Development Program Asset No. 1, 2018). p. 13. [London: Jigsaw Consult. DOI: 10.5281/zenodo.1204703. License: Creative Commons Attribution-ShareAlike 4.0.]
https://digitalprinciples.org/resource/donor-organizations-the-principles-for-digital-development-a-landscape-assessment-and-gap-analysis/

[75] Brescia, Raymond H, "Social Change and the Associational Self: Protecting the Integrity of Identity and Democracy in the Digital Age," (Penn State Law Rev. Vol. 125 2021): p. 773,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3745404

[76] Ford, Bryan, "Identity and Personhood in Digital Democracy: Evaluating Inclusion, Equality, Security, and Privacy in Pseudonym Parties and Other Proofs of Personhood," (Swiss Federal Institute of Technology in Lausanne, 2020), https://arxiv.org/pdf/2011.02412v1.pdf; Haßler, B., Brugha, M., Muyoya, C., Mitchell, J., Hollow, D., & Jackson, A. *Donor Organizations & the Principles for Digital Development: A Landscape Assessment and Gap Analysis.* (Principles for Digital Development — Resource Development Program Asset No. 1, 2018). p. 13. [London: Jigsaw Consult. DOI: 10.5281/zenodo.1204703. License: Creative Commons Attribution-ShareAlike 4.0.]https://digitalprinciples.org/resource/donor-organizations-the-principles-for-digital-development-a-landscape-assessment-and-gap-analysis/

[77] Brescia, Raymond H, "Social Change and the Associational Self: Protecting the Integrity of Identity and Democracy in the Digital Age," (Penn State Law Rev. Vol. 125 2021): p. 773,
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3745404.

The regulatory framework used to design identification systems should consider the different impacts it could have within different communities.[78] Legal frameworks, technologies, requirements, procedures, and data usage must not enable or reinforce discrimination against particular groups, such as those who may face increased risks of exclusion for cultural, political, and economic - people living in poverty, women, children, rural populations, racial, ethnic, linguistic, and religious minorities, persons with disabilities, sexual and gender minorities, migrants, asylum seekers, refugees, forcibly displaced and stateless persons among others.[79] In such cases, there is prevailing importance of social, political, and cultural context and design systems that meet these contexts in a respectful way.[80] The New Zealand government publicly acknowledges these good practices as it states that "everyone is able to use [its] digital identity services without risk of discrimination or exclusion".[81]

Overall, recommendations aiming to tackle "exclusion by design"[82] – and hence promote inclusion by design or "design justice"[83] – evoke a "rights-based" or "rights-affirming" approach[84], and impact

[78] Silva, João Marco; Vitor Fonte; Antonio Sousa. 2021. "Towards a Bottom-up Approach to Inclusive Digital Identity Systems" In *Proceedings of the 14th International Conference on Theory and Practices of Electronic Governances*, Athens, Greece, Oct. 6-8 2021. p.525. New York, NY. Association for Computing Machinery. https://dl.acm.org/doi/10.1145/3494193.3494317; Thales DIS. "Using technology to provide a unique legal identity for nations and citizens" *Digital Identity & Security Blog. THALES.* Aug. 27 2020. https://dis-blog.thalesgroup.com/government/2020/08/27/using-technology-to-provide-a-unique-legal-identity-for-nations-and-citizens/?_ga=2.39388067.1845615917.1670001932-343735903.1669756256; OCR Labs (2022). Accessibility and Inclusivity at OCR Labs. https://ocrlabs.com/accessibility-&-inclusivity/.

[79] The World Bank, *Principles on Identification for Sustainable Development: Toward the Digital Age* (World Bank, 2021), p. 12 https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf

[80] ID 2020, "The Alliance Manifesto," 2022, https://id2020.org/manifesto; Karisma, Fundación. "Principios para un sistema de identidad que proteja los derechos humanos" *Blog de Principios. ID Colombia.* Dec. 7 2021. https://digitalid.karisma.org.co/2021/12/07/principios-id/; DGX Digital Identity Working Group. *Digital Identity in response to COVID-19: DGX Digital Identity Working Group. (*Digital Transformation Agency [Commonwealth of Australia] 2022) https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf; Barker, Sara and Rahman, Zara, *Understanding the Lived Effects of Digital ID: A Multi-Country Study,* (The Engine Room, 2020) p.58, https://digitalid.theengineroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf.

[81] "Trust Framework Principles." *New Zealand Government Blog. Digital.Govt.NZ.* Jan. 18 2022. https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/trust-framework/trust-framework-principles/

[82] Anri van der, Vrinda Bhandari, Shruti Trikanad , and Yesha Tshering Paul, *Towards the Evaluation of Socio-Digital ID Ecosystems in Africa*, (Research ICT Africa, 2021) https://researchictafrica.net/wp/wp-content/uploads/2021/11/Comparative-Report_5.11.21-2.pdf

[83] Costanza-Shock, S. (2020). *Design Justice.* The MIT Press. https://designjustice.mitpress.mit.edu/

[84] Privacy International, "Letter from global CSOs to the World Bank," Sept. 6 2022, https://privacyinternational.org/advocacy/4945/letter-global-csos-world-bank; Barker, Sara and Rahman, Zara, *Understanding the Lived Effects of Digital ID: A Multi-Country Study,* (The Engine Room, 2020) p.57,https://digitalid.theengineroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf.

assessments[85] when creating a digital ID system. But little guidance is provided regarding how to implement this type of approach. Research ICT Africa goes a bit further by also recommending mechanisms for the public resolution of complaints of exclusion and that the system architecture considers sustainability issues.[86]

Ultimately, recognizing these contextual nuances demands a collective framework transcending the impacts on a specific individual.[87]

VI. STEPS AHEAD

This policy paper sought to explore the various approaches, guidelines and good practices that different groups of stakeholders around the globe have adopted to enhance inclusion in digital identity policies and systems. Thanks to this mapping, we proposed an Inclusion Assessment Framework that could be utilized by policymakers and practitioners to evaluate a policy's or system's level of inclusion. Although this mapping did not mean to be exhaustive, it identified a series of "expected actions"/"elements" of how to ensure an inclusion lens is the core one when digital identity systems are designed and implemented.

The next step forward is to implement the Assessment Framework to evaluate either existing digital identity systems and policies or to design future ones. The framework could be improved and complemented by applying it to assess inclusion, and identify or build solutions to make digital identity systems more inclusive. Although the mapping of core actions provides a series of practices that could foster inclusion, this initial work leaves more questions than answers:

---

[85] Privacy International, "Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba" Jan. 27, 2022. https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma; "Trust Framework Principles." *New Zealand Government Blog. Digital.Govt.NZ*. Jan. 18 2022. https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/trust-framework/trust-framework-principles/.

[86] Anri van der, Vrinda Bhandari, Shruti Trikanad , and Yesha Tshering Paul, *Towards the Evaluation of Socio-Digital ID Ecosystems in Africa*, (Research ICT Africa, 2021) https://researchictafrica.net/wp/wp-content/uploads/2021/11/Comparative-Report_5.11.21-2.pdf (p. 41)

[87] The World Bank, *Principles on Identification for Sustainable Development: Toward the Digital Age* (World Bank, 2021), p.12, https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf

- How can awareness be effective in a world where information asymmetries are the rule and not the exception?
- Are there any solutions for building digital identity systems that are non-binary and flexible to allow for all types of communities to be holistically represented?
- How can stakeholders foster collaborative efforts to design, build and implement digital identity systems that unlock their benefits for all?

These are all questions that could guide the potential implementation of the Framework and future developments of digital identity systems and policies.

Another step envisioned ahead could be the development of the Digital Identity Living Hub. The Digital Identity Living Hub would be designed as a living repository where communities of stakeholders around the globe could share their good practices around fostering inclusion and human rights around digital identity systems, both at the technical and at the policy levels. Its goal would be to foster a continued dialogue between sectors through an active and growing hub of resources and connections, hopefully facilitating solutions for current and incoming technical and policy gaps.

Digital identity systems are currently posing challenges for human rights and are deepening exclusion, especially in the Global South. Incorporating elements of inclusion such as the ones explored throughout this policy paper both at the technical and at the policy levels is crucial to effectively advance human rights in digital IDs and to ensure that these systems are beneficial to all – especially to underrepresented communities and populations in the Global South.

Digital identity holds the promise of promoting inclusion and driving efficiency and competitiveness. It can provide significant opportunities for countries to transform government services, financial systems, foster inclusion (e.g., by promoting greater access to goods and services), and increase formalization (e.g, reducing fraud, protecting rights, increasing transparency and promoting digitization). To get there, we need to foster best practices and facilitate solutions that are truly inclusive and leave no one behind. We hope that this Framework and extracted practices support the path towards more inclusive digital identity systems and policies that unlock their value and benefits for all.

VII. ANNEXES

A. References

Access Now "National Digital Identity Programmes: What's next? - Access Now.".Access Now, May 2018. https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf.

Anri van der, Vrinda Bhandari, Shruti Trikanad , and Yesha Tshering Paul. "Towards the Evaluation of Socio-Digital ID Ecosystems in Africa." Research ICT Africa, November 2021. https://researchictafrica.net/wp/wp-content/uploads/2021/11/Comparative-Report_5.11.21-2.pdf.

Bailur, Savita, and Hélène Smertnik. "Identification and Identity for Children in a Digital Age." Medium. Caribou Digital, June 4, 2020. https://medium.com/caribou-digital/identification-and-identity-for-children-in-a-digital-age-2409dc633ffa.

Baker, Sara, and Zara Rahman. "Understanding the Lived Effects of Digital ID. Page 56-57" DIGITAL ID. The Engine Room, October 2019. https://digitalid.theengineroom.org/.

Bhalla, Nita. "Feature-Uganda Sued over Digital ID System That Excludes Millions." Reuters. Thomson Reuters, May 16, 2022. https://www.reuters.com/article/uganda-tech-biometrics-idUSL3N2X32RG.

Bhatt, Priyal, Sarah Moulton, and Elizabeth Sutterlin. "Identified but Unheard: Assessing the Impacts of Digital ID on Civic and Political Participation of Marginalized Communities." Identified but Unheard Assessing the Impacts of Digital ID on Civic and Political Participation of Marginalized Communities. National democratic Institute, June 2021. https://drive.google.com/file/d/1gUESfiedxNAMXRDfoTF8EstDUbQbPf4I/view.

Barbosa, Alexandre, Celina Carvalho, Cláudio Machado, and Janaina Costa. "Report: Good ID in Latin America." Report | Good ID in Latin America, July 2020. https://somos.itsrio.org/report_good_id.

Bogle, Ariel, Michael Workman, and Dunja Karagic. "Why Are so Many Minor Parties Talking about Digital ID Laws?" Minor parties spread 'big brother' fears as they ramp up campaign against proposed digital ID laws - ABC News. ABC News, May 1, 2022. https://www.abc.net.au/news/2022-04-26/minor-parties-campaign-against-digital-id-proposals/101014152.

Brescia, Raymond H. "Social Change and the Associational Self: Protecting the Integrity of Identity and Democracy in the Digital Age." SSRN, December 16, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3745404.

Costanza-Shock, S. (2020). *Design Justice*. The MIT Press. https://designjustice.mitpress.mit.edu/

Claudine Lim Manager at The Principles for Digital Development Claudine first joined the Digital Impact Alliance in October 2017. "Donor Organizations & the Principles for Digital Development: A Landscape Assessment and Gap Analysis." Principles for Digital Development, February 3, 2020. https://digitalprinciples.org/resource/donor-organizations-the-principles-for-digital-development-a-landscape-assessment-and-gap-analysis/.

Digital Government Exchange | DGX. . "Digital Identity in Response to Covid-19 - Tech." DGX Digital Identity Working Group. Digital Government Exchange. Accessed December 11, 2022. https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf.

Digital Principles Org. "Pulse on the Principles | Principles on Digital Development - Paper Series." Principles for Digital Development, March 22, 2022. https://digitalprinciples.org/.

Estonian Government. "Estonia - We Have Built a Digital Society & We Can Show You How." e-estonia, November 29, 2022. https://e-estonia.com/.

Ford, Bryan. "Identity and Personhood in Digital Democracy: Evaluating Inclusion, Equality, Security, and Privacy in Pseudonym Parties and Other Proofs of Personhood." arXiv.org, November 4, 2020. https://arxiv.org/abs/2011.02412v1.

Gelb , Alan, and Anit Mukherjee. "Building on Digital ID for Inclusive Services: Lessons from India." Center for Global Development. Center for Global Development, September 2019. https://www.cgdev.org/sites/default/files/building-digital-id-inclusive-services-lessons-india.pdf.

Government of Uganda. "ACTS SUPPLEMENT No. 3 Ministry of ICT & National Guidance – Uganda." Government of Uganda. UPPC, Entebbe, March 26, 2015. https://ict.go.ug/.

Handforth, Calum, and Kendrick Lee. "How Digital Can Close the 'Identity Gap': United Nations Development Programme." UNDP, May 19, 2022. https://www.undp.org/blog/how-digital-can-close-identity-gap..

Hanmer, Lucia, and Mariana Dahan. "Identification for Development: Its Potential for Empowering Women and Girls." World Bank Blogs. World Bank, December 2, 2015.

https://blogs.worldbank.org/digital-development/identification-development-its-potential-empowering-women-and-girls.

Hernández, Marianne Díaz. "Digital Identity: Our Five Calls to Action for the World Bank." Access Now, October 6, 2022. https://www.accessnow.org/digital-identity-world-bank/.

Hernández, Marianne Díaz. "World Bank Must Protect Human Rights in Digital ID Systems." Access Now, September 12, 2022. https://www.accessnow.org/open-letter-to-the-world-bank-digital-id-systems/.

Hirschfeld, Anna, and Stephen Dunn. "How to Make Digital Identity Inclusive - Public Digital." How to make digital identity inclusive -. Public Digital, February 3, 2022. https://public.digital/2022/02/03/how-to-make-digital-identity-inclusive.

Holloway, Kerrie, Reem Al Masri, and Afnan Abu Yahia. "Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises." ODI, October 6, 2021. https://odi.org/en/publications/digital-identity-biometrics-and-inclusion-in-humanitarian-responses-to-refugee-crises/.

ID2020 | Manifesto. Identity2020 Systems Inc. Accessed December 11, 2022. https://id2020.org/manifesto.

Karisma Foundation. "Principles for an Identity System That Protects Human Rights." Principios para un sistema de identidad que proteja los derechos humanos. Karisma Foundation, December 7, 2021. https://digitalid.karisma.org.co/2021/12/07/principios-id/.

Keyes, Os. "The Misgendering Machines: Trans/HCI Implications of Automatic Gender ..." Iron Holds Resources. Proceedings of the ACM on Human-Computer Interaction, November 1, 2018. https://ironholds.org/resources/papers/agr_paper.pdf.

Leyen, Ursula von der. "European Digital Identity." European Commission. Accessed December 11, 2022. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en#key-principles.

New Zealand Digital Government "Trust Framework Principles." Accessed December 13, 2022. https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/trust-framework/trust-framework-principles/.

Pankanti, Sharath, and Anil Jain. "Chapter 23 - Fingerprint Recognition." Essay. In *The Essential Guide to Image Processing* , edited by Al Bovik, Second Edition ed., 649–76. Academic Press, n.d. https://doi.org/10.1016/B978-0-12-374457-9.00023-8. (https://www.sciencedirect.com/science/article/pii/B9780123744579000238)

Privacy International. "Data Protection Impact Assessments and ID Systems: The 2021 Kenyan Ruling on Huduma Namba." Privacy International, January 27, 2022. https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma.

Silva, Joao Marco, Vitor Fonte, and Antonio Sousa. "Towards a Bottom-up Approach to Inclusive Digital Identity Systems: Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance." ACM Other conferences, October 1, 2021. https://dl.acm.org/doi/10.1145/3494193.3494317.

Stanley, Jay. "Digital Ids Might Sound like a Good Idea, but They Could Be a Privacy Nightmare: News & Commentary." American Civil Liberties Union, September 29, 2021. https://www.aclu.org/news/privacy-technology/digital-ids-might-sound-like-a-good-idea-but-they-could-be-a-privacy-nightmare.

Sumner, Stuart. "Biometrics and the Future." ScienceDirect. ScienceDirect, August 27, 2015. https://www.sciencedirect.com/science/article/pii/B9780128034057000102.

Sutterlin, Elizabeth. "Digital ID: A Tool for Inclusion, or Just Confusion?" DemTools, June 22, 2021. https://dem.tools/blog/digital-id-tool-inclusion-or-just-confusion.

Thales DIS. "Using Technology to Provide a Unique Legal Identity for Nations and Citizens." Thales blog. Thales DIS, August 27, 2020. https://dis-blog.thalesgroup.com/government/2020/08/27/using-technology-to-provide-a-unique-legal-identity-for-nations-and-citizens/?_ga=2.39388067.1845615917.1670001932-343735903.1669756256.

UNDESA. "SDG Indicators - Metadata Repository." United Nations. United Nations Department of Economic and Social Affairs (DESA). Accessed December 10, 2022. https://unstats.un.org/sdgs/metadata/?Text=&Goal=&Target=16.1.

UNHCR. "UNHCR Strategy on Digital Identity and Inclusion." UNHCR Blog. Accessed December 11, 2022. https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf.

World Bank. "Argentina ID Case Study." Open Knowledge Repository. World Bank, Washington, DC, 2020. https://openknowledge.worldbank.org/handle/10986/33403.

World Bank. "Creating a Good ID System Presents Risks and Challenges, but There Are Common Success Factors." Creating a good ID system presents risks and challenges, but there are common success factors | Identification for Development. World Bank. Accessed December 11, 2022.

https://id4d.worldbank.org/guide/creating-good-id-system-presents-risks-and-challenges-there-are-common-success-factors.

World Bank "Development Projects : Mexico National Digital Identity System to Facilitate Inclusion - p172647." World Bank. Accessed December 11, 2022. https://projects.worldbank.org/en/projects-operations/project-detail/P172647.

World Bank Development Report. "Enabling Digital Development: Digital Identity." 2016, available at http://documents.worldbank.org/curated/en/896971468194972881/310436360_20160263 021000/additional/102725-PUB-Replacement-PUBLIC.pdf

World Bank. 2019. ID4D Practitioner' Guide: Version 1.0 (October 2019). Washington, DC: World Bank. License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

World Bank. "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.

World Bank "Principles on identification for sustainable development: toward the digital age." Documents & reports - all documents | The World Bank. The World Bank. Accessed December 11, 2022. https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf.

World Bank. "Technology Landscape for Digital Identification." 2018. Washington, DC: World 127 Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), available at http://pubdocs.worldbank.org/en/199411519691370495/ID4DTechnologyLandscape.pdf

World Economic Forum. "Identity in a Digital World." World Economic Forum, September 2018. https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf.

B. Elements of Inclusion – Definitions and Examples

Category	Definition	Example
Accessibility	Whenever a guideline refers to the means by which an individual or group can access a digital identity system.	1. Simplify: simplify registration processes and forms. 2. Automate: automating and making readily available and secure online processes. 3. Decentralize: decentralizing and making available electronic NIRA services at Sub-county and Parish levels. **Acceptance Speech Of The Executive Director, Uganda_National Identification & Registration Authority**
Free choice between multiple identity systems	It refers to the possibility that individuals and groups have of picking the digital identity system that best works for them	(4) Provide alternative Routes Service teams should aim for equal outcomes, rather than a singular service. Trying to support all users to use the most sophisticated digital channels will result in exclusion. **How to Make Digital Identity Inclusive. Anna Hirschfeld, Stephen Dunn**
Information asymmetries	The guidelines address information asymmetries and gaps	"2. Sin barreras de acceso 2.2. Las asimetrías de información (transparencia y comunicación pública)" **Inclusión. Fundación Karisma**
Technology gaps	The guidelines acknowledge the technological, connectivity and infrastructure gaps as fundamental to ensuring equity in digital identity systems	(3) Individuals may have no access to smartphones or the internet **Towards a bottom-up approach to an inclusive digital identity system. Marco Silva, Vitor Fransico Fonte, Antoniao Sousa**
Supports digital literacy and bears different literacy levels in mind	The guidelines seek to support digital and data literacy, bearing in mind literacy disparities across sectors and communities	5 - Translating relevant policy instruments to local languages, and using language that is less technical (p. 41); 10 - Frequently and in accessible language(s) publishes the terms and conditions of MoUs, including the fees payable for access by private sector entities, terms of access, period of time, mechanisms implemented to safeguard data, and other costs involved (p. 42); **Comparative report. Research ICT Africa (RIA) and the Centre for Internet and Society (CIS).**

Control over data	Guidelines allow people to have control over their data and decide the uses it can be given	"People retain control over their information in line with legislative requirements, including the Privacy Act." **Trust Framework principles. New Zealand**
Informed Consent	Whenever a guideline incorporates informed consent as a fundamental part of a digital identity system – which implies that individuals and communities know about its risks and benefits	"Personal data should not be used for secondary, unconnected purposes without a person's informed consent, unless otherwise required or authorized under law (for example, as may be necessary and proportionate).23 Identity providers and other stakeholders should be transparent about identity management; develop appropriate resources to raise people's awareness of how their data will be used; and provide accessible and user-friendly tools to manage their data, provide informed consent, and address grievances (pg. 18)" **Principles on Identification for Sustainable Development. World Bank.**
Manage unintended consequences: tackle misuse and abuse	The guidelines intend to tackle and avoid unintended consequences, especially misuse and abuse of data	"Digital identity carries significant risk if not thoughtfully designed and carefully implemented. We do not underestimate the risks of data misuse and abuse, particularly when digital identity systems are designed as large, centralized databases. (Principle 6)". **Alliance Manifesto. ID2020 Systems**
Changing identity	The practices recognize that identity changes over time and gives people the chance to adapt their digital identity to such changes	Individuals should not be compelled to put their personal, unchangeable, biometric data at great risk of privacy intrusions for the sole purpose of "proving" legal identity, which can be verified in a variety of different ways (pg. 6). Self-sovereign identity systems also fundamentally bake user consent into the design. The user would also have a great deal more control over to update, change, add, or delete their personal data as they see fit, putting control in her hands (pg. 7). **Recommendations and digital rights safeguards. AccessNow.**

Gender lens	A differential approach is adopted with respect to women, girls, LGBTQI+ and other communities	: Literacy rates are lower amongst refugees, especially women, and refugees with disabilities (especially girls) are disproportionately excluded from accessing education. CAMEALEON and CaLP also found evidence of shop workers keeping refugees' banking cards, an action that is surely facilitated by pervasive anti-refugee sentiment and refugees' precarious migration status, which stifles reporting to authorities. **An Intersectional Approach to Digital Humanitarianism. Jenna Imad Harb**
Inclusion by design (mindful of vulnerable groups)	Guidelines are mindful of vulnerable groups and incorporate technologies and policies to be inclusive by the design	"2 - Establish and follow policies and legislation that protect the rights of people affected by a digital ID system (p. 57). 2.1. Focus on rights-affirming legislation that prioritises the needs of the people over the interests of the implementing institution (p. 57). 2.3. Consider how power asymmetries will affect informed consent and develop policies reflecting these imbalances. If informed consent cannot be meaningful in this environment, explore ways to replace or further support consent processes in order to respect people's rights and dignity (p. 57). 3 - Recognise the importance of social, political and cultural context and design systems that meet these contexts in a respectful way (p. 58)." **Understanding the Lived Effects of Digital ID- A Multi-Country Study. The Engine Room**
Explicit against discrimination	The guidelines are explicit about the need to act against discrimination and sets a series of practices to do so	"Nondiscrimination. All identification systems should be free from discrimination in policy, in practice, and by design. This includes ensuring that legal frameworks; requirements and procedures to register, obtain, or use identification; and the data that are collected or displayed on credentials do not enable or reinforce discrimination against particular groups, such as those who may face increased risks of exclusion for cultural, political, economic or other reasons (pg. 12)" **Principles on Identification for Sustainable Development. World Bank**

Clear dissemination plan to be an effective method for widespread inclusion	The principles set out a clear dissemination plan to include people in the conversation around digital identity and share information about the risks and benefits of the technologies and policies being implemented	"High-impact distribution channels It is possible to reach out to large populations of people through widely used technology or distribution channels, such as mobile network operators. Tapping into existing, far-reaching channels can be an effective method for widespread inclusion. (pg. 20)" **Identity in a Digital World: Insight Report. Section on Inclusion. World Economic Forum.**
Support policymaking	The guidelines intend to support policymaking processes with regards to digital identity	"The ID2020 Alliance recognizes that taking these ideas to scale requires a robust evidence base, which will inform advocacy and policy. As such, ID2020 Alliance-supported pilots are designed around a common monitoring and evaluation framework. (Principle 10)" **Alliance Manifesto. ID2020 Systems.**
Support advocacy efforts	The guidelines intend to support advocacy efforts around digital identity	"The ID2020 Alliance recognizes that taking these ideas to scale requires a robust evidence base, which will inform advocacy and policy. As such, ID2020 Alliance-supported pilots are designed around a common monitoring and evaluation framework. (Principle 10)" **Alliance Manifesto. ID2020 Systems.**
Checks and balances: M&E + Accountability	Whenever guidelines establish mechanisms of monitoring and evaluation, as well as of accountability for stakeholders working around a digital identity policy and/or system	"The use of identification systems should be independently monitored (for efficiency, transparency, exclusion, misuse, etc.) to ensure that all stakeholders comply with applicable laws and regulations, appropriately use identification systems to fulfill their intended purposes, monitor and respond to potential data breaches, and receive individual complaints or concerns regarding the processing of personal data (pg. 20)" **Principles on Identification for Sustainable Development. World Bank.**

C. Summary of guidelines per stakeholders

Type of stakeholder	Issuer	Name of guidelines	Year	Overview of the guidelines
IGO	ID2020 Systems	Four P's of digital ID	2020	(1) Private (2) Portable (3) Persistent (4) Personal
		Alliance Manifesto	2020	(1) Prove one's identity (2) Trusted way to prove who they are (3) Accessibility to services, especially to marginalized communities (4) Alternatives to state-led systems for communities such as refugees (5) Individual control over one's identity (6) Protection against misuse and abuse (7) Privacy protection and technical standards for interoperability (8) Sustained and transparent collaboration for regulatory and policy frameworks (9) Technical interoperability, and thus trust and recognition (10) Common monitoring and evaluation framework to support advocacy efforts
IGO	European Union	European Digital Identity	2019-2024	(1) Available to any EU citizen, resident, or business in the EU who wants to use it (2) Widely useable as a way of identification or to confirm certain personal attributes for the purpose of access to public and private digital services across the EU (3) Giving full control to users to choose which aspects of their identity, data and certificates they share with third parties, and keep track of such sharing
IGO	World Bank	Principles on Identification for Sustainable Development	2021	Inclusion: (1) Ensure universal access for individuals, free from discrimination. (2) Remove barriers to access and use. Design: (3) Establish a trusted—unique, secure, and accurate—identity. (4) Create a responsive and interoperable platform. (5) Use open standards and prevent vendor and technology lock-in. (6) Protect privacy and agency through system design. (7) Plan for financial and operational sustainability. Governance: (8) Protect personal data, maintain cyber security, and safeguard people's rights through a comprehensive legal and regulatory framework. (9) Establish clear institutional mandates and accountability. (10) Enforce legal and trust frameworks through independent oversight and adjudication of grievances.

IGO	AccessNow	Recommendations and digital rights safeguards	2018	Governance: (1) Undertake transparent, inclusive and open consultations at the initiation of any digital ID programme proposal (2) Ensure a defined and restricted scope of use for the digital ID programme, provided for in the law; (3) Make enrollment and use of the digital ID voluntary (4) Create independent and well-designed mechanisms for grievance and redress; (5) Ensure inclusion at the enrollment stage, and no exclusion during implementation, due to technology or infrastructural capacity gaps Data Protection and Privacy: (6) Limit the purpose for which these data are collected and used. Put in place proper measures to prevent user profiling based on the data volunteered (7) Grant individuals rights related to their own data, such as accuracy, rectification,and opt-out (8) Institute robust data protection frameworks to which digital ID programmes are subject (9) Minimize the amount of and type of data governments and associated service providers collect (10) Restrict lawful interception and monitoring of digital ID use and implement measures for accountability Cybersecurity (only relevant for mapping) (11) Provide a legal and policy framework that incentivises reporting and disclosure of vulnerabilities; (12) Take steps to notify affected parties in case of breach of data
IGO	World Economic Forum	Identity in a Digital World: Insight Report. Section on Inclusion	2018	To include all individuals and give them the access they need, identity systems must provide: (1)Equal opportunity: Everyone within the target population is able to establish and use digital identities that can be authenticated. (2) Safeguards against discrimination: No one faces special barriers in establishing and using identities or risks discrimination or exclusion as a result. (3) Mechanisms to manage unintended consequences, such as data and security standards that exclude individuals who should be able to join. (4) Accessibility and multiplicity: It should be easy for individuals of any socioeconomic or demographic segment to enroll in identity systems of their choice. (5) Design for all: To avoid excluding or marginalizing anyone, identity systems would consider and design for differences in abilities, age, digital literacy, access to technology and use-cases (6) Minimum data: Design could mitigate discrimination or unintended consequences by collecting, using or disclosing only information that is critical for a given transaction. (7) Standards for inclusion: A digital identity framework will be more inclusive if it has standards for identity data and for interactions with trust anchors that all individuals can meet. (8) High-impact distribution channels: It is possible to reach out to large populations of people through widely used technology or distribution channels, such as mobile network operators.

Academia	Marco Silva, Vitor Francisco Fonte, Antoniao Sousa	Towards a bottom-up approach to inclusive digital identity system	2021	(1) Sources should be able to keep acting autonomously without coordination (2) Sources should not be required to have full-time access to the internet (3) Individuals may have no access to smartphones or the internet (4) Individuals may be required to act as proxies to others (e.g., parents and children) (5) The system must guarantee sources and individuals privacy (6) Individuals should have access to mechanisms allowing recovery and correction of data about them (7) Identity representation and underlying services must be designed towards inclusiveness and usability (8) The system might provide incentive mechanisms aiming at sources engagement
Academia	Anna Hirschfeld, Stephen Dunn	How to Make Digital Identity Inclusive	2022	(1) Ensure that you need to verify identity (if you can avoid it you should) (2) Design for Change (3) Reach out, Research and Understand user needs (4) Provide alternative Routes (5) Prevent Barriers
Academia	Elizabeth Sutherland	Digital ID: A tool for inclusion, or just confusion?	2022	(1) Digital ID Systems must be Designed and Deployed Inclusively - From conceptualization to implementation, consideration needs to be given to the impact on persons with disabilities, LGBTQI+ communities, and other vulnerable populations. A first step is involving these groups or their representatives in the design and implementation process. (2) Civic Education on Digital ID is a necessary part of Deployment -Information on the reason for, impact of, and deployment of digital ID systems should be accessible and understandable to all members of the public. (3) DIGITAL ID SYSTEMS SHOULD BE IMPLEMENTED ONLY AFTER STRONG DATA PRIVACY AND PROTECTION PRACTICES ARE ESTABLISHED - sufficient community consultation with marginalized groups during the design and rollout process of a digital ID system is needed to ensure that potential barriers to uptake for marginalized populations have been addressed.

Academia	Raymond H Bresia	Social Change and the Associational Self: Protecting the Integrity of Identity and Democracy in the Digital Age	2021	(my takeaways) (1) it's not just identity, it's our political selfs. (2)focus on the importance of the integrity of individual and group identity as a collective and public good itself, as a product of, and which is manifest in, our associational ties. (3) maintaining identity in its relation to community (4) Attributes and cultural encumbrances are not fixed or static. We can change both ourselves and the world around us. Through these processes of choice and change, we realize self determination, both on the individual and societal levels. (5) social capital manifests itself in "networks of civic engagement [which] foster sturdy norms of generalized reciprocity and encourage the emergence of social trust." (Direct quote) The associational self is the self that can: (1) realize his or her identity; (2) build trust with others to help create cooperation, reciprocity, and mutual trust that can be leveraged to advance social change; and (3) serve as the lever of such change to effectuate the collective self-determination that shapes society into the collective self-image—the essence of collective self-determination. An exploration of each of these concepts follows.
Academia	Bryan Ford	Identity and Personhood in Digital Democracy: Evaluating Inclusion, Equality, Security, and Privacy in Pseudonym Parties and Other Proofs of Personhood	2020	(1)Inclusive: Any real human person should be able to participate, regardless of nationality, wealth, race, gender, connections, education, or expertise. (2) Equal: All participants must be treated equally for democratic deliberation and decision-making purposes: i.e., "one person, one vote." (3) Secure: Digital personhood must protect both individuals and the democratic collective from compromise in the digital and physical domains. (4) Private: Digital personhood must guarantee each participant's freedom to communicate, associate, and express their true intent in democratic processes.
Academia	Jenna Imad Harb	An Intersectional Approach to Digital Humanitarianism	2022	Considerations: 1) Literacy is essential, but not universal 2) Transportation is required, but not equally accessible 3) Photo identification is taken for granted as a necessity, but it's unwanted for some
		Aadhaar Myth Busters	2022	[Access to services] It is clearly mentioned in Section 7 that until a person is assigned an Aadhaar number, he/she cannot be denied ration or pension or such other entitlements for want of Aadhaar and the concerned department should verify the identity of the person using alternate means of identification as per the relevant notification.
State	India Unique Identification Authority of India			

		Aadhaar Enrolment	2022	1. Aadhaar enrolment is free of cost. 2. You can go to any authorized Aadhaar enrolment center anywhere in India with your proof of identity and proof of address documents 3. UIDAI process accepts a wide range of PoI (Proof of Identity) and PoA (Proof of Address) documents. View the list of supporting documents. Common proofs of identity and address are election photo ID card, Ration card, passport and driving license. 4. In case you do not have above common proofs, Certificate of Identity having photo issued by Gazetted Officer/Tehsildar certificate proforma as prescribed by UIDAI is also accepted as PoI. Certificate of Address having photo issued by MP or MLA /Gazetted Officer/Tehsildar on letterhead or by Village Panchayat head or its equivalent authority (for rural areas) is accepted as valid PoA. Even if someone in a family does not have individual valid documents, the resident can still enroll if his/her name exists in the family entitlement document. In this case the Head of Family in entitlement document needs to be enrolled first with a valid PoI & PoA document. The head of the Family can then introduce other members in the family while they are enrolling. UIDAI accepts many document types as Proof of Relationship. Please View the list of supporting documents. 5. In the absence of a valid Proof of Identity (PoI) document and valid Proof of Address (PoA) document, an introducer's service can be leveraged. An introducer is a person appointed by the Registrar and should have a valid Aadhaar number.
		Usage of Aadhaar	2022	[Access to services] Aadhaar and its platform offers a unique opportunity to the government to streamline their delivery mechanism under the welfare schemes, thereby ensuring transparency and efficiency.
		Features of Aadhaar	2022	1. Uniqueness: this is achieved through the process of demographic and biometric de-duplication. 2. Portability: it can be authenticated anywhere on-line. 3. Random number: Person willing to enroll has to provide minimal demographic information along with biometric information during the enrollment process. The Aadhaar enrolment process does not capture details like caste, religion, income, health, geography, etc. 4. Scalable technology architecture: The UID architecture is open and scalable. Resident's data is stored centrally and authentication can be done online from anywhere in the country. 5. Open source technologies: Such applications are built using open source or open technologies and structured to address scalability in a vendor neutral manner and allow co-existence of heterogeneous hardware within the same application.
State	World Bank + NIRA	World Bank. 2018. ID4D Country Diagnostic: Uganda, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO))	2018	No specific list of principles

	Reuters	-	2022	"(...) an alliance of charities has sued the government, arguing that vulnerable groups have been denied access to potentially life-saving services due to flaws in the national ID card rollout."
	Uganda_Parliament	Registration of Persons Act, 2015	2015	Section 66 - Mandatory use of national identification cards. (1) A ministry, department or agency of government or any other institution providing a public service shall require a person accessing the service to produce a national identification number or national identification card or alien's identification number or alien's identification card.
	Uganda_National Identification & Registration Authority	FAQ'S ON MASS ENROLMENT AND RENEWAL	2022	1. The new card will support a feature that requires the owner of the card to give consent, in a seamless manner, to anyone who wishes to view or retrieve their information in keeping with the Data Privacy and Protection Act, 2019. Hence providing full visibility to persons accessing one's information. 2. The new card leverages Public Key Infrastructure (PKI) to issue individual digital certificates used to sign every record in the National Identification Register. This feature allows for third parties to confidently transact with certainty that the person in the online transaction is properly identified. It will therefore promote e-commerce as it will give confidence to online transactions and subsequently lower the cost of electronic transactions and credit to Uganda.
		Acceptance Speech Of The Executive Director	2022	1. Simplify: simplify registration processes and forms. 2. Automate: automating and making readily available and secure online processes. 3. Decentralize: decentralizing and making available electronic NIRA services at Sub-county and Parish levels. 4. Technology: Requisition of requisite future technologies for a secure card with biometric features. 5. Synergy: building synergy with partners and key stakeholders (...) to improve the availability, use, and integrity of data. 6. Human resource: building a professional, agile customer-centric, and formidable workforce.
	Parliament	World Bank. 2019. Argentina ID Case Study: The Evolution of Identification, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).	2012	"RENAPER has also established some policies to waive fees for people living in poverty, vulnerable people, or those living in remote areas. For example, RENAPER does not charge fees for IDs issued during mobile campaigns in rural or remote areas; nor to individuals seeking to change their sex on their DNI in order to reflect an individual's self-perceived gender identity, in accordance with law number 26.743 on Gender Identity. Likewise, individuals not able to afford a DNI can apply for a "certificate of poverty" issued by the minister of social development or by the provinces to waive fees. Requirements to issue the certificate varies according to each province but usually includes a proof of residence (for example, electricity or telephone bill) and the presence of a witness." (World Bank. 2019. Argentina ID Case Study: The Evolution of Identification, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO). P. 06)

State

	Argentina_Sistema de Identidad Digital (SID)]	Ciudadanos - Una nueva tecnología al servicio de todos	2022	Ventajas del servicio 1. Verificación de Identidad del Ciudadano 2. Brinda transparencia y calidad de gestión. 3. Ahorra tiempo y achica distancias porque permite resolver gran variedad de trámites online. 4. La validación la realiza el Estado a través del Renaper. 5. Tiene un alto nivel de seguridad que garantiza la privacidad de los datos. Los valores biométricos de los ciudadanos no salen del entorno seguro del RENAPER ni son almacenados en el dispositivo. 6. Cada organismo o empresa que se adhiera a la solución podrá autogestionarla para acceder a información completa sobre el servicio y utilidades como descargas, monitoreo de transacciones, reportes, entre otros. 7. Validez legal para los trámites que el ciudadano necesite realizar ante organismos públicos y empresas.
State	Estonian Police and Guard Board	Estonia_e-Estonia	2022	1. There must be interoperability between different organizations and information systems. In other words they must be able to work together and data only needs to be requested from the citizen once. 2. Exemptions from paying state fee - If it is not possible to pay the state fee, the PBGB has the right based on the person's financial situation, on the basis of an application justified by a government institution or local government to reduce the state fee rate or exempt the person from paying it (Estonian Police and Guard Board). 3. An ID-card is a compulsory identity document issued by the Police and Border Guard Board to all Estonian citizens and the citizens of the European Union permanently residing in Estonia.
CSO-NGO	Privacy International	Digital National ID systems: Ways, shapes and forms	2021	(i) Open source approach. (ii) Encryption is crucial to keeping data safe from unwanted third parties and to provide users with a reliable authentication process. (iii) Physical decentralization should be expected in any at-scale system to reduce (and attempt to eliminate) single points of failure, as well as potentially speeding up access. (iv) The design, deployment and governance of large socio-technical systems can establish a different public order and power entrenchment among social and political groups. (v) Transparency.
		Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba	2022	(i) Impact assessments: to understand the positive and negative impact of a particular data processing activity or larger system, identify the risks, and then take measures to prevent or mitigate them accordingly through a variety of measures.

		Privacy International's response to the call for input to a report on the right to privacy in the digital age by the UN High Commissioner for human rights	2022	"In the most concerning cases, the data collected as part of the digital ID systems scheme could be used to identify and target perceived opponents, as reported following the Taliban takeover of Afghanistan". (p. 12) // "(...) private companies play a significant role in implementing these systems, not only by providing the relevant technologies, but by setting up and managing databases of whole populations". (p. 12)
CSO-NGO	ACLU	Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom	2021	(i) No police officer access to phones: holders never need to relinquish control of their smartphone to any Verifier (p. 32). (ii) Unlinkable presentations: the Issuer cannot know where or to whom a Holder is presenting their ID, and Verifiers cannot conspire with each other or with Issuers to compile records of presentations (p. 32). (iii) Granular control over data released: Holders have complete control over what data is released from their IDs (p. 32). (iv) A standardized provisioning process: the process by which data from DMVs or other Issuers is loaded onto people's devices should be standardized so that anyone can write a compliant mDL app and Holders will have choices in which app they use. (p. 32) (v) Transparent source code (p. 32). (vi) IDs that don't "phone home": should not incorporate remote revocation capabilities and should be designed to operate offline only (...) (p. 33). (vii) A "right to paper": People should have a right to obtain and use a paper or other physical identity document instead of or in addition to a digital ID (p. 33). (viii) Restrictions on ID demands: Legislatures should consider enacting laws that limit ID demands in commercial contexts outside of specified circumstances (p. 33).

CSO-NGO	Research ICT Africa (RIA) and the Centre for Internet and Society (CIS)	Comparative report	2021	1 - Formulating gender-sensitive policies (p. 39). 2 - Developing dedicated policy instruments pertaining to the prevention, mitigation and resolution of risks pertaining to the digital components of national ID (p. 40); 3 - Advancing and entrenching privacy-by-design principles in policy instruments pertaining to digital identity (p. 40); 4- Developing, adopting and/or implementing relevant policy instruments to protect and promote data subjects' rights as far as digital identity initiatives are concerned (e.g., data protection and cybersecurity legislation) (p. 40); 5 - Translating relevant policy instruments to local languages, and using language that is less technical (p. 41); 6 - Ensuring administrative justice mechanisms as an access and recourse component of emerging digital identity environments (p. 41); 7 - Ratifying the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), if they have not (p. 41). 8 - Establishing mechanisms for the public resolution of complaints of exclusion (p. 41); 9 - Developing separate functions for distinct, independent regulators for data protection and privacy (e.g., an information commissioner or regulator), and (digital) identity management. The latter should have oversight over the licensing of agencies to perform registration and authentication responsibilities (41). 10 - Frequently and in accessible language(s) publishes the terms and conditions of MoUs, including the fees payable for access by private sector entities, terms of access, period of time, mechanisms implemented to safeguard data, and other costs involved (p. 42); 11 - Assesses the privacy concerns and other risks of sharing digital identity data with stakeholders from the private sector on a case-by-case basis (p. 42); 12 - Establish technical mechanisms for safeguarding data with the private sector, including the means of auditing access to and security of the data (p. 42); 13 - Foster transparency in granting access to digital identity information (p. 42); 14 - Conduct risk and human rights impact assessments before sharing digital identity data (p. 42); 15 - Consider the creation of data trusts to enable private sector entities access to certain non-sensitive identity data if they meet certain criteria, and establish a relevant oversight mechanism for setting standards and allowing safe access (p. 42); 16 - Mandate transparency and accountability by requiring external annual financial and risk audits and reporting to parliament (p. 42). 17 - Design digital identity approaches that are suited to the target population, keeping in mind restrictions (e.g., a lack of electricity or Internet access) as well as the capabilities of target audiences (p. 43); 18 - Design approaches that embrace the data minimisation principle (i.e., only collect such data that are strictly necessary) (p. 43); 19 - Adopt approaches that are not only safe-by-design, but also cognisant of potential risks (p. 43); 20 - Prioritize well-designed decentralized approaches, also to advance public service delivery; 21 - Develop system architecture that takes into account issues of sustainability (p. 43); 22 - Work transparently and in a manner that prioritizes the "explainability" of the workings of the technical infrastructure involved; (p. 43) 23 - Develop system documentation to enable technicians and implementers to continually update and adapt

				system architecture (p. 43); 24 - Remain aware of administrative justice obligations in relation to public private partnerships (p. 43). 25 - Taking necessary measures to ensure internal rules and regulations are developed that comply with customers' data protection and privacy rights (p. 43); 26 - Being transparent and publicly disclose any MoUs or similar legal agreements with public sector actors to facilitate access to identity databases (p. 43); 27 - Working responsibly with data obtained from national ID databases (p. 43).
CSO-NGO	70 + activists, academics, and civil society organizations	Letter from global CSOs to the World Bank	2022	1. Invite and fund an independent, rights-based assessment of the World Bank's role in supporting digital ID systems globally. 2. Assess existing evidence and cease activities that heighten the risk of human rights violations. 3. Enforce greater transparency about activities of the World Bank regarding digital ID. 4. Create opportunities for sustained, high-level engagement with civil society and other experts. 5. Increase funding and resources for baseline studies and contextual analysis, cost-benefit studies, and independent rights-based assessments and evaluations. 6. Environments where human rights risks are too high, or where evidence-based policymaking, civil society engagement, rule of law, and rights-based assessments are simply not possible. In such cases, the Bank and other funders should heed the evidence and decline to support new or upgraded digital ID systems.
CSO-NGO	ITS Rio	Good ID in Latin America	2020	1. Inclusion: Digital identification can only be considered appropriate when it promotes inclusion. 1.1. Beware to not reproduce the current exclusion problem digitally. 1.2. Access to basic rights and services should not depend on digital identification. 2. User Value: Balance Individual and Institutional Interest. 2.1. Making sure that digital identification schemes are leveraging people's rights, not underpinning their civil liberties and rights. 2.2. Do not join the hype at the expense of effective user value. 2.3. When innovation brings real value to the user and inclusion, go for it.
State	New Zealand	Trust Framework principles		**Trust and Legal Frameworks for the Digital ID program** Consent is always required Personal information will not be held in centralized database The system is opt-in Sharing between government departments remains controlled Privacy and security standards are built in Rules incorporate Te Ao Māori perspectives of identity Identity theft risks are managed

CSO-NGO	Fundación Karisma	Principios para un sistema de identidad que proteja los derechos humanos	2021	1. Inclusión: Los Estados tienen la obligación de promover condiciones para el acceso igualitario e inclusivo a la identidad legal para todas las personas. 2. No discriminación: Los sistemas deben tratar a todas las personas en condiciones de igualdad y sin discriminación por razón de su origen o nacionalidad. 3. Seguridad digital: Los sistemas de identidad deben proteger los datos de las personas de injerencias ilegítimas. 4. Privacidad: Los sistemas de identidad deben estar diseñados con un enfoque de privacidad por diseño. 5. Sostenibilidad: Los sistemas de identidad deben ser sostenibles financiera y operacionalmente. 6. Estado de derecho: Los sistemas de identidad deben estar estructurados integralmente en los marcos regulatorios con responsabilidades y procedimientos claramente definidos.
		Inclusión	2021	1. Cobertura universal 2. Sin barreras de acceso 2.1. Los costos directos e indirectos de los procesos de registro 2.2. Las asimetrías de información (transparencia y comunicación pública) 2.3. El acceso a tecnología e infraestructura física (online y offline) 2.4. La flexibilidad del sistema para ser accesible a varios tipos de usuarios y 2.5. Los tiempos asociados a los procesos de registro o la expedición de permisos de permanencia.
		No discriminación	2021	1 - Prevenir que el registro al sistema se convierta en un prerrequisito para el acceso de servicios básicos para las personas más vulnerables 2 - Eliminar de los sistemas de identificación las sanciones por falta de inscripción 3 - El diseño del sistema no debe utilizar los datos para convertirse en un mecanismo de vigilancia o de criminalización de la población 4 - El sistema no debe enfocarse en una política securitista y dominada por la fuerza pública 5 - En el diseño del sistema se debe minimizar la recolección de datos que contienen las credenciales para evitar ejercer violencias

CSO-NGO	The Engine Room	Understanding the Lived Effects of Digital ID- A Multi-Country Study	2020	1 - Prioritize meaningful public and civil society involvement and engagement throughout the project (P. 56). 1.1. From creation and design through implementation, ensure that easily accessible information about the system is proactively shared in a way that reaches diverse members of society. (p. 56) 1.2. Carry out ongoing public consultations rather than one-off opportunities, and ensure that people whose rights are often denied, such as disabled people, elderly people, low-income people, informal labourers, rural residents, ethnic and religious minorities, migrants, sex workers and LGBTQI groups, are included (p. 56-57). 1.3. Build relationships with a range of civil society organizations that can provide feedback to strengthen the system (p. 57). 1.4. Set up multi-step feedback processes to ensure that both negative and positive feedback will reach influential people and inform improvements and iterations of the system (p. 57). 2 - Establish and follow policies and legislation that protect the rights of people affected by a digital ID system (p. 57). 2.1. Focus on rights-affirming legislation that prioritizes the needs of the people over the interests of the implementing institution (p. 57). 2.2. Design grievance-reporting mechanisms and processes to address problems in a timely manner (p. 57). 2.3. Consider how power asymmetries will affect informed consent and develop policies reflecting these imbalances. If informed consent cannot be meaningful in this environment, explore ways to replace or further support consent processes in order to respect people's rights and dignity (p. 57). 3 - Recognise the importance of social, political and cultural context and design systems that meet these contexts in a respectful way (p. 58). 3.1. Ensure that information and all steps of the system are provided in relevant local languages, including those of significant migrant populations (p. 58). 3.2. Establish a community engagement plan to understand (p. 58): 3.2.1. The cultural perceptions that could affect system roll-out, especially if biometric data is included (p. 58) 3.2.2.. What a meaningful informed consent process could look like (p. 58). 4 - Provide ongoing training for staff implementing or involved in digital ID systems (p. 58). 4.1. Ensure key processes throughout the system, including registration, renewal, grievance reporting and legal support are accessible. Ensure onboarding of new staff includes a focus on the context of a digital ID system and other key policies such as data protection. (p. 58) 4.2. Train staff to invite questions and answer them respectfully, and ensure supervisors conduct regular reviews of staff interaction with target populations (p. 59). 4.3. Create internal space for staff to share major barriers they face in registering people, the grievances people express to them and ideas for solving these problems (p. 59).

State	State	Digital identity interoperability principles	2022	Principle 1: Openness Principle 2: Transparency Principle 3: Reusability Principle 4: User-centricity Principle 5: Inclusion and accessibility Principle 6: Multilingualism Principle 7: Security and privacy Principle 8: Technology neutrality and data portability Principle 9: Administrative simplification Principle 10: Preservation of information Principle 11: Assessment of effectiveness and efficiency
Private-Tech	Thales Group	Key principles of legal digital identity	2022	Key principles of legal digital identity 1. Inclusivity: Digital identity must be accessible to all, without discrimination, and using technologies that are adapted to the specific environment and existing infrastructure. 2. Efficiency: Digital identity needs to be secure, efficient, affordable and sustainable. It must rely on open standards and guarantee interoperability with different existing technologies, helping to provide governments with a choice in terms of equipment, and compatibility with their infrastructure. 3. Security: Digital identity must guarantee confidentiality of the data collected and be part of a legal framework of trust. Governments who deploy digital identity solutions must ensure the security of the identity verification solutions they provide to the private sector.
Private-Tech	OCR Labs	The best ways to make digital identity verification accessible and inclusive	2021	No specific list of principles

Private-Tech	Tethys	Building a Secure Identity for Citizens	2022	1. Robust, Secure, and Scalable - Tethys uses enhanced encryption to keep data secure at rest and in transit. Biometric digital ID verification mitigates against identity fraud. 2. Implement, protect, and enhance Privacy by Design - Individuals begin with maximum privacy. Any data shared to partners will be by intentional choice. 3. Inclusive, open, and meets broad stakeholder needs - Tethys works with every partner that embraces these principles. The Tethys algorithm is also designed to create a unique instance for everyone to avoid data bias. 4. Transparent in governance and operation - The administration of identities within Tethys will be open to scrutiny and accessible to auditors. 5. Provide Canadians choice, control, and convenience - Tethys provides a convenient digital ID with data sharing fully controlled by each person. 6. Built on open, standards-based protocols - The Tethys team is committed to design according to these principles. We are meeting and collaborating with many of the groups at the forefront of digital transformation. 7. Interoperability with international standards - We are helping to design these standards. Tethys will work with any reasonable standards that do not conflict with other privacy directives. 8. Cost-effective and open to competitive market forces - Tethys is less expensive to implement and maintain than a traditional ID system. 9. Able to be assessed and audited - Tethys will provide any independent auditors with access to the correct data and procedures to demonstrate our commitment to security and privacy. 10. Minimal Data Transfer and no new databases - Tethys is not a new database. Tethys is an identity app that connects the multiple databases already in use by governments, charities, and businesses.
IGO	World Bank (ID4D)	ID4D Practitioners Guide	2022	(1) Good ID enable multiple development goals (2) creating a good I system presents risks and challenges, but there are common success factors (3) There is no one-size-fits-all solution for creating a foundational ID system that is inclusive and trusted. Instead, governments and other stakeholders must undertake an in-depth planning process to ensure that the design and implementation of a foundational ID system is appropriate to the country context and fit-for-purpose to achieve national priorities while respecting people's inalienable rights. (4) Principles of identification for sustainable development include: Inclusion, Design, Governance
Private-Tech	Principles for Digital Development	Responsible Data	2020	(1) Design with with the user (2) Understand the existing ecosystem (3) Build for sustainable (4) Address privacy & security (5) Go beyond procedural privacy and security (6) responsibly reuse data when being data driven (7) Understand the data ecosystems and mitigate harms (8) Address risks from open data (9) Be collaborative with responsible partners (10) Be transparent and accountable for data

Private-Tech	Principles for Digital Development	Donor Organizations & the principles for digital development: a landscape assessment and gap analysis	2020	(1) Identify existing knowledge and practice of donors, as well as gaps, vis-à-vis achieving their goals in a digital world (2) Understand how the internal processes of donor organizations (e.g., procurement processes, internal training, evaluation practices) can be enhanced to improve desired outcomes in technology-based development programs (3) Identify how the Digital Impact Alliance can best support coordination between donors and implementers/grantees to promote the Principles for Digital Development (4) Understand how the Principles for Digital Development can be adapted and articulated to serve as a road map for achieving donors' digital strategies
IGO	UN Habitat	Building & Securing Digital Public Infrastructure: A playbook for local and regional governments	2022	(1) Improve the convenience and accessibility of services by digitizing them (2) Create a data governance framework that sets standards and responsibilities (3) safeguard public trust by protecting smart city assets