STUDYING DIGITAL IDs FOR SMALLHOLDER FARMERS: AN OVERVIEW OF THE CURRENT APPLICATIONS IN THE GLOBAL SOUTH

ABSTRACT

How can we make sure that farmers have a unique identification, despite the lack of formal identity cards or land ownership? This report focuses on the role of Digital IDs in enabling autonomous data ownership for farmers by exploring data governance and D.ID issues and the necessary technological tools in the Global South. This report aims to create an understanding of a country's digital readiness for farmers' digital information management tools.

Javier Canales Luna, Independent Consultant
Sidi Amar, Researcher at Maastricht University

CONTENT

1. Introduction

Agricultural development is one of the most powerful tools to end extreme poverty. Agriculture accounts for nearly one-third of global gross domestic product (GDP) –more than 500 million smallholder farms worldwide play a significant role in food production as well as the genetic diversity of the food supply, mitigating risks of nutritional deficiencies and ecosystem degradation[1]– and the majority of the world's poor live in rural areas and make a living through agriculture.[2] Increasing smallholder farmers' earnings from farming and off-farm activities are viewed as a key strategy to improve the quality of life in rural areas. The livelihood conditions of smallholder farmers are complex. In developing countries, smallholder farmers are one of the groups that face more difficulties accessing services and opportunities provided by public and private entities.[3] Poverty, remoteness and low digital literacy are usual factors that contribute to the difficult situation of farmers. These problems are exacerbated when farmers lack official identification documents. According to data from the World Bank ID4D Programme, in 2018 there were an estimated 1 billion people globally without official proof of identity.[4] Within this group, the rural poor—many of whom are smallholder farmers—are among the most vulnerable to this lack of official identity documents.

ID systems play a critical role in political, economic and social development. For individuals, ID systems are the basis to provide legal identity, an objective reflected in goal 16.9 of the Sustainable Development Goals (SDGs): "providing legal identity for all, including birth registration". Moreover, having the ability to prove one's identity (ID) is frequently the entry point to access several basic services, such as healthcare, education, financial services, connectivity and social protections. As regards agriculture, a robust and inclusive ID system can help smallholder farmers in various ways, such as registering livestock, engaging with agribusinesses and financial services providers, creating data-driven farmer profiles, and even increasing their incomes by improving access to new markets as well as economic and education opportunities.

While paper-based ID systems have been around for a long time, as technology advances, governments, NGOs and other stakeholders are exploring new digital solutions to narrow the identity gap. Notably, the transformative potential of mobile technology has been defined as a key opportunity for accelerating the scale and reach of inclusive digital identity (D.ID) systems that can empower citizens, protect their privacy and stimulate economic and social development.[5] While developed countries are gradually transitioning from well-established analogue ID systems to D.ID systems, in the Global South —where legacy ID systems tend to be weak, incomplete or even absent—, there is a stark enthusiasm for D.ID systems, with

[1] Fanzo, J. 2017. From big to small: the significance of smallholder farms in the global food system. The Lancet Planetary Health, 1(1), e15–e16. https://doi.org/10.1016/S2542-5196(17)30011-6
[2] World Bank 2018a. The Role of Digital Identification in Agriculture: Emerging Applications. https://id4d.worldbank.org/sites/id4d/files/ID4D-Agriculture-Emerging-Applicaitons-Summary.pdf
[3] USAID 2018. Digital Farmer Profiles: Reimagining Smallholder Agriculture.https://www.usaid.gov/sites/default/files/documents/15396/Data_Driven_Agriculture_Farmer_Profile.pdf
[4] World Bank 2018b. The World Bank ID4D 2018 Global Dataset. http://id4d.worldbank.org/global-dataset
[5] GSMA 2017. Driving Adoption of Digital Identity for Sustainable Development: An End-user Perspective Report. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/02/Driving-Adoption-of-Digital-Identity-for-Sustainable-Development_An-End-user-Perspective-Report.pdf

a growing number of identity programmes supported by governments, donors and international organisations.

However, the deployment of D.ID systems that are robust, inclusive and sustainable is not an easy task. On the one hand, the ID landscape is becoming more complex and crowded. Multiple ID systems (both analogue and digital), developed for different purposes, issued by different actors and with varying degrees of acceptance can coexist within the same country. This can create difficulties to navigate the system. Without a universally-accepted identity document, individuals must cope with the additional cost, time and effort it takes to apply for services that require more than one form of identity or additional relevant information. On the other hand, the D.ID landscape is rapidly evolving, with emerging technologies and advances in biometrics that are expanding the design options for identifying and authenticating individuals. At the same time, these advances introduce new concerns related to data privacy, control over data sharing and use, and surveillance.

Any project entailing the identification of people will need to take into consideration the increasing complexity of the D.ID landscape and carefully assess the potential benefits and pitfalls of the project. To avoid potential violations of human rights and ensure sustainability, D.ID systems should be designed and conceptualised to adopt legal, ethical, technological and governance safeguards.

This report focuses on the role of D.ID systems in enabling autonomous data ownership for farmers by exploring data governance models and the necessary technological tools in the Global South. The study aims to develop an approach to understanding a country's digital readiness for farmers' Digital Information Management tools.

Section 2 presents the main categories of ID systems and introduces the existing digital ID systems. Section 3 presents all the different stakeholders in the ID systems. Section 4 analyses the state of the D.ID systems and the technology drivers that are changing the D.ID landscape. Section 5 provides a summary of the current trends, progress and obstacles of D.ID systems in the Global South. Finally, Section 6 provides assessments and recommendations about the infrastructural readiness of a country for farmers' digital information management tools.

2. Categorising ID Systems

2.1. Foundational vs Functional ID systems

The most common classification of ID systems distinguishes two types: foundational and functional ID.

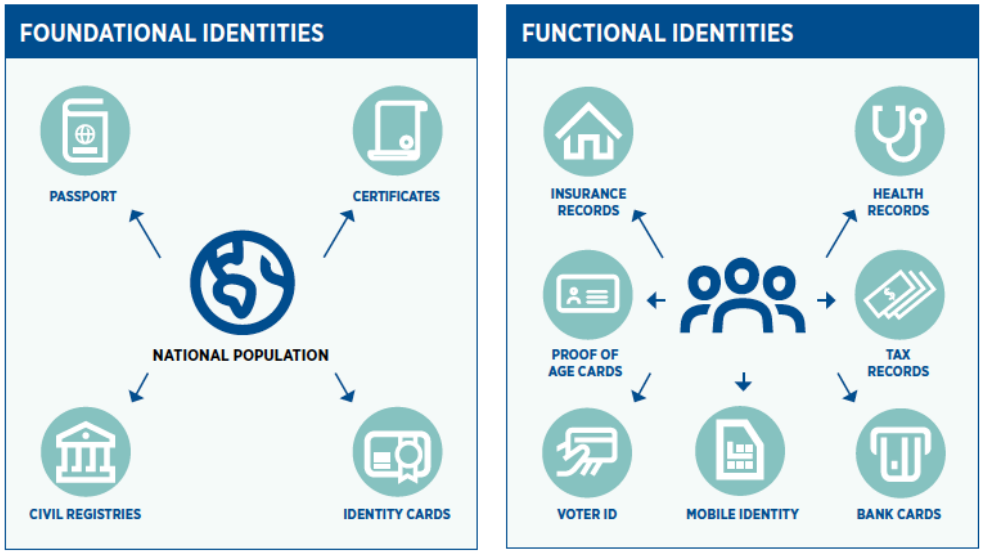
Foundational ID systems are generally developed to provide identification for a national population. Modern foundational ID systems are often established by government institutions and confer credentials that can be used as proof of legal identity.[6] These credentials often

[6] Legal identity is defined as the basic characteristics of an individual's identity. e.g., name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally-recognized identification authority. Legal identity is retired by the issuance of a death certificate by the civil registration authority upon registration of death.

take the form of identity cards, passports or birth certificates. While the main objective of foundational ID systems is often to provide identity as a public good, they can also underlie multiple general purposes, such as access to social services or health records.[7]

By contrast, functional ID systems are created for a specific purpose. They can be issued by a wide array of actors and they often aim to cover only some subset of the total population. Examples of functional IDs are driver's licenses, voter registration cards or IDs issued by financial institutions. Despite their limited scope and the goal-specific purpose, in some countries—and particularly those that do not have a robust foundational ID system beyond civil registration—functional ID systems are used as de facto proof of identity.

Given the different nature and scope of foundational and functional ID systems, both types of systems can coexist in the same country. For example, a given person may have one foundational ID and a variety of functional IDs.



Source: GSMA[8]

Both foundational and functional ID systems can be either paper-based or digital. Digital identities are defined as a collection of electronically captured and stored attributes and credentials that can uniquely identify a person. D.ID systems allow us to authenticate who we are over digital channels, including mobile interfaces, internet browsers, or internet-enabled central authentication points.

Paper-based systems are rapidly giving way to systems involving the use of digital solutions for registration, authentication, data transfer, and storage. Compared to paper-based systems, D.ID systems improve efficiency, strengthen security, and enhance scalability, as they can be linked to diverse services.

However, as with other technologies such as GPS or Artificial Intelligence, D.ID systems are subject to a so-called “dual-use”: they could be beneficial or harmful according to the use.

[7] World Bank ID4D Initiative. Types of ID systems. https://id4d.worldbank.org/guide/types-id-systems
[8] GSMA 2019. Mobile-enabled Economic Identities for Smallholder Farmers in Ghana. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/Mobile-enabled-economic-identities-for-smallholder-farmers-in-Ghana.pdf

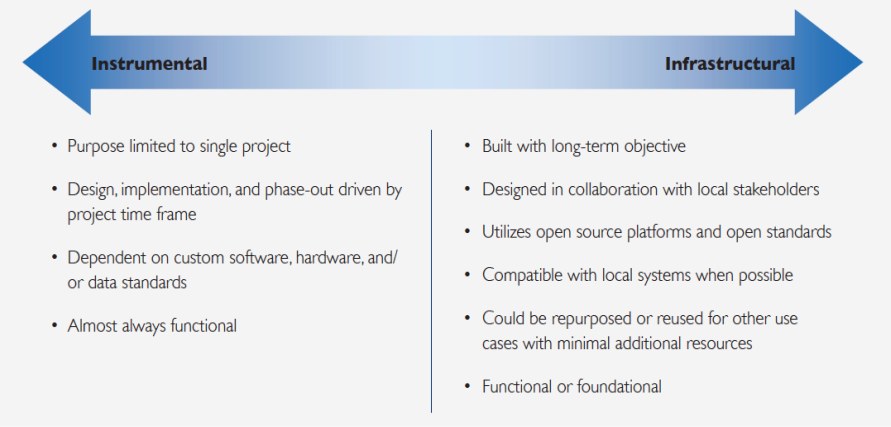
Digital identity programmes create an inherent risk of a power imbalance between the State (and other D.ID issuers) and the D.ID users. If poorly designed or misused, D.ID systems can serve harmful or undesired purposes, which could result in risks to human rights. Such programmes have the potential to turn a digital ID into a pervasive means of surveillance. Further, concerns have been raised regarding potential violations of the right to privacy and insufficient protection of personal data. Moreover, as D.ID systems entail the collection and storage of huge amounts of sensitive personal data in a centralised database, they are susceptible to cyberattacks and data breaches.

2.2. Instrumental vs Infrastructural approaches to D.ID systems development

Besides the traditional distinction between foundational and functional ID systems, several institutions have proposed alternative ways to classify ID systems. One of them, developed by USAID, focuses on the design of ID systems to distinguish instrumental and infrastructural approaches to D.ID systems development.[9]

According to USAID, most D.ID systems, especially in the Global South, are designed within the context of a particular project supported by a given donor or investor, in a way that is tailored to the specific problems, particularities and time frame of such a project. This instrumental approach tends to result in isolated, single application ID systems, which contribute to the increasing fragmentation of the D.ID landscape. In the long run, this situation leads to increased costs, overburdens end-users, and can exacerbate the systemic problems stakeholders hope to solve.

An Infrastructural approach, on the other hand, sees D.ID systems as a core infrastructure to support other systems and activities. Infrastructural systems can be repurposed for similar projects and are compatible with existing local systems. In general, they contribute to a more cohesive and durable ID ecosystem by creating pathways between the multiple ID systems that exist in a given context. Instrumental and infrastructural approaches should be seen as a spectrum (see the image below), meaning that many D.ID systems have some elements of both approaches.



[9] USAID 2017. Identity in A Digital Age: Infrastructure for Inclusive Development. https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

Source: USAID[10]

The infrastructural approach is relevant in that it places the development of D.ID systems in the broader context of the D.ID landscape of a given country. A fragmented D.ID landscape results in inefficiencies, and redundant and unsustainable investments, that ultimately fail to close the identity gap. By contrast, an infrastructural approach prioritises, whenever possible, long-term goals, reuse, repurposing and harmonisation of D.ID systems (with due regard to privacy and data protection concerns), and collaboration between stakeholders.

3. The stakeholders in the ID systems

Throughout the identification lifecycle (including data capture, validation, storage, and transfer; credential management; and identity verification and authentication), a range of stakeholders is often involved in building, maintaining, and using an ID system. Important stakeholders in the context of government-recognized ID systems include[11]:

Individuals

People are at the heart of identification systems. Ideally, they should have the right to know and exert adequate control over how personal data is collected, utilized, stored, and shared as both the subject of these systems and the end-users who use their identity to access rights and services. Understanding and reacting to people's ID-related requirements and concerns, preserving their privacy and personal data, and maintaining their agency throughout the identity lifecycle must be the beginning point for developing an ID system that can help them achieve their development goals.

Governments

Governmental entities are frequently the principal providers of foundational ID systems, such as ID authorities, civil registrars, Ministries of ICT, Interior, or Justice, and so on. Other government agencies, such as the Ministries of Social Protection, Health, Education, Justice, Tax, Customs, and Election Administration, rely on these core systems to engage with individuals and/or provide functional ID systems themselves.

Additional government entities regulate ID systems, provide supervision, and may be involved in the implementation of certain components or the establishment of technical and data format standards. National cybersecurity agencies, for example, assist ID agencies in reducing cybersecurity risks and responding efficiently to breaches, while ICT ministries may provide infrastructure or shared services, such as a data centre, government cloud, or public key infrastructure (PKI).

Private sector

Most ID system components and infrastructure are developed, innovated, and supplied by private firms. Furthermore, commercial organizations may act as ID providers, either as part of their primary business (e.g., as part of federated or decentralized digital authentication models) or to identify and authenticate consumers for other services (e.g., financial services) (e.g., financial service providers and mobile operators). Furthermore, many private businesses

[10] *Ib.*, p. 12

[11] World Bank 2019a. ID4D Practitioner' Guide: Version 1.0 (October 2019). Washington, DC: World Bank

rely on government-issued identification cards to identify their clients (e.g. requiring government-issued credentials to open bank accounts, register SIM cards, or create credit reporting systems). Governments have also worked with private enterprises to provide digital ID platforms, such as mobile identification and digital authentication platforms, or to fulfil certain responsibilities inside a government-provided ID system such as data collecting.

Civil society
Civil society is a term used to describe a group of NGOs, community-based organizations, and other local organizations that are crucial partners in driving ID demand and aiding people in acquiring the proof of identity they need to fully participate in economic, political, and social life. Civil society actors are also valuable prospective collaborators and sources of critical input on ID system strategy and implementation.

International organisations
Development and humanitarian organizations may provide ID system support in the form of finance and technical assistance, or they may be involved in the creation of ID systems to manage programs.

4. Digital ID systems and technology

4.1. What is digital ID?

For decades, people have carried various forms of analogues identification documents, such as ID cards, driver's licences, and passports. Emerging D.ID systems attempt to replicate this concept in the online world. D.ID systems are those that use digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication.[12] At root, a D.ID system is like any other proof of ID: it gives public and private bodies the confidence that the person they are dealing with is who they claim to be. But in the digital world, this capability provides a multitude of new opportunities.

Robust D.ID systems with widespread coverage can produce a wide array of advantages for individuals, governments and the private sector. For individuals, D.ID systems can ease access to benefits, rights and services. For governments, these systems can improve public administration, planning, and service delivery, improving trust in the public sector. In addition, D.ID systems can improve transparency and reduce fraud, thereby increasing resource efficiency. Finally, for the private sector, D.ID systems also play a critical role. To interact with customers and offer services, companies need to verify and authenticate their identities. Where ID systems are limited in coverage or absence, companies need to invest considerable resources in these tasks, often entailing the development of an in-house ID system. With inclusive, well-established D.ID systems, companies can reduce operating expenses and transaction costs, as the credentials provided by customers would suffice to prove identity.

[12] World Bank ID4D Initiative. Types of ID systems. https://id4d.worldbank.org/guide/types-id-systems

Also, when D.ID systems enjoy wide coverage and are interoperable, companies can use the system to build services and applications on top of it.[13]

D.ID can form the foundation of a host of applications in many aspects of an individual's life, work, and social interactions. The potentially pervasive nature of digital ID makes it akin to being used in many applications that are designed to generate benefit but are also capable of causing harmful or undesirable outcomes.[14] For example, a government might misuse digital ID programs by deploying them for political and social control, while a private-sector firm might misuse digital ID for commercial gain by influencing consumers in ways that they do not understand or desire.

The above-mentioned considerations highlight the importance of design and safeguards when developing D.ID systems. In this vein, White et al. have defined a list of attributes that D.ID systems should have to be considered "good"[15] for the privacy and security of the user's data:

- **Verified and authenticated to a high degree of assurance.** Every interaction with the D.ID system (enrolment, authentication or authorisation) should meet high-assurance standards, irrespective of the technology employed
- **Unique.** Individuals should have only one identity in the system and every entry should correspond to only one person.
- **Established with individual consent.** Individuals should have the right to know what they are registering for, what personal data will be collected and how it will be used.
- **Protects user privacy and ensures control over personal data.** The D.ID system needs to be compliant with privacy principles and the data protection framework within a country (if existent and effective, otherwise the best available principles should be adopted), providing technical measures to adequately ensure privacy and data protection.

4.2. How do D.ID systems work?

The D.ID process generally comprises three different stages: verification, authentication, and authorisation.

Enrolment

During enrolment or verification, individuals provide personal data to an ID-providing institution. Such personal records must be sufficiently unique and stable to ensure that the match remains valid over time. Each system will also have a set of requirements regarding what information is required to prove one's identity. Many systems rely on "breeder documents" such as birth certificates and build upon birth registries or similar population

[13] World Bank. 2018. Private Sector Economic Impacts from Identification Systems, Washington, DC: World Bank. https://documents1.worldbank.org/curated/en/219201522848336907/Private-Sector-Economic-Impacts-from-Identification-Systems.pdf
[14] van der Bruggen, K. 2011. Possibilities, intentions and threats: Dual use in the life sciences reconsidered, Science and Engineering Ethics, 2011, Volume 18, Issue 4, pp. 741–56.
[15] *Op cit,* White, O., et al. 2019, p. 2.

databases. Biographical information could be complemented with biometrics (e.g. fingerprints or iris scans) to provide additional uniqueness.[16]

Which attributes and evidence is captured during this phase, the methods and standards used to capture them, and the resulting data quality will have important implications for the inclusivity and trustworthiness of the identity, the speed of data collection, program cost, interoperability with other ID systems, and its utility for various stakeholders.[17]

During the enrolment process duplicates in the database must be avoided, that is, to ensure that every person is different from every other person enrolled. Once the enrolment process is complete, the ID-issuing institution gives new ID holders a token or credential (e.g., a unique number or a card) that can be used to prove their identity. For an ID to be considered digital, the credentials issued must store data electronically and/or be usable in a digital environment (e.g., being machine-readable and/or usable on the internet).[18]

Authentication

Once an individual is enrolled, she can assert an ID to access a service and transact. After she presents ID credentials, an authenticator queries the ID database to confirm that her assertion matches the information linked to the credential at enrolment.

Authentication factors fall into one of three categories as shown in the figure below:

- something you have (e.g., a physical card, mobile device, or digital cryptographic key);
- something you know (e.g., a password, PIN, or answer to a secret question);
- something you are (e.g., your fingerprint or other biometry).

Using multiple factors increases the level of assurance (i.e., security or trustworthiness) in a transaction.

Source: World Bank[19]

[16] *Ib.,* p. 13.
[17] World Bank 2019a. ID4D Practitioner' Guide: Version 1.0 (October 2019). Washington, DC: World Bank
[18] *Op cit*. World Bank 2019a, p. 19.
[19] *Op cit*. World Bank 2019a, p. 20.

The use of data during authentication differs from enrolment. When enrolling new users, each entry must be compared against the entire database to check for duplicates. When authenticating, it is only necessary to check whether a given set of credentials exists in the database. As a result, authentication typically requires less information than enrolment.

Authorisation

Once a D.ID system has confirmed that the set of tokens presented matches a known person in the database, service providers determine which services the authenticated user is authorised to access (e.g., withdrawing cash or voting).

Authorization decisions are separate from the authentication of credentials. In some cases, a service provider will have a "whitelist" of authorised individuals and will check whether an authenticated ID holder is on the list. An authorization database matches public tokens to information about which services each user may access.

4.3. D.ID technology landscape

New technologies and trends are bringing distinct opportunities to add value for both individuals and institutional actors. The landscape is rapidly evolving, and with a more diverse and complex "menu" of technologies, deciding the design of a new ID system can be challenging. The following sections provide an overview of the most important technological breakthroughs in the ID landscape.

Biometrics

Biometric technologies use physical characteristics, such as unique patterns in iris or hand shape, to identify people automatically. Biometrics are collected during enrolment and linked to the external personal documentation (e.g., birth certificate, passport) that a person must provide in this phase to prove her identity. To uniquely distinguish one person from all others registered in the system, sufficient high-quality biometric data must be collected. For example, India's Aadhaar ID system requires ten fingerprints and two iris scans to enrol a person.

Once the D.ID system knows the person's claimed identity, it can usually authenticate her whenever she presents the required biometric characteristic. This task requires less precision than in the enrolment phase. For instance, a single fingerprint or a shorter voice recording may suffice.

Many D.ID programmes, especially in the Global South, entail the collection, storage and use of biometric data of individuals as the primary means of establishing and authenticating their identity. Two advances in biometric technology explain this trend.[20] First, biometric identification kits are decreasing in size and cost. This is applicable for both enrolment and authentication. Regarding enrolment, there is an increasing number of specialised devices that are designed to capture biographic data, fingerprints, iris scans, face images and signatures.[21] Since these devices are portable, it would be easier to reach remote areas for enrolment purposes. As for authentication, modern smartphones are game-changers, as they are already capable of capturing biometrics such as fingerprints, facial data and voice records.

[20] *Op cit.* USAID 2017, pp. 45-47.
[21] See, for example, CardLogix: https://www.cardlogix.com/product-category/biometrics/

Given the rapid uptake of mobile phones in the Global South, these devices are expected to become important authentication platforms (see next section). Second, as technology evolves, new biometrics are available to uniquely identify individuals, including palm veins or behavioural biometrics such as handwriting style.

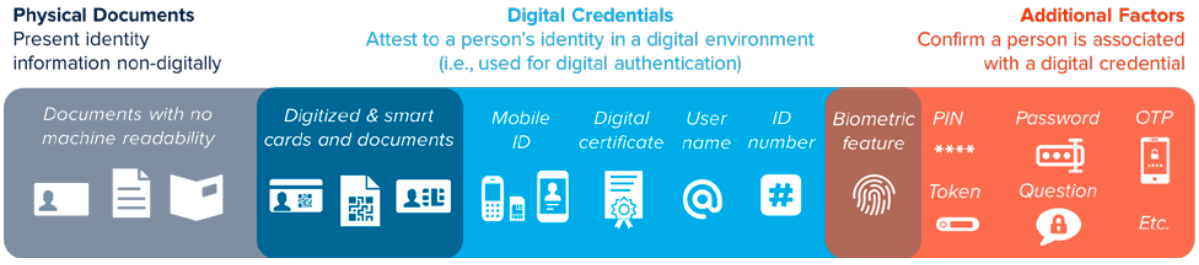
However, no biometric ID system works perfectly. Problems are generally caused by changes, either natural or accidental, in the physical characteristics of the person. For example, simple cuts or dryness in hands due to manual work may exclude people from fingerprint-based systems. Also, although rare, the system could fail as a result of a coincidental similarity to another person's biometrics.

Biometrics-based ID systems also raise surveillance concerns. Although biometrics are often labelled as a private token, many biometrics are not truly private. For example, it may be possible to scan irises from a distance or high-quality facial pictures, and fingerprints can be retrieved from any smooth surface. Such passive biometric capture creates the danger of a national database that can track people covertly, at a distance or in motion, without their knowledge or consent.

Finally, biometric systems pose risks to data protection and privacy rights. While other credentials such as an identity card or a password can be easily replaced, if a biometric credential is stolen or compromised, getting a new one is hardly possible. This is especially dangerous if biometric data is —as it often happens— stored in a single centralised database, as it creates a single point of failure in the case the data is hacked or stolen.

Digital Credentials

A credential can be defined as any document, object, or data structure that vouches for the identity of a person through some method of trust and authentication.[22] Advances in digital technology have led to the digitisation of physical credentials, which now include magnet stripes, barcodes, or chips that enable them to authenticate people in the digital sphere. As societies become more digital, an increasing number of D.ID systems are providing digital-only credentials, such as mobile IDs, digital certificates or usernames. Such credentials are stored in electronic devices and servers and are often linked to biometric data for authentication purposes.



Source: World Bank[23]

Mobile phones play a critical role in the development of digital credentials. Since they are becoming rapidly ubiquitous, including in many developing countries, they are regarded as an

[22] *Op cit.,* World Bank 2019a, p. 157.
[23] *Ib.,* p.157.

attractive pathway for the implementation of inclusive and low-cost D.ID systems compared to physical-based ones.

However, mobile-based D.ID systems may not work in countries with low connectivity or limited phone and network connectivity. In such cases, the ID system should provide alternative, more accessible options for authentication. For these reasons, the choice of credentials should be subject to consultation with stakeholders, taking into account economic, social and legal considerations as well as context-based constraints.

5. Current situation of ID systems in the Global South

Many projects entailing the development of ID systems are located in countries of the Global South, where the identity gap is more acute. Every country presents particularities and different levels of progress regarding the implementation of ID systems. An analysis of the current identity landscape of these countries is a valuable exercise for governments, private actors, and other entities planning new ID systems and those hoping to optimise existing systems. To maximise the utility of identification in the medium- and long-term, it is important to first take a holistic view of existing ID systems and stakeholders within the identity ecosystem and assess their strengths and weaknesses, particularly regarding system coverage, quality, and the enabling legal framework.[24]

An identity ecosystem is defined as the set of identification systems and their interconnections within a country. An identification system consists of the databases, processes, technology, credentials, and legal frameworks associated with the capture, management, and use of personal data for a general or specific purpose.[25]

When we look at the ID landscape in the Global South, Identification systems are becoming more common across Latin America, Southeast Asia, and Sub-Saharan Africa. The driving force behind creating a national identity system varies from country to country. Surveillance, fair and democratic elections, and fostering national unity are among the most mentioned reasons for implementing an identity system.[26]

5.1. Challenges to developing ID systems in the Global South

Building an ID system that meets developmental goals has many challenges, in any context, such as ensuring its durability and mitigating the potential risks to privacy and inclusivity. Following an extensive review of experiences in multiple countries at varying levels of development, the World Bank has highlighted a list of the main risks to implementing new or upgraded ID systems in the Global South. Although the context of every country is different, the following are common challenges that countries face to a greater or lesser extent[27]:

- **Exclusion.** The establishment of D.ID systems can deepen exclusion in two ways. First, the formalisation of a new ID system and the tightening of identification

[24] *Op cit*. World Bank 2019a, p. 32.
[25] World Bank 2018c. Guidelines for ID4D Diagnostics, Washington, DC: World Bank. https://documents1.worldbank.org/curated/en/370121518449921710/Guidelines-for-ID4D-Diagnostics.pdf
[26] ITU 2016. Review of National Identity Programs
[27] *Op cit*. World Bank 2019a, pp. 5-8.

requirements risk further marginalising vulnerable populations. Second, the failure of biases of D.ID systems (e.g. failure of biometric authentication mechanisms, collecting data that is difficult for some people to provide, poor data quality, etc.) can lead to the exclusion of people from the D.ID system or accessing related services. Therefore, the design of D.ID systems should include provisions to make them inclusive, with special attention to .populations that are at higher risk of exclusion.

- **Privacy and security violations.** Inherent in the capture, storage, and use of sensitive personal data are risks associated with privacy violations, data theft and misuse, identity fraud, and discrimination. The emergence of new technologies and the increased collection and use of personal data by state and non-state actors compound these concerns and bring new threats from cybercrime and cyberattacks. IT systems, therefore, require strong legal and regulatory frameworks and a privacy-and-security-by-design approach to mitigate these risks and ensure data protection and user control. Cybersecurity of the system within a secure environment should be part of the a priori design.
- **Vendor or technology "Lock-in".** Dependency on a specific technology or vendor can result in "lock-in" and/or dependency, increasing costs and reducing the flexibility of the system to meet a country's needs as they develop.
- **Unsuitable or unsustainable technology and design choices.** In many cases, countries have adopted high-cost systems that have failed to achieve development goals because they were unsuitable for the context or unsustainable in the medium or long term. Ensuring that systems provide a good return on investment and are sustainable over time requires a detailed appraisal of local context and capacity and robust procurement guidelines.
- **Weak civil registration systems**. Civil registries are key to ensuring legal entities for every individual by providing documents such as birth or death certificates. In developed countries, ID systems are commonly linked to civil registries. However, developing countries have historically lagged in the establishment of strong civil registries. Without such documents, many people living in these countries may have trouble proving their identity before ID systems, thereby risking further exclusion.
- **Limited connectivity and other infrastructure.** In many countries, rural and remote areas lack reliable mobile and internet connectivity. This can create difficulties when implementing D.ID systems that require power and connectivity during enrolment (e.g., for data transfer or duplicate biometric enrolment check) and for authentication. Furthermore, core ICT infrastructure, such as secure data centres, may not exist. In addition, the general lack of infrastructure such as reliable roads in rural areas and regions with difficult terrain makes certain households difficult to reach and can increase the time and cost of enrolment. If these issues are not addressed through technology choices and outreach, ID systems are likely to be exclusionary in low connectivity areas.
- **Lower literacy levels.** In developing countries, significant portions of the population may have lower literacy levels, both in terms of reading ability and the use of digital technology. This may translate into difficulties with enrolment, as well as the use of these systems for segments of the population who are likely to be among the most vulnerable. It also has implications for people's ability to provide informed consent to the collection and use of their data. As with low connectivity, illiteracy rates should be reflected in system design and implementation to minimise the potential for exclusion.

- **Poor procurement.** Low- and middle-income countries may have weak capacity and institutions to handle procurement and vendor contract management for an ID system, which is complex because of the wide range of technologies available and different types of procurement that need to be completed. Further exacerbating this challenge are the tight deadlines that governments and donors often impose for the introduction of an ID system, which puts pressure on providers to reduce their planning time. The consequences of poor procurement processes and vendor contract management include failed procurements, delays (e.g. because of appeals), and vendor and technology lock-in.

5.2. Current trends in the Global South

In the following subsections, we provide an overview of the current situation of ID systems in Southeast Asia, Latin America and Africa.

Southeast Asia

Among the countries of the Global South, the most remarkable developments are taking place in Southeast Asia. By 2019, five of the 10 member states in the Association of Southeast Asian Nations (ASEAN) — Brunei, Indonesia, Malaysia, Singapore and Thailand—, had already fully digitalised their foundational ID systems, while other countries in the region have similar projects on the way.[28] Many of these D.ID systems use smartcards with data such as private keys and biometrics stored on the chip.

Most of these systems have been conceived as a foundation for the development of e-commerce, e-government and the digital economy. As a result, they are expected to facilitate both public and private transactions in the future. Some systems are already showing progress in this direction. For example, India's digital ID system – known as Aadhaar – has directly led to the opening of over 150 million new bank accounts, many of which were for people who were previously unable to open one, whereas Thailand's digital ID system provided a basis for the government to realise universal health coverage within three years.[29] . Equally, there is a general ambition in the region to advance ID systems that enable interoperability and transactions across borders.

However, the progress has not been without problems, and valid concerns have been expressed over the lack of personal data protection and potential exclusion. Also, while the countries are going toward fully leveraging their new systems, additional efforts should be made to integrate their national IDs with their civil registries.

Latin America

Unlike other countries in the Global South, Latin America has a remarkably similar cultural, religious, and colonial heritage. This common ground is reflected in how identification is perceived in the region. The first step of an identity system is the individual's civil registration for issuing a legal identity. Identity management in the region is usually carried out by a central

[28] World Bank 2019b. The Digital Economy in Southeast Asia: Strengthening the Foundations for Future Growth. Information and Communications for Development. World Bank., p.110.
[29] *Ib*. P.110.

identification authority for enrolment and the issuance of credentials. Unfortunately, as most Latin American countries were governed by dictatorships in the second half of the last century, ID systems were often appropriated for surveillance and persecution (e.g., biometric identification facilitated the persecution of opponents of the regime). Thus, the paradoxical history of identification in Latin American countries shows how identification can be used for good and bad purposes.

In recent years, we see important progress in the adoption of ID systems in Latin America. All countries have government certification authorities, which is regarded as a fundamental element for the establishment of digital identification. Additionally, there is a fluid exchange of good practices among countries, and projects have been proposed to allow interoperability between the identification databases of different countries.

Although there is an effort by many countries to provide identity services to their citizens, important challenges remain. According to ID4D, in Latin America and the Caribbean, in 2018 there were around 50 million people with no identification documents. Most of them are vulnerable populations living in complex socioeconomic conditions, mostly in remote areas. A significant part of the population of Latin America does not yet have access to basic infrastructure, a precondition for the proper implementation of digital ID systems. Low levels of electricity, telecommunications, and data infrastructure augment the digital divide between the rural and the urban[30], and high illiteracy rates are fundamental challenges.

Africa

The lion's share of the identity gap is now in Sub-Saharan Africa.[31] Based on the World Bank's Identification for Development (ID4D) program's database, more than 40 per cent of those lacking IDs in the world live in Africa. This overrepresentation is partly because it is the region with the lowest birth registration rates; while these have risen impressively in some African countries, they remain low or have fallen in others. And while almost every country in the region has opted to have a national ID system— most of them are digital and make use of biometrics— some countries have not yet been able to fully implement their ID systems.[32]

National ID initiatives are underway in much of Africa. Some of these are greenfield projects as in Liberia and Malawi, while others involve better integration of the ID system into government programs such as cash transfers as in Mauritania. Lesotho and São Tomé and Príncipe have recently completed full integration of their civil registration and national ID systems. Côte d'Ivoire started associating each SIM card with an identity card number in 2012 and renewed the process in 2017, this time with biometric data.[33] At the same time, regional bodies such as the Economic Community of West African States (ECOWAS) and the East African Community (EAC) have been developing plans and piloting programs for

[30] Domínguez, M. 2018. Access and use of information and communication technologies in Mexico: determining factors. PAAKAT: Revista De Tecnología Y Sociedad. Vol. 8 No. 14.
[31] World Bank 2017. The State of Identification Systems in Africa: Country Briefs. World Bank, Washington, DC. World Bank. https://openknowledge.worldbank.org/handle/10986/28310
[32] Kayser-Bril, Nl. 2019. Identity-management and citizen scoring in Ghana, Rwanda, Tunisia, Uganda, Zimbabwe and China. Algorithm Watch, p. 5.
[33] Kautcha, D. 2018. Côte d'Ivoire: La ré-identification des abonnés mobiles sera achevée le 31 mars prochain, Koaci.com. Archived at http://archive.fo/PlUlx

interoperability of ID systems to allow for free movement of people and better cross-border access to services.[34]

But many challenges persist in the region. For birth registration, these include low birth registration rates; the prevalence of manual, paper-based civil registration processes in most countries; and the scarcity of infrastructure, including registration offices, in some countries. As for national IDs, covering the full population is still a great issue, especially in larger countries, meaning that there is still a high proportion of people with no identification credentials. Moreover, there are important gaps in the legal and institutional framework of the countries to assure privacy, cybersecurity and protection of personal data. Data protection legislation exists in some countries but remains incomplete. Following a study on the ID landscape in 17 African countries, the World Bank concluded that "a majority of countries lack adequate legal frameworks to support and regulate modern identity management systems".[35] These gaps are especially relevant in the light of the increasing collection of biometric data for identification purposes in many of the new D.ID systems. Finally, another challenge to advancing D.ID systems in Africa is the scarce number of local technology providers, which results in a high reliance on contractors from Europa, North America and Asia.

6. Assessing the infrastructural readiness of a country for farmers' digital information management tools

Digital ID systems are built on the existing information and communication infrastructure in a country. There is a need to incorporate the currently fragmented institutional experiences of applying information and communication technologies in rural development and food security. According to a report by the FAO[36], the following are the main issues and recommendations related to infrastructural problems of digital information systems in the rural regions of developing countries.

6.1. Policies/ Governance

Current national policies regarding the use of communication and information technologies are mainly oriented towards the management of the telecommunications infrastructure. Rural populations are disadvantaged in terms of access to information and the necessary communication and information technologies.
Broad and equitable access to communication and information technologies in rural areas should be ensured in tandem with the ongoing processes of decentralization, democratization and policy review, in the context of global and national considerations of governance.
There is also a need to adopt policies and awareness with regard to capacity building in the context of the new possibilities offered by communication and information technologies.

Recommendations:

[34] *Op cit.* World Bank 2017. pp. V-VI
[35] *Op cit.* World Bank 2017. p. 12.
[36] FAO, Le rôle des technologies de l'information et de la communication dans le développement rural et la sécurité alimentaire. Rapport de la Premire Consultation sur la Gestion de l'Information Agricole. Available at: https://www.fao.org/3/x7936f/X7936f09.htm#Atelier%202 [Accessed April 8, 2022].

- A specific policy must be put in place to ensure equitable access of rural populations to information and communication and information technologies.
- Decision-makers also need to advocate for the use of information and communication technologies for development, which would require a coalition of stakeholders and new institutional partnerships.

6.2. Finances and sustainability

Communication and information technologies for rural development do not receive sufficient priority in national budgets. Strategies need to be formulated to ensure financial sustainability for the use of these technologies in rural development.

Recommendations:

- The development of open and dynamic policies for the rural telecommunications sector is generating a very strong demand for the expansion of services. These changes should continue in a context of social responsibility and careful consideration of the needs of underserved populations. Part of the revenue from telecommunications should be used to support and promote the expansion of communication and information technology infrastructure in rural areas.
- Investments in these technologies should be evaluated in the context of their contributions to the long-term development of human capital in areas such as health care, vocational training (e.g. for employment), continuing education and environmental management.
- There is a need to provide investment structures and policies to stimulate initial demand (thereby reducing investment risks) for information and communication technologies in rural areas and to promote the use of investments in infrastructure.

6.3. Design

Communication and information technology strategies for rural areas need to be developed taking into account linguistic, cultural, socio-economic and infrastructural differences. The private sector should also be encouraged to invest in the design of communication and information technologies suitable for use in rural areas.

Individuals or communities can become content designers, adapt technologies and create information resources that meet their needs.

Recommendations:

- The socio-economic context should be duly taken into account in the design of communication and information technology projects. Local initiatives should be encouraged to explore the possibilities offered by these technologies and incorporate participatory communication and learning processes. Appropriate needs assessment methodologies (e.g., participatory rural communications assessment) would be needed.
- Projects should be launched to examine the specific needs for the choice and use of communication and information technologies in the field of rural development (for example, technological solutions and special standards for the collection, processing

and storage of information in rural areas), with particular regard to cultural and linguistic diversity.
- Communication and information technologies should be linked to traditional forms of communication to meet identified needs and reach specific groups (e.g., rural radio linked to the Internet).
- There is a need to move away from central repositories of information to an approach that links widely available sources of information to a large number of providers.

6.4. Capacity building

Realising the opportunities offered by information and communication technologies for rural development and food security requires an information culture and new skills.

Recommendations:

- There is a need to sensitize decision-makers and stakeholders, including regional organizations, on the need to invest in capacity building in communication and information technologies at all levels of formal and out-of-school education. This includes training development workers to incorporate communication and information technology into their activities. In addition, emphasis should be placed on training women and young people in the use of communication and information technologies and ensuring that disadvantaged groups benefit from them.
- The private sector should be encouraged to extend its current participation in technical training for communication and information technologies to rural areas and efforts should be made to have new training availabilities in freeware as well as private.

6.5. Content/ Apps

There is currently a dearth of content, applications and access to existing data of particular relevance to rural development and food security. Beyond physical access, data must be up-to-date, searchable and easily applied by a wide variety of users.
It is now possible to involve small-decentralized content providers by ensuring that information is available in local languages and takes into account local cultures.

Recommendations:

- The information needs of various users should be identified to allow the development of content and applications specific to users and take into account local factors. The role of civil society and the private sector is essential in this identification process.
- Rural development institutions should provide local support to rural people for the development of their content and applications.

6.6. Field studies

At present, information about the use and effects of information and communication technologies on rural development is incomplete.

Recommendations:

- There is a need to expand the monitoring, evaluation and description of successful and unsuccessful applications of information and communication technologies for rural development and to develop models to identify investments and future strategic programs.
- Research and pilot projects on the role of information and communication technologies in supporting rural development should be strengthened.