Center for Global Development

CGD NOTES

Using Identification for Development: Some Guiding Principles

2/22/16 (http://www.cgdev.org/publication/using-identification-development-some-guiding-principles)

Alan Gelb and Anna Diofasi

There is growing recognition of the importance of identification for sustainable development. Its role is recognized formally in target 16.9 of the Sustainable Development Goals, which calls for providing "legal identity for all, including through birth registration" by 2030. Identification is also an enabler of many other development targets, from social protection (delivering support) to financial inclusion (opening bank or mobile accounts and establishing a credit record) to women's empowerment.

Having a recognized identity is crucial for achieving several development outcomes:

- It is essential to realize political and social rights and to participate in a modern economy.
- A well-functioning ID system can strengthen state capacity and reduce corruption and waste by making programs and subsidies more effective and transparent.
- Effective identification, including for remote and electronic transactions, can reduce transactions costs and create economic opportunities, including for the poor.

At the same time, driven by a number of powerful factors related to security, development and new technology, many countries have been introducing new ID programs or upgrading existing ones to increase their capabilities. Conventional ID systems are rapidly giving way to digital ID or e-ID systems, even in poor countries. Almost all of the new systems and most upgrades to existing ones involve the use of digital databases, data analysis and transfer, and digital biometric technology.

The question is not whether this trend will continue but how and how effectively the new systems will support inclusive development. The guiding principles below draw on our ongoing study of ID systems and their applications to suggest lessons. Figure 1 provides an overview of the structure of this paper.

ID is essential for development…

Realization of social and political rights

More (cost) effective administration of programs

Greater economic opportunities

…but it's **not easy**.

No single, simple concept of ID

No single system for providing ID

However, there are some common **goals and risks**:

✓ GOALS

Inclusion – provide ID for all

Robustness – unique, verifiable ID

Integration for cost effectiveness

✗ RISKS

Exclusion of individuals

Misuse of data

Wasteful deployment

Center for Global Development

Learn more at www.cgdev.org

There is No Single, or Simple, Concept of Identity and No Single System for Providing It.

Legal identity is not the whole story: identity need not be associated with national status. SDG 16.9 refers to “legal identity”, a concept usually associated with status, for example, as a national or citizen of a country. But this is not the only type of identity that is relevant for participation, capacity, and opportunity. National status is central to some areas of rights and participation, like the ability to travel, but not particularly relevant for many others, such as access to social transfers or to hold a small financial account. Gelb and Clark (2012) develop the concept of “official identity,” the identity needed to participate in a complete range of interactions where identity may be needed. Official identity can be provided by both “foundational” systems: multi-purpose systems that may (Peru) or may not (India, Aadhaar) provide “legal identity”; and “functional” systems related to some specific function or program such as disaster relief or a driver’s license.

Not all ID systems can yet be based on civil registration. Most advanced economies base their ID systems on a well-maintained continuous civil registry (the “OECD model”). Actions to strengthen and modernize civil registration starting from birth are essential, both to provide the basis for the ID system and to improve health-related data. But with the average birth registration rate around 40% in low-income countries, many ID systems today must start from a different, population registration, baseline. In countries with seriously deficient civil registries, a ‘clean slate’ approach that involves complete re-registration into a population registry can be the most cost-effective and inclusive option. Over time, most systems will probably converge to the OECD model, but this will take years in some countries because of the backlog in civil registration. Nevertheless, civil registration and ID should not be thought of as separate processes. The goal should be to converge towards identity for life.

Countries have very different ID architectures. The legal, institutional, and technological arrangements to register and identify people differ a great deal. Some countries have developed strong centralized systems, either in a Ministry (Home Affairs, Justice) or an autonomous agency dedicated to providing registration and identification services (Pakistan’s NADRA, Peru’s RENIEC or India’s UIDAI). Some have multiple incompatible competing systems—voter ID, tax ID, bank ID, pension ID as well as an un-developed national ID system (Mexico, Nigeria, Tanzania). Some still rely on “local ID” that is administered at the community level (Ethiopia). Globally, even among OECD countries with a strong tradition of civil registration, there is not a single “model” ID system. Programs to help countries harness the potential power of ID for development need to take account of these different starting points as well as the priorities at hand. To ensure that the ID system is taken up and used, they need to take into account the demand for identity services as well as the supply.

ID cards are one among several options. While identity cards continue be used widely in many countries, technological advances now allow authentication of registered individuals at a relatively low cost (and low technological capacity) against a central, biometric database. Authentication is also increasingly linked to devices such as mobile phones.

-

The Systems are Different but the Goals are Common

ID systems should aim to maximize the realization of the three development outcomes listed above: access to rights, improved government effectiveness, and access to economic opportunities. They need to be constantly evaluated against these criteria.

To realize their development benefits ID systems should have three basic features:

1. They should be inclusive—providing identity for all.
2. They should be robust—providing unique and verifiable identity.
3. They should be cost-effective—which requires integration into applications and – as appropriate – within the system

They must also minimize three risks:

4. exclusion, whether related to income, national status or other factors;
5. misuse, against the interests of the population the ID is intended to serve; and
6. waste – their benefits should justify their (often considerable) costs.

The remainder of these principles offer suggestions to help maximize the benefits and minimize the risks.

1. Making ID programs inclusive

Enrollment should be as close to universal as possible across all parts of the population, including women, children, minorities, and other vulnerable groups. Policymakers should strive to eliminate barriers to registration, whether rooted in policy, logistics, or the cost of obtaining an ID. This is more helpful than making ID (or registration) compulsory although it may, of course, be legitimately required for particular purposes.

Minimize requirements for enrollment.
Imposing strict documentary pre-requisites, such as having to produce a birth certificate or to prove that one's parents and grandparents were citizens can pose insurmountable barriers for many most in need of recognition. India's Aadhaar UID program has enrolled some 960 million people. It has no pre-requirements, separating questions of legal status from identity and accepting "introductions" for those with no other credentials. Similarly, voter registration drives in many countries, for example, Tanzania in 2015, show how quickly "credential-lite" programs can be rolled out to include virtually the entire adult population. In some countries it may be necessary to use such a "credential-lite" program for development-related ID if the rollout of a national ID is constrained by overly restrictive requirements or excessively slowed by other factors.

Provide basic ID for free. With average enrollment costs typically around $3-$6, many will not be able to afford an official ID if they are charged the full price for registration. With ID being a public good that plays a crucial role in enabling individuals to exercise their rights, basic ID should be provided free. Registration can be encouraged by linking it to benefits and programs (South Africa). Countries can cross-subsidize the extension of basic ID by charging for priority services and also for authentication services provided by the ID system to banks and others (Pakistan, Peru). Some of the budgetary savings enabled by a strong ID system (elimination of ghost workers and pensioners, savings from subsidy reform) can also be recycled back into the system.

Reduce barriers for remote communities.
Especially in remote areas mobile units (Pakistan, Peru, Malaysia) can make ID more accessible. An increasing number of countries are also making use of online registration and birth registration via mobile phones (Kenya, Tanzania).

Reduce legal and socio-cultural barriers to women's enrollment. Different legal and social norms contribute to the exclusion of women and their children from ID programs, and from the rights and opportunities conferred by them. In some countries, male relatives must be present for a women to register. Unmarried mothers and their children may face stigmatization when birth certificates are issued without the father's name and thus opt not to register them at all (Indonesia). Providing official ID on an equal legal basis to men and women can be a first step but is often not sufficient. It may be useful to deploy all-female registration units (Pakistan) and provide added incentives for women's registration, such as Nepal's tax rebate when land is registered to women.

Consider lowering the age of enrollment. Many countries enroll only at age 18. This can increase uncertainty over their identity. Especially as birth certificates are easily forged it can be helpful to lower the age of enrollment to include children as young as 5 with biometrics (Aadhaar, also some other countries) as well as younger children with identity numbers linked to those of their parents. This can also be useful for service delivery.

Enlist partners. NGOs can play a vital role in connecting government authorities with underserved communities. The Female-headed Household Empowerment Program (PEKKA) has played a key role in supporting civil registration in Indonesia through helping to convene "one stop shop" rural registration fairs among other initiatives.

Set up grievance mechanisms for those unable to enroll or to be authenticated. Even the most technologically advanced systems have their limitations. Some registrants may not be able to provide quality biometrics; others may be falsely rejected from the system as 'duplicates'. Each ID system should have an accessible grievance mechanism for those who cannot enroll or authenticate their identities and monitor its business process for timeliness and customer satisfaction.

2. Providing Robust Identity — Unique and Verifiable

Some traditional "local" ID systems, can provide reasonably robust and unique identity based on tight community administration. But these systems break down as people become more mobile and require portable credentials, including to enable remote authentication. An ID system must ensure the uniqueness of each identity[1] and allow flexible options for individuals to authenticate themselves, whether against a credential (card, mobile) or directly against the central register.

The main identity asset is the database not the "card". For users of a card-based system the card is the face of the system but the core of the system is the database that underpins the issue of the cards and also enables other mechanisms to authenticate identities. Robust systems should be able to verify both the validity of the identity (and linked credential, if exists) and link the stored identity information to the registered user.

Only multi-modal biometrics can ensure uniqueness in large populations. Almost all of the new systems being put in place in developing countries involve digital biometrics, usually fingerprints and face and sometimes iris. They greatly increase precision and enable the most basic identity question (are you the person registered as you?) to be separated from the biographic and contextual information traditionally associated with identity. This can facilitate "credential-lite" programs useful for development. Biometrics are essential for establishing a credible population baseline in countries with poor civil registration.

Biometrics introduce their own vulnerabilities. Some people cannot provide high-quality prints but the use of iris, in addition to fingerprints, increases inclusion by increasing the percentage of people who can be biometrically enrolled and use biometrics for authentication. Only limited data should be included in cards; templates transmitted for authentication should be encrypted with the public key of the ID agency; templates held by the database should also be encrypted when not needed for authentication. Images, where kept, must be isolated and stored separately. Revocable biometric templates are not yet in use; more research in this area would be useful.

Offer maximum flexibility for authentication. Over time, evolving preferences and technology lead to changes in the way that users authenticate themselves. One option is direct authentication against the database (Aadhaar) and its costs are falling rapidly, including through developing iris cameras for mobiles. Cards will continue to be useful in many countries (and for many applications) for the foreseeable future. Countries should aim to offer a wide range of alternatives. Where appropriate they can facilitate 2 factor authentication (card+PIN (Estonia), mobile number+iris-scan (Aadhaar)). To keep costs low, countries can offer different types of cards, a simple one for basic use and a more advanced one, for example to those seeking an ICAO-compliant travel document.

Match system capabilities at points-of-service (POS). Not all applications require the same level of identity assurance; for some, just visual inspection of a card or an OTP sent to a mobile number linked to the ID number is sufficient. But there is little point in rolling out a sophisticated system (a card with fingerprints in the chip) while not making provision to use its capabilities when needed (no readers deployed). Reliable POS authentication can be particularly effective at reducing fraud and leakages; it can also support more complex applications, such as tracking of healthcare patients in cases where repeated treatment is critical (such as for TB or HIV patients). Without providing for POS capability much of the functionality of an ID system can be wasted.

Develop (and apply) performance standards. There is very little public data available on the field performance of biometric registration and authentication systems. However, data released by India's UIDAI about the inclusiveness and accuracy of its biometric enrollment process could serve as a benchmark for other countries looking to adopt similar systems. Standards were also critical for that program's competitive procurement process that holds down costs and prevents vendor capture.

3. Cost-effectiveness - via integration into applications and within the system

Successful ID systems must provide benefits at minimal, or at least acceptable, costs. Based on standard cost ranges and estimates of potential savings – for the budget and also for users - a strong ID system can be a very good investment. The savings from reforming just one of India's numerous programs were sufficient to recoup the entire costs of the Aadhaar program over about one year. Yet there are many examples of costly programs that have failed to provide benefits.

Consider identity as a service and involve the users. Successful programs require a combination of effective supply of ID services and also demand for them They should be developed through an inclusive consultation process (a "user group" or a "social cabinet") and also with some financial incentive to the ID agency based on ID uptake and use (Pakistan, Peru, others). This will also help to ensure that the program includes a common understanding of the necessary POS infrastructure. Use is critical to motivate the demand for registration and ID, for example through linking them to social grants (South Africa, others). Use is also essential to help ensure that data such as current address are reasonably updated or that countries can keep the links between their population, family and household registers reasonably current (Pakistan).

Should countries have a single all-purpose ID system? Perhaps but this is a national choice. Most countries are developing integrated ID systems with one number used for all programs and formal interactions. This has many benefits for government and citizens -- single registration, economies of scale and scope, the ability to have a user-centric view of services and eliminate waste and fraud across multiple programs. Some applications, such as strengthening tax administration, are not possible without a single ID number that can link assets, income and other indicators of wealth. Conversely, highly fragmented systems are wasteful and preclude some uses.

At the same time, it may not be possible to have a single system. For example if demanding enrollment requirements prevent the poor from obtaining a national ID there may be no option but to have a second "social" ID. Some are concerned about the potential risks of integrated systems, including surveillance, data privacy and vulnerability of the central register. Some programs, such as Austria's eID and GOV.UK Verify aim to de-link any central ID (and ID number) from the functional IDs used to access different types of services to make it more difficult to create a transactions record across multiple data bases. Many poor countries are not yet at this stage, as they are still seeking to consolidate their basic population, family and household registers but it is something to consider for the longer-run.

Improve coordination between different donors as well as between donors and policymakers. Donors have been supporting ID systems for many years, generally in the context of specific programs. This has sometimes led to or exacerbated a situation where there are costly multiple incompatible ID systems that reduce incentives to register for a central system. Donors should engage with stakeholders to develop and support a strategic plan for increasing the robustness, coverage and coherence of the systems of the countries with which they work and try to avoid supporting a multitude of ID programs.   If it is necessary to use a separate system for social transfers (perhaps because the national ID is issued under very restrictive conditions) having a single "social ID" rather than multiple systems will help to rationalize different programs.

Even if full integration is not possible, strive for interoperability. Even if, for various reasons, it is not possible to have an integrated system immediately, the use of common standards for data capture and analysis makes it easier to integrate in the future. For example, biometric voter registration kits in Tanzania are compatible with the registration kits for its (slow!) national ID program.

Monitor the results of programs and e-Government services enabled by the system. Many countries are moving on, from creating new systems towards expanding potential uses both off- and online. India's Aadhaar, for example, is developing a range of advanced services, such as a digital signature, which will become more important with the transition to e-services and e-government. To help keep the ID program accountable, country authorities and donors should monitor the implementation and performance of programs using the system. Digital ID enables an unprecedented level of information, for example on whether transfers have been received by those eligible, whether they have been received on time, how people have chosen to receive them, or whether there is leakage. These are useful metrics for evaluating the effectiveness of ID programs and associated service delivery. Grievance mechanisms should also be monitored for timeliness on a case basis. More detailed monitoring, as for India's LPG program, can also provide estimates of budgetary impact and customer satisfaction.

ID Systems also Share Common Risks, which Need to be Assessed and Addressed Early On.

While strong and inclusive ID programs offer many potential benefits, experience to date highlights a number of risks. We can group them into three categories.

4. Exclusion

Strong identification can be a tool for inclusion and the realization of rights but it can equally formalize and perpetuate exclusion.

Scrutiny of national status risks leaving millions stateless. People may be excluded through greater scrutiny of their national status. Some 10 million stateless persons and their descendants are at risk of being left without a nationality in the long term but this is the tip of the iceberg. Complex and restrictive nationality laws in many countries provide no path to citizenship for children with foreign-born parents or grandparents and may limit the ability of mothers to pass on their citizenship to their offspring. The number of people whose claims to nationality are indeterminate is not known but is likely to be far higher than the number of people formally recognized as stateless. Formalizing identity has already led to exclusion in some countries (Dominican Republic), and the African Union has recognized the problem. The possibility of exclusion needs to be factored into decisions on how (and whether) to assist countries to strengthen their ID systems and whether the national ID is indeed appropriate as the key to accessing social protection or other services.

Other factors such as gender, time, complexity of administrative process and costs, can also pose obstacles for the poor as noted above. Programs need plans to address these issues, since having no official identity further perpetuates marginalization and poverty, creating a vicious cycle.

5. Misuse of personal data

The rapid accumulation of electronic data raises issues that go well beyond ID systems but the misuse of ID data to facilitate surveillance, discrimination, or to access personal information for commercial use is a serious problem. Only about half of the world's countries have laws that conform to the basic requirements to protect an individual's privacy as set out in the OECD Fair Information Principles. Few poor countries do, and even where such laws exist the capacity to enforce them is often chronically weak. Many governments have not absorbed the nature of this critical challenge and it poses at least a reputational risk for development partners. The threat is external as well as internal: some countries have seen massive breaches of personal data through malicious external attacks (USA, South Korea). At the same time, strong ID is essential to limit identity theft – another misuse of personal data.

Make Privacy Impact Assessments (PIAs) a part of the planning of any major ID program. PIAs may not pinpoint every risk but will help to focus on the implications of the legal, institutional, design and technical elements of the system for data privacy and security. Development partners involved in the system should provide funding for assessments up front as well as capacity support, if needed, during the initial years of operation of the system. A Privacy Advocate or Ombudsman should be appointed, with authority and resources to respond to breaches and to violations of agreed business rules on sharing data, and have the power to seek redress and penalties, including (and especially) against public officials.

Minimize data to focus on identification. Data that can be used to profile individuals or discriminate against them, such as ethnicity or religion, should not be included in the database. Neither should information relating to income level or eligibility for various programs. Such data is properly held in the appropriate program register.

Provide users with information and control over their identity data. Countries like Estonia and Chile have strict rules for data exchange between different authorities and service providers, supported by heavy penalties for infringement. Individuals can check to see which services and agencies have accessed their records, except for law enforcement and security. The use of match-on-card authentication can also help mitigate the risk of identity theft by giving users physical control over their credentials and perhaps reduces incentives to hack into the central data base.

An independent ID authority could help to insulate ID programs from political interference. Several countries, such as Peru (RENIEC) and Pakistan (NADRA) have tasked an autonomous agency with providing registration and identification services. Separation of the ID system from a government ministry and treating it as a technical service facility can perhaps discourage the misuse of the system and its data for politically motivated purposes. Whether such an institutional arrangement is possible depends on country-specific factors but is something that might be encouraged.

6. Ineffective or wasteful deployment

Several factors may inflate the costs and limit the benefits of ID systems.

Excessive fragmentation due to institutional competition exacerbated by lack of coordination among donors. When no entity has a clear mandate for ID provision, a number of programs tend to emerge as bureaucracies seek to widen their influence and secure future resources. Wasteful, repeated, voter registration is a clear example.

Non-competitive or corrupt procurement of ID technology or loading up with unnecessary features. Governments may be pressured by vendors to include features that are not essential. For example, the rapid growth of private mobile banking in some countries suggests that the value of enabling the ID card serve also as a mobile wallet may be low. Development partners might constitute an expert advisory group of individuals with no direct financial interest in the industry to serve as a resource for governments that need to manage the procurement process but lack the capacity to do so. Recognizing the complexity, they can also develop standards and indicative costing guidelines, drawing on good practice. They can help ensure that countries are not locked in to vendor-specific systems.

Limited integration due to the political economy of ID. Not all countries have a political economy that will accept the discipline that a strong ID system can enforce on elites. ID systems might be applauded for enabling poor female-headed-households to access grants and to help eliminate fraud in such programs, but they may be resisted when it comes to strengthening tax administration by linking the earnings and assets of elites (Pakistan). Development partners must take into account the fact that the balance of use of any system – for good or for ill, between security-related and development applications, between inclusion and exclusion, or for applications that relate to the rich as well as the poor -- will depend on the political economy of the country.

[1] Uniqueness is defined in a statistical sense to mean a very low incidence of multiple identities.