PRINCIPLES ON IDENTIFICATION

FOR SUSTAINABLE DEVELOPMENT: TOWARD THE DIGITAL AGE

ENDORSING ORGANIZATIONS

Asian Development Bank (ADB)

Bill & Melinda Gates Foundation (BMGF)

Center for Global Development (CGD)

Digital Impact Alliance (DIAL)

ID4Africa

International Organization for Migration (IOM)

Mastercard

Omidyar Network

Organization of American States

OSCE Office for Democratic Institutions and Human Rights (ODIHR)

Plan International

Secure Identity Alliance (SIA)

The GSMA

UNHCR, The UN Refugee Agency

United Nations Children's Fund (UNICEF)

United Nations Development Programme (UNDP)

United Nations Economic Commission for Africa (ECA)

World Bank Group

Facilitated by: World Bank Group and Center for Global Development

PRINCIPLES ON IDENTIFICATION FOR SUSTAINABLE DEVELOPMENT:

TOWARD THE DIGITAL AGE

PRINCIPLES

INCLUSION:
UNIVERSAL COVERAGE AND ACCESSIBILITY

1. Ensuring universal coverage for individuals from birth to death, free from discrimination.
2. Removing barriers to access and usage and disparities in the availability of information and technology.

DESIGN:
ROBUST, SECURE, RESPONSIVE, AND SUSTAINABLE

3. Establishing a robust—unique, secure, and accurate—identity.
4. Creating a platform that is interoperable and responsive to the needs of various users.
5. Using open standards and ensuring vendor and technology neutrality.
6. Protecting user privacy and control through system design.
7. Planning for financial and operational sustainability without compromising accessibility.

GOVERNANCE:
BUILDING TRUST BY PROTECTING PRIVACY AND USER RIGHTS

8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.
9. Establishing clear institutional mandates and accountability.
10. Enforcing legal and trust frameworks though independent oversight and adjudication of grievances.

PURPOSE

We believe that every person has the right to participate fully in their society and economy. Without proof of identity, people may be denied access to rights and services—they may be unable to open a bank account, attend school, collect benefits such as social security, seek legal protection, or otherwise engage in modern society. No one should face the indignity of exclusion, nor be denied the opportunity to realize their full potential, exercise their rights, or to share in progress. No one should be left behind.

The organizations endorsing these shared Principles recognize the potential of strengthened identification systems to support development and the achievement of the Sustainable Development Goals.[1] We believe that creating inclusive, secure, and trustworthy identification systems can empower individuals and enhance their access to rights, services, and the formal economy. It can also strengthen the capacity of governments, the private sector, NGOs, and development partners to administer programs and deliver services transparently, efficiently, and effectively. The development benefits of improving identification systems may increase substantially with the adoption of digital technology, and many countries are already moving in this direction. However, at the same time that building identification systems—particularly digital ones—creates opportunities to further development goals, it may also create a number of challenges and risks.

---

1 Identity is a set of attributes that uniquely describes an individual or entity. The provision of identification—"proof of identity"—is embodied in SDG Target 16.9, which requires the provision of "legal identity for all, including birth registration." In addition, identification is a key enabler of numerous other Targets, including 1.3 (implementing social protection systems), 1.4 (ensuring that the poor and vulnerable have control over land, property, and financial assets), 5a (giving poor women equal access to economic resources, including finance), 5b (enhancing the use of technology, including ICT to promote women's empowerment), 10.7 (safe and responsible migration and mobility), 10c (reducing the cost of remittance transfer), 12c (phasing out harmful fuel subsidies), 16a (strengthening the capacity to fight terrorism and crime), 16.5 (reducing corruption), and many others.

This Declaration therefore identifies a set of common Principles fundamental to maximizing the benefits of identification systems for sustainable development while mitigating many of the risks. These Principles are intended to apply to the broad concept of "legal identification" systems: those that register and identify individuals to provide government-recognized credentials (e.g., identifying numbers, cards, digital certificates, etc.) that can be used as proof of identity.[2] Under this inclusive definition, legal identification need not be linked with nationality or citizenship.[3]

Many countries have made significant strides in providing legal identification; however, much work remains to be done. The goal of these Principles is thus to foster cooperation around the implementation of identification systems according to a shared set of values and standards. These Principles build upon existing international norms, and we recognize that they will need to evolve over time to incorporate a broader range of stakeholder perspectives, as well as new technologies and lessons from implementation.

We hope that the Principles will be endorsed by a progressively wider range of stakeholders—including governments, intergovernmental organizations, private firms, local and international NGOs, and development partners. By using these Principles to shape a common approach to identification, stakeholders will be better able to align and guide their support, facilitate discussion at a country, regional and/or global level, and work together to foster robust and inclusive identification systems that further sustainable development outcomes.

2 Currently, most legal identification is provided by or on behalf of governments. In the future, other models may be possible, but governments should retain the ultimate accountability for legal identification.

3 Some legal identification systems, such as the national ID programs of Peru, Pakistan and many other countries, are linked to national status, while others are not. India's Aadhaar system, for example, has de-linked the concept of nationality from identification in order to establish the uniqueness of the country's 1.2 billion residents and create a platform for secure authentication by third parties for service delivery. See Gelb & Clark (2013). As set out in the Principles, basic legal identification should in any event be provided to all persons resident on the territory.

BACKGROUND

Some 1.5 billion people in the developing world lack proof of legal identity.[4] This "identification gap" is a serious obstacle to participation in political, economic and social life. Without a secure and trustworthy way to prove their identity, a person may be unable to exercise the range of human rights set out in international laws and conventions. A lack of identification also makes it difficult to open a bank account, vote, obtain formal employment, access education or healthcare, receive a social transfer, buy a SIM card, or seek legal redress. Furthermore, states with weak identification systems have difficulty with government administration, planning, and service delivery, including collecting taxes, targeting social programs, responding to emergencies, disasters and epidemics, managing their borders, and providing security.[5]

Achieving inclusive development, therefore, requires a sustained effort to address the world's identification gap. Target 16.9 of the Sustainable Development Goals (SDGs) aims to achieve "legal identity for all, including birth registration" by 2030. To this end, governments in many countries—along with international organizations, donors and private-sector partners—have begun serious efforts to strengthen legal identification systems, including civil registries, national IDs, and population databases, as well as voter registries, social transfer databases, travel documents and others.

In many cases, these reforms include transitioning from paper-based identification systems to digital ones; a shift that offers new opportunities and challenges. Digital technologies, such as cloud computing, biometrics, mobile networks and devices, and smartcards, can increase the security, accuracy, and convenience of identifying and authenticating individuals. As public and private service providers increasingly transition into the digital realm, the ability to prove who you are will be essential for participation in the digital environment.

---

4 Estimates by the World Bank ID4D Dataset, as of February 2016. This dataset will be updated annually.

5 Gelb, A. & Clark, J. 2013. "Identification for Development: The Biometrics Revolution," *Center for Global Development Working Paper 315*; World Bank. 2016. *Identification for Development Strategic Framework.*

As a result, digital identification systems can create huge savings for citizens, governments, and businesses by reducing transaction costs, increasing efficiency, and driving innovation in service delivery, particularly to the poorest and most disadvantaged groups in society. Many developing countries have already used such systems to improve governance, boost financial inclusion, reduce gender inequalities by empowering women and girls, and increase access to health services and social safety nets for the poor. They also offer huge potential to address the identity gaps experienced by tens of millions of migrants and refugees. New technological advances—coupled with the application of these Principles—can offer the countries the opportunity to leapfrog traditional approaches by establishing digital identity ecosystems. Nevertheless, these Principles apply to both digital and paper-based systems.

With these opportunities, however, come important challenges and risks. Efforts to improve legal identification systems—whether digital or paper-based—may face political challenges, including the ability to sustain a long-term commitment to identification projects across numerous stakeholders and to overcome resistance from parties that benefit from weak identification systems. Ensuring that all individuals are included in the system can be a huge challenge, particularly for remote and rural residents, the forcibly displaced, stateless persons, and other marginalized groups. Furthermore, in the absence of strong data protection laws, regulatory frameworks, and practices, identification systems may reduce trust and undermine individual rights to privacy and consent regarding the use of their personal information. In some cases, they may put vulnerable groups at serious risk of harm. These risks are heightened in an era of digital identification and big data. In some contexts, the proliferation of new technologies has created concerns regarding sustainability, particularly when there is vendor lock-in or when technology choices are not well suited to the use-case or country capacity.

Addressing these challenges is critical for ensuring that legal identification systems are effective and available to all **end-users**—the individuals who must prove their identity to access rights and services. This requires a coordinated, sustained effort by key stakeholders involved in the provision and use of these systems, including:

- **Individuals.** Individuals are end-users of identification systems, as they require proof of identity to access rights and services. They are at the center of identification systems and have the right to know and exercise appropriate control over how their data is collected, used, stored, and shared.
- **Governments.** Government agencies are typically the primary providers of legal identification systems. This includes, but is not limited to, civil registers, including birth, death, and marriage registration, population registers, national IDs, passports, voter registers and cards, etc. Government agencies are also users of identification systems for program administration, such as social protection programs, tax collection, and providing driving licenses.
- **Private sector.** Private companies are the main developers, innovators, and suppliers of identification system infrastructure. In addition, many private companies rely on legal identification systems to identify their customers (e.g. to open bank accounts, register SIM cards, or create credit reporting systems). Governments have also partnered with private companies to deliver forms of identification—such as mobile identity and digital certificates—that expand the reach and utility of legal identification systems to underserved populations.
- **International organizations and NGOs.** By providing protection, legal assistance, and other services, international organizations, civil society and community organizations are important partners for generating demand for identification and assisting people in accessing the identification they need to fully engage in economic, political, and social life.
- **Development partners.** Development agencies, other donors, and humanitarian actors provide support for legal identification systems in the form of funding and technical assistance, and may also be involved in establishing identification systems to administer programs.

A shared vision across the range of stakeholders, aligned through this set of common Principles, will help foster robust and inclusive identification systems that enable economic opportunities and sustainable development outcomes.

PRINCIPLES

INCLUSION: UNIVERSAL COVERAGE AND ACCESSIBILITY

Identification systems should strive for continuous universal coverage from birth to death, free from discrimination and accessible to all individuals.

1. Ensuring universal coverage for individuals from birth to death, free from discrimination.

- *Universality.* Countries should fulfill their obligations to provide legal identification to all residents—not just citizens—from birth to death, as set out in international law and conventions and their own legislative frameworks.[6] This includes the commitment to universal birth registration for those born on national territory, which is an essential part of identity management.[7]

- *Non-discrimination.* Legal, procedural, and social barriers to enroll in and use identification systems should be identified and mitigated, with special attention to poor people and groups who may be at risk of exclusion for cultural, political or other reasons (such as women, children, rural populations, ethnic minorities, linguistic and religious groups, migrants, the forcibly displaced, and stateless persons). Furthermore, identification systems and identity data should not be used as a tool for discrimination or infringe on individual or collective rights.

---

6 States have the sovereign right to determine eligibility for citizenship in accordance with international law. While proof of citizenship will be limited to citizens, States should provide legal identification to *all* persons resident on their territory, including birth registration. They should also provide proof of citizenship to all persons entitled to it without discrimination of any kind.

7 For example, Article 7 of the *Convention on the Rights of the Child* (CRC) states: "The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents." The CRC has been ratified by every member state of the UN except for the United States, which has signed but not ratified the treaty. In practice, however, virtually all births in the US are registered.

2. Removing barriers to access and usage and disparities in the availability of information and technology.

- *Direct and indirect costs.* Cost should not be a barrier to access identification services. Civil registration and first birth and death certificates should be free of charge to the individual, as should the initial issue of a legal identity credential that is mandatory. If fees are charged for certain additional services (such as reissuance of lost credentials), rates should be reasonable, proportional to costs incurred, and transparent to the public. The indirect costs of obtaining identification—including fees for supporting documents, travel costs, and cumbersome administrative procedures—should also be minimized.

- *Information and technology disparities.* Stakeholders must work to ensure user literacy regarding legal identification systems in order to foster a culture of understanding and trust, and to reduce information asymmetries that might prevent individuals from accessing identification-related services or benefits. With the rise of digital systems, no one should be denied identification services or associated services because they lack ICT connectivity or technical knowledge. Stakeholders should work together to ensure both online and offline infrastructure can be extended to provide "last-mile" access and connectivity, particularly for those in rural areas.[8]

8 One implication is that off-line, as well as on-line, identification needs to be possible.

DESIGN: ROBUST, SECURE, RESPONSIVE, AND SUSTAINABLE

Identification systems should be robust, context-appropriate, and interoperable. While they should respond to user demand and long-term needs, they should collect and use only the information necessary for the system's explicit purpose. Open standards and vendor neutrality help to ensure financial and operational efficiency and sustainability.

3. Establishing a robust—unique, secure, and accurate—identity.

- *Robustness.* Accurate, up-to-date information is essential for the trustworthiness of any identification database and credentials used for authentication. Identification systems should provide a statistically unique[9] and verifiable identity for the course of an individual's life, from birth to death, with safeguards against tampering (alteration or other unauthorized changes to data or credentials), identity theft and other errors occurring throughout the identity lifecycle.

4. Creating a platform that is interoperable and responsive to the needs of various users.

- *Responsiveness.* Identification providers should work to ensure that identification and authentication services are flexible, scalable, and meet the needs and concerns of end-users (individuals). They should also meet the needs of public agencies and private companies that use—or could use—this identity as a foundation for other services or operations.

- *Interoperability.* Interoperability increases efficiency and allows multiple stakeholders to leverage the benefits of the identification system, both within a country and across borders. Domestically, this includes the ability of different databases or registries (e.g., national ID and civil registration systems) to communicate with each other and/or exchange information in a timely and low-cost manner, subject to appropriate privacy and security safeguards.[10]

---

9 Statistically unique means that the probability that any individual can have multiple identities within the same system (i.e., duplicate identities) is very low—no system is completely fool-proof. This should be distinguished from the possibility that a person may have multiple mechanisms to authenticate their identity, as in a federated system.

10 Cross-border interoperability can facilitate migration and trade, but controls should be put in place to protect the security of vulnerable groups, such as refugees, whose personal data must often be shielded from their home country.

5. Using open standards and ensuring vendor and technology neutrality.

- *Open standards.* Open design principles enable market-based competition and innovation.[11] They are essential for greater efficiency and improved functionality of identification systems, both within country and also across borders.

- *Vendor and technology neutrality.* Robust ICT procurement guidelines must be in place to facilitate competition and innovation and prevent possible technology and vendor "lock-in," which can increase costs and reduce flexibility to accommodate changes over time. Technology neutrality and diversity should be fostered to increase flexibility and avoid system design that is not fit for purpose or suitable to meet policy and development objectives.

---

11 For example, ISO/IEC has developed standards covering many aspects of identification systems. For more, see World Bank. 2016. "Technical Standards for Digital Identity Systems: Formulating a Strategic Approach."

12 The Fair Information Practices (FIPs) are a set of internationally-recognized principles for protecting personal information, including collection limitation, purpose specification, data quality, security, accountability, and openness.

13 Such risk impact assessments should be carried out by the responsible entity that creates, collects, shares or uses data for authentication and identification purposes linked to the specific use case. Examples of existing standards for levels of assurance for identity proofing include ISO/IEC 29115 and those issued by eIDAS, UK Cabinet Office, NIST, and others.

14 "Sensitive personal information" can vary by context but commonly includes information that could be used to create fraudulent identities and to profile or target individuals. The release of identifying information may involve particularly serious risks to certain people, for example, asylum-seekers and refugees.

6. Protecting user privacy and control through system design.

- *Privacy by design.* Identification systems should be designed with the privacy of the end-user in mind. No action should be required on the part of the individual to protect his or her personal data. Information should be protected from improper use by default, through both technical standards and preventative business practices.

- *Proportionality and minimal disclosure.* Data collected and used for identification and authentication should be fit for purpose and proportional to the use case, and managed in accordance with global norms for data protection, such as the Fair Information Practices (FIPs).[12] Authentication protocols should only disclose the minimal data necessary to ensure appropriate levels of assurance. These levels should reflect an assessment of the level of risk in the transactions and can be based on recognized international standards.[13] Identification systems—including credentials and numbering systems—should not disclose sensitive personal information.[14]

7. Planning for financial and operational sustainability without compromising accessibility.

- *Sustainability.* Identification systems should be designed for long-term fiscal and operational stability, without compromising accessibility for end-users. This may involve different financial models including reasonable and appropriate service fees for identity verification, offering enhanced or expedited services to users, public-private partnerships (PPPs), recuperating costs through efficiency gains and reduced leakages, and other funding sources. Commercial models for identification systems should be designed to incentivize high standards of trustworthiness for all parties in the value chain.

GOVERNANCE: BUILDING TRUST BY PROTECTING PRIVACY AND USER RIGHTS

Identification systems must be built on a legal and operational foundation of trust and accountability between government agencies, international organizations, private sector actors and individuals. People must be assured of the privacy and protection of their data, the ability to exercise control and oversight over its use, and processes for independent oversight and the redress of grievances.

8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.

- *Legal and regulatory frameworks.* Identification systems must be underpinned by legal and regulatory frameworks and strong policies that promote trust in the system, ensure data privacy and security, mitigate abuse such as unauthorized surveillance in violation of due process, and ensure provider accountability. Legal frameworks should be clear in delineating liability and recourse for end-users, and should be overseen by independent regulatory bodies with appropriate powers. They should also protect end-users against inappropriate access and use of their data by third parties' for undue commercial surveillance or unlawful profiling. Frameworks require the right balance between regulatory and self-regulatory models that does not stifle competition, innovation, or investment.

- *User rights.* Identification services should provide end-users (individuals) with genuine choice and control over the use of their data, including the ability to selectively disclose only those attributes that are required for a particular transaction. Users should be given simple means to have inaccurate data corrected free of charge and to obtain a copy of personal information held about them. Personal information should not be used for secondary, unconnected purposes without the user's informed consent, unless otherwise required under the law. Stakeholders should be transparent about identity management, develop appropriate resources to raise users' awareness of how their data will be used, and provide them with tools to manage their privacy. Identification providers should ensure that the initial process to correct errors is administrative rather than judicial in order to increase speed of resolution and reduce costs. Data sharing arrangements should also be transparent, fully documented, and only agreed to in the best or vital interests of the individual(s) concerned.

9. Establishing clear institutional mandates and accountability.

- *Institutional mandates.* Ecosystem-wide trust frameworks must establish and regulate comprehensive governance arrangements for identification systems. This should include specifying the terms and conditions governing the institutional relations among participating parties, so that the rights and responsibilities of each are clear to all.

- *Accountability.* There should be clear accountability and transparency around the roles and responsibilities of identification system providers.

10. Enforcing legal and trust frameworks though independent oversight and adjudication of grievances.

- *Oversight.* The use of identification systems should be independently monitored (for efficiency, transparency, exclusion, misuse, etc.) to ensure that all stakeholders 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.

- *Adjudication.* Disputes regarding identification and the use of personal data that are not satisfactorily resolved by the providers (for example, refusal to register a person or to correct data, or an unfavorable determination of a person's legal status) should be subject to rapid and low-cost review by independent administrative and judicial authorities with authority to provide suitable redress.

Photo Credits | Cover Top: UN Women/Fatma Elzahraa Yassin; Page 7: UNICEF/BANA2012-02020/Jannatul Mawa; Page 15: UN Media/Jashim Salam; Page 11: Sébastien Rieussec/Safran

ENDORSING ORGANIZATIONS

Empowered lives.
Resilient nations.

We welcome additional organizations to join us in endorsing these Principles and hope to maintain this as a living document to be updated based on lessons of experience.

February 2017