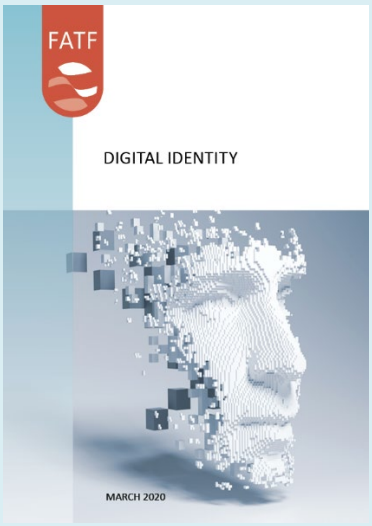
Digital Identity

APPENDIX C:

Principles on Identification for Sustainable Development



Citing reference:

FATF (2020), "Appendix C" in *Guidance on Digital Identity,* FATF, Paris, www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

APPENDIX C: PRINCIPLES ON IDENTIFICATION FOR SUSTAINABLE DEVELOPMENT

This Guidance highlights several concrete ways that countries can develop digital ID ecosystems that allow them to reap the benefits of these systems while mitigating the risks described in Section IV. To begin, countries should follow the ten *Principles on Identification for Sustainable Development*, which have now been endorsed by over 25 international organisations, development agencies, and other partners.[60] Although these *Principles* were developed to support the creation of "good" government-recognized ID systems, they apply more broadly and can be adopted by both public- and privately provided and used identity systems and services.

Table 3. Principles on Identification for Sustainable Development

	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 through independent oversight and adjudication of grievances.

Goal 1. Ensure inclusion

The first two principles are intended to ensure that no one is left behind by ID systems, in support of SDG 16.9. *Principle 1* requires countries to fulfil their obligations to provide legal identification to all residents—not just citizens—from birth to death and free from discrimination, as set out in international law and conventions and their own legislative frameworks. This includes the commitment to universal birth registration for those born on in their territory or jurisdiction, but also extend to digital ID systems, particularly when these are a pre-requisite for accessing basic public and private sector services, such as banking, SIM cards, and cash transfers.

In recognition of the fact that certain groups will face disproportionate difficulties in accessing identity services—and digital services in particular—*Principle 2* requires practitioners to identify and mitigate legal, procedural, and social barriers to enrol in and use digital ID systems, with special attention to poor people and groups who may be at

60 World Bank. 2017. *Principles on Identification for Sustainable Development: Toward the Digital Age*. Washington, DC: World Bank Group. id4d.worldbank.org/principles. A list of endorsing organisations can be found on the website.

risk of exclusion for cultural, political or other reasons (such as women and gender minorities, children, rural populations, ethnic minorities, linguistic and religious groups, persons with disabilities, migrants, the forcibly displaced, and stateless persons). Furthermore, digital ID systems and identity data should not be used as a tool for discrimination or infringe on individual or collective rights.

Goal 2. Design robust, secure, responsive, and sustainable ID systems

In addition to providing universal coverage, digital ID systems should be robust to fraud and error, useful for a variety of stakeholders, and sustainable, while also protecting user privacy and adopting open standards to facilitate innovation and avoid vendor and technology lock-in.

Specifically, *Principle 3* states that accurate, up-to-date identity information is essential for ensuring the trustworthiness of identities and attributes used in transactions. In addition, identities must be unique to the context, avoiding duplicate identities or using identifiers that could be attributed to multiple people. Furthermore, digital ID systems must have safeguards against tampering (alteration or other unauthorized changes to data or credentials), identity theft, data misuse, and other errors occurring throughout the identity lifecycle.

Principle 4 highlights the need for identification and authentication services to be flexible, scalable, and meet the needs and concerns of people (users) and relying parties (e.g., public agencies and private companies). To ensure that identity-related systems and services meet specific user needs, practitioners should engage the public and important stakeholders throughout planning and implementation. The value of digital ID systems to relying parties is highly depended on their portability and interoperability with multiple entities—subject to appropriate privacy and security safeguards—both within a country and across borders.

For government-recognized digital ID in particular, *Principle 5* further emphasizes the need for vendor neutrality to increase flexibility and avoid system design that is not fit for purpose or suitable to meet policy and development objectives. This requires robust procurement guidelines 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. In addition, open design principles enable market-based competition and innovation. They are essential for greater efficiency and improved functionality of digital ID systems, and for enduring interoperability. Similarly, open APIs also support efficient data exchange and portability by ensuring that a component of the digital ID system—e.g., a particular type of credential—can be replaced with minimal disruption.

In addition to architecture that is responsive and flexible, *Principle 6* emphasizes that digital ID systems must protect people's privacy and control over their data through system design. This is crucial for mitigating many of the risks to privacy and data protection identified in Section IV of this Guidance. Designing with people's privacy in mind means that no action should be required on the part of the individual to protect his or her personal data. Information should be protected from improper and unauthorized use by default, through both technical standards and preventative business practices.

These measures should be complemented by a strong legal framework (as emphasised below in *Principle 8*).

For example, data collected and used for identification and authentication should be fit for purpose, proportional to the use case and managed in accordance with global norms for data protection, such as the OECD's Fair Information Practices (FIPs) and with reference to emerging international best practices, such as the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act. Authentication protocols should only provide "yes or no" confirmation of a claimed identity or—if mandated by an AML or CCC-related law—only disclose the minimal data necessary for the transaction. The method of authentication should reflect an assessment of the level of risk in the transactions and can be based on recognized international standards and frameworks for levels of assurance. Furthermore, credentials and identifier numbering systems should not unnecessarily disclose sensitive personal information (e.g., reference numbers should be random).

Principle 7 recognizes the importance of designing public-sector systems that are financially and operationally sustainable while still maintaining accessibility for people and relying parties. This may involve different business models including reasonable and appropriate service fees for identity verification services, offering enhanced or expedited services to users, carefully designed and managed public-private partnerships (PPPs), recuperating costs through efficiency and productivity gains and reduced leakages, and other funding sources that do not compromise the goal of providing proof of identity that is accessible for all and meets the needs of people and relying parties.

Goal 3. Build trust by protecting privacy and user rights

The final group of principles addresses how digital ID systems should be governed to protect user privacy and rights, system security, and clear accountability and oversight.

Principle 8 sets out the requirements for a comprehensive legal framework. Digital ID systems must be underpinned by policies, laws and regulations 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. This typically includes an enabling law and regulations for the digital ID system itself as well as laws and regulations on data protection, digital or e-government, electronic transactions and commerce, AML, civil registration, limited-purpose ID systems, and freedom of information, among others.

The enabling law and regulations for a digital ID system should clearly describe the purpose of the system, its components, the roles and responsibilities of different stakeholders, how and what data is to be collected, liability and recourse for digital ID holders (subjects) and relying parties, the circumstances in which data can be shared, correction of inaccurate data attributes, and how inclusion and non-discrimination will be maintained. Laws and regulations on data protection and privacy should also include oversight from an independent oversight body (e.g. a national privacy commission) with appropriate powers to protect subjects against inappropriate access and use of their data by third parties for commercial surveillance or profiling without informed consent or

legitimate purpose. Frameworks require the right balance between regulatory and self-regulatory models that does not stifle competition, innovation, or investment.

In addition, *Principle 9* highlights the need for clear institutional mandates and accountability in the governance of digital ID systems. Ecosystem-wide trust frameworks must establish and regulate governance arrangements for ID 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. There should be clear accountability and transparency around the roles and responsibilities of identification system providers.

Finally, *Principle 10* emphasizes that the ID system should include clear arrangements for the oversight of these legal and regulatory requirements. The use of ID systems should be independently monitored (for efficiency, transparency, exclusion, misuse, etc.) to ensure that all stakeholders appropriately use identification systems to fulfil their intended purposes, monitor and respond to potential data breaches, and receive individual complaints or concerns regarding the processing of personal data. Furthermore, 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 unfavourable 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.