The role of electronic transactions and national digital ID systems in the digital economy

In the digitalization of economies, an effective digital ID program democratises access to electronic transactions and services that are offered digitally, such as education, healthcare and financial services. The absence of a universal digital ID system accentuates exclusion in a digital economy.

The brief, written in close collaboration with Macmillan Keck, seeks to identify specific attributes of electronic transactions and national digital ID frameworks that can help policymakers and regulators build a digital economy that includes — and serves — everyone.

BRIEF

February 2022

Macmillan Keck

Seharish Gillani,
Ahmed Dermish, and
Jeremiah Grossman
of the UNCDF
Policy Accelerator

Summary

To support the digital economy, electronic transactions frameworks translate conventional legal concepts that are essential for conducting commerce into digital equivalents. This includes recognizing the legal effect of electronic signatures in commercial transactions in place of traditional paper-based equivalents. Digital signatures are a subset of electronic signature that utilize the cryptography of public key infrastructure and digital certificates to provide additional security and reliability.

Digital ID systems electronically store and capture an individual's digital identity, allowing them to be used to support digital services or electronic transactions. National digital ID systems are foundational systems implemented by, or under the auspices of, government that are available to the general population. International organizations have developed best practices and safeguards for designing and implementing national digital ID systems, including ensuring that a system is inclusive and supported by proper data protection, cybersecurity, and data security frameworks.

Individuals typically register with these systems by supplying biographical and, increasingly, biometric data. The systems then validate the data and deduplicate the individual's identity to ensure that the same individual is not already registered and that the individual is unique in the system. Credentials are then issued which allow the individuals to authenticate their identity to relying parties. Many national digital ID systems utilize a centralized model, where the government or an entity designated by it acts as the sole provider of the system. Others have adopted federated models, and a new movement advocates decentralised self-sovereign identities that allow for even more individual control.

Considerations while reading this brief

1. Which challenges related to digital ID systems and electronic transactions in the digital economy are most prominent in your market, both a) in general and b) for underserved groups such as women and low-income people?

2. Do digital ID systems and electronic transaction regulations in your country address:
   - **Digitization:** The application of digital ID system and electronic transaction regulation to the digital economy?
   - **Inclusivity:** The specific digital ID system and electronic transaction challenges faced by women, low-income people, and/or other underserved groups?

3. Which entities are responsible for the regulation of digital ID systems and electronic transactions? Are responsibilities clear, and are mechanisms in place to avoid regulatory arbitrage? If not, how could this be improved?

Electronic transactions

Electronic transactions underlie the digital economy

The digital economy encompasses and depends upon economic activities implemented through digital technologies and services.[1] Many of these activities rely on ***electronic transactions:*** the use of electronic documents, messages, and records to conclude transactions that were traditionally ink-and-paper based. The legal frameworks that support electronic transactions translate conventional legal concepts that are essential for conducting commerce, such as what constitutes an "original" paper-based document or the timing of receipt of a paper-based contract offer, into electronic equivalents.[2] This provides norms, certainty, and recourse for the parties conducting business through electronic transactions.

Electronic signatures

Many commercial and other legal actions require the ***signature*** of one or more parties to be considered legally effective. In the broadest sense, a signature is the name or mark of an individual that establishes a connection between the individual and a signed item. It allows others to identify the individual, verify the authenticity of the signed item, and confirm the connection between the two.[3] A ***wet signature*** refers to the traditional means of applying ink to a paper document to generate a signature.

In the context of electronic transactions, wet signatures are often impractical, as they increase transaction costs and impede the speed that often inspires their appeal. An ***electronic signature*** – which broadly refers to the use of data in an electronic form that can be associated with a document or record and serve as evidence of the intent of the individual to sign – provides an alternative to a wet signature. There are a wide range of electronic signatures, of which the simplest involve placing one's name at the bottom of an email or taking a digital scan of a wet signature.[4] Legal frameworks commonly support the use of electronic signatures by ensuring that a signature is not denied legal effect, validity, or enforceability solely due to its electronic form.[5] However, these frameworks often exclude certain transactions, including those that are highly personal or subject to existing statutory requirements. For example, the United States ESIGN Act specifically excludes documents governed by statute that relate to wills, codicils, testamentary trusts, and matters of family law, such as adoption or divorce.[6]

Digital signatures

Not all electronic signatures are created equal, and the type of electronic signature may affect its evidentiary significance in establishing the connection between the individual and a signed item. A ***digital signature*** is a subset of electronic signatures with added security features. Digital signatures typically use ***public key infrastructure (PKI)***, a type of encryption involving a pair of encryption "keys," one public and one private. When an individual attaches a digital signature to a document, he or she uses a unique private key, known only to the individual, to encrypt it. That private key is associated with a unique public key, which the individual can share with others, and is used by the recipient to decrypt the digital signature. Because the two keys are associated with one another and not any other keys, when one successfully decrypts the digital signature, it verifies that the signature and the document to which it is attached has not been modified since the digital signature was created.

In addition, when a digital signature is created, a ***digital certificate*** is attached to the digital signature that verifies the identity of the signer to the recipient.[7] Digital certificates are issued by ***certificate authorities***, trusted entities that are often expressly recognized or credentialed under domestic legal frameworks.[8] The signer must register with the certificate authority, linking his or her identity to the public key. By successfully decrypting a digital signature and receiving an accompanying digital certificate from a trusted certificate authority, the receiver has assurance that the signature and document have not been altered and that the signer is the individual he or she claims to be.

Many legal frameworks recognize the difference between the trustworthiness of basic electronic signatures and digital signatures, with some even further stratifying the subtypes of digital signatures. For example, the EU's eIDAS regulation recognizes basic electronic signatures, "advanced electronic signatures" (which are similar to digital signatures), and "qualified electronic signatures," which provide the highest level of assurance and are digital signatures with a certificate issued by an entity specifically certified for that purpose created using a particular type of device. Only with respect to qualified electronic signatures are all Member States required to ensure legal equivalence between wet and electronic signatures in.[9]

National digital ID systems

Secure and reliable identification supports the digital economy

Enabling parties to verify each other's identity is critical to ensuring the security and reliability of the electronic transactions that drive the digital economy. For example, lenders need to be confident their loans are disbursed to the person associated with the credit record that they have reviewed. Similarly, consumers require confidence that the online vendor with whom they transact is the person she or he purports to be. Even the digital certificates that support digital signatures ultimately require the signer to successfully register and identify herself or himself to the certificate authority.

As of 2018, an estimated 1 billion individuals lacked basic identity documents, mostly in Sub-Saharan Africa and South Asia.[10] Due to gendered social norms and disparate application requirements (such as additional documentation or signatures requirements for married women), women face greater obstacles to obtaining official identity documents.[11] As a result, 45% of women over the age of 15 in low-income countries lack identification, compared to 30% of men.[12] Of the approximately 1.7 billion people who lacked a bank account in 2017, nearly 20% attributed this to the lack of identification documents.[13] One out of every two women in low-income economies does not have a national ID or similar identity credential, according to the ID4D-Findex survey.[14] Furthermore, refugees, stateless persons, people with disabilities, and people living in rural and remote areas often face the greatest hurdles to obtaining official IDs.[15] In response, the United Nations' Sustainable Development Goal 16, Target 16.9 aims to "provide legal identity for all, including birth registration" by 2030.

What is an ID system?

An individual's ***identity*** is a set of attributes that uniquely describe that individual within a given context.[17] In this context, ***uniqueness*** means that only one individual can claim an identity and each individual can claim only one identity.[18] For example, an individual's

name and date of birth is likely sufficient to establish the individual's unique identity within a small community. However, in a populous country where certain names are common, these attributes alone may be insufficient to establish uniqueness. When identity attributes are electronically stored and captured or when they are used in the context of digital services or electronic transactions, they may be considered a ***digital identity.***[19] A ***digital ID system*** uses digital technology for all functions of the system, from data capture and storage to uses of a digital identity by individuals.[20]

ID systems administered or supported by governments are often divided into ***foundational ID systems***, which establish a core digital identity and provide identification to the general population for a wide variety of transactions and services (e.g., national ID and civil registration systems), and ***functional ID systems***, which address the specific needs of a particular sector or use case (e.g., driver's license and voter registration systems).[21] The distinction is not always clear-cut. In the absence of a proper foundational ID system, a functional ID system can evolve to take on more of a foundational role. For example, the United States social security numbers were originally used exclusively to track income for social security eligibility, but today they are used for many purposes, such as tax collection, credit evaluation, and financial transactions.[22] The contextual barriers to access foundational IDs posing restrictive requirements to register, such as the need to present a witness, proof of permanent address, and stringent requirements for updating data (e.g., changes to last names after marriage[23]) can exclude vulnerable populations.

By enabling proof of identity, digital ID systems can empower and facilitate access to basic financial, health, and social services.[24] On the supply side, businesses, governments, and other institutions can benefit from lower costs of user or customer onboarding, reductions in losses from identity fraud, and access to a wider labour pool.[25] Governments can also potentially benefit from increased revenues from more efficient, accurate, and inclusive tax collection[26] and more transparent, accurate, and effective distribution of subsidies. For example, Nigeria's government incorporated digital ID into its payroll system for police officers and eliminated over 80,000 "ghost officers" bogus accounts that were improperly drawing salaries.[27]

National digital ID systems

National digital ID systems are foundational in nature and implemented by, or under the auspices, of government.[28] They are typically available to the local general population, including citizens and long-term residents, as well as citizens living abroad. However, some systems limit eligibility to citizens only, such as Botswana's *Omang* card.[29]

The large number of individuals lacking identification in low-income countries is often attributed to poorly-functioning civil registration systems or paper-based national ID systems.[30] Today, the technology necessary to support and implement a national digital ID system has become increasingly affordable, allowing many low-income countries to leapfrog paper-based systems altogether.[31] Not surprisingly, the implementation of national digital ID systems in both low-income and developed countries has become widespread.[32]

However, like all new technologies, national digital ID systems have potential drawbacks. The vast collection of sensitive personal data creates opportunity for abuse, such as government or corporate surveillance and discrimination against vulnerable minorities.[33] Their digital nature also leaves them vulnerable to cyberattacks and other data security risks. Like traditional identification systems, they can purposely or inadvertently exclude marginalized groups.

To minimize these risks, international organizations have developed best practices and safeguards for designing and implementing national digital ID systems. These include ensuring that a system is inclusive, meaning is it universally accessible to a population and free from discrimination or other undue barriers to registration and use.[34] In addition, because these systems involve the collection and generation of large amounts of personal data, proper data protection, cybersecurity, and data security frameworks are essential (see briefing papers on data protection and cybersecurity and data security).[35]

How do national digital ID systems work?

Registration

Registration in a national digital ID system may be explicitly mandatory, meaning there is a legal obligation to register. For example, the Philippine Identification System Act requires every citizen and resident to register with PhilSys, the country's national digital ID system.[36] Other systems are ostensibly voluntary but become implicitly mandatory because registration is necessary to access basic public services. For example, registration for Pakistan's National Identity Card is voluntary, but a card is necessary to open a bank account, obtain a passport or gas or electricity connection, pay a utility bill, or enter into a transaction with the State.[37] Directly linking a digital ID system to access to public and private services can incentivize digital ID uptake, but in the absence of proper safeguards, such a requirement could deprive underserved populations of important services, particularly in countries where the digital ID ecosystem is in an emerging stage.[38]

The process typically begins by gathering the attributes from individuals that will be used to establish a digital identity. This may include ***biographical data***, such as name, date of birth, sex, and address, as well as ***biometric data***, such as fingerprints, iris scans, facial images, and signatures. As of 2018, some 83 countries collected biometric data (fingerprint or iris) as part of a foundational ID system.[39] Critics have opposed the mandatory collection of biometrics, arguing that individuals should not be required to place their sensitive, unchangeable biometric data at risk of disclosure or misuse when alternative approaches exist.[40]

Once collected, biographical data is typically ***validated*** to ensure that the individual is the person she or he claims to be. Validation techniques often include supplying existing identification documents, such as a birth certificate or passport. In populations where an absence of such documents is common, attestations by members of the community may be required. For example, in Tanzania, a list of individuals with photos may be posted in a community to allow members of the public to assist with correcting inaccurate information. Applications may also be vetted by "village and district security committees," which include representatives of various agencies, including the immigration department, police, and

local government.[41] Once an individual's identity is validated, a system typically uses ***deduplication*** techniques to ensure that the same individual is not already registered. Biometric data recognition technologies are considered the most accurate deduplication techniques.[42]

Registration requirements can be especially difficult for women to fulfil. Presenting a witness to obtain a national ID can be challenging for women in certain socio-cultural contexts, particularly when registration points are limited and require women to also cover travel costs for a witness. Similarly, functional IDs can be more accessible to men, whereas temporary foundational IDs might be more accessible to women if they are in close proximity to a woman's home (e.g., an affidavit from a village elder). In Nigeria, 12 percent of men (aged 15+) have a driver's license compared to one percent of women. The limited integration of foundational and functional ID databases can further exacerbate the challenges for registration. For example, a woman might need permission from her husband or father to travel every time she needs to apply for an ID, receive credentials, update or renew credentials, or apply for a specific service. In addition, women may also be less literate than men and therefore less likely to have the skills to navigate the application process or to understand the value of a digital ID for themselves and their children. Lastly, women can also experience legal barriers to registration when ID-related policies lack specificity or contain gender-biased provisions. For example, in Papua New Guinea, the law establishes a father as the 'responsible person' to modify a child's identity credentials (unless he is deceased or doesn't have custody) and this can limit a mother's ability to make any necessary updates or changes on the child's behalf.[43]

Issuance of credentials

After an individual is registered in a national digital ID system, she or he is typically issued a ***credential***: a document, object, or data structure that vouches for the individual's identity.[44] Unique ID numbers and physical ID cards (often enhanced with machine-readable microchips, bar codes, or QR codes) are traditional forms of credentials, but digital app-based or SIM-based mobile credentials are becoming more common. For example, Moldova's national ID system assigns each citizen a 13-digit personal identification number at birth, issues a physical card, and offers a SIM-based credential.[45]

In some circumstances, women may lack full control over their credentials. For example, research has found that sometimes women's in-laws or employment agencies take their IDs, thereby limiting their freedom of movement.[46]

Use cases

A primary use case for an ID system is ***authentication***: the process of proving that a registered individual is the person he or she claims to be. In a digital system, authentication is achieved by presenting one or more authentication factors to assert the individual's identity, which are verified electronically. Generally, these factors comprise something inherent in the person (e.g., a biometric like a fingerprint or iris scan), something a person knows (e.g. a password or a PIN), or something a person possesses (e.g. a physical or electronic credential).[47] To strengthen authentication, many systems require use of multiple factors. Once authenticated, a ***relying party*** – the public- or private-sector service provider that uses the system to authenticate individuals – has a high degree of assurance that it is communicating or transacting with

the correct individual. Authentication can therefore be used to support electronic transactions.

Some digital ID systems include ***authorization*** functionality, which allows the ID system to communicate to relying parties whether an individual has a particular attribute. For example, a system may confirm that an individual is old enough to receive a particular government benefit. Others include ***attribution*** functionality, which allows individuals to use the system to generate binding signatures, often using digital signatures.[48]

Models and institutions

Many countries that have implemented national digital ID systems use a ***centralised model***, where the government or an entity designated by it acts as the sole provider of a national ID system.[49] This is the model utilized by India's Aadhaar system (operated by the Unique Identification Authority of India)[50] and Nigeria's national ID system (operated by the National Identity Management Commission).[51] Such entities may be part of an existing ministry/department or autonomous, independent authorities. They may assume responsibility for implementing the system, including conducting registration, issuing credentials, certifying relying parties, and receiving and addressing user complaints.

Some critics of centralized national digital ID systems argue that they preclude competition between multiple systems that could lead to greater efficiency and better outcomes for users.[52] Other countries rely on a ***federated model***, where multiple government-accredited entities can provide government-recognized digital ID.[53] For example, the UK's GOV.UK Verify system uses certified private companies that are bound to follow prescribed procedures and standards as identity providers.[54]

A range of mechanisms are used to fund national digital ID systems. Some are funded directly by governments or with assistance from donor organizations. Others make use of partnerships with private-sector providers. User fees can also support these systems. While fees for registration are generally discouraged, as they may serve as a barrier to inclusion, they may be imposed on individuals seeking expedited services or replacement of lost credentials, or on relying parties for use of authentication functionality.

Emerging issues

Self-sovereign identity

Some critics have argued that the national digital ID systems implemented by governments have proven lacking in privacy controls, vulnerable to cyberattack, and largely incompatible with one another. In particular, some have cited a 2018 data breach of India's Aadhaar that resulted in the theft of personal data of more than 1 billion people as evidence of the inherent insecurity of any centralised system.[56]

In response, a movement has formed advocating for the use of self-sovereign identity (SSI), a framework which envisions a decentralised identity management system that operates independently of third-party public actors and prioritises security, privacy, individual autonomy, and self-empowerment.[57] Underlying SSI is the belief that an individual should own and control her or his digital identity without the intervention of administrative authorities.[58]

As envisioned, SSI is enabled by ***digital wallets*** available on mobile devices, which can be used to store and manage digital credentials such as digital passports, digital diplomas, and digital titles to property. These credentials can be accessed by the individual user, who has the sole power to determine with whom they should be shared and the extent of the sharing. For example, an individual can prove that she or he is over 21 years of age without having to reveal an actual age, unlike when presenting a conventional ID document. Because the digital credentials are available in a digital wallet, they are entirely portable and readily available.[59]

Underlying SSI is the use of ***distributed ledger technology (DLT)***, the technology that underlies blockchain. When digital credentials are issued, an encrypted proof of the issuance (not the credential itself) is registered in a virtual, decentralised ledger, including a time stamp and digital signature of the issuer. The ledgers themselves are immutable, and any updates to the status of the entry – for example, if the credential were revoked – would also be recorded in the ledger. When a digital credential is presented to a third party, the third party can easily view the entries in the ledger to verify its authenticity.[60]

Because of the decentralised nature of SSI, digital identities remain portable and interoperable across multiple platforms.[61] Also, because there is no centralised authority managing the authentication process, there is no ability to track and record the use of digital credentials by the individual, thus eliminating concerns about unwanted government or corporate surveillance.

Additional resources

Resources for further reading

- Mason, Stephen, Electronic Signatures in Law: Fourth Edition
- UNCITRAL, Model Law on Electronic Commerce with Guide to Enactment 1996
- UNCITRAL, Model Law on Electronic Signatures with Guide to Enactment 2001
- World Bank Group, ID4D, Practitioner's Guide
- World Bank Group, ID4D, ID Enabling Environment Assessment (IDEEA) Guidance Note
- ITU, Digital identity in the ICT ecosystem: An overview

Organizations

- World Bank, ID4D, Identification for Development
- Access Now
- Unique Identification Authority of India
- National Identity Management Commission (Nigeria) 4

Notes

[1] See OECD, *A Roadmap toward a Common Framework for Measuring the Digital Economy, Report for the G20 Digital Economy Task Force* (2020) at 34, acknowledging no common definition and proposing the following one: "The Digital Economy incorporates all economic activity reliant on, or significantly enhanced by the use of digital inputs, including digital technologies, digital infrastructure, digital services and data. It refers to all producers and consumers, including government, that are utilising these digital inputs in their economic activities." Available at https://www.oecd.org/going-digital/topics/measurement/.

[2] See UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996. Available at https://uncitral.un.org/en/texts/ecommerce.

[3] Determann, Loretta, "Electronic Form Over Substance: eSignature Laws Need Upgrades," Hastings Law Journal Vol 72:1385 (May 2021). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3436327.

[4] Determann, Loretta, "Electronic Form Over Substance: eSignature Laws Need Upgrades," Hastings Law Journal Vol 72:1385 (May 2021). Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3436327.

[5] See, e.g., US Electronic Signatures in Global and National Commerce Act, 2000, §106; Saudi Arabia's Electronic Transaction law, 2007, Art 5; EU Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Art 25.

[6] At §103.

[7] Digital certificates have other uses beyond digital signatures, including securing credit card transactions, data transfers and web browsing.

[8] E.g., Malawi's Electronic Transactions and Cyber Security Act, 2016, §51 grants the Malawi Communications Regulatory Authority the power to accredit "certification authorities."

[9] EU Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Arts 3, 25, 26 & 32.

[10] World Bank Group, ID4D, Practitioner's Guide, Version 1.0 (October 2019) at 1. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[11] Dahan & Hanmer, The Identification for Development (ID4D) Agenda,: Its Potential for Empowering Women and Girls at 12-13.

[12] McKinsey Global Institute, *Digital Identification: A Key to Inclusive Growth, Summary of Findings* (January 2019) at 3. Available at https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf.

[13] McKinsey Global Institute, *Digital Identification: A Key to Inclusive Growth, Summary of Findings* (January 2019) at 3. Available at https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf.

[14] See World Bank Group, Inclusive and trusted digital ID can unlock opportunities for the World's most vulnerable, (August 2019). Available at https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable

[15] See World Bank Group, Inclusive and trusted digital ID can unlock opportunities for the World's most vulnerable, (August 2019). Available at https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable

[16] See, United Nations Website, Department of Economic and Social Affairs, Sustainable Development, The 17 Goals. Available at https://sdgs.un.org/goals/goal16

[17] Based on the definition in World Bank Group, ID4D, Practitioner's Guide, Version 1.0 (October 2019) at Glossary. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[18] See World Bank Group, ID4D, Practitioner's Guide, Version 1.0 (October 2019) at 4. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[19] See, World Bank Group, ID4D, Practitioner's Guide, Version 1.0 (October 2019) at Glossary. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide. See also, ITU, *Digital identity in the ICT ecosystem: An overview* (2018) at 5. Available at https://www.itu.int/pub/D-PREF-BB.ID01-2018.

[20] Adapted from World Bank Group, ID4D, *Practitioner's Guide, Version 1.0* (October 2019) at Glossary. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[21] See, ITU, *Digital identity in the ICT ecosystem: An overview* (2018) at vi. Available at https://www.itu.int/pub/D-PREF-BB.ID01-2018. See also, World Bank Group, ID4D, *Practitioner's Guide, Version 1.0* (October 2019) at 12. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[22] World Bank Group, ID4D, I*D Enabling Environment Assessment (IDEEA) Guidance Note* (2018) at 10-11. Available at https://id4d.worldbank.org/legal-assessment.

[23] GSMA.com, Available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/04/Exploring-the-Gender-Gap-in-Identification-Policy-Insights-from-10-Countries-Web.pdf

[24] World Bank Group, ID4D, *Practitioner's Guide, Version 1.0* (October 2019) at 3. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[25] McKinsey Global Institute, *Digital Identification: A Key to Inclusive Growth, Summary of Findings* (January 2019) at 12. Available at https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf.

[26] McKinsey Global Institute, *Digital Identification: A Key to Inclusive Growth, Summary of Findings* (January 2019) at 13. Available at https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf.

[27] Udo, Bassey, "Over 80,000 'ghost officers' uncovered in Nigerian Police," Premium Times (26 March 2018). Available at https://www.premiumtimesng.com/news/headlines/263052-over-80000-ghost-officers-uncovered-in-nigerian-police.html.

[28] See, World Bank Group, ID4D, I*D Enabling Environment Assessment (IDEEA) Guidance Note* (2018) at 9. Available at https://id4d.worldbank.org/legal-assessment.

[29] See, Republic of Botswana website, National ID Card Application. Available at .

[30] World Bank Group, ID4D, *Practitioner's Guide, Version 1.0* (October 2019) at 1. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[31] McKinsey Global Institute, *Digital Identification: A Key to Inclusive Growth, Summary of Findings* (January 2019) at 5. Available at https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf

[32] See World Privacy Forum website, National IDs Around the World – Interactive map. Available at https://www.worldprivacyforum.org/2017/07/national-ids-around-the-world/

[33] See, e.g., Guo & Noori, This is the real story of the Afghan biometric databases abandoned to the Taliban (August 2021).

[34] In addition to reducing traditional access barriers such as distance and cost, governments may need to actively engage with historically marginalized groups to ensure equitable uptake of digital identity services. See World Bank, Inclusive and trusted digital ID can unlock opportunities for the World's most vulnerable (August 2019).

[35] See, e.g., World Bank Group, *Principles on Identification for Sustainable Development: Toward the Digital Age - Second Edition* (March 2021). Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/213581486378184357/principles-on-identification-for-sustainable-development-toward-the-digital-age.

[36] Philippine Identification System Act, Republic Act No. 11055, 24 July 2017, at §9. Available at https://neda.gov.ph/philsys/.

[37] World Bank Group, ID4D, I*D Enabling Environment Assessment (IDEEA) Guidance Note* (2018) at 51. Available at https://id4d.worldbank.org/legal-assessment.

[38] For example, a study in Jharkhand, India found that requiring beneficiaries of food subsidies to link their Aadhaar number to their accounts led to a reduction in benefits for 23% of beneficiaries. Muralidharan et al., Balancing corruption and exclusion: Incorporating Aadhaar into PDS (2020).

[39] ITU, *Digital identity in the ICT ecosystem: An overview* (2018) at 3. Available at https://www.itu.int/pub/D-PREF-BB.ID01-2018.

[40] See, e.g., Access Now, *National Digital Identity Programmes: What's Next?* (May 2018) at 6. Available at https://www.accessnow.org/accessnow-digital-id-paper.

[41] World Bank Group, The State of Identification Systems in Africa: A Synthesis of Country Assessments, 2017 at 41. Available at http://documents.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf. See also, World Bank Group, ID4D, *ID Enabling Environment Assessment (IDEEA) Guidance Note* (2018) at 58-59. Available at https://id4d.worldbank.org/legal-assessment.

[42] World Bank Group, ID4D, *Practitioner's Guide, Version 1.0* (October 2019) at 154-155. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[43] GSMA, *Exploring the Gender Gap in Identification: Policy Insights from 10 Countries* (2019).

[44] World Bank Group, ID4D, *Practitioner's Guide, Version 1.0* (October 2019) at 157. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[45] World Bank Group, ID4D, *Practitioner's Guide, Version 1.0* (October 2019) at 166. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[46] Bailur & Smertnik, When ID works for women: What's the role of identification in helping women get access to work? (March 2019).

[47] See, World Bank Group, ID4D, *Practitioner's Guide, Version 1.0* (October 2019) at 170. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide. See also, World Bank Group, ID4D, ID Enabling Environment Assessment (IDEEA) Guidance Note (2018) at 37. Available at https://id4d.worldbank.org/legal-assessment.

[48] World Bank Group, ID4D, I*D Enabling Environment Assessment (IDEEA) Guidance Note* (2018) at 38-39. Available at https://id4d.worldbank.org/legal-assessment.

[49] See, World Bank Group, ID4D, *Practitioner's Guide, Version 1.0* (October 2019) at 16-17. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide. See also, ITU, *Digital identity in the ICT ecosystem: An overview* (2018) at 5. Available at https://www.itu.int/pub/D-PREF-BB.ID01-2018.

[50] See, Unique Identification Authority of India website. Available at https://uidai.gov.in/.

[51] See, National Identity Management Commission website. Available at https://nimc.gov.ng/.

[52] See, e.g., Access Now, *National Digital Identity Programmes: What's Next?* (May 2018) at 6 & 34. Available at https://www.accessnow.org/accessnow-digital-id-paper.

[53] See, World Bank Group, ID4D, *Practitioner's Guide, Version 1.0* (October 2019) at 16-17. Available at https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide. See also, ITU, *Digital identity in the ICT ecosystem: An overview* (2018) at 5. Available at https://www.itu.int/pub/D-PREF-BB.ID01-2018.

[54] World Bank Group, ID4D, I*D Enabling Environment Assessment (IDEEA) Guidance Note* (2018) at 67. Available at https://id4d.worldbank.org/legal-assessment. See, UK.GOV Verify website, Introducing UK.GOV Verify. Available at https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

[55] Lim, Jonathan, "Self-Sovereign Identity: The Harmonising of Digital Identity Solutions through Distributed Ledger Technology," Australian National University Journal of Law and Technology Vol 1(2) (September 2020). Available at https://anujolt.org/article/17432-self-sovereign-identity-the-harmonising-of-digital-identity-solutions-through-distributed-ledger-technology.

[56] Lim, Jonathan, "Self-Sovereign Identity: The Harmonising of Digital Identity Solutions through Distributed Ledger Technology," Australian National University Journal of Law and Technology Vol 1(2) (September 2020). Available at https://anujolt.org/article/17432-self-sovereign-identity-the-harmonising-of-digital-identity-solutions-through-distributed-ledger-technology.

[57] Giannopoulou A & Wang F, "Self-sovereign identity," Internet Policy Review, 10(2) (2021). Available at https://policyreview.info/glossary/self-sovereign-identity.

[58] López, Marcos Allende, Inter-American Development Bank, *Self-Sovereign Identity, The Future of Identity: Self Sovereignty, Digital Wallets, and Blockchain* (2020). Available at https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignity-Digital-Wallets-and-Blockchain.pdf.

[59] López, Marcos Allende, Inter-American Development Bank, *Self-Sovereign Identity, The Future of Identity: Self Sovereignty, Digital Wallets, and Blockchain* (2020). Available at https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignity-Digital-Wallets-and-Blockchain.pdf.

[60] López, Marcos Allende, Inter-American Development Bank, *Self-Sovereign Identity, The Future of Identity: Self Sovereignty, Digital Wallets, and Blockchain* (2020). Available at https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignity-Digital-Wallets-and-Blockchain.pdf.

[61] Lim, Jonathan, "Self-Sovereign Identity: The Harmonising of Digital Identity Solutions through Distributed Ledger Technology," Australian National University Journal of Law and Technology Vol 1(2) (September 2020). Available at https://anujolt.org/article/17432-self-sovereign-identity-the-harmonising-of-digital-identity-solutions-through-distributed-ledger-technology.

About UNCDF

The UN Capital Development Fund makes public and private finance work for the poor in the world's 46 least developed countries (LDCs). UNCDF offers "last mile" finance models that unlock public and private resources, especially at the domestic level, to reduce poverty and support local economic development. UNCDF pursues innovative financing solutions through: (1) financial inclusion, which expands the opportunities for individuals, households, and small and medium-sized enterprises to participate in the local economy, while also providing differentiated products for women and men so they can climb out of poverty and manage their financial lives; (2) local development finance, which shows how fiscal decentralization, innovative municipal finance, and structured project finance can drive public and private funding that underpins local economic expansion, women's economic empowerment, climate adaptation, and sustainable development; and (3) a least developed countries investment platform that deploys a tailored set of financial instruments to a growing pipeline of impactful projects in the "missing middle."

The UNCDF Policy Accelerator works with governments to help them create policies and regulations that include everyone in the digital economy, shares practical tools and guides based on our technical assistance model and our go-to resources, and provides scholarships to policymakers and regulators to study with our world-class partner organisations.

About Macmillan Keck

Macmillan Keck Attorneys & Solicitors advises clients on strategy, advocacy, deals, controversies and reforms in the digital economy. The firm's clients include telecom operators, digital financial service providers, online health and education providers, other digital content, application and service providers, governments and sector and competition regulatory authorities, and international organisations. The firm has successfully completed numerous complex projects across a majority of countries in every continent.

Disclaimer

This publication was last reviewed in February 2022.

policy.accelerator@uncdf.org

policyaccelerator.uncdf.org | uncdf.org

FIND US