Visa
Economic
Empowerment
Institute

Fostering Digital Equity
and Inclusion

Policy enablers for advancing digital identity frameworks: Insights and recommendations for public and private sectors

LUIS DA SILVA, MARIE JORDAN, GRACE LYKINS AND AMINA TIRANA[1] / SEPTEMBER 2021

Insights

- Digital identification that is inclusive and equitable for everyone, everywhere is a common good. It benefits people, businesses, governments, and numerous other entities including education and health systems.
- Governments can foster digital equity and financial inclusion through the enabling environment of laws, policies and regulations for digital identity, as well as purposeful design that incorporates digital identity in government services and national strategies.
- Data security, privacy and participant trust are critical to wide-scale use of digital identity.
- Risk-based, proportional financial regulations can enable more inclusive use of digital identification, including by under-represented, low-income and unbanked individuals.

In many ways, an individual's identity determines the types of services, products, and information he or she can access; it is an essential tool of commerce, livelihood, and welfare. Traditionally, individuals validated their identities using physical documentation,

[1] Luis ds Silva is Senior Identity Product Director; Marie Jordan is Senior Standards Management Director; Grace Lykins is Director of Global Government Engagement and Amina Tirana is the Visa Economic Empowerment Institute's Equity and Inclusion Fellow.

VISA

such as a birth certificate or a driver's license. Too often, this has resulted in the exclusion from services of individuals who lack legally required, tangible proof points, including access to banking and other financial services, telecommunications, and social support services. According to the World Bank, more than one billion people worldwide lack formal identification (World Bank Group, 2018). The majority of these individuals live in Sub-Saharan Africa and South Asia (see World Bank Group, 2018). Even more people, an estimated 3.4 billion, have a formal identification but cannot use it on digital channels (see White, 2019 and USAID, 2017). This creates a downward spiral of exclusion for these people and the institutions and companies seeking to serve them. The implication of this disparity is significant, especially as the world becomes more and more digital—a process accelerated by the COVID-19 pandemic—and the impact of digital inclusion versus exclusion or lower benefit compounds.

Transforming identity from paper-based systems to digital systems is the next frontier in financial inclusion and digital equity. This note discusses key policies that can accelerate and expand access to and use of digital identity to help individuals and governments realize maximum and equitable benefits.

A digital identity uses trusted data from an authoritative source to initially verify an individual's identity ("verification") and then authenticate that individual each time the identity is used ("authentication").[2] Digital identity is a unique digital representation of an individual that is made of validated attributes and credentials and is therefore trusted; exists for the benefit of the individual represented, who is its owner, and has control over its use; and is used to interact with other parties on behalf of its owner. Because digital identity does not rely on paper-based documentation, which is inaccessible to some individuals, it holds significant potential to advance inclusive access to financial and government services, commerce, economic activity, health services and much more.

Recognizing this potential, as well as opportunities for cost savings and process efficiencies, governments are establishing frameworks and guidelines to underpin the use of digital identities. One of the most globally watched policy initiatives is underway in Europe. In June 2021, the European Union published its proposal to renew the European eID framework, which mandates that Member States introduce a national digital identity framework (called an eID scheme) to be recognized at European Union and national levels. Furthermore, each Member State's framework must be interoperable across the European Union's geographic borders, and each Member State must issue a European Digital ID Wallet based on a toolkit with common standards. The European Commission will outline common technical standards by the end of 2022. In some instances, countries are turning to standards developed by companies and industry collaboration as they develop their frameworks and guidelines.[3]

To realize the full potential of digital identity frameworks in a globally connected world, policymakers should ensure interoperability between national or regional technical specifications, as well as regulatory harmonization among existing national laws. This necessitates the use of common standards and other globally recognized best practices to prevent a patchwork of incompatible systems under which the benefits of digital identities fall short of their potential reach. Policymakers can take steps to enable the uptake of digital identity and channel technology's potential to advance progress toward diverse social and economic outcomes by investing in the four areas below see Visa (2019) for a detailed discussion of biometrics as an enabler of financial inclusion. Similarly, international standard setting organizations, that include both public and private sector organizations, can work toward the same goals of interoperability, harmonization and dialogue on partnership to enable digital identity to advance socio-economic outcomes.

[2] An authoritative source of data can be a public or private organization, depending on the context and use case.

[3] For example, the Standards Council of Canada is working with the government to develop a minimum set of requirements to ensure that digital credentials and trust services are interoperable among businesses and governments and create a seamless experience for users. See SCC 2021.

Policy enablers to foster greater use of digital identity

1. Identity Frameworks and Risk-Based Financial Regulation

Digital identity, including biometrics-based technologies, should relate to a national legal identification framework, which governs verification of an individual's identity. Risk-based, proportional financial regulations can enable more widespread, inclusive use of digital identification to ease and expedite account openings and authentication, including for low-income and unbanked individuals (see FATF 2020). To achieve this, governments can consider doing one or more of the following:

- Strengthening the national identification framework so that it covers all citizens and includes possibilities for self- or peer-identification in specific, limited circumstances. National frameworks should be developed with global interoperability in mind to ensure optimal use across borders, especially because one's identity is not geographically constrained in today's globally connected world. This is discussed in further detail in section 3 below.
- Establishing multiple ways for citizens to establish their biometric identity in order to prevent further dis-enfranchising or marginalizing those without access or with limited access.
- Developing or joining voluntary data exchanges that share identity information in privacy-protective ways, including biometrics. These may reduce costs overall and improve the speed and efficiency of account opening and transactions, and thus the overall experience for consumers. However, it is imperative that governments and providers take care to ensure appropriate security and privacy standards in such registries.
- Utilizing proportional, risk-based financial regulatory frameworks with tiered know-your-customer (KYC) to enable individuals to open a simplified transactional and payment account with basic identity information, while protecting the integrity of the financial system.

2. Data Security and Trust

Data security and participant trust are critical to the success of financial and digital inclusion, and wide-scale use of digital identity. These outcomes can be advanced through laws and regulations that protect consumer rights, support consumer choice, respect data privacy, and adopt strong security standards, without prescribing a certain form. Governments should look to do the following:

- Strengthen data security and privacy laws through a sound legal framework to increase consumer confidence in the use of data-driven technologies like digital identity as well as in the formal financial sector. Aligning with established global standards, for example on how public and private entities manage and share biometric and personal digital data, can advance this goal, reduce costs for national stakeholders, and ensure international interoperability, thereby facilitating efficient cross-border transactions.
- Enact regulations to ensure consumer protection, such as requirements for clear and transparent disclosures around data use and consumer choice, to ensure that underserved populations receive the same privacy rights as more advantaged populations.
- Educate merchants, consumers, financial institutions and technology providers on the use of digital identity, as well as how to protect digital identity data in order to help grow trust and usage.

3. Improving Infrastructure through Innovation and Interoperability

An effective digital identity system will generally require robust and reliable infrastructure, including electricity and telecommunications, as well as biometric registries and databases. Erratic, slow, or expensive connectivity can discourage usage by people, small business owners and employees, and government agencies. Digital identity is often most effective in supporting inclusive digital payments and building scale when combined with other innovations such as branchless banking, and ways to leverage existing networks. Governments can consider doing one or more of the following:

- Developing policies that promote the interoperability of infrastructure and networks to facilitate economies of scale and sustainable business models. Sustainability in turn encourages providers to create new and innovative digital solutions. Interoperable systems, developed using common technical standards, promote cross-border connectivity in a digital world that increasingly transcends geographic borders.
- Investing in improving the overall infrastructure of a country, *e.g.*, electricity grids, telecommunications and digital data networks, biometrics scanners, and identity registries. Concurrently, private sector and government providers can continue to design and innovate solutions to overcome known challenges around reliable electricity and connectivity and reduce costs.
- Enabling agents and other models of branchless banking to use digital identity as a secure, convenient method to verify or authenticate consumers. Allowing different models of branchless banking can further drive reach and scale and provide flexibility for providers to develop solutions appropriate to local infrastructure and markets.
- Encouraging new entrants, such as financial technology (fintech) firms, to expand the types of solutions available to meet the needs of specific segments of populations and businesses, including underserved populations. Furthermore, ensuring that non-financial institutions and new entrants are subject to the same prudential regulations concerning consumer privacy and data protection as financial institutions can provide consumers security and trust across the ecosystem.

4. National Strategies and Government Promotion

Governments can implement impactful policy and infrastructure changes to advance digital equity and financial inclusion in their countries and regions. Policymakers can increase the scale and use of digital authentication and digital identities, while simultaneously reducing costs, by adopting any, or a combination, of the following levers:

- Integrate the application of digital authentication and identity into national strategies and action plans for payment systems and financial inclusion – and other national priorities. This facilitates coordination across ministries, while helping to maximize investment, leverage existing human and physical infrastructure, promote interoperability, and avoid competing standards or policies.
- Leverage government services to introduce digital identities to consumers. For example, a number of governments have already included biometric verification as a requirement to receive social support. This can help to jumpstart the use of biometric and digital identity in the market and build scale and user trust. However, these systems must provide a level of flexibility, as least during an initial phase-in period to avoid unintended exclusion if non-digital options are not also available while these systems scale.
- Design digital identification-enabled programs that layer in additional services, and tie services such as voting, land and property registration, and mass transit ticketing to biometric authentication. Such purposeful design can further increase demand, use, convenience, and scale.

Digital identification that is inclusive and equitable for everyone, everywhere is a common good. It benefits people, businesses, governments, and numerous other entities including education and health systems. For their part, governments can create equitable, trustworthy and secure digital identity services through the principles stated above, providing their citizens with greater accessibility to better services, all while lowering costs and improving efficiency. If implemented appropriately, digital identities can be a critical step toward empowering citizens to participate in the digital world and full digital equity.

Sources

Financial Action Task Force (FATF). (2020). *Guidance on Digital Identity*. FATF. www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

Standards Council of Canada (SCC). (2021). National technical specification for digital credentials to provide greater privacy and security for Canadians. SCC. https://www.scc.ca/en/news-events/news/2021/national-technical-specification-for-digital-credentials-provide-greater-privacy-and-security-for

USAID. (2017) *Identity in a Digital Age: Infrastructure for Inclusive Development*. USAID. https://www.usaid.gov/digital-development/digital-id.

Visa. (2019). *Assessing the Role of Biometrics in Advancing Financial Inclusion*. https://usa.visa.com/content/dam/VCOM/regional/na/us/about-visa/documents/assessing-the-role-of-biometrics-in-financial-inclusion-visa.pdf

White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, C., Sperling, O. (2019, January). *Digital Identification: A Key to Inclusive* Growth, McKinsey Global Institute. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

World Bank. (2018). *Identification for Development* [Dataset], available at https://id4d.worldbank.org/global-dataset.

About theVisa Economic Empowerment Institute

The VEEI is a non-partisan center of excellence for research and public-private dialogue established by Visa.

The VEEI's overarching mission is to promote public policies that empower individuals, small businesses, and economies. It produces research and insights that inform long-term policy within the global payments ecosystem. Visa established the VEEI as the next step in its ongoing work to remove barriers to economic empowerment and to create more inclusive, equitable economic opportunities for everyone, everywhere.

Visit: visaeconomicempowermentinstitute.org